

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



Master Agreement Number SPSD26-0563LS_PAL
for
Data Communications
between
the State of Montana
and
Palo Alto Networks.

This Master Agreement is entered into by the State of Montana ("Lead Entity") and the following contractor (each a "Party" and collectively the "Parties") as a result of Solicitation Number SPB-RFP-2025-0563LS (the "RFP") for the purpose of providing Data Communications through the RFXPremier cooperative purchasing program:

Palo Alto Networks ("Contractor")
1950 Opportunity Way Floor 10
Reston, VA 20190

MASTER AGREEMENT CONTACTS

Contractor's contact for this Master Agreement is:

Paul Kodack
Director, GTM Programs & Operations
pkodack@paloaltonetworks.com
908.521.8837

Lead Entity's contact for this Master Agreement is:

Lauren Spatzierath
Procurement Operations Manager
Lauren.Spatzierath@mt.gov
406.444.0118

TERM. This Master Agreement is effective as of the date of the last signature below, whichever is later, and will terminate on 09.30.2033 unless terminated sooner or extended or renewed in accordance with the terms set forth herein. Renewals totaling up to 3 years following the initial term may be exercised upon mutual agreement by the Parties.

ATTACHMENTS. This Master Agreement includes the following attachments:

- Attachment 1: Supplemental Materials
- Attachment 2: Scope of Work
- Attachment 3: Cost Proposal

Request for Proposals for
Data Communications

Issued by the State of Montana

Solicitation Number: SPB-RFP-2025-0563LS



SIGNATURE. The undersigned for each Party represents and warrants that this Master Agreement is a valid and legal agreement binding on the Party and enforceable in accordance with the Master Agreement’s terms and that the undersigned is duly authorized and has legal capacity to execute and deliver this Master Agreement and bind the Party hereto.

IN WITNESS WHEREOF, the Parties have executed this Master Agreement.

DS

Signed by:

Phil Egelston

40B6FED36491458

Signature

Phil Egelston

Printed Name

Senior Director, Associate General Counsel

Title

2026-07-22

Date

Signed by:

John Thomas

49E3FEF749684B6...

Signature

John Thomas

Printed Name

Chief Procurement Officer

Title

7/23/2026

Date

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



MASTER AGREEMENT

RFXPREMIER MASTER AGREEMENT TERMS AND CONDITIONS

1. Definitions

- 1.1 Acceptance** means acceptance of goods and services as set forth in Section 9 of this Master Agreement.
- 1.2 Contractor** means a party to this Master Agreement, whether a person or entity, that itself or through Fulfillment Partners delivers Products or performs Services under the terms set forth in this Master Agreement.
- 1.3 Eligible Entity** means all states (as well as the District of Columbia and US territories), cities, counties, districts, other political subdivisions of any State, Institutions of Higher Education, K-12, quasi-governmental entities, service districts, healthcare institutions, transportation districts, tribes/tribal organizations, or nonprofit organizations.
- 1.4 Embedded Software** means one or more software applications which permanently reside on a computing device owned by the Purchasing Entity, and which are not otherwise subject to a term license. The Purchasing Entity's license to use such Software applications will be subject to the terms and conditions of Contractor Supporting Materials attached to the Order and incorporated in the Order by reference.
- 1.5 END USER LICENSE AGREEMENT (EULA)** means the End User License Agreement published by Contractor and included in Contractor's response and as Attachment 1 to this Contract and made a part of this Agreement by reference herein.
- 1.6 END USER SUPPORT AGREEMENT (EUSA)** means the End User Support Agreement attached to Contractor's EULA and included in its response as a part of Attachment 1 to this Agreement and made a part of this Agreement by reference herein
- 1.7 Fulfillment Partner** means a third-party contractor and authorized by Contractor, and approved by a Participating Entity under a Participating Addendum, or other means, who may to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Products or Services under this Master Agreement and billing Purchasing Entity for such Products or Services. Contractor may, upon written notice to the Participating Entity, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to additional terms and conditions.
- 1.8 Intellectual Property** means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.
- 1.9 Lead Entity** means the Entity administering any resulting Master Agreement(s) who is a party to this Master Agreement.
- 1.10 Master Agreement** means the underlying agreement consisting of this Master Agreement and all related attachments executed by and between the Lead Entity, acting in cooperation with RFXPremier, and the Contractor, as now or hereafter amended.

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- 1.11 RFXPremier** is a division of the Procurement Professionals Alliance (“PPA”). RFXPremier facilitates administration of the PPA cooperative group contracting consortium for the benefit of states (as well as the District of Columbia and US territories), cities, counties, districts, other political subdivisions of any State, Institutions of Higher Education, K-12, quasi-governmental entities, service districts, healthcare institutions, transportation districts, tribes/tribal organizations, or nonprofit organizations. RFXPremier is identified in the Master Agreement as the recipient of reports and may perform contract administration functions relating to collecting and receiving reports, as well as other contract administration functions as assigned by the Lead Entity.
- 1.12 Order or Purchase Order** means any purchase order, sales order, or other document used by a Purchasing Entity to order the Products. or Services as authorized under the Master Agreement and a Participating Addendum, if applicable, and accepted or processed by the Contractor. Each Order or Purchase Order includes and incorporates by reference the Master Agreement and Participating Addendum, if applicable. An accepted Order or Purchase Order may include Supporting Materials, provided that Supporting Materials are subject to the Order of Precedence listed in Section 3.1 - Order.
- 1.13 Participating Addendum** means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any additional Participating Entity-specific language or other requirements (*e.g.*, ordering procedures specific to the Participating Entity, entity-specific terms and conditions, etc.).
- 1.14 Participating Entity** means a state (as well as the District of Columbia and US territories), city, county, district, other political subdivision of a State, Institution of Higher Education, K-12, or a nonprofit organization under the laws of some states properly authorized to enter into a Participating Addendum, that has executed a Participating Addendum.
- 1.15 Product or Products and Services** means any equipment, Software (including Embedded Software and Cloud Software), Subscriptions (as defined below), or other deliverable supplied or created by the Contractor pursuant to this Master Agreement. The term Product includes goods supplied or created by the Contractor pursuant to this Master Agreement, but exclude any Third-Party Products as defined in Section 14.3 (Third-Party Goods and Services) below.
- 1.16 Published Specifications** mean the applicable user manual, acceptable use policies, privacy and product data sheets, and other corresponding documents published by Contractor that are customarily available to end users of the Product(s).
- 1.17 Purchasing Entity** means a Participating Entity that 1) issues a Purchase Order against the Master Agreement or 2) executes a Participating Addendum and becomes financially committed to the purchase.
- 1.18 Professional Services** means professional services, consulting services or other work as confined in a Statement of Work (“SOW”) or a service description (“Service Description” or “SD”). Notwithstanding anything to the contrary, Professional Services shall not be defined to include maintenance support services.
- 1.19 Subscriptions** means software-as-a-service and cloud-delivered security services, including updates, provided by Contractor, regardless of whether a fee is charged for its use. Support Services and professional services are not considered Subscriptions under this Agreement.

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

- 1.20 Support Services** means the maintenance, support services and customer success services provided by Contractor or its representative in effect at the time such maintenance, support services and/or customer success services are ordered and as further set forth in the End User Support Agreement attached to Contractor's EULA and made a part of this Agreement by reference. Notwithstanding anything else to the contrary, Support Services are not a "Service," but rather are a Product offering.
- 1.21 Supporting Materials** means materials and documents which the parties identify as incorporated in an Order or Purchase Order either by attachment or reference. Supporting Materials may include (as examples) product lists, hardware or software specifications, standard or negotiated service descriptions, data sheets and their supplements, supplementary terms, policies, and statements of work (SOWs), published warranties and service level agreements, user agreements, and license agreements, and may be available to Participating Entity in hard copy or by accessing a designated Contractor website.

2. Term of Master Agreement

- 2.1 Initial Term.** The initial term of this Master Agreement is for seven (7) years. The term of this Master Agreement may be amended beyond the initial term for three (3) additional years at the Lead Entity's discretion and by mutual agreement and upon review of requirements of Participating Entities, current market conditions, and Contractor performance. The additional years may be in increments of three (3) 12-month terms. This Master Agreement will not exceed ten (10) years total. The Lead Entity may, prior to execution, adjust the effective date or duration of the initial term or renewal period of any Master Agreement for the purpose of making the Master Agreement coterminous with others.
- 2.2 Amendment Limitations.** The terms of this Master Agreement will not be waived, altered, modified, supplemented, or amended in any manner whatsoever without prior written agreement of the Lead Entity and Contractor.
- 2.3 Amendment Term.** The term of this Master Agreement may be amended to extend past the initial term and stated renewal periods for a reasonable period by assigning the Master Agreement to another third-party to assume the obligations of Lead Entity (the "New Lead Entity"), per section 14.4.2, if in the judgment of the New Lead Entity a follow-on competitive procurement will be unavoidably delayed (despite good faith efforts) beyond the planned date of execution of the follow-on master agreement. This subsection will not be deemed to limit the authority of a Lead Entity under the applicable laws, rules and regulations to otherwise negotiate contract extensions.

3. Order of Precedence

- 3.1 Order.** Any Order placed under this Master Agreement will consist of the following documents:
- 3.1.1** A Participating Entity's Participating Addendum ("PA");
 - 3.1.2** RFXPremier Master Agreement, including all attachments thereto;
 - 3.1.3** A Purchase Order or Scope of Work/Specifications issued against the Master Agreement, or issued against a Participating Addendum;
 - 3.1.4** Supporting Materials accepted by a Purchasing Entity as part of an Order or Purchase Order;

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- 3.1.5 The Solicitation or, if separately executed after award, the Lead Entity's bilateral agreement that integrates applicable provisions;
 - 3.1.6 Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead Entity.
 - 3.2 **Conflict.** These documents will be read to be consistent and complementary. Any conflict among these documents will be resolved by giving priority to these documents in the order listed above. Contractor Supporting Materials that apply to this Master Agreement are only those that are expressly accepted by the Purchasing Entity and must be in writing and attached to an Order or Purchase Order as an Exhibit or Attachment (including hyperlinks therein).
 - 3.3 **Participating Addenda.** Participating Addenda will not be construed to diminish, modify, or otherwise derogate any provisions in this Master Agreement between the Lead Entity and Contractor. The term of a Participating Addendum will not exceed the term of this Master Agreement, except when a Participating Entity determines an extension of its Participating Addendum is necessary to avoid a lapse in contract coverage and is permitted by law.
 - 4. **Participants and Scope**
 - 4.1 **Eligibility for Participation.** Any Eligible Entity may utilize this Master Agreement as a Participating Entity or Purchasing Entity.
 - 4.2 **Requirement for a Participating Addendum.** Contractor may not deliver Products under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed.
 - 4.3 **Applicability of Master Agreement.** The Master Agreement is applicable to any Order issued against it by a Purchasing Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum, subject to Section 3. For any Order submitted directly against the Master Agreement by a Purchasing Entity that is not subject to a Participating Addendum, such Order shall be subject to the terms of Contractor Supporting Materials by default unless agreed in writing otherwise by such Purchasing Entity and Contractor. For the purposes of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Purchasing Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the written consent of the Purchasing Entity and Contractor, may be included in the Purchase Order used by the Purchasing Entity to place the Order. For the avoidance of doubt, any contingencies, or additional or conflicting terms in a Purchase Order or Order are deemed rejected by Contractor unless Contractor has expressly agreed to such terms in signed writing. Mere acceptance or processing of a Purchase Order or Order containing such terms shall not constitute express consent.
 - 4.4 **Obligated Entities.** Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities: i) within the scope of those Participating Addenda; or ii) who have issued a Purchase Order against the Master Agreement. Participating Entities permitted to participate may use an informal competitive

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

process to determine which Master Agreements to participate in through execution of a Participating Addendum. Participating Entities incur no financial obligations on behalf of other Purchasing Entities.

4.5 [Reserved]

4.6 Eligibility for a Participating Addendum or Order. All eligible entities may sign their own Participating Addendum or Order. In all instances, the entity must ensure that they have the requisite procurement authority to execute a Participating Addendum.

4.7 Prohibition on Resale. Subject to any specific conditions included in the solicitation or Contractor's proposal as accepted by the Lead Entity, or as explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products purchased under this Master Agreement. Absent any such condition or explicit permission, this limitation does not prohibit payments by employees of a Purchasing Entity for Products; sales of Products to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

4.8 Individual Customers. Except as may otherwise be agreed to by the Purchasing Entity and Contractor, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead Entity has in the Master Agreement and as the Participating Entity has in the Participating Addendum, including but not limited to any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

4.9 Release of Information. Throughout the duration of this Master Agreement, Contractor must secure from the Lead Entity prior approval for the release of information that pertains to the potential work or activities covered by the Master Agreement. This limitation does not preclude publication about the award of the Master Agreement or marketing activities consistent with any proposed and accepted marketing plan.

4.10 No Representations. The Contractor shall not make any representations of RFXPremier, the Lead Entity, any Participating Entity, or any Purchasing Entity's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent.

5. RFXPremier Provisions

5.1 Applicability. RFXPremier is not a party to the Master Agreement. The terms set forth in Section 5 are for the benefit of RFXPremier as a third-party beneficiary of this Master Agreement.

5.2 Administrative Fees

5.2.1 RFXPremier Fee. Contractor shall pay to RFXPremier, or its assignee, a RFXPremier Administrative Fee of four tenths of one percent (0.4% or 0.004) no later than sixty (60) days following the end of each calendar quarter. The RFXPremier Administrative Fee must be submitted quarterly and is based on all sales of products and services under the

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

Master Agreement (less any charges for taxes or shipping). The RFXPremier Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with a vendor's response to the Lead Entity's solicitation.

- 5.2.2 Entity Imposed Fees.** Some Participating Entities may require an additional fee be paid by Contractor directly to the entity on purchases made on that entities Participating Addendum. For all such requests, the fee rate or amount, payment method, and schedule for such reports and payments will be incorporated into the applicable Participating Addendum. Unless agreed to in writing by the Participating Entity, **Contractor may not adjust the Master Agreement pricing to include the entity's fee for purchases made by Purchasing Entities on the Participating Addendum. No such agreement will affect the RFXPremier Administrative Fee percentage or the prices paid by Purchasing Entities outside the jurisdiction of the Participating Entity requesting the additional fee.**
- 5.2.3 Interest on Late Payment.** If the Contractor does not pay the RFXPremier Administrative Fee within sixty (60) days following the end of each calendar quarter as required by Section 5.2.1, then Contractor shall accrue interest on the unpaid amounts at the rate of 1% per month.
- 5.2.4 Administrative Fee Updates.** RFXPremier reserves the right to update the RFXPremier Administrative Fee. If the RFXPremier Administrative Fee is updated, any renewals exercised shall be contingent upon Contractor's acceptance of the updated RFXPremier Administrative Fee.

5.3 RFXPremier Summary and Detailed Usage Reports

- 5.3.1 Sales Data Reporting.** In accordance with this section, Contractor shall report to RFXPremier all Orders under this Master Agreement for which Contractor has invoiced the ordering entity or individual, including Orders invoiced to Participating Entity or Purchasing Entity employees for personal use if such use is permitted by this Master Agreement and the applicable Participating Addendum ("Sales Data"). Timely and complete reporting of Sales Data is a material requirement of this Master Agreement. Reporting requirements, including those related to the format, contents, frequency, or delivery of reports, may be updated by RFXPremier with reasonable notice to Contractor and without amendment to this Master Agreement. RFXPremier shall have exclusive ownership of any media on which reports are submitted and shall have a perpetual, irrevocable, non-exclusive, royalty free, and transferable right to display, modify, copy, and otherwise use reports, data, and information provided under this section.
- 5.3.2 Summary Sales Data.** "Summary Sales Data" is Sales Data reported as cumulative totals by state. Contractor shall, using the reporting tool or template provided by RFXPremier, report Summary Sales Data to RFXPremier for each calendar quarter no later than thirty (30) days following the end of the quarter. If Contractor has no reportable Sales Data for the quarter, Contractor shall submit a zero-sales report.
- 5.3.3 Detailed Sales Data.** "Detailed Sales Data" is Sales Data that includes for each Order all information required by the Solicitation or by RFXPremier, including customer information, Order information, and line-item details. Contractor shall, using the reporting tool or template provided by RFXPremier, report Detailed Sales Data to

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

RFxPremier for each calendar quarter no later than thirty (30) days following the end of the quarter. Detailed Sales Data shall be reported in the format provided in the Solicitation or provided by RFxPremier. The total sales volume of reported Detailed Sales Data shall be consistent with the total sales volume of reported Summary Sales Data.

- 5.3.4 Sales Data Crosswalks.** Upon request by RFxPremier, Contractor shall provide to RFxPremier tables of customer and Product information and specific attributes thereof for the purpose of standardizing and analyzing reported Sales Data (“Crosswalks”). Customer Crosswalks must include a list of existing and potential Purchasing Entities and identify for each the appropriate customer type as defined by RFxPremier. Product Crosswalks must include Contractor’s part number or SKU for each Product in Offeror’s catalog and identify for each the appropriate Master Agreement category (and subcategory, if applicable), manufacturer part number, product description, eight-digit UNSPSC Class Level commodity code, and (if applicable) EPEAT value and Energy Star rating. Crosswalk requirements and fields may be updated by RFxPremier with reasonable notice to Contractor and without amendment to this Master Agreement. Contractor shall work in good faith with RFxPremier to keep Crosswalks updated as Contractor’s customer lists and product catalog change.
- 5.3.5 Executive Summary.** Contractor shall, upon request by RFxPremier, provide RFxPremier with an executive summary that includes but is not limited to a list of states with an active Participating Addendum, states with which Contractor is in negotiations, and any Participating Addendum roll-out or implementation activities and issues. RFxPremier and Contractor will determine the format and content of the executive summary.
- 5.4 RFxPremier Cooperative Program Marketing, Training, and Performance Review**
- 5.4.1 Staff Education.** Contractor shall work cooperatively with RFxPremier personnel. Contractor shall present plans to RFxPremier for the education of Contractor’s contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of RFxPremier procurements, the master agreement and participating addendum process, and the manner in which eligible entities can participate in the Master Agreement.
- 5.4.2 Onboarding Plan.** Upon request by RFxPremier, Contractor shall, as Participating Addendums are executed, provide plans to launch the program for the Participating Entity. Plans will include time frames to launch the agreement and confirmation that the Contractor’s website has been updated to properly reflect the scope and terms of the Master Agreement as available to the Participating Entity and eligible Purchasing Entities.
- 5.4.3 Annual Contract Performance Review.** Contractor shall participate in an annual contract performance review with the Lead Entity and RFxPremier, which may at the discretion of the Lead Entity be held in person and which may include a discussion of marketing action plans, target strategies, marketing materials, Contractor reporting, and timeliness of payment of administration fees.
- 5.4.4 Use of RFxPremier Logo.** The RFxPremier and PPA logos may not be used by Contractor in sales and marketing until a separate logo use agreement is executed with PPA.

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- 5.4.5 Most Favored Customer.** Contractor shall, within thirty (30) days of their effective date, notify the Lead Entity and RFXPremier of any contractual most-favored-customer provisions in third-party contracts or agreements that may affect the promotion of this Master Agreement or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this Master Agreement. Upon request of the Lead Entity or RFXPremier, Contractor shall provide a copy of any such provisions.
- 5.5 RFXPremier eMarketPlace.** RFXPremier Cooperative may provide an eMarketPlace solution for public entities to access a central online platform to view and/or purchase the goods, services, and solutions available from RFXPremier's cooperative Master Agreements. If RFXPremier offers such an eMarketPlace, Contractor agrees to cooperate in good faith with PPA, and any third party acting as an agent on behalf of PPA, to integrate Contractor's industry presence into the eMarketPlace. Specific terms of this integration shall be negotiated at the time of implementation of any eMarketPlace.
- 5.6 Cancellation for Under or Non-Utilization.** In consultation with RFXPremier, the Lead Entity may, in its discretion, cancel the Master Agreement or not exercise an option to renew, when utilization of Contractor's Master Agreement does not warrant further administration of the Master Agreement. The Lead Entity may also exercise its right to not renew the Master Agreement if the Contractor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. Cancellation based on nonuse or under-utilization will not occur sooner than two years after execution of the Master Agreement. This subsection does not limit the discretionary right of either the Lead Entity or Contractor to cancel the Master Agreement or terminate for default subject to the terms herein. This subsection also does not limit any right of the Lead Entity to cancel the Master Agreement under applicable laws.
- 5.7 RESERVED.**
- 5.8 Additional Agreement with PPA.** Upon request by RFXPremier, awarded Contractor shall enter into a direct contractual relationship with PPA related to Contractor's obligations to RFXPremier under the terms of the Master Agreement, the terms of which shall be the same or similar (and not less favorable) than the terms set forth in the Master Agreement.
- 6. Pricing, Payment & Leasing**
- 6.1 Pricing.** The discounts contained in this Master Agreement or offered under this Master Agreement represent the minimum discount to any Purchasing Entity.
- 6.1.1** All discounts must be guaranteed for the initial term of the Master Agreement.
- 6.1.2** Following the initial term of the Master Agreement, any request for discount rate adjustment must be for an equal guarantee period and must be made at least 45 days prior to the effective date.
- 6.1.3** Requests for a price or rate adjustment must include sufficient documentation supporting the request. Any adjustment or amendment to the Master Agreement will not be effective unless approved in writing by the Lead Entity.
- 6.1.4** No retroactive adjustments to prices or rates will be allowed.
- 6.2 Payment.** Unless otherwise agreed upon in a Participating Addendum or Order, Payment will be made to Contractor's reseller partners within thirty (30) days following the date the entire order

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

is delivered or the date a correct invoice is received, whichever is later. After 45 days the Contractor's reseller partners may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance, unless a different late payment amount is specified in a Participating Addendum or Order, or otherwise prescribed by applicable law. Payments will be remitted in the manner specified in the Participating Addendum or Order. Payments may be made via a purchasing card with no additional charge.

- 6.3 Leasing or Alternative Financing Methods.** The procurement and other applicable laws of some Purchasing Entities may permit the use of leasing or alternative financing methods for the acquisition of Products under this Master Agreement. Where the terms and conditions are not otherwise prescribed in an applicable Participating Addendum, the terms and conditions for leasing or alternative financing methods are subject to negotiation between the Contractor and Purchasing Entity.

7. Ordering

- 7.1 Order Numbers.** Master Agreement order and purchase order numbers must be clearly shown on all acknowledgments, packing slips, invoices, and on all correspondence.
- 7.2 Quotes.** Purchasing Entities may define entity-specific or project-specific requirements and informally compete the requirement among companies having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to the Purchasing Entity's rules and policies. The Purchasing Entity may in its sole discretion determine which contracted vendors (including Fulfillment Partners) should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost, and other factors considered.
- 7.3 Applicable Rules.** Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor and Contractor Fulfillment Partners, as applicable, are expected to become familiar with the Purchasing Entity's rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.
- 7.4 Required Documentation.** Contractor shall not begin work without a valid Purchase Order or other appropriate commitment document under the law of the Purchasing Entity.
- 7.5 Term of Purchase.** Orders shall be placed with Contractor Fulfillment Partners and accepted or rejected by Contractor Fulfillment Partners during the term of the Master Agreement and Participating Addendum. All Orders must be consistent with the terms of this Master Agreement and applicable Participating Addendum.
- 7.1.1** Orders must be placed pursuant to this Master Agreement prior to the termination date thereof, but may have a delivery date or performance period up to 120 days past the then-current termination date of this Master Agreement. All Support Services and Subscription agreements whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and Support Services and Subscriptions established per each written agreement). No new leases, Support Services, Subscriptions or other agreements for services may be executed after this Master Agreement has expired. For the purposes of this section, renewals of Support Services, Subscriptions and other service or

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- maintenance agreements shall not be considered “new”, subject to the limits on time frame established per each written agreement.
- 7.5.1** Notwithstanding the previous, Orders must also comply with the terms of the applicable Participating Addendum, which may further restrict the period during which Orders may be placed or delivered.
 - 7.5.2** Provided that Purchasing Entities pay for ordered goods or services performed, the financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon entity funds for that purpose being appropriated, budgeted, and otherwise made available.
 - 7.5.3** Notwithstanding the expiration, cancellation or termination of this Master Agreement, Contractor shall perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration, cancellation, or termination of this Master Agreement, or in any manner inconsistent with this Master Agreement’s terms.
 - 7.5.4** Orders for any separate indefinite quantity, task order, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.
- 7.6 Order Form Requirements.** All Orders pursuant to this Master Agreement, at a minimum, must include:
- 7.6.1** The services or supplies being delivered;
 - 7.6.2** A shipping address and other delivery requirements, if any;
 - 7.6.3** A billing address;
 - 7.6.4** Purchasing Entity contact information;
 - 7.6.5** Pricing consistent with this Master Agreement and applicable Participating Addendum and as may be adjusted by agreement of the Purchasing Entity and Contractor;
 - 7.6.6** A not-to-exceed total for the products or services being ordered; and
 - 7.6.7** The Master Agreement number or the applicable Participating Addendum number, provided the Participating Addendum references the Master Agreement number.
- 7.7 Orders Placed with Contractor Reseller Partners.** All orders will be placed with Contractor’s named reselling partners. Contractor will not accept orders directly from Purchasing Entities.
- 7.8 Communication.** All communications concerning administration of Orders placed must be furnished solely to the authorized purchasing agent within the Purchasing Entity’s purchasing office, or to such other individual identified in writing in the Order.
- 7.9 Contract Provisions for Orders Utilizing Federal Funds.** Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

Addenda and Purchasing Entities for incorporation in Orders placed under this Master Agreement.

8. Shipping and Delivery

- 8.1 Shipping Terms.** Unless otherwise agreed upon in a Participating Addendum or Order, all deliveries by Contractor's resellers will be F.O.B. destination, freight pre-paid, with all transportation and handling charges paid by the Contractor or Fulfillment Partner.
- 8.1.1** Notwithstanding the above, responsibility and liability for loss or damage will remain the Contractor's or the Contractor's reseller until delivery when responsibility will pass to the Purchasing Entity except as to latent defects, fraud, and Contractor's warranty obligations.
- 8.2 Minimum Shipping.** The minimum shipment amount, if any, must be contained in the Master Agreement. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an Order to be shipped without transportation charges that is back ordered will be shipped without charge.
- 8.3 Inside Deliveries.** To the extent applicable, all deliveries will be "Inside Deliveries" as designated by a representative of the Purchasing Entity placing the Order. Inside Delivery refers to a delivery to a location other than a loading dock, front lobby, or reception area. Specific delivery instructions will be noted on the order form or Purchase Order. Costs to repair any damage to the building interior (*e.g.*, scratched walls, damage to the freight elevator, etc.) caused by Contractor or Contractor's carrier will be the responsibility of the delivering party. Immediately upon becoming aware of such damage, Contractor shall cause its Fulfillment Partner to notify the Purchasing Entity placing the Order.
- 8.4 Packaging.** All products must be delivered in the manufacturer's standard package. Costs must include all packing and/or crating charges. Cases must be of durable construction, in good condition, properly labeled and suitable in every respect for storage and handling of contents. Each shipping carton must be marked with the commodity, brand, quantity, item code number and the Purchasing Entity's Purchase Order number.

9. Inspection and Acceptance

- 9.1 Laws and Regulations.** Any and all Products offered and furnished must comply fully with all applicable Federal, State, and local laws and regulations.
- 9.2 Applicability.** Unless otherwise specified in the Master Agreement, Participating Addendum, or ordering document, the terms of this Section 9 will apply. This section is not intended to limit rights and remedies under the applicable commercial code.
- 9.3 Inspection.** All Products are subject to inspection at reasonable times and places before Acceptance. Contractor shall provide right of access to the Lead Entity, or to any other authorized agent or official of the Lead Entity or other Participating or Purchasing Entity, at reasonable times, to monitor and evaluate performance, compliance, and/or quality assurance requirements under this Master Agreement.
- 9.3.1** Products that do not substantially conform to Contractor's Published Specifications may be rejected. Failure to reject upon receipt, however, does not relieve the contractor of liability for material (nonconformity that substantial impairs value) latent or hidden defects subsequently revealed when goods are put to use.

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- 9.3.2** Acceptance of such goods may be revoked in accordance with the provisions of the applicable commercial code, and the Contractor is liable for any resulting expense incurred by the Purchasing Entity related to the preparation and shipping of Product rejected and returned, or for which Acceptance is revoked.
- 9.4 Failure to Conform.** Unless otherwise agreed upon in a Participating Addendum or Order, if any Professional Services do not substantially conform to the applicable SOW or SD (as defined above, the Purchasing Entity may require the Contractor to perform the Professional Services again in conformity with the SOW or SD requirements as agreed, at no increase in Order amount. When defects cannot be corrected by re- performance, the Purchasing Entity may require the Contractor to take necessary action to ensure that future performance conforms to the SOW or SD and reduce the contract price to reflect the reduced value of services performed. Please also refer to Section 9.5 Acceptance and Section 10 Warranty.
- 9.5 Acceptance Testing.** Purchasing Entity may establish a process, in keeping with industry standards, to ascertain whether the Product meets the standard of performance or specifications prior to Acceptance by the Purchasing Entity.
- 9.5.1** The Acceptance Testing period will be ten (10) calendar days, unless otherwise specified, starting from the day after the Product is delivered. After the expiration of such period, if the Purchasing Entity has not notified Contractor of any non-conformity the Products will be deemed accepted.
- 9.5.2** If the Product does not substantially conform with its Published Specifications during the initial period of Acceptance Testing, Purchasing Entity may, at its discretion, continue Acceptance Testing on a day-to-day basis until the standard of performance is met.
- 9.5.3** Upon rejection, the Contractor will identify the issue and seek to cure any non-conformity within a mutually agreeable time period or have fifteen (15) calendar days (whichever is greater) to cure any non-conformity. If after the cure period, the Product still has not met the standard of performance or specifications, the Purchasing Entity shall utilize the warranty and/or options provided in Contractor's EULA and EUSA.
- 9.5.4** Contractor shall pay all costs related to the preparation and shipping of Product returned pursuant to the section.
- 9.5.5** Reserved.

10. Warranty

- 10.1 Applicability.** Unless otherwise specified in the Master Agreement, Participating Addendum, or ordering document, the terms of this Section 10 will apply.
- 10.2 Warranty of Products.** Product warranties shall be as contained in Contractor's EULA that is attached to this Agreement as Attachment A and incorporated herein by reference..
- 10.3 Warranty of Professional Services.** The Contractor warrants that the Professional Services provided substantially conform to the SOW or SD requirements and shall be performed by competent personnel in a professional manner pursuant to industry standards.

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE SERVICES PERFORMED AND ANY ITEMS FURNISHED UNDER THIS

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

CONTRACT, INCLUDING BUT NOT LIMITED TO, DATA, REPORTS, DOCUMENTATION, DELIVERABLES, HARDWARE AND SOFTWARE OF ANY KIND, AND ANY RECOMMENDATIONS OR CONCLUSIONS CONTAINED THEREIN, ARE PROVIDED "AS IS. CONTRACTOR MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, THAT THE SERVICES WILL RENDER YOUR NETWORK AND SYSTEMS SAFE FROM MALICIOUS CODE, INTRUSIONS, OR OTHER SECURITY BREACHES. CONTRACTOR SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS OR PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT, AS WELL AS ANY WARRANTIES ALLEGED TO HAVE ARISEN FROM CUSTOM, USAGE, OR PAST DEALINGS BETWEEN THE PARTIES

10.4 Warranty Claims. Upon breach of a warranty, the Contractor will repair or replace (at no charge to the Purchasing Entity) the Product or Service whose nonconformance is discovered and made known to the Contractor pursuant to the terms of its EULA.

10.5 Reserved.

10.6 Warranty Period Start Date. The warranty period will begin upon delivery, as set forth in Section 9.

11. Product Title

11.1 Conveyance of Title. Upon Acceptance by the Purchasing Entity, Contractor or Contractor's Fulfillment Partner (when an Order is fulfilled by Contractor's Fulfillment Partner) shall convey to Purchasing Entity title to the Product, except for any portion of the Product which is provided subject to a nonexclusive subscription license or is Embedded Software, free and clear of all liens, encumbrances, or other security interests.

11.2 Embedded Software. If there is a transfer of title to the Product as contemplated in Section 11.1 (Conveyance of Title) above, such transfer must include a license to use any Embedded Software in the Product which shall be subject to the terms of Contractor's Supporting Materials. If Purchasing Entity subsequently transfers title of the Product to another entity, Purchasing Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title pursuant to Contractor's Secondary Market Policy. Notwithstanding the foregoing, any sale or transfer permitted by this subsection must be consistent with license rights granted for the use of the Embedded Software.

11.3 License of Pre-Existing Intellectual Property. License of Pre-Existing Intellectual Property shall be as detailed in the Contractor's EULA.

11.4 Unless otherwise specified in the Master Agreement, Participating Addendum, or ordering document, the terms of this Section 11 will apply.

11.5 No Ownership in Contractor Software. Notwithstanding anything to the contrary, in no event shall Purchasing Entity receive ownership or title rights to any Contractor Software or cloud services.

11.6 Purchasing Entity Data. Except in an aggregated and anonymized format that does not identify the Purchasing Entity or individual users, Purchasing Entity retains full right and title to its data.

12. Indemnification and Limitation of Liability

12.1 General Indemnification. The Contractor shall defend, indemnify and hold harmless PPA, RFxPremier, the Lead Entity, Participating Entities, and Purchasing Entities, along with their

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

officers and employees ("Indemnified Party"), from and against third-party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property arising from any act, error, or omission of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to performance under this Master Agreement. If the Contractor fails to pursue the defense or settlement of the third-party claim, the Indemnified Party may assume the defense or settlement of the third-party claim and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in relation to the third-party claim as finally awarded by a court of competent jurisdiction or as mutually agreed in a settlement approved by both the Indemnified Party and Contractor.

The foregoing indemnification obligations are conditioned upon the Indemnified Party promptly notifying the Contractor in writing of the claim, suit, or proceeding for which the Contractor is obligated under this Subsection, cooperating with, assisting, and providing information to the Contractor as reasonably required, and granting the Contractor the exclusive right to defend or settle such claim, suit or proceeding; provided that any such settlement or compromise includes a release of the Indemnified Party from all liability arising out of such claim, suit or proceeding.

12.2 Intellectual Property Indemnification. The Contractor shall defend, indemnify and hold harmless PPA, RFxPremier, the Lead Entity, Participating Entities, Purchasing Entities, along with their officers and employees ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use infringes Intellectual Property rights of another person or entity ("Intellectual Property Claim").

12.2.1 The Contractor's obligations under this Section 12.2 will not extend to any Intellectual Property Claim based on:

- 12.2.1.1** a combination of the Product or Service with any other product, system, or method, unless the other product, system, or method is (a) provided by the Contractor or the Contractor's subsidiaries or affiliates; (b) reasonably required to use the Product or Service in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function;; or
- 12.2.1.2** Contractor's compliance with any designs, specifications, requirements, or instructions by any Indemnified Party or a third party on Indemnified Party's behalf; or
- 12.2.1.3** the alteration or modification of the Contractor's Product by anyone other than Contractor or its designee; or
- 12.2.1.4** the amount or duration of use made of Contractor's Product or Services offered by Indemnified Party to external or internal Purchasing Entity, or revenue earned by the Indemnified Party; or
- 12.2.1.5** use of a Product not in accordance with or in violation of this Agreement or the Published Specifications; or
- 12.2.1.6** failure to use: (a) the most recent version of a Product or Service; or (b) an equally compatible and functionally equivalent non-infringing version

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



of a Product or Service provided by Contractor to address such an Intellectual Property Claim.

- 12.2.2** The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. If the Indemnified Party fails to provide reasonable notice-and that failure prejudices Contractor's ability to defend, settle, or respond to the claim, then Contractor's obligation to defend, indemnify, or hold harmless the Indemnified Party with respect to that Intellectual Property Claim will be reduced to the extent Contractor has been prejudiced. In addition, such failure to provide reasonable notice shall relieve Contractor of any obligation to reimburse for Indemnified Party's attorneys' fees incurred prior to notification. To the greatest extent allowable by law, if the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of the Intellectual Property Claim. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible.
- 12.2.3** The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of the Intellectual Property Claim and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in relation to the Intellectual Property Claim as finally awarded by a court of competent jurisdiction or as mutually agreed in a settlement approved by both the Indemnified Party and Contractor.
- 12.2.4** Unless otherwise set forth herein or in a Participating Addendum, Order, or Contractor Supporting Materials incorporated in an Order, Section 12.2 is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.
- 12.2.5** If such an Intellectual Property Claim has occurred, or in the Contractor's opinion is likely to occur, the Contractor shall either procure for the Participating Entity the right to continue using the materials or Products or Services or replace or modify materials or Products or Services to make them non-infringing and functionally equivalent. If an option satisfactory to the Participating Entity is not reasonably available, the Participating Entity shall return the materials or Products to the Contractor and stop using the infringing Services, upon written request of the Contractor and at the Contractor's expense, and Contractor shall refund to the Indemnified Party the remaining net book value of the Contractor's Product and a prorated amount for the remaining Services. The refund shall be determined in accordance with generally accepted accounting principles.

12.3 Limitation of Liability

- 12.3.1 General Limitation of Liability.** Except as provided in Section 12.3.2, notwithstanding anything else herein, all liability of Contractor and its suppliers to any Purchasing Entity or Participating Entity (and any Purchasing Entity under the

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

Participating Entity) for claims arising under this Master Agreement, the applicable Participating Addendum, or otherwise shall be limited to the greater of (i) ten million dollars (\$10,000,000.00) or (ii) the money paid to Contractor by the Participating Entity under this Master Agreement in the twelve (12) month period prior to the event or circumstances that first gave rise to such liability. This limitation of liability is cumulative and not per incident.

- 12.3.2 Exception to General Limitation of Liability.** The limitation of liability in Section 12.3.1 does not apply to: (i) liability for damage or loss caused by injury to persons or tangible property; (ii) Contractor's liabilities and obligations under Section 12.2; or (iii) matters for which liability cannot be excluded or limited under applicable law.
- 12.3.3 Limitation on Indirect Damages.** To the extent permitted by applicable law, except as provided in Section 12.3.4, neither Party shall be liable for any special, indirect, incidental, punitive, exemplary, reliance, or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products or Services to which this Agreement relates, regardless of the theory of liability and whether or not each Party was advised of the possibility of such damage or loss.
- 12.3.4 Exception to Limitation on Direct Damages.** Contractor's liability for a breach of its system security or unauthorized disclosure of Confidential Information are not subject to the limitations in Section 12. Notwithstanding the foregoing, in no event shall Contractor be liable for greater than ten million dollars (\$10,000,000), in the aggregate, for direct damages related to breach of its system security or unauthorized disclosure of Confidential Information under this Master Agreement. The aggregate liability under Section 12.3.4 shall be in addition to any liability under Section 12.3.1. For the purposes of this agreement, "Direct Damages" are defined to include the reasonable costs that result from a data breach. The reasonable costs may include for up to twelve (12) months of credit monitoring to affected individuals unless more is required otherwise by law, the reasonable costs of giving legally required notices to affected individuals, reasonable costs of forensic analysis of the extent of a data breach, and the affected individuals' reasonably proven economic damages shall be deemed direct damages.

13. Insurance

- 13.1 Term.** Unless otherwise agreed to between Contractor and Participating Entity, Contractor shall acquire maintain such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of A.M. Best's Insurance Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.
- 13.2 Class.** Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better,

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- in the most recently published edition of A.M. Best's Insurance Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.
- 13.3 Coverage.** Unless otherwise agreed to between Contractor and Participating Entity, coverage must be written on an occurrence basis. The minimum acceptable limits will be as indicated below:
- 13.3.1** Contractor shall maintain Commercial General Liability insurance covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than \$1 million per occurrence and \$2 million general aggregate. If Contractor does not maintain such insurance covering independent contractors, Contractor shall ensure its subcontractors' insurance satisfies this requirement;
- 13.3.2** Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.
- 13.4 Notice of Cancellation.** Contractor shall pay premiums on all insurance policies. Unless otherwise agreed to between Contractor and Participating Entity, Contractor or Contractor's insurer shall provide notice to a Participating Entity within 30 days after Contractor is first aware of expiration, cancellation or nonrenewal of such policy or is first aware that cancellation is threatened or expiration, nonrenewal or expiration otherwise may occur.
- 13.5 Notice of Endorsement.** Prior to commencement of performance, Contractor shall provide to the Lead Entity a written endorsement to the Contractor's general liability insurance policy or other insurance industry standard documentary evidence acceptable to the Lead Entity that (1) provides that written notice of cancellation will be delivered in accordance with the policy provisions, and (2) provides that the Contractor's liability insurance policy will be primary, with any liability insurance of any Participating Entity as secondary and noncontributory.
- 13.6 Participating Entities.** Unless otherwise agreed to between Contractor and Participating Entity, Contractor shall provide to Participating Entities the same insurance obligations and documentation as those specified in Section 13, except the endorsement or documentation is provided to the applicable Participating Entity.
- 13.7 Furnishing of Certificates.** Unless otherwise agreed to between Contractor and Participating Entity, Contractor shall furnish to the Lead Entity copies of certificates of insurance for all required insurance applicable to this Master Agreement in a form sufficient to show required coverage within thirty (30) calendar days of the execution of this Master Agreement and prior to performing any work. Copies of renewal certificates of all required insurance will be furnished within thirty (30) days after any renewal date to the applicable state Participating Entity. Failure to provide evidence of coverage may, at the sole option of the Lead Entity, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.
- 13.8 Disclaimer.** Insurance coverage and limits will not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

14. General Provisions

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

14.1 Records Administration and Audit

14.1.1 The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and Orders placed by Purchasing Entities under it to the extent and in such detail as will adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead Entity, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. The Lead Entity may terminate this Master Agreement, without incurring any liability, for the Contractor's refusal to allow access as required by this section. This right will survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Master Agreement, whichever is later, or such longer period as is required by the Purchasing Entity's state statutes, to assure compliance with the terms hereof or to evaluate performance hereunder.

14.1.2 Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead Entity, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or Orders or underpayment of fees found as a result of the examination of the Contractor's records.

14.1.3 The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement that requires the Contractor to self-audit contract obligations and that permits the Lead Entity to review compliance with those obligations.

14.2 Confidentiality, Non-Disclosure, and Injunctive Relief

14.2.1 Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity or Purchasing Entity's clients.

14.2.1.1 Any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity ("Confidential Information").

14.2.1.2 Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information.

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

14.2.1.3 Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity; or (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

14.2.2 Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement.

14.2.2.1 Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information.

14.2.2.2 Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead Entity immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of Section 14.2 of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person.

14.2.2.3 Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. In the event it is not possible or practicable to return such information, Contractor may, at Purchasing Entity's option, destroy such Confidential Information utilizing industry standard processes, or shall maintain possession of such Confidential Information and maintain its confidentiality for as long as necessary.

14.2.2.4 If applicable law, regulation, or document retention policy prevents Contractor from destroying or returning all or part of the Confidential Information, Contractor will maintain the security and confidentiality of

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



all such retained Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits, and evidence of the performance of this Master Agreement.

14.2.2.5 Contractor may publicize the Contract term, scope and price without prior written approval. However, Contractor may not use the Montana State seal, any State logo, or claim any State endorsement as to the Contract without prior written approval by the State of Montana.

14.2.3 Injunctive Relief. Contractor acknowledges that Contractor's breach of Section 14.2 may cause irreparable injury to the Purchasing Entity that cannot be adequately compensated in monetary damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

14.2.4 Purchasing Entity Law. These provisions will be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

14.2.5 RFXPremier. Subject to public information laws, the rights granted to Purchasing Entities and Contractor's obligations under this section will also extend to RFXPremier's Confidential Information, including but not limited to Participating Addenda, Orders or transaction data relating to Orders under this Master Agreement that identify the entity/customer, Order dates, line-item descriptions and volumes, and prices/rates. This provision does not apply to disclosure to the Lead Entity, a Participating Entity, or any governmental entity exercising an audit, inspection, or examination pursuant to this Master Agreement. To the extent permitted by law, Contractor shall notify the Lead Entity of the identity of any entity seeking access to the Confidential Information described in this subsection.

14.2.6 Public Information. This Master Agreement and all related documents are subject to disclosure pursuant to the Lead Entity's public information laws. Under Montana public information laws, this Contract, referenced documents, including pricing documents, are all deemed public information.

14.3 RESERVED.

14.4 Assignment/Subcontracts

14.4.1 Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead Entity. Notwithstanding the foregoing, Contractor may, with prior written consent from Participating Entities, which consent shall not be unreasonably withheld, enter into subcontracts with third parties as Fulfillment Partners. Fulfillment Partners are Subcontractors who may provide products and services under this Master Agreement at the price discounts established in this Master Agreement and bill Purchasers directly for such products and services. In addition, Contractor may, without permission, utilize subcontractors to perform

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

Services sold under this Master Agreement and provide cloud-based Products and Services. Contractor may, upon written notice to the Participating Entity, add or delete authorized Fulfillment Partners as necessary, at any time during the term. For clarity, Fulfillment Partners have no authority to amend this Master Agreement or to bind Contractor to any additional terms or conditions.

- 14.4.2** The Lead Entity reserves the right to assign any rights or duties, including written assignment of contract administration duties, to RFXPremier and other third parties.
- 14.5 Changes in Contractor Representation.** The Contractor must, within thirty (30) calendar days, notify the Lead Entity in writing of any changes in the Contractor's key administrative personnel managing the Master Agreement. The Lead Entity reserves the right to approve or reasonably reject changes in key personnel, as identified in the Contractor's proposal. The Contractor shall propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.
- 14.6 Independent Contractor.** Contractor is an independent contractor. Contractor has no authorization, express or implied, to bind the Lead Entity, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and shall not hold itself out as agent except as expressly set forth herein or as expressly set forth in an applicable Participating Addendum or Order.
- 14.7 Termination.** Unless otherwise set forth herein, this Master Agreement may be terminated by either party upon sixty (60) days' written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon thirty (30) days' written notice, unless otherwise limited or stated in an applicable Participating Addendum. Termination may be in whole or in part. Any termination under this provision will not affect Orders outstanding at the time of termination and the rights and obligations attending thereto, including any right of a Purchasing Entity to indemnification by the Contractor, rights of payment under any then-outstanding Orders in accordance with Section 7.53 herein, rights attending any warranty or default in performance in association with any Order, and requirements for records administration and audit. Termination of the Master Agreement due to Contractor default may be immediate.
- 14.8 Force Majeure.** Neither party to this Master Agreement shall be held responsible for delay or default caused by fire, riot, unusually severe weather, other acts of God, or acts of war which are beyond that party's reasonable control. Either party may terminate this Master Agreement upon determining such delay or default by the other party will reasonably prevent successful performance of the Master Agreement.
- 14.9 Defaults and Remedies**
- 14.9.1** The occurrence of any of the following events may be an event of default under this Master Agreement:
- 14.9.1.1** Nonperformance of material contractual requirements;
- 14.9.1.2** A material breach of any material term or condition of this Master Agreement;

**Request for Proposals for
Data Communications**

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- 14.9.1.3** Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading;
 - 14.9.1.4** Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or
 - 14.9.1.5** Any material default specified in another section of this Master Agreement.
 - 14.9.2** Upon the occurrence of an event of default, the Lead Entity shall issue a written notice of default, identifying the nature of the default, and providing a period of time specified by the Lead Entity but in no event shorter than thirty (30) calendar days in which Contractor shall have an opportunity to cure the default. The Lead Entity shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead Entity, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis.
 - 14.9.3** If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and the Lead Entity shall have the right to exercise any or all of the following remedies:
 - 14.9.3.1** Any remedy provided by law;
 - 14.9.3.2** Termination of this Master Agreement and any related Contracts or portions thereof;
 - 14.9.3.3** Suspension of Contractor from being able to respond to future bid solicitations;
 - 14.9.3.4** Suspension of Contractor's performance; and
 - 14.9.3.5** Withholding of payment until the default is remedied, if applicable to an Order under the Participating Addendum
 - 14.9.4** Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and shall have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Unless otherwise specified in an Order, a Purchasing Entity shall provide written notice of default as described in this section and have all of the rights and remedies under this paragraph and any applicable Participating Addendum with respect to an Order placed by the Purchasing Entity. Nothing in these Master Agreement Terms and Conditions will be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- 14.9.5** If this Contract is not renewed at the end of this term, if the Contract is otherwise terminated before project completion, or if particular work on a project is terminated for any reason, Contractor shall, upon mutual agreement of the parties, provide transition assistance for a reasonable, mutually agreed period of time after the expiration or termination of this Contract or particular work under this Contract. The purpose of this assistance is to allow for the expired or terminated portion of the services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such services to the Participating Entity or its designees. The parties agree that such transition assistance is governed by the terms and conditions of this Contract, except for those terms or conditions that do not reasonably apply to such transition assistance. State shall pay Contractor for any resources, Products, or Professional Services utilized in performing such transition assistance at the most current Contract rates. If the Participating Entity terminates a project or this Contract for cause, then State may offset the cost of paying Contractor for the additional resources Contractor utilized in providing transition assistance with any damages the Participating Entity may have sustained as a result of Contractor's breach.
- 14.10 Waiver of Breach.** Failure of the Contractor, Lead Entity, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies will not operate as a waiver under this Master Agreement, any Participating Addendum, or any Purchase Order. Any waiver by the Contractor, Lead Entity, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Contractor, Lead Entity or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order will not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, any Participating Addendum, or any Purchase Order.
- 14.11 Debarment.** The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, or declared ineligible-from participation in public procurement or contracting by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead Entity.
- 14.12 No Waiver of Sovereign Immunity**
- 14.12.1** In no event will this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of the Lead Entity, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.
- 14.12.2** This section applies to a claim brought against the Participating Entities who are states only to the extent Congress has appropriately abrogated the state's sovereign immunity and is not consent by the state to be sued in federal court. This section is also not a waiver by the state of any form of immunity, including but not

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

14.13 Governing Law and Venue

14.13.1 The procurement, evaluation, and award of the Master Agreement will be governed by and construed in accordance with the laws of the Lead Entity sponsoring and administering the procurement. The construction and effect of the Master Agreement after award will be governed by the law of the state serving as Lead Entity. The construction and effect of any Participating Addendum or Order against the Master Agreement will be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's state.

14.13.2 Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the state serving as Lead Entity. Venue for any claim, dispute or action concerning the terms of the Master Agreement will be in the state serving as Lead Entity. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum will be in the Purchasing Entity's state.

14.13.3 If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead Entity for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead Entity is a party; the state where the Participating Entity or Purchasing Entity is located if either is a named party.

14.14 Assignment of Antitrust Rights. Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided in that state for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at the Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action to the extent the assignment is necessary for the Participating Entity to overcome a federal or state government's bar on indirect purchases.

14.15 Survivability. Unless otherwise explicitly set forth in a Participating Addendum or Order, the terms of this Master Agreement as they apply to the Contractor, Participating Entities, and Purchasing Entities, including but not limited to pricing and the reporting of sales and payment of administrative fees to RFXPremier, shall survive expiration of this Master Agreement and shall continue to apply to all Participating Addenda and Orders until the expiration thereof.

14.16 Compliance with Law. Both parties agree to comply with the laws and regulations applicable to their respective business and, with respect to Contractor, those laws and regulations applicable to its general provision of the Products and Services under this Master Agreement, without regard to any entity's particular use of such Products or Services.

14.17 Severability. If any provision of this Master Agreement is deemed by a court or other tribunal of competent jurisdiction to be invalid or unenforceable, the remaining terms of this Master

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

Agreement will remain in full force and effect, and the provision affected will be construed so as to be enforceable to the maximum extent permissible by law.

- 14.18 Entire Agreement.** This Master Agreement, along with any attachment or exhibit hereto, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in an Order or Participating Addendum with a Participating Entity. Except as otherwise expressly set out in this Master Agreement, any amendment of any provision of this Master Agreement will be effective only if in writing and signed by duly authorized representatives of both parties.

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



Attachment 1

SUPPORTING MATERIALS

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



Attachment 2 SCOPE OF WORK

This Scope of Work (SOW) describes the deliverables available through this Master Agreement and the scope of what Contractors are expected to offer Participating Entities and Purchasing Entities. This SOW defines the scope of the Master Agreement and is not intended to limit the products and services a Contractor may offer within the defined scope.

I. OBJECTIVES

A. Scope of Work Objectives:

1. **Data Communications:** For the purposes of this Scope of Work and the resulting Master Agreements, **Data Communications is defined as the products and services that provide the technological capabilities to transmit, receive, and manage digital information through information technology networks.** This SOW seeks the Contractor to provide all aspects of data communications capabilities in a holistic solution, that includes hardware, software, and services, to develop, establish, maintain, secure, and expand data communications networks.
2. **Original Equipment Manufacturer (OEM):** For the purposes of this Scope of Work and the resulting Master Agreements, **OEM is defined as a Contractor that designs and manufactures data communications hardware.** The OEM (Awarded Contractor) shall provide data communications solutions consisting of the hardware as well as software solutions and services to support the hardware. Offerors are strongly encouraged to review this definition as it pertains to this SOW, to determine its eligibility to submit a proposal. All Offerors must affirm their OEM status (as defined in this section) in Attachment G, Offeror Response Worksheet.

B. Approach and Considerations: The scope of work approach will not establish individual product award categories but will seek to award to OEMs that manufacture data communications hardware and be capable of supporting that hardware through a holistic approach of software, cloud networking, services, etc. to provide the interested Participating Entities secure data communications capabilities in various protocols (data formatting, transmission, and error handling such as TCP/IP, HTTP, FTP, etc.). As stated, there will not be individual award categories, however, this SOW seeks solutions to be provided consisting of, but not limited to, the following common Data Communication fields:

- **Networking:** The infrastructure and systems that enable connectivity and data transfer, including routers, switches, network management and network optimization tools.
- **Unified Communications:** Data Communications products and technologies that integrate various communications to provide the capability of exchanging digital

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



information seamlessly including, but not limited to, voice, video, and text and other forms of media.

- **Wireless Networking:** Technologies that enable data communication over wireless mediums, including Wi-Fi access points, wireless controllers, and related management tools.
- **Security:** Solutions that ensure confidentiality, integrity, and availability of data and network resources, including firewalls, intrusion detection/prevention systems, encryption technologies, and secure access controls.
- **Facilities Management:** Products and technologies that provide digital capabilities to manage, monitor, and control various facilities functions utilizing access control systems, security and surveillance, energy and climate control, alert and emergency response systems, etc.

The definition of Data Communications above will consist of the following and defined in the below sections of this SOW. Some content and scope in the sections may cross between hardware and software.

- Hardware
- Software
- Services

This Scope of Work is meant to be solution-based, the following content in this SOW is meant to provide guidelines and framework for Data Communications solutions, it is not meant to limit the scope or restrict the solutions or systems. It is strongly encouraged to propose emerging technologies (such as Artificial Intelligence, Internet of Things) under the multiple categories so long as it is considered within the scope of Data Communications, by the definition encompassing this SOW, and adds or enhances the overall solution for the customer. The products must be able to address customers' business needs and integrate into the overall solution.

II. DATA COMMUNICATIONS: HARDWARE

A. Networking: Routers – A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keeps the networks connected to the Internet. Below is a list of routers, this list is not limited to the routers that can be provided under this scope:

- 1. Branch Routers** — A multiservice router typically used in branch offices or locations with limited numbers of users and supports flexible configurations/feature. For example: security, VoIP, wan acceleration, etc.

**Request for Proposals for
Data Communications**

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

- 2. Network Edge Routers** — A specialized router residing at the edge or boundary of a network. This router ensures the connectivity of its network with external networks, a wide area network or the Internet. An edge router uses an External Border Gateway Protocol, which is used extensively over the Internet to provide connectivity with remote networks.
 - 3. Core Routers** — High performance, high speed, low latency routers that enable Enterprises to deliver a suite of data, voice, and video services to enable applications such as Internet Protocol Television (IPTV) and Video on Demand (VoD), and Software as a Service (SaaS).
 - 4. Service Aggregation Routers** — Provides multiservice adaptation, aggregation and routing for Ethernet and IP/MPLS networks to enable service providers and enterprise edge networks simultaneously host resource-intensive integrated data, voice and video business and consumer services.
 - 5. Carrier Ethernet Routers** — High performance routers that enable service providers to deliver a suite of data, voice, and video services to enable next-generation applications such as IPTV, Video on Demand (VoD), and Software as a Service (SaaS)
- B. Networking: Switches** — A networking hardware device that connects multiple technology devices within a local area network (LAN). It forwards data packets to the correct destination device, ensuring efficient communication. These can be managed, unmanaged, layer 2/3 devices that are used to connect segments of a LAN (local area network) or multiple LANs and to filter and forward packets among them. Below is a list of switches, this list is not limited to the switches that can be provided under this scope:
- 1. Campus LAN – Access Switches** — Provides initial connectivity for devices to the network and controls user and workgroup access to internetwork resources.
 - 2. Campus LAN – Core Switches** — Campus core switches are generally used for the campus backbone and are responsible for transporting large amounts of traffic both reliably and quickly.
 - 3. Campus Distribution Switches** — Collect the data from all the access layer switches and forward it to the core layer switches. Traffic that is generated at Layer 2 on a switched network needs to be managed or segmented into Virtual Local Area Networks (VLANs), Distribution layer switches provides the inter-VLAN routing functions so that one VLAN can communicate with another on the network. Distribution layer switches provide advanced security policies that can be applied to network traffic using Access Control Lists (ACLs).
 - 4. Data Center Switches** — Data center switches, or Layer 2/3 switches, switch all packets in the data center by switching or routing good ones to their final destinations, and discard unwanted traffic using Access Control Lists (ACLs) a minimum of 10 Gigabit speeds. High availability and modularity differentiate a typical Layer 2/3 switch from a data center switch. Ability to remotely disable and enable individual ports. Support

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

“NetFlow” or equivalent. Jumbo frame supports EVPN over MPLS or BGP (9k bytes), plug and play fabric formation. Ultra-low latency through wire-speed ports with nanosecond port-to-port latency and hardware- based Inter-Switch Link (ISL) trunking.

5. Carrier Aggregation Switches — Carrier aggregation switches route traffic in addition to bridging (transmitted) Layer 2/Ethernet traffic that are designed for Ethernet networks that support video and high-bandwidth applications. Supports a variety of interface types, especially those commonly used by service providers.
6. Carrier Ethernet Access Switches – A carrier Ethernet access switch can connect directly to the customer or be utilized as a network interface on the service side to provide layer 2 services.
7. MPLS and Ethernet-Based WAN Solutions – Modern, scalable WAN technologies replacing legacy SONET networks.
8. Switch Features and Capabilities – the following list includes desired features and capabilities as necessary for the appropriate switch, as applicable:
 - Security Features: SSHv2 (Secure Shell Version 2), 802.1x (Port Based Network Access Control), Port Security, DHCP (Dynamic Host Configuration Protocol) Snooping, Two-Factor or Multi-Factor Authentication (2FA/MFA), MacSec encryption, Role-based access control lists (ACL)
 - Fast Ethernet/Gigabit Ethernet - 802.3bz (multi-gig interfaces 2.5Gbps and 5 Gbps)
 - 1/10/25/40/100/400 Gbps Support
 - PoE (Power over Ethernet) - up to 90/95W on all ports
 - Port Mirroring
 - Span Taps
 - Support of IPv6 and IPv4
 - Swappable powerlines and fans
 - AC or DC power supply minimum DC input ranging from 18V to 32 VDC and 36V to 72 VDC
 - Switch-port auto recovery
 - Dynamic Trunking Protocol (DTP)
 - Per-VLAN Rapid Spanning Tree (PVRST+)
 - IGP (Interior Gateway Protocol) routing, including non-proprietary such as IS-IS, OSPF, iBGP
 - EGP (Exterior Gateway Protocol) routing, including Border Gateway Protocol (BGP)
 - VPLS (Virtual Private LAN Service) Support
 - VRRP (Virtual Router Redundancy Protocol) Support

C. Networking: Storage

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

The emergence of new technologies creates an emphasis on storage devices that are connected via networks to servers to data to be accessed, managed, and shared efficiently across multiple systems. The goal is to provide managed centralized storage, increased scalability, and improved data protection and backup solutions.

This scope seeks various storage solutions that facilitate several use cases including, but not limited to, enterprise data centers, high performance computing, virtualization environments, artificial intelligence, security systems, backup and redundancy systems, and disaster recovery systems. Below is a list of storage solutions that are desired, this list is not limited to the storage devices or solutions that can be provided under this scope:

1. **Storage Area Network (SAN):** These devices are high-speed and specialize in block-level storage for data centers. This solution is protocol-independent and can be Fibre Channel (FC), FCOE or similar SAN topology for private cloud storage in virtualized environments.
2. **Network Attached Storage (NAS):** storage system at the file level connected to an IP network.
3. **Fabric and Blade Server Switches:** A Fibre Channel switch is a network switch compatible with the Fibre Channel (FC) protocol. It allows the creation of a Fibre Channel fabric, which is currently the core component of most SANs. The fabric is a network of Fibre Channel devices, which allows many-to-many communication, device name lookup, security, and redundancy. FC switches implement zoning; a mechanism that disables unwanted traffic between certain fabric nodes.

D. Optical Networking

High-capacity networks based on optical technology and components that provide routing, grooming, and restoration at the wavelength level as well as wavelength-based services.

1. **Core DWDM (Dense Wavelength Division Multiplexing) Switches** — Switches used in systems designed for long haul and ultra long-haul optical networking applications.
2. **Edge Optical Switches** — Provide entry points into the enterprise or service provider core networks.
3. **Optical Network Management** — Provides capabilities to manage the optical network and allows operators to execute end-to-end circuit creation.
4. **IP over DWDM (IPoDWDM)** — A device utilized to integrate IP Routers and Switches in the OTN (Optical Transport Network).

E. Wireless Networking

Wireless networking hardware are physical devices that enable data transmission without the use of physical cables, using radio waves, microwaves, or infrared signals to connect computers, mobile devices, and networks.

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

1. **Wireless Access Points (WAP)** – A device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. Capabilities should include:
 - 802.11a/b/g/n/ac/ and later
 - 2.4GHz, 5GHz, and 6GHz support
 - Should be capable of controller via DHCP, or automatically discovering cloud management system
 - Support for WPA2/WPA3
 - UL2043 plenum rated for safe mounting in a variety of indoor environments
 - Support AES-CCMP (128-bit)
 - Provides real-time wireless intrusion monitoring and detection
2. **Wireless Router** – Combination of a router and wireless access point, provides both internet access and Wi-Fi connectivity.
3. **Outdoor Wireless Access Points** – Outdoor APs are more rugged devices. Should be able to tolerate the elements of weather to tolerate a wide temperature range, high humidity, exposure to water, dust and oil, be able to be deployed virtually anywhere, provide real-time wireless intrusion monitoring and detection.
4. **Wireless LAN Controllers** — An onsite or offsite solution utilized to manage Light-weight access points in large quantities by the network administrator or network operations center. These devices are gateways that control user traffic aggregation. The WLAN controller automatically handles the configuration of wireless access points. Capabilities should include:
 - Ability to monitor and mitigate RF interference/self-heal
 - Support seamless roaming from AP to AP without requiring re-authentication
 - Support configurable access control lists to filter traffic and deny wireless peer to peer traffic
 - System encrypts all management layer traffic and passes it through a secure tunnel
 - Policy management of users and devices provides ability to de-authorize or deny devices without denying the credentials of the user, nor disrupting other AP traffic
5. **Wireless LAN Network and Cloud-Based Services and Management** — Enables network administrators to quickly plan, configure and deploy a wireless network, as well as provide additional WLAN services. Some examples include wireless security, asset tracking, and location services. Capabilities should include:
 - Provide for redundancy and automatic failover
 - Historical trend and real time performance reporting is supported
 - Management access to wireless network components is secured
 - RFC 1213 compliant
 - Automatically discover wireless network components

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- Capability to alert for outages and utilization threshold exceptions
 - Capability to support Apple's Bonjour Protocol / mDNS
 - QoS / Application identification capability
 - Zero-touch access point provisioning
 - Network-wide visibility and control
 - RF optimization,
 - Firmware updates
6. **Mobile Device Management (MDM)** — MDM technology is utilized to allow employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged government information and applications in a secure manner. Capabilities should include:
- Ability to apply corporate policy to new devices accessing the network resources, whether wired or wireless
 - Provide user and devices authentication to the network
 - Provide secure remote access capability
 - Support 802.1x
 - Network optimization for performance, scalability, and user experience
 - BYOD/unmanaged device configuration (such as SecureW2 or CloudPath)

F. Security Hardware

1. **Intrusion Detection/Protection and Firewall Appliances** — Provide comprehensive inline network firewall security from worms, Trojans, spyware, key loggers, and other malware. This includes Next-Generation Firewalls (NGFW), which offer a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks.
 - Non-disruptive in-line bump-in-the-wire configuration
 - Network-address translation (NAT), stateful protocol inspection (SPI) and virtual private networking (VPN), etc.
 - Application awareness, full stack visibility and granular control
 - Capability to incorporate information from outside the firewall
 - Upgrade path to include future information feeds and security threats
 - SSL decryption to enable identifying undesirable encrypted applications (Optional)
2. **Data Center and Virtualization Security Products and Appliances** — Products designed to protect high-value data and data center resources with threat defense and policy control.
3. **Application Delivery and Security** — Includes application deliver controllers, load balancers, and Layer 7 Firewalls. Can be physical and virtual load balancers, WAFs, SSL offloading, and advanced traffic management.

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



III. DATA COMMUNICATIONS: SOFTWARE and CLOUD

Please note that software and cloud offerings are to be related to the functionality and solution-based data communications systems and solutions scope. It is recognized that advancements in technology have provided emerging solutions that do not require hardware or on-premises solutions to provide network and data communications capabilities. This Contract will not require software or cloud services to be tied to a hardware purchase, however, the software and cloud offerings must strictly relate to Data Communications as per the definition established in this Scope of Work.

Below is a list of software solutions, this list is not limited to the software solutions that can be provided under this scope:

A. Networking Software Solutions

Software covers a wide array of solutions required to support network operation and management within the scope of data communications. These consist of management tools to optimize area networks, or to ensure performance, optimization, capacity, data migration, data reduction and efficiency.

1. **Networking Software** – Software that runs on a server, or within the Cloud, and enables the server to manage data, users, groups, security, applications, and other networking functions. The network operating system is designed to allow transfer of data among multiple computers in a network, typically a local area network (LAN), a private network or to other networks. Networking software capabilities should include:
 - Restartable Process
 - High availability options
 - Targeted operating systems, i.e. DC, campus, core, WAN
 - Operating System Efficiencies
 - Network analysis tools (solutions utilized to collect, classify, analyze, and securely store log messages)
 - Load balancing – supports multiple balances in the same system, layer 4+7
 - Reporting
 - WAN optimization
 - Data compression
 - Network analysis tools (solutions utilized to collect, classify, analyze, and securely store log messages)
2. **Software Defined Networks (SDN)** – Virtually manages flow control and can include SDN virtualized switches, routers, and controllers. These applications enable intelligent networking.
3. **Automated Management Software for Network, Cloud, and Data Centers** — Software products and solutions for network automation, cloud computing, and IT systems management to ensure secure, reliable, and scalable network operations.
 - Automate routine and repetitive tasks

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

- Implement monitoring and alerting for proactive system maintenance
 - Provision, configure, and manage cloud resources (IaaS, PaaS, SaaS)
 - Automate backup, scaling, and deployment processes
 - Monitor server health, storage systems, and power usage
 - Ensure cloud security with identity management, encryption, and compliance controls
4. Edge Computing – Distributed processing near data sources to reduce AI and IoT applications.
 5. DDI (DHCP, DNS, IPAM) Management Platforms – Integrated platforms for automating and securing core network services (DHCP, DNS, IP address management).

B. Security Solutions

Security of networks is paramount for the success of this scope of work and one of the most important aspects to ensure the confidentiality, integrity, and availability of data transmitted over communications networks. Security solutions will secure the data in transit across wired and wireless networks, prevent unauthorized access, inception, and tampering of communications. Security solutions will align with industry standards. The security solutions will enhance monitoring of the network. It is expected that networks be equipped with cutting edge security technology. Network systems need to be aware of the ever-changing landscape of threats, how to detect them, prevent them, and in cases where the threat is present, eliminate the threat.

Please note that this section refers to an array of desired security products. This does not supplement security requirements found in the Master Agreement Terms and Conditions. While some products may overlap or require additional negotiation with the Participating Entity, the MA security terms should be a baseline that take precedence and apply to all of the offerings.

Below is a list of security solutions, this list is not limited to the offerings that can be provided under this scope:

1. Network Security – These security measures will require a comprehensive solution that protect the network and digital infrastructure from cyber threats. These security measures include, but are not limited to:
 - Remote Browser Isolation (RBI): Keeps web content off endpoints to prevent drive-by downloads and malicious scripts.
 - Incident Response Solutions: Rapid-deployment networking solutions for emergency response, including drone communication hubs.
 - Zero Trust OT Security: Focused on securing operational technology environments with strict identity verification.
 - Zero Trust Network Access (ZTNA): Provides secure, identity-based access to applications regardless of location.
 - Malware Analysis & Sandboxing: Isolates and analyzes suspicious files or behavior in a secure environment before execution.

**Request for Proposals for
Data Communications**

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

-
- DNS Security: Blocks access to malicious domains and provides visibility into domain-level threats.
 - AI Access Security: Controls and monitors access to AI tools and platforms, helping prevent misuse or data leaks.
 - Data Center Security: Protects physical and virtual infrastructure in centralized or hybrid data centers.
 - Data Loss Prevention (DLP): Prevents sensitive data from being lost, leaked, or misused.
 - Intrusion Detection and Prevention (IDPS): Monitors and blocks suspicious or malicious network activity.
 - AI-Driven Network and Security Management - For automation, anomaly detection, predictive maintenance, and self-optimizing networks.
 - IoT Security: Protects connected devices and their communication from exploitation.
2. Cloud Security – Consists of securing the communication channels, protocols, and endpoints involved in data exchanges across cloud services. These cloud security measures include, but are not limited to:
- Cloud Secure Web Gateway: Protects users from malicious internet traffic, enforcing security policies in the cloud.
 - Cloud Access Security Broker (CASB): Bridges the gap between cloud service usage and enterprise security policies.
 - Cloud Security Posture Management: Continuously monitors and evaluates cloud configurations to ensure they meet security and compliance standards.
 - Cloud Workload Protection: Secures applications and services running in cloud environments by protecting workloads from vulnerabilities and threats.
 - Cloud Visibility, Compliance, & Governance: Provides centralized insight into cloud resources while enforcing policies for regulatory compliance and governance.
 - Secure Access Service Edge (SASE): Converges networking and security services into a single cloud-delivered platform.
 - Security Service Edge (SSE): Consolidates cloud-delivered security functions such as SWG, CASB, and ZTNA.
 - Cloud-Native Networking and Security: Tools and services supporting hybrid/multi-cloud deployments and modern security architecture.
 - Cloud Threat Detection: Identifies suspicious behavior, misconfigurations, and active threats across cloud environments using analytics and threat intelligence.
 - Infrastructure as Code (IaC) Security: Scans and secures infrastructure templates (e.g., Terraform, CloudFormation) to detect misconfigurations before deployment.

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



3. **Identities and Access Management** – Consists of managing user identities, controlling access to systems and data, and ensuring that access is granted based on the principle of least privilege. These management security measures include, but are not limited to:
 - **Privileged Access Management (PAM):** Secures, monitors, and controls access to critical systems by privileged users to reduce the risk of insider threats and credential abuse.
 - **Identity as a Service (IDaaS):** Delivers cloud-based identity management capabilities such as single sign-on (SSO), authentication, and user provisioning as a service.
 - **Access Management:** Controls and enforces who can access what resources, when, and under what conditions, often integrating with authentication and authorization policies.
 - **Identity Governance and Administration (IGA):** Provides policy-based controls to manage user identities, access rights, and lifecycle processes across the enterprise.
 - **Directory Services:** Centralizes user identity data and authentication across systems, typically using technologies like LDAP, Active Directory, or cloud directories.
 - **Micro and Macro Segmentation Solutions:** Granular (micro) and broad (macro) network segmentation for enhanced security and compliance.
 - **Identity Analytics:** Uses data analysis and machine learning to detect anomalies, assess risks, and support access decisions in real-time.

- C. Unified Communications** – Integrated data communications solutions that can include hardware, software, and services.

Unified Communications (UC) is a solution that integrates multiple communications tools and technologies into a single cohesive end-user interface to enhance business communication. UC features include, but is not limited to the following:

1. **Voice Calling (VoIP):** Internet-based voice communication, includes E911 support.
 - Support for analog, digital, and IP endpoints
 - Flexibility to configure queue depth and hold time, play unique announcements and Music on Hold (MoH), log in and log out users from a queue and basic queue statistics
 - Enterprise Telephony Features (CFx, Transfer, CID, Shared line appearance, One Number Service, etc.)
2. **Video Conferencing:** Real-time video meetings and virtual collaboration.
3. **Instant Messaging (Chat):** Real-time text communication. Solutions that allow communication over the Internet Protocol, within the enterprise, and remotely, as well as with guest users that offers quick transmission of text-based messages from sender to receiver. In push mode between two or more people using personal computers,

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

Desktop (Windows/Mac/VDI/Linux), Mobile/Smartphone, Tablet, along with shared clients, instant messaging basically offers real-time direct written language-based online chat. Instant messaging may also provide video calling, file sharing, PC-to-PC voice calling and PC-to-regular-phone calling

4. Email and Voicemail Integration: Unified inbox for different types of messages.
5. Presence Information: Shows user availability (e.g., available, busy, offline).
6. File Sharing & Collaboration Tools: Enables real-time co-editing and document sharing.
7. AI driven communication tools leveraging machine learning that automate and enhance communication experience and abilities.

D. Facilities Management, Monitoring and Control – Integrated data communications solutions that can include hardware, software, and services.

This integrated solution provides the capabilities of monitoring systems and control mechanisms to track, manage, and optimize building performance in areas such as energy, safety, HVAC, lighting, access, and IT infrastructure.

1. Monitoring – The use of technology such as sensors (hardware) and software to track building conditions and security. It can include environmental metrics, power usage, equipment usage and fault detection.
2. Control – The use of technology to automatically or manually manage and control systems in a physical space utilizing monitored data. It can include remote equipment operation, HVAC and lighting systems, power management and backup systems.
3. Security Systems – The use of data communications systems to provide video surveillance, facial recognition, thermal imaging, smart sensors, real-time alerts and forensic search. The employment of AI solutions that enable video surveillance and analytics is desired.

IV. DATA COMMUNICATIONS: SERVICES

This SOW seeks not only hardware and software offerings above, but a comprehensive service offering to ensure that all purchases of data communications hardware and software perform properly and optimally. The Contactor shall be responsible for the performance of all aspects of the contract, including the performance of all subcontractors.

A. Services and Consulting

To ensure success of data communications systems and networks, the SOW requires that the Contractor provide holistic solutions consisting of services including, but not limited to the following service areas:

1. Installation

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

- Site Survey and Assessment – Includes preinstallation site assessments to identify cabling paths, equipment locations, power requirements, and potential constraints
- Network Cabling and Physical Infrastructure – Installation of secured cabling systems and testing of all cables to ensure connectivity.
- Equipment Installation – Mount and install all hardware including firewalls, switches, routers, wireless access points, etc. Configure hardware to design and system specifications, including integrating power supplies.
- Wireless Network Deployment – Install and test wireless access points, optimize signal strength, secure access points by configuring encryption and protocols.
- Configuration and Integration – Load base configurations on hardware, integrate new hardware with existing systems.
- Testing and Validation – Includes performance testing, fault tolerance, connectivity and document results.

2. Maintenance

- Preventative Maintenance – Perform routine inspections and testing of data comm systems.
- Corrective Maintenance – Respond to system failures, cable faults, or connectivity issues. Replace faulty or defective components, restore service and limit downtime.
- Performance Monitoring – Monitor performance, analyze data traffic efficiency, identify congestion.
- System Configuration Management – Maintain backup copies of data comm system configurations, track and document changes to network.

3. Troubleshooting and Helpdesk

- Support Services – Provide Tier 1 (basic), Tier 2 (intermediate), and Tier 3 (advanced) support for data communication systems. Offer support in multiple channels (phone, email, chat, remote in)
- Incident Management – Log, categorize, prioritize, and track all incidents through a centralized ticketing system
- Guide users through troubleshooting steps for simple issues (e.g., cable checks, adapter settings)

4. Security

- Security Architecture and Design – Includes firewall and perimeter defense consulting.
- Updates and Patching – apply critical updates to system, test and update firewall rules, scan the system for network vulnerabilities.

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



- Data Encryption and Secure Transmission – Encrypt data in transit using protocols like TLS, IPSec, and VPNs. Secure communications between network nodes, cloud services, and remote users.

5. Training

- Conduct training and knowledge transfer sessions for Participating Entity staff and end users.
- Platforms for upskilling staff in AI, automation, network management, and cybersecurity.
- Provide user guides and quick-reference materials.

B. Service Level Considerations

This SOW seeks quality services administered with successful performance while recognizing that there are multiple potential Participating Entities with many different needs. This service level outline is meant to provide framework for the Contractor to incorporate as required and as appropriate per the service level agreed upon by the Contractor and Participating Entity.

1. Performance Guidelines:

- Assign a contract manager to act as a liaison and contact person between the Purchasing Entities and the Contractor for the purpose of resolving issues or problems related to any part of this contract.
- Follow the Participating Entities' state and local laws and regulations, especially labor and prevailing wage laws as well as all federal law (i.e. Davis-Bacon Act).
- Employ skilled and experienced professionals for the specific task required to ensure highest quality and neat and expeditious performance.
- Be licensed in each region, state, jurisdiction, etc. where Contractor is approved and awarded to work. Contractor or subcontractor performing work requiring a license must have obtained the license prior to commencing work. The Participating Entity reserves the right to reject a response if the responder fails to provide the Participating Entity adequate documentation of any required license. The Participating Entity reserves the right to verify any required license prior to final award and at any time during the work. The Contractor is responsible for the costs of obtaining or maintaining any licenses, permits, or other costs and shall not pass the cost through on an invoice.
- Be responsible for obtaining all necessary permits, plan reviews, and inspections required for the work when applicable. Permits and Plan Reviews required by local authorities or the State shall be secured and paid for by the Contractor.
- Provide all necessary payroll and prevailing wage reports along with any required statements of compliance along with their invoice.
- Comply with each Participating Entity's cabling, electrical, and construction materials requirements.
- Hazardous Materials – The Contractor is responsible for compliance with any Participating Entity requirements regarding hazardous materials. If the

Request for Proposals for
Data Communications

Issued by the **State of Montana**



Solicitation Number: SPB-RFP-2025-0563LS

Contractor encounters a hazardous material or substance not addressed in the quote and if reasonable precautions will be inadequate to prevent foreseeable bodily injury or death to persons resulting from a material or substance, including but not limited to asbestos or polychlorinated biphenyl (PCB), encountered on the site by the Contractor, the Contractor shall, upon recognizing the condition, immediately stop work in the affected area and report the condition to the Participating Entity.

- Final Acceptance of Completed Service by the Participating Entity – Upon completion of installation, maintenance, or repair services, Contractor must submit a request for written final acceptance of service completion from the Participating Entity. After receiving written final acceptance of completion of the service from the Participating Entity, the Contractor may issue an invoice to the Participating Entity. Contractor must satisfy all other Contract submittal requirements necessary for the service prior to submitting the request for written acceptance of service completion. If agreed upon by Participating Entity and Contractor, milestone payments are permitted. The milestones will be in writing and a part of the quote/contract between the Participating Entity and Contractor.

2. Request for Quote

- Provide a quote to any Purchasing/Participating Entity for data communications services and projects prior to any installation.
- Provide a not to exceed number of hours at the time of quote to complete the service and indicate whether the service will be performed on or off site.
- Provide the Participating Entity with a written quote of the amount of additional time needed to complete the service which the Participating Entity must approve in writing before continuing with the service, in the event the number of quoted not to exceed hours is met, but more time is needed to complete the service.
- Provide Contractor's name and subcontractor's name, and representatives.
- Date of quote and contract number at the top.
- Hardware, software, third party products information that will be used in the data communications solution – including price, extended pricing, quantity, license agreements, additional service level agreements.
- Estimated Quantity – clear and concise number of hours for all positions that will perform work.
- Any retainage information based on Participating Entity requirements.
- Any performance bond information based on Participating Entity requirements.
- Any additional fringe costs such as: mileage, lodging, freight, as agreed upon with the Participating Entity.

Request for Proposals for
Data Communications

Issued by the **State of Montana**

Solicitation Number: SPB-RFP-2025-0563LS



Attachment 3

COST PROPOSAL

Pricing for this Agreement is set forth in the Cost Proposal, attached hereto and incorporated by reference. The Cost Proposal is maintained as a separate Excel workbook titled **Palo Alto Networks Cost Proposal.xlsx**

Attachment H - Cost Proposal

Solicitation Number: SPB-RFP-2025-0563L

Data Communications

Offeror Name: **Palo Alto Networks, Inc.**

Data Comm Hardware Sector	Offeror's Minimum Discount	Sales: Direct or Through Supplier Partner
Networking Routers	NA	NA
Networking Switches	NA	NA
Networking Storage	NA	NA
Optical Networking	NA	NA
Security Hardware	10%	Through Supplier Partner

Data Comm Software Sector	Offeror's Minimum Discount	Sales: Direct or Through Supplier Partner
Networking Software Solutions	NA	NA
Security Solutions	10%	Through Supplier Partner
Unified Communications	NA	NA
Facilities Management, Monitoring and Control	NA	NA

Service Type	Maximum Hourly Rate
Integrator	\$609.00
Architect	\$609.00
Engineer	\$609.00
Installer	\$609.00
Training	\$609.00
Other- Unit 42	\$390.00
Other- Professional Services	0%
Other- Lab	0%

* not offered in an hourly rate

* not offered in an hourly rate

Attachment H - Cost Proposal
Solicitation Number: SPB-RFP-2025-0563LS
Data Communications



Offeror Name: **Palo Alto Networks, Inc.**

Third-Party Offerings									
Product Name	Product Category	Item Number	Manufacturer	UOM	QTY per UOM	List Price	% Discount	Net Price	Notes
Palo Alto Networks does not propose any Third Party Offering									
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[Add additional rows as needed.]

Attachment H - Cost Proposal

Solicitation Number: SPB-RFP-2025-0563LS

Data Communications

Offeror Name: **Palo Alto Networks, Inc.**



1. Describe your relationship with price competitiveness and how do you ensure that the contractual pricing is competitive?

Our relationship with price competitiveness is vital, especially within the State, Local, and Education (SLED) segment, where providing the best value is paramount. We ensure contractual pricing is highly competitive by utilizing a SLED-specific Pricing Guide that locks in pre-negotiated, aggressive discounts often exceeding those for commercial customers; this guide is continually benchmarked against market rates to guarantee these competitive discounts are consistently offered to SLED customers across the entire U.S. Palo Alto Networks would be able to offer a higher discount on hardware and software if maintenance support was discounted separately.

2. What measures have been put in place that will enhance cost savings. What tools and communication/transparency capabilities does the Offeror currently have to support this?

Palo Alto Networks' cost-saving measures are heavily focused on consolidating security point solutions into a unified platform and leveraging AI and automation to drive massive operational efficiencies, both for itself and its customers.

These measures shift the focus from traditional cost-cutting to Total Economic Impact (TEI), where a higher initial investment is justified by significant long-term savings in labor, complexity, and breach avoidance.

3. How will you manage pricing volatility?

Palo Alto Networks manages pricing volatility primarily through its recurring subscription revenue model and its strategic focus on platform consolidation. This foundational business approach generates predictable cash flow and enhances its long-term pricing power by making its offerings indispensable to customers. Tactically, while the core business model offers stability, the company's product price files (SKUs) are updated monthly for products under contract, and a comprehensive, once-annual pricing review is conducted to reflect any necessary adjustments, such as those related to inflation.

4. Do you provide any tools that assists users in evaluating the total cost of ownership of products offered during the purchasing process (i.e., Contractor tools to assist buyers in identifying equipment that runs more efficiently or that utilizes fewer supplies, etc.).

5. Location of data – please provide details around your pricing models when it pertains to where data is stored. Please provide scenarios in which the location of data is provided as an option with different price points available? What is the markup when it is US soil only?

Palo Alto Networks offers a strong US-only data residency option for our public sector customers and highly regulated industries. This is primarily delivered through our cloud-based platforms that have achieved the highest levels of U.S. Government compliance:

- **FedRAMP High Authorization:** Palo Alto Networks has achieved FedRAMP High Authorization for our major cloud platforms, including Prisma Cloud, Prisma Access, and Cortex XSIAM. This designation requires hosting and processing data within secure, compliant data centers located on U.S. soil (specifically in U.S. Government Cloud regions, such as AWS GovCloud or Azure Government). This ensures strict adherence to U.S. Federal data residency requirements.
- **Prisma Cloud Government Cloud Services:** Our cloud security platform is hosted in segregated U.S. Government cloud environments. This ensures that the metadata, logs, and sensitive security event data collected by the platform are processed and stored within the continental U.S., meeting the demands of customers with stringent data locality needs.
- **Local Cloud Infrastructure:** For all commercial customers, Palo Alto Networks deploys local cloud infrastructure globally, including multiple regions within North America. Customers can select these specific U.S. regions for their data storage, ensuring their security logs and intelligence data comply with domestic data residency policies.



END USER LICENSE AND SUPPORT AGREEMENT

This End User License Agreement (“**Agreement**”) is made and entered into as of the latter date of execution (“**Effective Date**”) by and between:

[Counter Party Name] (**End User**”, “**Customer**”)

And,

[Insert Proper Palo Alto entity] (collectively,

"Palo Alto Networks")

Palo Alto Networks and End User may also be referred to herein individually as a “**Party**” or collectively as the “**Parties**” throughout this Agreement.

IN WITNESS WHEREOF, Parties hereto have caused their respective authorized representatives to execute this Agreement as of the Effective Date.

Reviewed By:

[Insert Palo Alto Networks entity]

Signed:

Print Name:

Title:

Date:

Customer: [Counterparty Name]

Signed:

Print Name:

Title:

Date:



BY SIGNING THIS AGREEMENT, CUSTOMER IS BOUND BY THE TERMS CONTAINED HEREIN, INCLUDING, IF APPLICABLE, THE PROGRAM TERMS ASSOCIATED WITH THE PURCHASE OF AN ENTERPRISE PROGRAM FOUND AT www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/enterprise-agreement-for-attached-subscriptions.pdf AND https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/enterprise-agreement-for-hardware-support.pdf, WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT. IF CUSTOMER DOES NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS ATTACHED AS ATTACHMENT 1 AND HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT. ALL DOCUMENTS IN HYPERLINKS ARE ATTACHED TO THE END OF THIS DOCUMENT AS ATTACHMENTS 2-7 AND INCLUDED HEREIN BY THIS REFERENCE. ATTACHMENTS ARE AS FOLLOWS: ATTACHMENT 2, ENTERPRISE AGREEMENT FOR ATTACHED SUBSCRIPTIONS, ATTACHMENT 3, ENTERPRISE AGREEMENT FOR HARDWARE SUPPORT, ATTACHMENT 4 SECONDARY MARKET POLICY, ATTACHMENT 5 PALO ALTO NETWORKS DATA PROCESSING ADDENDUM, ATTACHMENT 6 PALO ALTO NETWORKS GRACE PERIODS, ATTACHMENT 7 IS ALL HYPERLINKS IN THE END USER SUPPORT AGREEMENT AND ARE REFERRED TO IN TOTAL AS PALO ALTO NETWORKS SUPPORT POLICIES.

If Customer is using a Product for proof of concept, trial, evaluation or other similar purpose (“**Evaluation**”), the terms of Section 11n below shall apply.

1. DEFINITIONS

“**Affiliate**” means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise. Customer acknowledges and authorizes Palo Alto Networks’ use of all Palo Alto Networks Affiliates to deliver Products and Support Services.

“**Customer Data**”, also referred to as “**End User Data**”, means data provided by or on behalf of Customer to Palo Alto Networks for processing as part of the delivery of the Product and Support Services. Customer Data does not include Systems Data.

“**Hardware**” means hardware-based products listed on Palo Alto Networks’ then-current price list or supplied by Palo Alto Networks.

“**Product**” means, collectively, Hardware, Software, Subscription, and any combination thereof.

“**Published Specifications**” mean the applicable user manual, acceptable use policies, privacy and product data sheets, and other corresponding documents published by Palo Alto Networks that are customarily available to end users of the Product(s).

“**Software**” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

“**Subscription(s)**” means software-as-a-service and cloud-delivered security services, including updates, provided by Palo Alto Networks, regardless of whether a fee is charged for its use. Support Services and professional services are not considered Subscriptions under this Agreement.

“**Support Services**” means the maintenance, support services and customer success services provided by Palo Alto Networks or its representative in effect at the time such maintenance, support services and/or customer success services are ordered and as further set forth in the End User Support Agreement.

“**Systems Data**” means data generated or collected by the Products or Support Services in connection with Customer’s use of those Products and Support Services, such as logs, file attributes, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, copilot inputs and outputs, potentially malicious files or security policy violations detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS. Customer’s rights to use the Products are limited to those expressly granted in this Section.

a. Software Use Rights

This Section 2a applies to Software only. Subject to compliance with this Agreement, upon Customer’s purchase, Palo Alto Networks grants Customer a limited, royalty-free, non-exclusive right to use the Software:

- i. in accordance with Published Specifications for the Software, and Hardware if applicable;
- ii. solely for the term and within the scope of the use rights purchased (e.g., number of users);
- iii. solely for internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and
- iv. through a third-party contractor providing IT services solely for Customer’s benefit, subject to their compliance with this Agreement.



All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This Section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to Customer's compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make the Subscriptions available twenty-four (24) hours a day, seven (7) days a week in accordance with the applicable service level agreement set forth at <https://www.paloaltonetworks.com/services/support/support-policies> (which may be updated from time to time and at any time), except for published downtime or any unavailability caused by circumstances beyond Palo Alto Networks' control including, but not limited to, a force majeure event described in Section 11g below. The applicable service level agreement sets forth Customer's sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability in the event that Palo Alto Networks does not meet the service level commitments stated therein. Palo Alto Networks grants Customer a non-exclusive right to access and use the Subscriptions:

- i. in accordance with Published Specifications for the applicable Subscriptions;
- ii. solely for the term and within the usage capacity purchased (e.g., number of workloads, number of unique users; number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, workloads, or the like);
- iii. solely for internal use for the purpose of securing Customer's infrastructure, unless agreed otherwise in a separate written contract with Palo Alto Networks; and
- iv. through Customer's third-party contractor providing IT services solely for Customer's benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions

Customer shall not:

- i. use any Product that is procured under a Lab, or NFR (not for resale) SKU in a production environment;
- ii. use the Products beyond the scope of the use right and/or capacity purchased;
- iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;
- iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;
- v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;
- vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that Customer (or a third-party contracted by Customer) runs on the Products, in whole or in part;
- vii. transfer, sublicense, or assign any rights under this Agreement to any third party except as expressly provided in Section 2d and/or Section 11a below, unless expressly authorized by Palo Alto Networks in writing;
- viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein, or as specifically permitted by the Published Specifications. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the [Palo Alto Networks license transfer procedure \(https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html\)](https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);
- ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;
- x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that Customer reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to Customer;
- xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;
- xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;
- xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or
- xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, acting as a managed services provider.

d. Affiliates

If Customer purchases Product for use by Customer's Affiliate, Customer shall:

- i. provide Customer's Affiliate with a copy of this Agreement;



- ii. ensure that Customer's Affiliate complies with this Agreement;
- iii. be responsible and liable for any breach of this Agreement by such Customer Affiliate; and
- iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from Customer's Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

Customer shall keep accounts and authentication credentials providing access to Products secure and confidential. Customer must notify Palo Alto Networks without undue delay about any misuse of Customer accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent Customer provides any suggestions or comments related to the Products ("**Feedback**"), Palo Alto Networks shall own the Feedback, have all rights to retain and use any Feedback in current or future products or services, without Customer's approval or compensation to Customer. Palo Alto Networks acknowledges that all Feedback is provided "AS IS" and agrees that it will not publicly release the Feedback in any manner that identifies Customer as the source of such Feedback, or that directly or indirectly connects the Feedback with Customer.

4. OVERUSE.

Fees for volume or capacity usage (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with Customer's actual usage at the end of each month or quarter for any volume- or capacity-based Products. To the greatest extent allowable under applicable law and regulation, Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or an authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. Customer will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within twenty (20) days from the occurrence of such overuse and pay as invoiced. Excluding public sector customers, if payment is not received in accordance with the invoice for such overuse, Palo Alto Networks shall terminate or suspend Customer's use of such Subscriptions in accordance with Section 5.b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective until terminated by the Parties in writing or as specified herein; provided that the terms and conditions in this Agreement shall apply to any extension or renewal of Products and additional capacity purchased.

b. Termination; Suspension

i. Either Party may terminate this Agreement at any time in the event the other Party breaches any material term, including but not limited to Section 2 above, and fails to cure such breach within thirty (30) days following notice. For any material breach that cannot be cured, the non-breaching Party shall have the right to terminate this Agreement immediately upon written notice.

ii. Palo Alto Networks may, at its discretion, suspend Customer's access to or use of the Software, Subscriptions or Support Services if Customer is in default with any payment obligations concerning the Products or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on Customer's behalf.

iii. In addition to the rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of the Software, Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the Products or services in manner or for a purpose that is not contemplated by the applicable Published Specifications and is likely to cause harm to Palo Alto Networks or a third party. For any such suspension, once the issue is resolved by Customer and confirmed by Palo Alto Networks, Palo Alto Networks shall reinstate the access to or use of the Software, Subscriptions and Support Services as quickly as commercially possible.

c. Effects of Termination

Upon termination, Customer shall immediately cease using the Software and in case of the Subscriptions and Support Services, Palo Alto Networks shall terminate Customer's use of or access to any Subscriptions and access to the Support Services. At Palo Alto Network's discretion, Customer shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty



Palo Alto Networks warrants that:

- i. Hardware will be free from defects in material and workmanship for one (1) year from the date of shipment;
- ii. Software will substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and
- iii. Subscriptions will perform materially to Published Specifications for the duration of the selected term.

As Customer's sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, (i) repair or replace the Hardware or (ii) correct the Software or the Subscriptions so as to materially meet the applicable Published Specifications.

Warranty claims for: (1) Hardware and/or Software must be made within thirty (30) days from the detection of a suspected defect/discrepancy in writing during the warranty period specified herein; and (2) Subscriptions can be made at any time during the applicable Subscription term. If Palo Alto Networks, determines in its sole discretion, that it is unable to repair or replace the Product, Customer will be entitled to a refund of the fees pre-paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Hardware may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for Customer's or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. Customer will pay the shipping costs for return of Hardware to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to Customer.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

- i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;
- ii. accident, negligence, abuse or misuse of a Product by persons other than Palo Alto Networks or its designee;
- iii. use of the Product other than in accordance with Published Specifications;
- iv. improper installation or site preparation or Customer's failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or
- v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED "AS IS". PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET CUSTOMER'S REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either Party, or Palo Alto Networks' suppliers, be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each Party was advised of the possibility of such damage or loss.

b. Direct Damages

Subject to Section 7a and 11n, to the fullest extent permitted by applicable law, in no event shall the total liability of either Party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of: (1) one million United States dollars (\$1,000,000); or (2) the total amount Customer paid for the Product on which the claim is based. The foregoing limitation in this Section 7b shall not apply to liability arising from:

- i. death or bodily injury, willful misconduct, fraud or gross negligence;
- ii. Section 2c and Section 8; and



- iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will indemnify, defend, at its expense, and hold Customer harmless for any third-party actions, claims, injunctions or suits against Customer alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "**Claim**"), and Palo Alto Networks will pay damages awarded in final judgment against Customer or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that Customer (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that Customer enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

- i. procure the right for Customer to continue using the Product;
- ii. replace or modify the Product to avoid the Claim; or
- iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Customer may return the Hardware and cease using the Software and/or Subscriptions and Palo Alto Networks shall grant Customer a credit for the price of the Hardware as depreciated on a straight-line five (5) year basis, or a credit for the prepaid unused portion of the Software and/or Subscriptions based on the applicable impacted term, commencing on the date Customer received such Hardware, Software or Subscriptions.

c. Exceptions

Palo Alto Networks' obligations under this Section 8 shall not apply to the extent any Claim results from or is based on:

- i. modifications to a Product made by a party other than Palo Alto Networks or its designee;
- ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;
- iii. failure to use: (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;
- iv. Palo Alto Networks' compliance with Customer's explicit or written designs, specifications or instructions; or
- v. use of a Product not in accordance with or in violation of this Agreement or the Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"**Confidential Information**" means the non-public information that is exchanged, communicated, transmitted, or otherwise made available as between the Parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing Party ("**Discloser**"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the Party receiving such information ("**Recipient**"). . Confidential Information also does not include information that Recipient can prove by credible evidence:

- i. was in the public domain at the time it was communicated to Recipient;
- ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;
- iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;
- iv. was disclosed to Recipient free of any obligation of confidentiality; or
- v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each Party will not use the other Party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:



- a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;
- b. on a confidential basis to its legal or professional financial advisors; or
- c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for a period of three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

The confidential treatment of Customer Data, Personal Data, and Systems Data are addressed in Section 10 below.

10. CUSTOMER DATA, PERSONAL DATA AND SYSTEMS DATA

a. Customer Data

Palo Alto Networks and its Affiliates will process Customer Data solely for the purposes of providing Products and Support Services to Customer pursuant to the terms of this Agreement. All rights in and to Customer Data shall remain the exclusive property of Customer.

b. Personal Data

To the extent Palo Alto Networks and its Affiliates processes personal data (as defined by applicable data protection laws) on Customer's behalf, such personal data will be processed in accordance with the [Data Processing Addendum](#), which is incorporated by reference herein.

c. Systems Data

Palo Alto Networks may use Systems Data for the purposes of providing Products and services to Customer, improving Products and services, developing new Products and services, managing its relationship with Customer, and for threat research purposes. Palo Alto Networks will not disclose Systems Data to any unaffiliated third-party that identifies Customer, Customer's customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

d. Data Confidentiality and Security

Customer Data, Personal Data, and Systems Data will be treated confidentially and Palo Alto Networks will implement and maintain technical and organizational measures designed to secure such data as described in Palo Alto Networks' Information Security Measures, which is incorporated by reference herein.

e. Generative AI

Palo Alto Networks will not use, and will not allow its subcontractors to use, (a) Customer Data, or (b) Systems Data that identifies Customer (including Customer's customers or end users), to train generative AI.

11. GENERAL

a. Assignment

Neither Party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other Party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without Customer's consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the Parties.

b. Auditing End User Compliance

Customer shall retain records pertaining to Product usage consistent with Section 2 above. Customer grants to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, Customer shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, Customer will be able to download Software via the server network located closest to Customer. The Product may require an authorization code to activate or access Subscriptions and Support Services. The authorization codes will be issued at the time of order fulfillment. The Subscription, warranty or Support Services term will commence in accordance with the grace period policy at <https://www.paloaltonetworks.com/support/support-policies/grace-period.html>

d. Compliance with Laws; Export Control

Each Party shall comply with all applicable laws in connection with its respective activities arising from this Agreement. Customer further agrees that Customer will not engage in any illegal activity, and Customer acknowledges that Palo Alto Networks reserves the right to notify Customer or an appropriate law enforcement agency in the event of such illegal activity. Both Parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.



e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either Party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in Customer's purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Neither Party shall be responsible for any cessation, interruption, or delay in the performance of its obligations (excluding payment obligations by Customer) as a result of a cause beyond its reasonable control, which shall include, without limitation, earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, civil or regulatory authority, availability of network and telecommunications services or any other cause, whether similar or dissimilar to any of the foregoing, which could not have been prevented with reasonable care.

h. Governing Law

If Customer is located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If Customer is located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

- i. for Customer, to the e-mail set forth on the Customer's website, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.
- ii. for Palo Alto Networks: legal@paloaltonetworks.com; or,
- iii. for either Party, by overnight delivery service or by certified mail sent to the address published on the respective Parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Software may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). These Open-Source Software license terms are consistent with the rights granted in Section 2 and may contain additional rights benefiting Customer. Palo Alto Networks represents and warrants that the Software, when used in conformance with this Agreement, does not include Open-Source Software that restricts Customer's ability to use the Software nor requires Customer to disclose, license, or make available at no charge any material proprietary source code that embodies any of Customer's intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing; Use of Name, Logo, Trademarks

Neither Party shall publicly communicate or use the name, logo or trademarks of the other Party without the prior written permission of the other Party.

n. Evaluations.

When Customer is using a Product (or feature of a Product) for an Evaluation, Customer may do so for thirty (30) days only unless Palo Alto Networks issues an extension or agrees in writing to a longer period of time for the Evaluation(s). Palo Alto Networks reserves the right to terminate an Evaluation at any time. Upon expiration or termination of an Evaluation, Customer shall cease using the Product(s) provided for in an Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations, only Sections 1, 2.a, 2.c, 2.d., 2.e, 3, 7a, 8, 9, 10, and 11 of this Agreement shall apply. Notwithstanding anything set forth herein to the contrary, except for Palo Alto Networks' indemnification obligations set forth in Section 8, the total liability of Palo Alto Networks for Evaluations shall not exceed the greater of: (i) ten thousand United States dollars (\$10,000); or (ii) the total cost (if any) of the applicable Evaluation.



For Evaluation of features or Products that have not yet been made generally available to customers, Customer shall not rely upon any such features or Product that were included in an Evaluation in making its purchasing decision of the generally available version of the Product.

EVALUATIONS ARE PROVIDED “AS IS” AND “AS AVAILABLE.” THE RISKS ARISING OUT OF THE USE OR PERFORMANCE OF THE EVALUATION REMAIN WITH CUSTOMER. PALO ALTO NETWORKS AND ITS SUPPLIERS EXPRESSLY DISCLAIM ALL REPRESENTATIONS, CONDITIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE; ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE; AND ANY GUARANTEE OF AVAILABILITY OR PERFORMANCE.

o. Survival

The provisions set forth in the following Sections, and any other rights or obligations of the Parties in this Agreement that, by their nature, should survive termination or expiration of this Agreement, will survive any expiration or termination thereof: Section 2, Section 3, Section 5, Section 7, and Section 11.

p. Waiver and Severability

The failure by either Party to enforce any provision of this Agreement will not constitute a waiver of future enforcement of that or any other provision. Any waiver or amendment of any provision of this Agreement will be effective only if in writing and signed by authorized representatives of both Parties. If any provision of this Agreement is held to be unenforceable or invalid, that provision will be enforced to the maximum extent possible and the other provisions will remain in full force and effect.

q. U.S. Government End Users

This Section 11q applies to United States Government, and to the greatest extent possible to U.S. located state, local and education end users only and does not apply to any other end users. The Software, Subscriptions and its documentation are “commercial items” and “commercial computer software documentation,” as such terms are used in FARS and DFARS. If the Software and its documentation and/or Subscriptions and its documentation are being acquired by or on behalf of the U.S. Government, then the U.S. Government’s rights in the Software and its documentation and Subscriptions and its documentation shall be as specified in this Agreement.



ATTACHMENT 1

END USER SUPPORT AGREEMENT (“EUSA”)

THIS EUSA SUPPLEMENTS THE PALO ALTO NETWORKS [END USER LICENSE AGREEMENT](#) TO WHICH IT IS ATTACHED BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER”, “END USER”, “YOU” or “YOUR”) AND (A) PALO ALTO NETWORKS, INC. AND ITS AFFILIATES, 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054 UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD AND ITS AFFILIATES, 22 BISHOPGATE, LEVEL 55, LONDON, EC2N 4BQ, ENGLAND, IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C)

BEING REFERRED TO HEREIN AS “PALO ALTO NETWORKS”). This EUSA sets forth the terms and conditions under which Palo Alto Networks will provide technical support services and customer success services for the Palo Alto Networks Products sold and/or licensed pursuant to the [End User License Agreement](#). In the event of a conflict between this EUSA and the End User License Agreement, this EUSA shall take precedence, but only with respect to the subject matter described below.

Contact: support.paloaltonetworks.com, 1.866.898.9087 in the U.S., +1.408.738.7799 outside the U.S.

1. SUPPORT PLANS AND SERVICES OFFERED

	PLATINUM	PREMIUM	STANDARD
Online Support	Yes	Yes	Yes
Telephone support	Yes - 24x7x365	Yes - 24x7x365	No
Initial Response Time	PLATINUM	PREMIUM	STANDARD
Severity 1 – Critical Product is down, critically affects Customer production environment. No workaround available yet.	≤ 15 minutes	≤ 1 hour	≤ 2 Business Hours
Severity 2 – High Product is impaired, Customer production up, but impacted. No workaround available yet.	≤ 30 minutes	≤ 2 hours	≤ 4 Business Hours
Severity 3 – Medium A Product function has failed, Customer production not affected. Support is aware of the issue and a workaround is available.	≤ 2 hours	≤ 4 hours	≤ 12 Business Hours
Severity 4 – Low Non-critical issue. Does not impact Customer business. Feature, information, documentation, how-to and enhancement requests from Customer.	≤ 4 hours	≤ 8 hours	≤ 48 Business Hours
Additional Services	PLATINUM	PREMIUM	STANDARD
Premium United States Government (“USG”) Support	N/A	Yes, if eligible	N/A
Security Assurance	Yes, if eligible	Yes, if eligible	N/A
Expert Assistance	Yes, if eligible	N/A	N/A
Focused Services including Plus and Elite tiers	Optional, if eligible	Optional, if eligible	N/A

HARDWARE RMA	4-HR PREMIUM OR 4-HR PLATINUM	PREMIUM OR PLATINUM	STANDARD
Advance Replacement Service: 4-Hour Replacement (available only for Hardware located within a specified range of Palo Alto Networks service locations)	Yes, if eligible	No	No
Advance Replacement Service: Next Business Day Service	N/A	Yes	No
Return and Repair	N/A	N/A	Yes



2. CUSTOMER SUCCESS PLANS AND SERVICES OFFERED*

	PLATINUM	PREMIUM	STANDARD
Online Technical Support	Yes	Yes	Yes
Telephone Technical support	Yes - 24x7x365	Yes - 24x7x365	No
Technical Support Initial Response Time	PLATINUM	PREMIUM	STANDARD
Severity 1 – Critical Product is down, critically affects Customer production environment. No workaround available yet.	< 15 minutes	≤ 1 hour	≤ 2 Business Hours
Severity 2 – High Product is impaired, Customer production up, but impacted. No workaround available yet.	< 30 minutes	≤ 2 hours	≤ 4 Business Hours
Severity 3 – Medium A Product function has failed, Customer production not affected. Support is aware of the issue and a workaround is available.	< 2 hours	≤ 4 hours	≤ 12 Business Hours
Severity 4 – Low Non-critical issue. Does not impact Customer business. Feature, information, documentation, how-to and enhancement requests from Customer.	< 4 hours	≤ 8 hours	≤ 48 Business Hours
Self-help guidance: - Online access to quick-start guides, best practices and training materials (pdf and video) - Online access to knowledge base and Support Portal	Yes	Yes	Yes
Customer Success	PLATINUM	PREMIUM	STANDARD
Customer Success Team Assistance (deliverables may vary based on the Product): - Onboarding guidance - Configuration guidance - Operational and integration guidance - Education and training	Optional, if eligible	Optional, if eligible	No
Additional Services	PLATINUM	PREMIUM	STANDARD
Premium United States Government (“USG”) Success	N/A	Yes, if eligible	No
Focused Services including Plus and Elite tiers	Optional, if eligible	Optional, if eligible	No

* This table may not be applicable for all Prisma Access Customer Success Plan(s) offered in certain countries in the Asia Pacific region. For more information, see Section 11.

3. DEFINITIONS

“**Affiliate**” means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

“**Business Hours**” mean Mondays through Fridays, 9:00 am – 5:00 pm local time, excluding local holidays.

“**Customer Success Plan**” or “**Success Plan**” refers to a specific offering to provide technical support and to help promote customer success as described in section 5 below.

“**Expert Assistance**” refers to a Platinum-level service feature that provides on-site assistance for critical issues, failure analysis, and support for planned events.

“**Hardware**” means hardware-based products listed on the Palo Alto Networks then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

“**Maintenance Releases**” mean bug fixes to the Software that: (i) are designated by a change in the 3rd set of digits of the version release number (e.g., v5.00.01 to v5.00.02); and (ii) are generally made available by Palo Alto Networks to its customers under valid support contracts at no additional cost.

“**Major Releases**” mean significant modifications or improvements to the Software that: (i) are designated by a change in the first digit of the version release number (e.g., v5.0 to v6.0); and (ii) are generally made available by Palo Alto Networks to its customers under valid support contracts at no additional cost.

“**Minor Releases**” mean minor modifications or improvements to the Software, cumulative bug fixes from Maintenance Releases since the last Minor Release and new bug fixes, as applicable, that: (i) are designated by a change in the second set



of digits of the version release number (e.g., v5.00 to v5.01); and (ii) are generally made available by Palo Alto Networks to its customers under valid support contracts at no additional cost.

“Online Support” means access to the Support Portal, online documentation and Palo Alto Networks’ user community located at <https://live.paloaltonetworks.com>.

“Product” means, collectively, Hardware, Software, Subscription, or any combination thereof.

“Security Assurance” refers to a specific service designed to give Customers access to security experts with unique threat intelligence knowledge and tools.

“Software” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

“Standard Support,” “Premium Support,” “Platinum Support,” “Premium USG,” “4-Hour Premium Support,” “4-Hour Platinum Support” and **“Support Plan”** refer to the various support programs offered by Palo Alto Networks, as further detailed in section 4 below.

“Subscription” means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Threat Prevention, Advanced URL Filtering, WildFire, regardless of whether a fee is charged for its use. Support Plans, Customer Success Plans, and professional services are not considered Subscriptions under this EUSA.

“Support Portal” means the website currently located at <https://support.paloaltonetworks.com>, or any successor site specified by Palo Alto Networks.

4. SUPPORT PLAN OPTIONS

Where applicable, you may choose from Standard, Premium, Premium USG, Platinum, 4-Hour Premium and 4-Hour Platinum Support, and you must register each Product for which you have purchased support on the Support Portal in order to access the features and benefits available to such Product. Based on your selection and payment of applicable fees, Palo Alto Networks shall:

a. Standard Support

- i. Maintain and support the list of currently-supported releases published on the Support Portal.
- ii. Make available all supported Maintenance Releases, Minor Releases and Major Releases.
- iii. Verify defects in the Software identified and submitted by Customers.
- iv. Correct material defects in the Software for the currently-supported Maintenance Releases.
- v. Provide access to the Support Portal, which contains the latest Software versions, fixes, feature releases, signature and Subscription updates, knowledge base/FAQ, case management, release notes, technical documentation, and Software downloads.
- vi. Use commercially reasonable efforts to ensure that the Support Portal is available 24x7.
- vii. Respond to Online Support cases based on the severity classifications in section 1 above.
- viii. Provide a return and repair service for Hardware defects.

b. Premium Support

Includes all the benefits of Standard Support, plus faster response times and the following:

- i. Provide technical telephone support on a 24x7x365 basis. You are required to open a support ticket online in the Support Portal before reaching out for telephone support.
- ii. Advance replacement for defective Hardware. Refer to section 6 (RMA Policy and Process), subsection b (Advance Replacement) below for additional details.
- iii. Security Assurance:
 - a. Access to security experts in the event you detect suspicious activity in your network.
 - b. Eligibility:
 - i. This service is only applicable to the Hardware and VM-Series virtualized Firewalls.
 - ii. You must have a Best Practice Assessment (BPA) completed within the last 3 months.
 - iii. On the BPA, you must meet a minimum security threshold based on industry average in the 7 key feature adoption areas: WildFire, anti-virus, anti-spyware, DNS sinkhole, vulnerability protection, Advanced URL Filtering and logging.
 - iv. Each Customer may seek Security Assurance services no more than once per year.

c. Premium USG Support (State, Local, Federal Government and Government contractors only)

Includes all the benefits of Premium Support delivered by U.S. citizens located in U.S.-based support centers.

d. Platinum Support (not available in Japan)

Includes all the benefits of Premium Support, plus faster response times and Expert Assistance:

- i. Planned Event Assistance: Upon your request and if scheduled 7 days in advance, Platinum senior engineers will assist with proactive maintenance activities such as Software upgrades or feature activations. May be utilized at a



Customer business event where a Platinum engineer will be on-call to assist as necessary. You may receive assistance on up to 4 planned events per year, with each event normally not exceeding 4 hours. This service is not designed for troubleshooting activities or Product installations.

- ii. **On-Site Assistance:** To address Severity 1 issues which cannot be resolved remotely; a field engineer may be dispatched to Customer's site when necessary, at the discretion of Palo Alto Networks management.
- iii. **Failure Analysis:** Upon request, Palo Alto Networks will conduct and provide Hardware failure analysis on returned units. Failure Analysis does not extend to End of Sale (EOS) Products announced at <https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-sale>.
- e. **Focused Services (optional, if eligible)**
 - i. Access to personalized support by an assigned account manager who will provide tailored support.
 - ii. **Eligibility:** All Products you use must be under valid Premium-level Support/Success Plans at a minimum, as applicable.
- f. **4-Hour Premium or 4-Hour Platinum Support (applicable to qualified Hardware only)**
Includes all the benefits of Premium or Platinum Support, as applicable, and delivery of replacement Hardware to you within four hours from the issuance of a RMA. This support option is available only for Hardware located within a specified range of a Palo Alto Networks service location. Eligibility must be determined, and the service sold, on a per-device basis. When covered, Palo Alto Networks will use commercially reasonable efforts to deliver replacements within the designated time frame.

5. CUSTOMER SUCCESS PLAN OPTIONS

Where applicable, you may choose from Standard Success, Premium Success, Premium USG Success, or Platinum Success. Upon provisioning of your production instance, you will be granted access to the Subscription and to the Support Portal. Based on your selection and payment of applicable fees, Palo Alto Networks shall:

- a. **Standard Success**
 - i. Respond to Online Support cases based on the severity classifications in section 2 above.
 - ii. Provide access to Online Support resources and materials 24x7.
 - iii. Maintain and support the list of Subscription release notes published on the Support Portal.
 - iv. Verify defects identified and submitted by Customers.
 - v. Correct material defects in the cloud software running in production.
 - vi. Use commercially reasonable efforts to ensure that the Support Portal is available 24x7.
- b. **Premium Success**
Includes all the benefits of Standard Success, plus faster response times and the following:
 - i. Provide technical support via telephone on a 24x7x365 basis. You are required to open a support ticket online in the Support Portal before reaching out for telephone support.
 - ii. Customer Success Teams Assistance (optional, if eligible).
 - iii. **Focused Services (optional, if eligible)**
 - a. Access to personalized support by an assigned account manager who will provide tailored support.
 - b. **Eligibility:** All Products you use must be under valid Premium-level Support/Success Plans at a minimum, as applicable.
- c. **Premium USG Success (State, Local, Federal Government and Government contractors only)**
Includes all the benefits of Standard Success, delivered by U.S. citizens located in U.S.-based support centers.
- d. **Platinum Success (not available in Japan)**
Includes all the benefits of Premium Success, plus faster response times.

6. RMA POLICY AND PROCESS

In situations when it is necessary for you to return a Hardware to Palo Alto Networks, you must ask Palo Alto Networks to issue a Return Material Authorization ("RMA") number prior to shipment. Each RMA number will be uniquely identified to track the processing of the returned Hardware. Hardware RMA is subject to the Palo Alto Networks RMA Process and Policy ("RMA Policy") found at

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/support/rma-process-policy.pdf.

- a. **Return and Repair**
You shall obtain a RMA number for the Hardware that you wish to return to Palo Alto Networks by contacting Support via telephone or the Support Portal. Support will work with you to confirm the Hardware problem and issue a RMA number to be used to ship the Hardware back to Palo Alto Networks. You shall repackage the Hardware in the original packaging (shipping damage that occurs from insufficient packaging is not covered), note the RMA number on the shipping label and ship the Hardware to the specified Palo Alto Networks location. You will be responsible for all shipping



costs incurred in returning the defective Hardware to Palo Alto Networks. Hardware will be repaired (or replaced) and shipped within 10 business days from receipt of the defective Hardware by Palo Alto Networks. Palo Alto Networks will pay all shipping costs incurred in shipping the repaired or replacement Hardware to you, except that if you are located outside the United States, you will be responsible for any taxes, duties, fees or other charges assessed in connection with importing the repaired or replaced Hardware into your country of destination.

b. Advance Replacement

You shall obtain an RMA number for the Hardware that you wish to return to Palo Alto Networks by contacting Support via telephone or the Support Portal. Support will work with you to confirm the Hardware problem and issue an RMA number to be used to ship the Hardware back to Palo Alto Networks. Subject to the RMA Policy, Palo Alto Networks will use commercially reasonable efforts to attempt to deliver a replacement Hardware to you by the next business day. Palo Alto Networks will pay all shipping costs incurred in shipping the replacement Hardware to you. Upon receipt of a replacement Hardware, you shall return the defective Hardware to Palo Alto Networks in the replacement Hardware's packaging (shipping damage that occurs from insufficient packaging is not covered), using the prepaid return airbill affixed to the exterior of the shipping carton, and arranging for the designated courier service for pickup. If Palo Alto Networks does not receive the returned Hardware within 10 business days after the delivered date of the replacement Hardware, you will be charged current list price of the replacement Hardware.

c. 4-Hour Replacement (applicable to qualified Hardware only)

You shall obtain an RMA number for the Hardware that you wish to return to Palo Alto Networks. Support will work with you to confirm the Hardware problem and issue a RMA number. Palo Alto Networks will use commercially reasonable efforts to aim to deliver a replacement Hardware to you within four hours after issuance of the RMA number. You must have an authorized representative available to accept delivery of the replacement Hardware. If Palo Alto Networks (or its subcontractor) is unable to complete delivery because you did not have an authorized representative available, Palo Alto Networks reserves the right to charge you for costs incurred in making a subsequent delivery.

7. YOUR OBLIGATIONS

During the term of your support contract, you must:

- a. Operate at the then-supported Maintenance Release;
- b. Use reasonable efforts to isolate, collect all error and log files to enable Palo Alto Networks to fulfill its obligations herein; and
- d. Notify Palo Alto Networks if you physically relocate device(s) covered by 4-Hour Replacement service to new location(s), including verification that the relocated device(s) remain within the geographical area covered by 4-Hour Replacement service.

Other support-related policies available at <https://www.paloaltonetworks.com/services/support/support-policies.html> may be applicable.

8. LIMITATIONS

The following services are expressly excluded from Support and Success Plans:

- a. Repair or replacement of Product required as a result of causes other than normal use, including without limitation:
 - i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks-authorized personnel;
 - ii. accident or negligence of your fault;
 - iii. user error or misuse of the Product; or
 - iv. causes external to the Product such as, but not limited to, failure of electrical systems or fire or water damage or hardware failure, operation system software failure or any other damage and failure not caused by Palo Alto Networks.
- b. Maintenance or technical services for any third-party software or hardware, where such third-party software or hardware was not provided by Palo Alto Networks.
- c. Palo Alto Networks reserves the right not to support Products which were not purchased via an authorized Palo Alto Networks distributor or reseller.

9. TERM AND TERMINATION

This EUSA is effective until terminated or, as applicable, in accordance with the term of your Support or Success Plan. Palo Alto Networks will send you renewal reminders in advance of the expiration date(s) of the applicable Support or Success Plan. At the end of the term (and each renewal term thereafter, if any), the applicable Support or Success Plan will automatically expire unless you renew. Either party may terminate this EUSA and the applicable Support and/or Success Plan(s) at any time in the event the other party breaches any material term of this EUSA and fails to cure such breach within thirty (30) days following such notice.



10. NO WARRANTY

Nothing in this EUSA shall be construed as expanding or adding to the warranty set forth in the Palo Alto Networks End User License Agreement. PALO ALTO NETWORKS MAKES, AND YOU RECEIVE, NO WARRANTIES OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, ARISING IN ANY WAY OUT OF, RELATED TO, OR UNDER THIS AGREEMENT OR THE PROVISION OF MATERIALS OR SERVICES THEREUNDER, AND PALO ALTO NETWORKS SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY INCLUDING MERCHANTABILITY AND

FITNESS FOR A PARTICULAR PURPOSE. Note that replacement Products under section 6 may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not.

11. SUPPLEMENTAL TERMS AND CONDITIONS

For the supplemental terms and conditions under which Palo Alto Networks will provide technical support services for the Cloud NGFW for AWS Products sold and/or licensed pursuant to the End User License Agreement, please see the Supplemental End User Support Agreement available at: <https://www.paloaltonetworks.com/legal/eusa/ngfwaws>.

For the supplemental terms and conditions under which Palo Alto Networks will provide technical support services for AIOps for NGFW Products sold and/or licensed pursuant to the End User License Agreement, please see the Supplemental End User Support Agreement available at: <https://www.paloaltonetworks.com/legal/eusa/aiops>.

For the supplemental terms and conditions under which Palo Alto Networks will offer Customer Success Plan for the Prisma Access Products in certain countries in the Asia Pacific region, please see the Supplemental End User Support Agreement available at: <https://www.paloaltonetworks.com/legal/eusa/prisma-access-cn>.

For the supplemental terms and conditions under which Palo Alto Networks will provide technical support services for Software Firewall Orchestration Hub used for Palo Alto Networks VM-Series firewalls sold and/or licensed pursuant to the End User License Agreement, please see the Supplemental End User Support Agreement available at: <https://www.paloaltonetworks.com/legal/eusa/automationsupport>.

Attachment 2



Enterprise Program **(For Attached Subscriptions)**

1. Scope and Description

This Enterprise Program for Attached Subscriptions (“**ELA**”) supplements the [End User Agreement](#) (or equivalent signed agreement) (the “**EULA**”) which governs the use of every Palo Alto Networks product/service. By purchasing an ELA, Customer agrees that the terms and conditions set forth in the EULA and the terms and conditions contained in this document shall apply. Capitalized terms used but not otherwise defined herein will have the meaning assigned to them in the EULA.

Palo Alto Networks has developed an Enterprise Program, which is a volume licensing arrangement that allows organizations to have access to firewall subscriptions for use in conjunction with the deployment and use of Palo Alto Networks Hardware in a customer’s hardware estate for the applicable Term (as defined below). This arrangement is designed to simplify the purchasing, renewal, and deployment of the Attached Subscriptions (as defined below), and to provide organizations with an efficient means of managing its network security expense. The features and benefits associated with the ELA are detailed below.

2. Term

When purchased, the term of this ELA shall be effective for the term duration specified on the quote (“**Term**”). Note that a 5 year Term is available only to select customer accounts, whose qualifications will be determined on a case-by-case basis by Palo Alto Networks.

3. Features and Benefits of an ELA

a. When purchased, the ELA entitles Customer to the following subscriptions during the Term (“**Attached Subscriptions**”):

- i. Advanced DNS Security;
- ii. PAA (includes Prisma Access Agent and GlobalProtect Gateway);
- iii. Advanced URL Filtering;
- iv. Advanced Threat Prevention;
- v. Advanced WildFire; and
- vi. Advanced SD-WAN (PAN-OS).

b. **Hardware Estate.** At purchase, Customer shall provide Palo Alto Networks with a forecast of any additional hardware firewalls it expects to add to its current hardware estate (“**Current Hardware Estate**”), if any, during the Term (such additional hardware growth forecasted to Customer’s Current Hardware Estate shall be referred to herein as the “**Forecasted Hardware Estate**”). Customer’s use of the Attached Subscriptions is subject to a Total Hardware Cap (as defined below) that is based on the “Current Hardware Estate” and “Forecasted Hardware Estate” calculated based on the current hardware list price. If Customer purchases additional hardware firewalls during the Term, Customer must pay for the Attached Subscriptions for the portion of hardware above the Total Hardware Cap; provided that: (i) in the case of a 1-year term, Palo Alto Networks shall provide Customer with unlimited access to the Attached Subscriptions at no additional charge; and (ii) in the case Terms greater than 1 year, Palo Alto Networks shall provide Customer access to the Attached Subscriptions subject to the applicable term’s Total Hardware Cap described in the table below:

<u>Term</u>	<u>Limit</u>
1-year Term	Customer shall have access to the Attached Subscriptions on an unlimited number of hardware firewalls so long as the new devices are: (a) purchased during the Term; and (b) registered to Customer's account within the Palo Alto Networks support portal.
Term greater than 1 year	Customer shall have access to the Attached Subscriptions on all Current Hardware Estate and utilize up to the Total Hardware Cap (defined below), so long as the new devices are: (a) purchased during the Term; and (b) registered to Customer's account within the Palo Alto Networks support portal. The " Total Hardware Cap " shall mean the Current Hardware Estate plus twenty percent (20%) above a net positive Forecasted Hardware Estate.

4. Re-purchases

Upon the expiration or early renewal of an ELA, as applicable, the Parties shall negotiate a new ELA, taking into account:

- a. Customer's existing deployment of hardware firewalls designated by Customer for use with the Attached Subscriptions under the then-current ELA; and
- b. Customer's projection of its future needs for the new and/or subsequent term.
- c. Any early renewal or recast of the ELA prior to the expiration of the Term ("**Repurchase**") is subject to the then-current ELA terms. If applicable, Customer will be given a pro-rata credit for any prepaid unused Term of the existing ELA in the early Repurchase quote. For clarity, in the event the existing ELA has not been paid in full, then such pro-rated credits will only be given if the remaining payment obligations have been met.

5. Over-consumptions

- a. Customer is responsible for managing the hardware associated with the Attached Subscriptions by monitoring such consumption via the Customer Support Portal using the consumption dashboard. Customer's deployment of the Attached Subscriptions is capped at the Total Hardware Cap. Fees for any over-consumption beyond the Total Hardware Cap must be reconciled with Customer's actual usage at the end of each month, to the extent permitted by applicable law. In the event Customer's deployment of the Attached Subscriptions exceeds the Total Hardware Cap ("**Over-consumption**"), Customer will no longer be able to deploy or increase its usage of the Attached Subscriptions unless Customer exercises one of the following options:
 - i. True-Forward Add-on SKU – Customer may request from Palo Alto Networks or its authorized reseller for a quote to increase its Forecasted Hardware Estate ("**Add-on SKU**") to enable Customer to increase its use of the Attached Subscriptions during the remainder of the Term. Upon placing a non-cancellable, non-refundable purchase order for such Add-on SKU(s), Customer may add the Attached Subscriptions to the additional hardware devices subject to the revised Total Hardware Cap based on the updated Forecasted Hardware Estate.
 - ii. Decommission - Customer may elect to remove a specific list of Palo Alto Networks' hardware devices from its Forecasted Hardware Estate in order to ensure deployment compliance with the Total Hardware Cap. Customer shall remove such devices promptly, but in no event more than sixty (60) days after Over-consumption. Upon Palo Alto Networks' validation that any devices marked as "decommissioned" have actually been decommissioned and removed from Customer's consumption dashboard so that the Customer is within the Total Hardware Cap, Customer may add the Attached Subscriptions to the additional hardware devices.

- iii. **Early Renew** – This subsection (iii) applies to a Term that is a minimum of three (3) years. Upon prior approval by Palo Alto Networks, Customer may request to renew early and recalculate the Forecasted Hardware Estate for a new Term to start at the time of Over-consumption (“**Early Renewal**”). Customer shall have sixty (60) business days to notify Palo Alto Networks, initiate the Early Renewal process and request a quote from Palo Alto Networks or its authorized reseller. For the avoidance of doubt, the then-current ELA terms shall apply for Customer’s Early Renewal.
- b. In the event Customer does not exercise one of the options set forth above, Palo Alto Networks shall have the right but not the obligation to terminate or suspend Customer’s use of such Subscriptions in accordance with the EULA and as permitted by applicable law.

6. End of Life Devices

Palo Alto Networks strongly recommends that Customer decommission hardware devices that have been announced as End of Life (“**EOL**”). In the event Customer elects to continue using any EOL hardware devices, Customer acknowledges that: (i) Customer will be using such hardware at its own risk beyond the date defined in the EOL announcement; and (ii) any EOL hardware devices in Customer’s Current Hardware Estate beyond the EOL date will count towards Customer’s Total Hardware Cap.

7. Add-on Subscriptions

Customer may purchase any of the *IoT Security, Enterprise DLP, SCM, AIops, and SaaS Security subscriptions* (“**Add-on Subscriptions**”) under this ELA and such Add-on Subscriptions shall be governed by the EULA.

When purchased, the pricing structure follows the same terms as provided for in this ELA. Add-on Subscriptions may be deployed on all hardware devices during the Term, subject to the applicable Total Hardware Cap, and subject to any applicable pro-rated credits.

8. Prisma Access and/or FW Flex Credits Purchase

This Section 8 only applies to Terms 3 years or greater. This option is not available for Public Sector customers.

Palo Alto Networks may provide an option to Customer, upon Customer’s request, every 12 months to receive pro-rated credits in accordance with the process set forth below.

- a. **Eligibility and Calculation of Pro-rated Credits.** During the Term, if Customer is not expecting to use the Total Hardware Cap for the remaining Term to its full capacity either due to hardware decommissioning, plans to move to the cloud or due to any other business reasons, then Customer can get eighty percent (80%) of the value of the Attached Subscriptions (including the value of any Add-on Subscriptions) based on the remaining dollars after deducting the dollars needed to maintain the Attached Subscriptions based on the Current Hardware Estate and the Forecasted Hardware Estate projection. Such remaining value can be credited to Customer as pro-rated credits (“**Pro-rated Credits**”) for the remainder of the Term and applied solely towards the purchase of Palo Alto Networks’ Prisma Access Product (only applicable for the mobile users and remote networks SKUs), cloud next generation firewalls (“**Cloud NGFW**”) and firewall flex credits (“**FW Flex**”). For clarity and the avoidance of doubt, only the value of the Attached Subscriptions, including Add-on Subscription, shall be considered to establish the Pro-rated Credit amount and the value of Customer’s hardware estate is expressly excluded. Pro-rated Credits are only available if and at the time that Customer makes a new or extended purchase of either Prisma Access, Cloud NGFW or FW Flex up to or over the amount of the Pro-rated Credits.
- b. **Use of Pro-rated Credits.** Pro-rated Credits may be used solely towards the purchase of Prisma Access, Cloud NGFW and/or FW Flex credits and, upon Customer’s request of such Pro-rated Credits, will be available no earlier than twelve (12) months after the commencement of the Term and Customer may use Pro-rated Credits once every 12 months thereafter. Any Pro-rated Credits granted to Customer under this ELA must be used in full at the time of purchase of Prisma Access, Cloud NGFW

and/or FW Flex credits and can only be applied towards a single transaction during the Term. There shall be no cash or other reimbursement for any Pro-rated Credits.

- c. **How to Request Pro-rated Credits.** In order to receive the benefit of the Pro-rated Credits, the Customer must submit a valid, non-cancellable purchase order for Prisma Access, Cloud NGFW or FW Flex credits to Palo Alto Networks or its authorized reseller. Customer shall be invoiced and responsible for all applicable taxes associated with the purchase of Prisma Access, Cloud NGFW or FW Flex credits, excluding income or property imposed on Palo Alto Networks.
- d. Customer's Attached Subscriptions and Add-on Subscription(s) (if any) usages shall be reduced accordingly for the remainder of the Term once Pro-rated Credits are issued.
- e. In the event the existing ELA has not been paid in full, then the Pro-rated Credits will only be given if the remaining payment obligations have been met.

9. Limitations

- a. This ELA does not apply to:
 - i. any divestiture of assets will not result in any credits or refunds to Customer and this ELA shall not apply to any hardware assets transferred as a result of a divestiture;
 - ii. M-Series and WF-xxx hardware appliances;
 - iii. hardware managed by a third party outside of Customer's account within the Palo Alto Networks support portal;
 - iv. hardware that Customer has designated to be supported by a third party;
 - v. software licenses including, but not limited to, AutoFocus, Cortex, Panorama central management software, Prisma Access, Prisma Cloud, FW-Flex (formerly VM-series);
 - vi. Palo Alto Networks' FedRAMP-authorized subscriptions.
- b. Once a purchase order is accepted by Palo Alto Networks it is non-cancellable and non-refundable and in no event, to the greatest extent allowable by applicable law can this ELA be terminated for convenience.
- c. Note that the purchase of this ELA does not modify any obligation pursuant to the [Palo Alto Networks End-of-Life Policy](#).

10. Compliance with Laws

There may be specific rules and regulations governing the use of software offerings in certain jurisdictions. Both Parties must abide by applicable laws. Customer shall be responsible for all costs resulting from the application of such laws which apply to Customer's use of this Attached Subscriptions including, but not limited to, taxes, fees, penalties, or fines. Palo Alto Networks shall not be liable for such costs.

11. Conflict

This ELA supplements the terms of the EULA between Customer and Palo Alto Networks that governs Customer's use of Palo Alto Networks Products. In the event of a conflict, this ELA shall take precedence, but only with respect to Customer's purchase of this ELA.

Attachment 3



Enterprise Program **(For Hardware Support)**

1. Description

This Enterprise Program (for Hardware Support) supplements the End User Support Agreement (or equivalent agreement) (the “EUSA”) which governs Palo Alto Networks’ provision of maintenance and support services. By purchasing an ESA, Customer agrees that the terms and conditions set forth in the EUSA and those contained in this document shall apply. Capitalized terms used but otherwise not defined herein will have the meaning assigned to them in the EUSA.

Palo Alto Networks has developed an Enterprise Program, a volume pricing arrangement which is valid for a specific period during which organizations may have unlimited access to support and maintenance for hardware firewalls purchased from Palo Alto Networks. The features and benefits associated with an ESA are detailed below. Each customer may select one support option—Platinum, Premium, or USG—but cannot combine them

2. Term

When purchased, the term of this ESA shall be effective for the term duration specified on the quote (“**Term**”). Note that 5 year Term is only available to select customer accounts, whose qualifications will be determined on a case-by-case basis by Palo Alto Networks.

3. Features and Benefits of an ESA

- a. When purchased, the ESA entitles Customer to support and maintenance for its entire estate of Palo Alto Networks hardware firewall products during the Term.
- b. Customers may select either Platinum-level support and maintenance or a Premium-level support and maintenance, but not a combination of both and whichever is purchased will cover all hardware, including M-Series and WF-XXX appliances.
- c. U.S. Government-level support program (“USG”) is available for customers that qualify as U.S. Government entities, but only for Premium-level support. USG is not available at the Platinum level.
- d. At purchase, Customer shall provide Palo Alto Networks with a forecast of any additional hardware firewalls it expects to add to its current hardware estate (“**Current Hardware Estate**”), if any, during the Term (such additional hardware growth forecasted to Customer’s Current Hardware Estate shall be referred to herein as the “**Forecasted Hardware Estate**”). Customer’s support and maintenance is subject to the Total Hardware Cap (defined below) that is based on the “Current Hardware Estate” and “Forecasted Hardware Estate” calculated based on the current hardware list price.
- e. If Customer purchases additional hardware firewalls during the Term, Customer must pay for additional support and maintenance; provided that: (i) in the case of a 1-year term, Palo Alto Networks shall provide Customer with support and maintenance for such additional firewalls at no additional charge; and (ii) in the case of terms greater than 1 year, Palo Alto Networks shall provide Customer support and maintenance subject to the applicable term’s Total Hardware Cap described in the table below:

<u>Term</u>	<u>Limit</u>
1-year Term	Customer shall have support and maintenance on an unlimited number of hardware firewall devices, as long as the new devices are: (a) purchased during the Term; and (b) registered to Customer's account within the Palo Alto Networks support portal.
Term greater than 1 year	Customer shall have support and maintenance on its total Current Hardware Estate and utilize up to the Total Hardware Cap (defined below), so long as the new devices are: (a) purchased during the Term; and (b) registered to Customer's account within the Palo Alto Networks support portal. The " Total Hardware Cap " shall mean the Current Hardware Estate plus twenty percent (20%) above a net positive Forecasted Hardware Estate.

4. Re-purchases

Upon the expiration or early renewal of an ESA, as applicable, the Parties shall negotiate a new ESA taking into account:

- a. Customer's existing deployment of hardware firewalls designated by Customer under the then-current ESA; and
- b. Customer's projection of its future needs for the new and/or subsequent term.
- c. Any early renewal or recast of the ESA prior to the expiration of the Term ("**Repurchase**") is subject to the then-current ESA terms. If applicable, Customer will be given pro-rata credit for any prepaid unused Term of the existing ESA in the early Repurchase quote. For clarity, in the event the existing ESA has not been paid in full, then such pro-rated credits will only be given if the remaining payment obligations have been met.

5. Over-Consumptions

a. Customer is responsible for managing the hardware associated with the support and maintenance by monitoring the consumption via the Customer Support Portal using the consumption dashboard. Customer's support and maintenance is capped at the Total Hardware Cap. Fees for any over-consumption beyond the Total Hardware Cap must be reconciled with Customer's actual usage at the end of each month, to the extent permitted by law. In the event Customer's actual usage exceeds the Total Hardware Cap ("**Over-consumption**"), Customer will no longer be entitled to any additional ESA entitlements during the Term unless Customer exercises one of the following options:

- i. True-Forward Add-on SKU - Customer may request a quote from Palo Alto Networks or its authorized reseller increase the Forecasted Hardware Estate ("**Add-on SKU**") to enable Customer to increase its ESA entitlements during the remainder of the Term. Upon placing a non-cancellable, non-refundable purchase order for such Add-on SKU(s), Customer may add the ESA entitlements to additional hardware devices subject to the revised Total Hardware Cap based upon the updated Forecasted Hardware Estate.
- ii. Decommission - Customer may elect to remove a specific list of Palo Alto Networks' hardware devices from its Forecasted Hardware Estate in order to ensure compliance with the Total Hardware Cap. Customer shall remove such devices promptly, but in no event more than sixty (60) days after Over-consumption. Upon Palo Alto Networks' validation that any devices marked as "decommissioned" have actually been decommissioned and removed from Customer's consumption dashboard so that Customer is within the Total Hardware Cap, Customer may add the ESA entitlements for additional hardware devices.
- iii. Early Renew – This subsection (iii) applies to a Term that is a minimum of three (3) years. Upon prior approval by Palo Alto Networks, Customer may request to renew early and recalculate the

Forecasted Hardware Estate for a new Term to start at the time of Over-consumption (“**Early Renewal**”). Customer shall have sixty (60) business days to notify Palo Alto Networks, initiate the Early Renewal process and request a quote from Palo Alto Networks or its authorized reseller. For the avoidance of doubt, the then-current ESA terms shall apply for Customer’s Early Renewal.

- b. In the event Customer does not exercise one of the options set forth above, Palo Alto Networks shall have the right, but not the obligation, to terminate or suspend Customer’s use of the support and maintenance entitlements under this ESA in accordance with the EULA and as permitted by applicable law.

6. End of Life Devices

Palo Alto Networks strongly recommends that Customer decommission hardware devices that have been announced as End of Life (“**EOL**”). In the event Customer elects to continue using any EOL hardware devices, Customer acknowledges that: (i) Customer will be using hardware at its own risk beyond the date defined in the EOL announcement; and (ii) any EOL hardware devices in Customer’s Current Hardware Estate beyond the EOL date will count towards Customer’s Total Hardware Cap; provided that in no event shall any EOL devices receive support or be counted towards this ESA beyond the timeframe set forth in Palo Alto Networks’ end of life policy, which can be found here: <https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-policy>.

7. IMPORTANT: PALO ALTO NETWORKS 4-HOUR REPLACEMENT SERVICE (aka “4-HR RMA”) IS NOT INCLUDED IN THE ESA PROGRAM BUT CAN BE PURCHASED A LA CARTE (for qualified hardware only). 4-HR RMA is an optional service that Palo Alto Networks makes available to eligible customers with qualified hardware. Qualifications and eligibility depends upon whether the hardware firewall located at the Customer site sits within a specified range of a Palo Alto Networks service location. Eligibility must be determined, and the service sold, on a per-device basis. When covered, Palo Alto Networks will use commercially reasonable efforts to have replacement hardware delivered to Customer within four hours of issuance of an RMA. 4-HR RMA is not included in the ESA program, but if Customers require 4-HR RMA on eligible devices, then customers must purchase and pay for the service separately. For more information, please refer to the RMA process found here: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/support/rma-process-policy.pdf. For clarity and the avoidance of doubt, if the 4-HR RMA is purchased as a separate offering, such offering will not be included under this ESA.

8. Prisma Access and/or FW Flex Credits Purchase

This Section 8 only applies to Terms of 3 years or greater. This option is not available for Public Sector customers.

Palo Alto Networks may provide an option to Customer, upon Customer’s request, every 12 months to receive pro-rated credits in accordance with the process set forth below.

- a. Eligibility and Calculation of Pro-rated Credits. During the Term, if Customer is not expecting to use the Total Hardware Cap for the remaining Term to its full capacity—either due to hardware decommissioning, plans to move to the cloud, or any other business reasons—then Customer can receive hundred percent (**100%**) of the value of the ESA associated with the decommissioned hardware as pro-rated credits (“**Pro-rated Credits**”) for the remainder of the Term. Such Pro-rated Credits may be applied solely towards the purchase of Palo Alto Networks’ Prisma Access Product (only applicable for the mobile users and remote networks SKUs), cloud next generation firewalls (“**Cloud NGFW**”), and firewall flex credits (“**FW Flex**”). For clarity and the avoidance of doubt, only the ESA value shall be considered to establish the Pro-rated Credit amount, and the value of Customer’s hardware firewalls is expressly excluded. Pro-rated Credits are only available if and at the time that Customer makes a new or extended purchase of either Prisma Access, Cloud NGFW,

or FW Flex up to or exceeding the amount of the Pro-rated Credits.

- b. **Use of Pro-rated Credits.** Pro-rated Credits may be used solely towards the purchase of Prisma Access, Cloud NGFW and/or FW Flex and, upon Customer's request of such Pro-rated Credits, will be available no earlier than twelve (12) months after the commencement of the Term and Customer may use Pro-rated Credits once every twelve (12) months thereafter. Any Pro-rated Credits granted to Customer under this ESA must be used in full at time of purchase of Prisma Access, Cloud NGFW and/or FW Flex and can only be applied towards a single transaction during the Term. There shall be no cash or other reimbursement for any Prorated Credits.
- c. **How to Request Pro-rated Credits.** In order to receive the benefit of the Prorated Credits, Customer must submit a valid, non-cancellable purchase order for Prisma Access, Cloud NGFW, or FW Flex to Palo Alto Networks or its authorized reseller. Customer shall be invoiced and responsible for all applicable taxes associated with the purchase of Prisma Access, Cloud NGFW or FW Flex, excluding income or property imposed on Palo Alto Networks.
- d. Customer's ESA coverage shall be reduced accordingly for the remaining Term once Pro-rated Credits are issued.
- e. In the event an existing ESA has not been paid in full, then the Pro-rated Credits will only be given if the remaining payment obligations have been met.

9. Limitations

- a. This ESA does not apply to:
 - i. any divestiture of assets will not result in any credits or refunds to Customer, and the ESA shall not transfer with any hardware assets transferred as a result of a divestiture of assets;
 - ii. hardware managed by a third party outside of Customer's account within the Palo Alto Networks support portal;
 - iii. hardware that Customer has designated to be supported by a third party; except where that third party is a Palo Alto Networks Authorized Support Center partner (ASC) and the customer is utilizing a partner-enabled support.
 - iv. inactive hardware that Customer has intentionally let lapse from support and chosen not to renew; provided that in the event Customer desires to include lapsed hardware under this ESA, additional support cost may apply;
 - v. software licenses and subscriptions including, but not limited to Cortex, Panorama central management software, Prisma, Threat Prevention, Advanced URL Filtering (this subscription replaces PANDB URL Filtering in ELAs), VM-Series, FW-Flex, and WildFire.
- b. Note that the purchase of this ESA does not modify any obligation pursuant to the [Palo Alto Networks End-of-Life Policy](#)
- c. Once a purchase order is accepted by Palo Alto Networks it is non-cancellable and non-refundable and in no event, to the greatest extent allowable by applicable law, can this ESA be terminated for convenience.

10. Compliance with Laws

There may be specific rules and regulations governing the use of hardware support in certain jurisdictions. Both Parties must abide by applicable laws. Customer shall be responsible for all costs resulting from the application of such laws which apply to Customer's use of this ESA including, but not limited to, taxes, fees, penalties, or fines. Palo Alto Networks shall not be liable for such costs.

11. Conflict

This ESA supplements the terms of the EUSA between Customer and Palo Alto Networks that governs Palo Alto Networks' provision of maintenance and support services. In the event of a conflict, this ESA shall take precedence, but only with respect to Customer's purchase of this ESA.

Attachment 4

(/)

Secondary Market Policy

The secondary market policy for previously owned Palo Alto Networks devices provides you with the necessary steps required to ensure that the secondary market device can be supported and used. If you are considering the purchase of previously owned Palo Alto Networks equipment on the secondary market, please review the requirements below prior to the secondary market purchase to determine if it will meet the requirements in this policy. If you have additional questions on the secondary market policy, please contact your local sales representative (/company/contact-sales).

Policy Requirements

Any licenses or subscriptions that come with the device are not transferrable to you and are considered expired by Palo Alto Networks. Palo Alto Networks will have no obligation to provide any support or services under any previous licenses or subscriptions that come with the purchased device.

Before hardware devices that are purchased on the secondary market may be licensed for use, including the activation of support and subscriptions, the following requirements must be met:

- Devices may not be lost or stolen. If the device is determined to be lost or stolen, then it will NOT be re-certified and will be requested to be returned to Palo Alto Networks. Palo Alto Networks may pay for shipment of the device, but will not pay for the device itself.
- Devices that are currently end-of-sale cannot be re-certified. For our current end-of-life policy and listing of products, please see our End-of-Life Announcements (/services/support/end-of-life-announcements).

- Upon receipt of a purchased device on the secondary market, you must place two orders through a Palo Alto Networks authorized local reseller. The first order must be for a non-refundable certification fee and the second for a one time activation fee and the purchase of a one year support subscription (you may purchase a longer support subscription if desired but the purchase it at minimum a one year subscription). The purchase of other subscriptions or services are optional.
- After the two orders have been placed, Palo Alto Networks will send instructions on the verification process that will be used to determine if the device is in good working condition. The verification process will involve verification tests to validate hardware is in good operating condition, the generation and uploading of a technical support file to our support portal, and may require an internet connection to allow a Palo Alto Networks engineer to test the device remotely.
- If the device is determined to NOT be in good working condition, the re-certification fee will not be refunded, and the second order will be cancelled.

Once all of the above steps are met, the remainder of your order will be processed and your Palo Alto Networks device will be ready to use.



Products and Services



Attachment 5

CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and Annexes (“DPA”), forms part of the Agreement (as defined below), by and between Customer and Palo Alto Networks (also referred to herein as a “Party” or collectively as the “Parties”). For the avoidance of doubt, execution of the Agreement shall constitute Customer’s signature and acceptance of this DPA and its Schedules, including Annex 1 to Schedule 1 (Standard Contractual Clauses), where applicable.

This DPA between Customer and Palo Alto Networks contains the legal terms and conditions that apply to the Processing of Personal Data by Security Solutions, where Customer is acting as the Controller of Personal Data and Palo Alto Networks is acting as a Processor of Personal Data. Unless otherwise specified in this DPA, the terms of the Agreement shall continue in full force and effect. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. In the event of any inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail.

1. DEFINITIONS

“**Affiliates**” means, solely for the purposes of this DPA, (i) with respect to Customer, its Affiliates as defined in the Agreement, and (ii) with respect to Palo Alto Networks, entities Controlled by, or under common Control with Palo Alto Networks that Process Personal Data under the direct authority of Palo Alto Networks in order to provide the Security Solutions, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

“**Agreement**” means any underlying Palo Alto Networks End User License Agreement, Master Services Agreement, Engagement Letter, Statements of Work, or other legally entered and binding written, or electronic agreement entered into between Palo Alto Networks and Customer that governs the provision of Security Solutions by Palo Alto Networks to Customer.

“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data

“**Data Protection Laws**” means all mandatory data protection laws that apply to the Processing of Personal Data under this DPA and the Agreement. Such laws may include, but are not limited to, European Data Protection Law, as defined herein, and U.S. Privacy Laws as defined herein, including the California Consumer Privacy Act, as amended (“CCPA”).

“**Data Subject**” means an identified or identifiable natural person to whom Personal Data relates.

“**Personal Data**” means any electronic information submitted by or on behalf of Customer to the Security Solutions(s) that (i) relates to an identified or identifiable natural person; and (ii) is defined as "personally identifiable information", "personal information", "personal data" or similar terms under Data Protection Laws .

“**Privacy Datasheet(s)**” means the applicable document located in Palo Alto Networks Trust Center, that further describes the Processing activities in relation to the Security Solutions provided to Customer under the Agreement.

“**Process**”, “**Processes**”, “**Processing**”, and “**Processed**” means any operation or set of operations performed upon Personal Data, whether or not by automatic means.

“**Processor**” means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

“**Security Incident**” means a breach of security, of which Palo Alto Networks becomes aware, leading to the



accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data in Palo Alto Networks' possession, custody, or control that compromises the security, confidentiality, or integrity of such Personal Data.

"Security Measures" means the technical and organizational measures implemented by Palo Alto Networks designed to secure Personal Data, which are incorporated by reference in Annex II, Schedule 1 of this DPA.

"Security Solution(s)" means, collectively, Palo Alto Networks Products, Support Services, and Unit42 Services purchased by Customer (as such equivalent terms are defined in the applicable Agreement(s) between the Parties), which Process Personal Data.

"Sub-processor" means an entity engaged by Palo Alto Networks to assist in fulfilling its obligations with respect to providing the Security Solution(s) pursuant to the Agreement or this DPA, insofar as such an entity Processes Personal Data on behalf of Palo Alto Networks. For the avoidance of doubt, Palo Alto Networks Affiliates may act as Sub-processors and Process Personal Data on behalf of Palo Alto Networks.

"Trust Center" means the dedicated Palo Alto Networks website that provides customers with comprehensive information, resources and documentation about the company's commitment to data privacy, security, and compliance, found at <https://www.paloaltonetworks.com/legal-notices/trust-center>.

2. PROCESSING OF PERSONAL DATA

2.1 Scope of Processing. Palo Alto Networks will only Process Personal Data in accordance with Customer's written instructions, the applicable Privacy Datasheets, Data Protection Laws, and this DPA. The Parties agree that this DPA, including all applicable Schedules, the applicable Privacy Datasheets, and the Agreement set out the Customer's written instructions to Palo Alto Networks in relation to the Processing of Personal Data by Palo Alto Networks. Palo Alto Networks shall promptly inform Customer if, in its opinion, any Customer instructions infringe Data Protection Laws.

2.2 Customer Obligations. Customer shall (i) comply with all applicable laws, including Data Protection Laws, in respect of its use of the Security Solution(s); (ii) ensure that any instructions provided to Palo Alto Networks are at all times in accordance with Data Protection Laws; (iii) collect all Personal Data and provide all required notices in accordance with Data Protection Laws and obtain all consents and rights necessary for the Processing of Personal Data; (iv) maintain at all times the accuracy, quality, and legality of Personal Data; and (v) provide to Palo Alto Networks the minimum amount of Personal Data necessary for the provision of the Security Solution(s).

2.3 Confidentiality of Processing. Palo Alto Networks shall ensure that any person who is authorized by Palo Alto Networks to Process Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

3. SUB-PROCESSING

3.1 As part of the provision of Security Solution(s), Palo Alto Networks may engage Sub-processors to Process Personal Data on Customer's behalf. Customer hereby grants Palo Alto Networks a general authorization to appoint and use the Sub-processors currently listed on the "List of Sub-processors" which is available in the Trust Center.

3.2 In the event Palo Alto Networks contracts the Processing of Personal Data to a new Sub-processor, Customer will be notified via email in advance of this change, provided Customer has subscribed to receive notifications through the Palo Alto Networks Support Portal, and the List of Sub-processors will be updated in the Trust Center. Customer will have fifteen (15) calendar days from the date of notification to notify Palo Alto Networks of Customer's objections based on reasonable grounds and only in respect to data protection concerns ("Review Period"). In such cases, Palo Alto Networks will then endeavor to offer alternate options for the delivery of the



relevant Security Solution(s) that does not involve the new Sub-processor. The Parties agree that Customer's non-response during the Review Period will be taken as the Customer's approval of such Sub-processor.

3.3 Palo Alto Networks will: (i) enter into a written agreement with all Sub-processors that imposes data protection terms as stringent as those set forth in this DPA; and (ii) remain fully liable for the Sub-processor's compliance with the obligations of this DPA.

3.4 Palo Alto Networks may engage Sub-processors located outside the jurisdiction in which the Personal Data was collected. In such cases, Palo Alto Networks will, where required, implement and maintain an appropriate transfer mechanism to ensure compliance with the Data Protection Laws. This may include, as appropriate, (i) Module 3 of the Standard Contractual Clauses; (ii) an adequacy decision or equivalent issued by the competent regulatory authority; or (iii) or any other mechanism permitted under the Data Protection Laws.

4. COOPERATION

4.1 Government requests for Personal Data. If a law enforcement, national security, or other government agency sends Palo Alto Networks a request (e.g. warrant, court order, or subpoena) to access Personal Data, Palo Alto Networks commits to following the process described [here](#).

4.2 Data Subject requests. In the event of a Personal Data request from a Data Subject related to a Customer is made directly to Palo Alto Networks, Palo Alto Networks shall inform the requestor that Palo Alto Networks is not authorized to directly respond to the request, and recommend the requestor submit the request directly to Customer, unless legally compelled to respond under the law applicable to such a request. Customer shall bear the responsibility for responding to all such requests. In the event Customer requires reasonable support from Palo Alto Networks in responding to a request from a Data Subject, it may contact privacy@paloaltonetworks.com for assistance.

4.3 Data Protection Impact Assessments. Taking into account the nature of the Processing and information available to Palo Alto Networks, Palo Alto Networks shall provide reasonable information regarding the Security Solutions to enable the Customer to carry out data protection impact assessments or similar evaluations and assessments if required by Data Protection Laws.

4.4 Supervisory/Regulatory Authorities. Palo Alto Networks shall provide reasonable assistance to Customer in the cooperation or prior consultations with supervisory authorities or other competent regulatory authorities.

5. SECURITY

5.1 Security Measures. Palo Alto Networks shall implement and maintain the Security Measures.

5.2 Customer Responsibilities. Customer is responsible for secure and appropriate use of the Security Solutions, to ensure a level of security appropriate to the risk in respect of the Personal Data.

5.3 Security Reports. Palo Alto Networks shall make available to Customer, upon written request and without undue delay (subject to appropriate confidentiality obligations), a summary copy of applicable third-party audit report(s) or certifications it maintains for its Security Solutions (e.g. ISO 27001 or SOC2 Type II standard), so that the Customer can verify Palo Alto Networks compliance with this DPA, the audit standards against which it has been assessed, and the standards specified in the Security Measures.

5.4 Security Incidents. Upon confirming that a Security Incident has occurred, without undue delay (no later than seventy-two (72) hours) Palo Alto Networks shall: (i) taking into account the nature of Palo Alto Networks Processing of Personal Data and the information available to Palo Alto Networks, send written notification to the Customer at either the email address listed in Customer's online privacy policy or the email address Customer



designates in the Palo Alto Networks Customer Support Portal; and (ii) promptly take such steps as Palo Alto Networks deems necessary and reasonable to contain, investigate, and mitigate the Security Incident to the extent the remediation is within Palo Alto Networks' reasonable control. Palo Alto Networks shall reasonably cooperate with Customer in any post Security Incident communication efforts. The obligations contained herein shall not apply to Security Incidents that are caused by Customer or Customer's users.

6. DELETION AND RETENTION

On termination or expiration of the Agreement, and upon Customer's written request, in accordance with the retention period set forth in the applicable Privacy Datasheet, Palo Alto Networks shall, without undue delay: (i) return a copy of Personal Data to the Customer by secure file transfer in such format as is reasonably requested by the Customer; or (ii) securely delete existing copies of Personal Data, unless continued retention is required and/or permitted by Data Protection Laws and/or mandatory applicable law. If Palo Alto Networks determines that continued retention is required and/or permitted by Data Protection Laws and/or mandatory applicable law, Palo Alto Networks shall ensure the confidentiality of such Personal Data and shall extend the protections of this DPA to such Personal Data.

7. LIMITATION OF LIABILITY

The liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement and shall not be modified by this DPA. Any claims brought by a party or its Affiliates under this DPA, whether in contract, tort or under any other theory of liability, shall be subject to the exclusions and limitations set forth in the Agreement, as permitted by applicable law and any claim under this DPA will be aggregated with any claims under the Agreement.

8. JURISDICTION-SPECIFIC SCHEDULES

Attached to this DPA are Schedules that provide terms specific to the Processing of Personal Data arising out of specific legal requirements from particular jurisdictions, which shall apply to the extent Personal Data is Processed in one or more of these jurisdictions. In the event of a conflict or inconsistency between this DPA and a Schedule, the Schedule applicable to Personal Data from the relevant jurisdiction shall prevail with respect to Personal Data from that relevant jurisdiction, but solely with regard to the portion of the provision in conflict or inconsistency. To the extent the Agreement or this DPA contemplates Personal Data transfers from a jurisdiction not included in this DPA, the Parties agree to comply with the relevant jurisdiction's legal requirements.

9. UPDATES TO DPA

In the event of changes to Data Protection Laws, including, but not limited to, the amendment, revision, or introduction of new laws, regulations, or other legally binding requirements to which either party is subject, the Parties agree to revisit the terms of this DPA, and negotiate any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any Schedules.



SCHEDULE 1

EUROPEAN ECONOMIC AREA

1. DEFINITIONS

1.1 **"EEA"** means the European Economic Area.

1.2 **"European Data Protection Law"** means the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" or "GDPR"), as implemented by countries within the EEA and/or other laws that are similar, equivalent to, or successors to the GDPR.

1.3 **"Standard Contractual Clauses"** means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.4 For the purpose of this Schedule 1, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable European Data Protection Law and all references to Data Protection Law or laws in the DPA shall be read in the context of EU or Member State Law.

2. TRANSFERS OUTSIDE OF THE EEA

2.1 Module 2 (Controller to Processor) of the Standard Contractual Clauses. To the extent that Customer, as a Controller, transfers any Personal Data from the EEA for Processing directly to any Palo Alto Networks entity or Affiliate in a third country not deemed by the European Commission to provide an adequate level of data protection, Module 2 (Controller to Processor) of the Standard Contractual Clauses will apply with respect to such transfers.

2.2 Module 3 (Processor to Processor) of the Standard Contractual Clauses. To the extent Palo Alto Networks transfers Personal Data from the EEA for Processing to any Sub-processor in a third country not deemed by the European Commission to provide an adequate level of data protection, Palo Alto Networks shall ensure such transfer is supported by a valid transfer mechanism, which may include use of the Module Three (Processor-to-Processor) of the Standard Contractual Clauses.

2.3 Where available, Palo Alto Networks will rely on existing adequacy decisions approved by the European Commission. In the event such adequacy decision is not available, or in the event of any change in Data Protection Laws or binding legal decision by the relevant judicial or competent authority renders an existing adequacy decision invalid or insufficient to support the transfer of Personal Data outside the of the EEA, Palo Alto Networks will rely on Standard Contractual Clauses as the legally valid data transfer mechanism. To the extent the execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. STANDARD CONTRACTUAL CLAUSES

3.1 To the extent applicable under Clause 2.1 of this Schedule 1, Module Two (Controller to Processor) of the Standard Contractual Clauses is incorporated by reference into this Schedule 1. For clarity, Annexes I and II of the Standard Contractual Clauses are attached to this Schedule 1. Signatures applied to the Agreement will be taken as equally signing and effectuating the Standard Contractual Clauses.

3.2 In respect to Clause 7 *Docking clause*, the option shall not apply.



3.3 In respect to Clause 9(a) *Sub-processors*, option 2 is selected and Customer grants a General Written Authorization for the use of Sub-processors listed [here](#). All other provisions contained in Clause 3 of this Schedule 1 shall apply.

3.4 In respect to Clause 11 *Redress*, the option shall not apply.

3.5 In respect to Clause 17 *Governing Law*, option 1 is selected and the governing law is that of The Netherlands.

3.6 In respect to Clause 18 *Choice of forum and jurisdiction*, the courts of The Netherlands shall resolve any disputes arising from the Standard Contractual Clauses.



ANNEX I TO SCHEDULE 1

A. List of Parties

Data exporter: The data exporter is the entity identified as the Customer in the Agreement, acting as a data exporter on behalf of itself and its Affiliates.

Data importer: The data importer is Palo Alto Networks.

B. Description of Transfer

1. *Categories of Data Subjects whose personal data is transferred*: The Personal Data transferred may relate to the following categories of Data Subjects: Employees, contractors, consultants, individuals belonging to Customer, Customer's clients', and partners' workforce and/or other individuals whose Personal Data is Processed as part of the provision of the Security Solutions .

2. *Categories of personal data transferred*: The Personal Data transferred may relate to the following categories of Personal Data: a) Identification and contact data (e.g., name, address, phone number, title, email, other contact details); b) Employment details (e.g., job title, role, manager); c) IT information (e.g., entitlements, IP addresses, usage data, cookies data, online identifiers); d) Domain and device information (e.g., MAC address, hostnames, International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), and qualified hostnames); e) Information contained in logs related to security events identified and captured by Security Solution(s); and/or f) Unstructured data provided to Palo Alto Networks for the purpose of providing services (e.g., packet capture (PCAP) for file testing).

For the specific categories of Personal Data Processed on a Security Solution per Security Solution basis, refer to the applicable Privacy Datasheets available at the Trust Center.

3. *Sensitive data transferred (if applicable)*: When Processing Personal Data, primarily with forensic investigations Security Solution(s) of which the purpose is to identify the underlying data, Palo Alto Networks may process sensitive Personal Data. The nature and scope of the sensitive personal data that is transferred may not be known until after the Processing has taken place and may include: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. *The frequency of the transfer (e.g., Whether the data is transferred on a one-off or continuous basis)*: The transfer of Personal Data between the Parties will occur on a continuous basis.

5. *Nature of the Processing*: Personal Data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analyzing, collecting, transferring, and making available Personal Data. Additional details regarding Palo Alto Networks' Processing activities are reflected in the applicable Privacy Datasheets, available at the Trust Center.

6. *Purpose*: The purpose of the Processing of Personal Data under this DPA is to enable Palo Alto Networks to deliver the Security Solution(s) (s) and perform its obligations as set forth in the Agreement (including this DPA) or as otherwise agreed by the Parties in mutually executed written form. For specific details on Palo Alto Networks purposes for Processing Personal Data under a specific Security Solution(s) , please refer to the applicable Privacy Datasheets available at the Trust Center.

7. *The period for which the personal data will be retained, or if that's not possible, the criteria used to determine that period*: Palo Alto Networks will retain Personal Data to fulfill the purposes for which it was collected and as necessary to comply with business requirements, legal obligations, resolve disputes, and enforce its rights. Specific data retention periods are listed for certain Security Solution(s) in the applicable Privacy Datasheets available at the Trust Center.



8. *For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:* Personal Data will be transferred to Palo Alto Networks Sub-processors as described in the applicable Privacy Datasheet available at the Trust Center.

C. Competent Supervisory Authority

Competent supervisory authority/ies to be chosen in accordance with Clause 13.



ANNEX II TO SCHEDULE 1

Description of the technical and organizational measures implemented by the data importer(s)

Palo Alto Networks Security Measures can be found at:

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/information-security-measures.pdf



SCHEDULE 2

UNITED KINGDOM

1. DEFINITIONS

1.1 **"Mandatory Clauses"** means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s199A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

1.2 **"Standard Contractual Clauses"** means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.3 **"UK"** means the United Kingdom.

1.4 **"UK Data Protection Law"** means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including: (i) the UK GDPR and UK Data Protection Act 2018; and/or (ii) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i) above.

1.5 **"UK GDPR"** as defined in Section 3 of the Data Protection Act 2018.

1.6 For the purposes of this Schedule 2, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable UK Data Protection Law and all references to Data Protection Law or laws in the DPA shall be read in the context of UK Law.

2. TRANSFERS OUTSIDE OF THE UK

2.1 To the extent that Customer transfers any Personal Data from the UK for Processing directly to any Palo Alto Networks entity or Affiliate in countries not deemed to provide an adequate level of data protection under UK Data Protection Law, the Parties agree to enter into and comply with Module 2 of the Standard Contractual Clauses (as amended by the Mandatory Clauses) and having selected the options identified in Clauses 3.2 - 3.6 of Schedule 1 above. Palo Alto Networks agrees that it is a "data importer" and Customer is the "data exporter" under the Standard Contractual (as amended by the Mandatory Clauses).

2.2 In the event of any change in UK Data Protection Law or binding legal decision by the relevant judicial authority that renders the data transfer mechanism described in Clause 2.1 of this Schedule 2 invalid or insufficient to support the transfer of Personal Data, and to the extent that Palo Alto Networks adopts an available alternative data transfer solution for the lawful transfer of Personal Data outside of the UK (as recognized under UK Data Protection Law) such as the UK Extension to the EU-U.S. Data Privacy Framework, the Parties agree that such transfer will be made in reliance on such alternative data transfer solution. To the extent the execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. MANDATORY CLAUSES

3.1 To the extent applicable under Clause 2.1 of this Schedule 2, Module Two (Controller to Processor) of the Standard Contractual Clauses and the Mandatory Clauses are incorporated by reference into this Schedule 2, and the Standard Contractual Clauses are amended in accordance with the Mandatory Clauses. For clarity, Annexes I and II of the Standard Contractual Clauses included in Schedule 1 are incorporated by reference to this Schedule 2. Signatures applied to the Agreement will be taken as equally signing and effectuating the Approved Addendum,



including the Mandatory Clauses.

3.2 Neither the Mandatory Clauses or this Schedule 1 shall be interpreted in a way that conflicts with rights and obligations provided for under UK Data Protection Law.

3.3 Data importer may end this DPA (including this Schedule 2) to the extent the Mandatory Clauses apply, in accordance with Clause 19 of the Mandatory Clauses.



SCHEDULE 3

SWITZERLAND

1. DEFINITIONS

- 1.1 “**FDIP**” means the Federal Data Protection and Information Commissioner.
- 1.2 “**GDPR**” or “**General Data Protection Regulation**” means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- 1.3 “**Swiss FADP**” means the Swiss Federal Act of 19 June 1992 on Data Protection, the Ordinance to the Swiss Federal Act on Data Protection and the revised Swiss Federal Act of 25 September 2020 on Data Protection which comes into force in 2023.
- 1.4. For the purpose of this Schedule 3, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable Swiss FADP and all references to Data Protection Law or laws in the DPA shall be read in the context of the Swiss FADP.

2. TRANSFERS OUTSIDE OF SWITZERLAND

- 2.1 To the extent that Customer transfers any Personal Data from Switzerland for Processing directly to any Palo Alto Networks entity or Affiliate in a third country not deemed to provide an adequate level of data protection under the Swiss FADP, Module 2 (Controller to Processor) of the Standard Contractual Clauses will apply with respect to such transfers.
- 2.2 In the event of any change in the Swiss FADP or binding legal decision by the relevant judicial authority that renders the data transfer solution identified in Clause 2.1 of this Schedule 3 invalid or insufficient to support the transfer of Personal Data, and to the extent that Palo Alto Networks adopts an available alternative data export solution for the lawful transfer of Personal Data outside of Switzerland (as recognized under the Swiss FADP) such as the Swiss-U.S. Data Privacy Framework, the Parties agree that such transfer will be made in reliance on such alternative data transfer solution. To the extent the execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. STANDARD CONTRACTUAL CLAUSES

- 3.1. To the extent applicable under Clause 2.1 of this Schedule 3, Module Two (Controller to Processor) of the Standard Contractual Clauses is incorporated by reference into this Schedule 3. Annexes I and II, as set forth in Schedule 1, shall form the Annexes to the Standard Contractual Clauses incorporated in this Schedule 3. Signatures applied to the Agreement will be taken as equally signing and effectuating the Standard Contractual Clauses.
- 3.2 References to General Data Protection Regulation and/ or GDPR shall be deemed to refer to the Swiss FADP.
- 3.3 All references to the competent supervisory authority shall be deemed to refer to the Federal Data Protection and Information Commissioner (“**FDPIC**”).
- 3.4 References to the “European Union”, “Union”, “EU”, and “Member State(s)/EU Member State(s)” shall be deemed to include Switzerland and references to the exporter in the EU shall be deemed to include the exporter in Switzerland.
- 3.5 Where the Standard Contractual Clauses use terms that are defined in the GDPR, those terms shall be deemed to have the meaning as the equivalent terms are defined in the Swiss FADP.
- 3.6 In respect to Clause 17 *Governing law*, the applicable law shall be Swiss law.



3.7 In respect to Clause 18 *Choice of forum and jurisdiction*, the Swiss courts shall resolve any disputes arising from the Standard Contractual Clauses.



SCHEDULE 4

U.S. PRIVACY LAWS

1. DEFINITIONS

1.1 **“U.S. Privacy Laws”** means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the U.S., including the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations.

1.2 **“Business”** or **“business”** means Customer, a for-profit legal entity that collects consumers' personal information (or has another entity collect consumers' personal information on its behalf) and determines the purposes and means of the Processing of Personal Data

1.3 For the purpose of this Schedule 4, all terms used herein not defined in this Schedule 4 will have the meaning assigned to them in the U.S. Privacy Laws, its implementing regulations or the Agreement and all references to Data Protection Law or laws in the DPA shall be read in the context of U.S. Privacy Laws.

2. COMMITMENTS UNDER U.S. PRIVACY LAWS

2.1 Palo Alto Networks agrees that:

2.1.1 It is acting solely as a “Service Provider” or “Processor” as defined under the U.S. Privacy Laws;

2.1.2 It will comply with, and provide at least the same level of privacy protection as is required under the U.S. Privacy Laws;

2.1.3 It will notify the business promptly after making the relevant determination if it determines that it can no longer meet its obligations under the U.S. Privacy Laws;

2.1.4 Customer will have the right to take reasonable and appropriate steps to (i) ensure that Palo Alto Networks uses Personal Data in a manner consistent with Customer’s obligations under the U.S. Privacy Laws; and (ii) upon reasonable notice, stop and remediate the unauthorized Processing of Personal Data by Palo Alto Networks.

2.1.5 To the extent Palo Alto Networks receives Personal Data in deidentified form from the Customer or deidentifies Personal Data received from Customer such that it cannot reasonably be linked to such Personal Data, directly or indirectly (“Deidentified Data”), Palo Alto Networks will (1) take reasonable measures to ensure that the Deidentified Data cannot be associated with a consumer or household; (2) publicly commit to maintain and use the Deidentified Data in a de-identified form and not attempt to re-identify the information (except that Palo Alto Networks may attempt to re-identify the data solely for the purpose of determining whether its deidentification processes are compliant with U.S. Privacy Laws); and (3) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and US Privacy Laws.

2.1.6 For the avoidance of doubt, Palo Alto Networks is permitted to deidentify Personal Data through a reliable state of the art anonymization procedure and use such Deidentified Data for its own business purposes, including without limitation for security and fraud detection and research and development of new products and services, provided such Deidentified Data cannot reasonably be linked to the Personal Data, directly or indirectly.

2.2 Except as otherwise permitted by the U.S. Privacy Laws, this DPA or the Agreement, Palo Alto Networks shall not:



2.2.1 retain, use or disclose Personal Data outside of its direct business relationship with Customer or retain, use or disclose Personal Data for any purposes other than the business purposes specified in this DPA or the Agreement;

2.2.2 combine Personal Data of consumers that Palo Alto Networks receives from, or on behalf of, Customer with Personal Data that Palo Alto Networks receives from, or on behalf of, another person or persons or collects from its own interaction with consumers for cross-context behavioral advertising; and

2.2.3 sell or share Personal Data, as those terms are defined by the U.S. Privacy Laws.

ATTACHMENT 6

(//)

Palo Alto Networks Grace Periods

Summary

This document defines Palo Alto Networks® *grace periods* for activation and entitlement of warranties, support contracts, and subscriptions. Grace periods exist to avoid penalizing our customers during the time it takes for hardware to ship, to clear customs if applicable, and to be received and processed at the destination. Grace periods do not apply to support contract renewals; support renewals always start at the end of the previous support contract regardless of any gap between the expiration date of the previous contract and the date on which the customer renews the support contract.

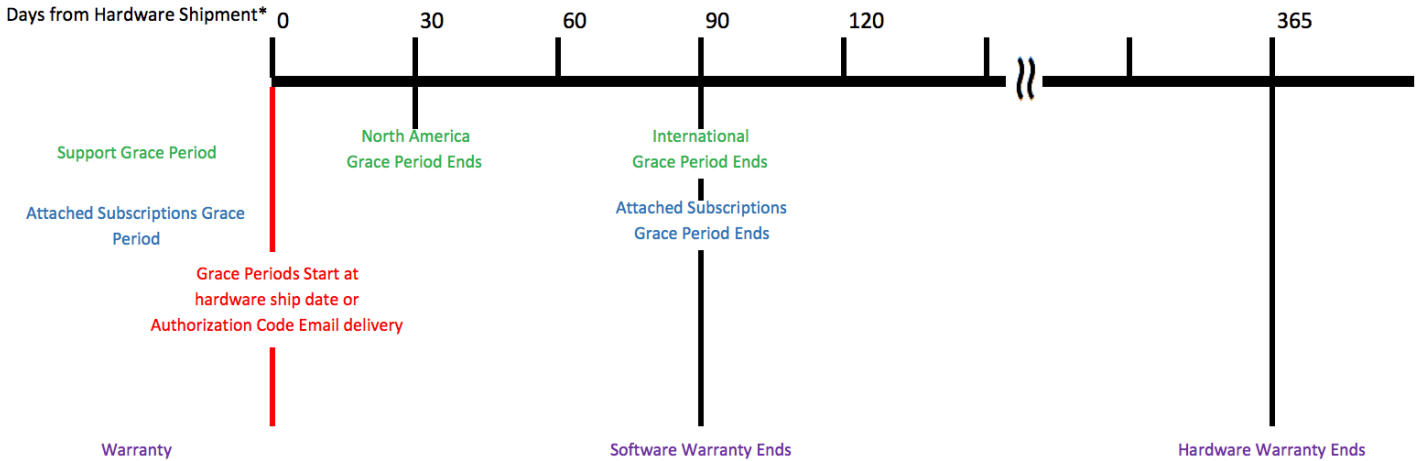
The policy defined in this document applies to all sales except *stocking order* sales to Palo Alto Networks authorized channels, for which the grace period begins on the day the distributor sells the product to a reseller as documented in the distributor's point-of-sale (POS) reports. Additionally, products sold as part of a stocking order cannot receive warranty or support service and cannot have any subscriptions attached to them until the distributor provides the necessary POS data to Palo Alto Networks.

When an applicable grace period expires, Palo Alto Networks reserves the right to register the product (hardware or software) as well as activate support and any purchased attached subscriptions on behalf of the product owner without notification.

For the purposes of this policy, *attached subscriptions* are subscriptions attached to a Palo Alto Networks hardware or software appliance and include GlobalProtect™ network security for endpoints, WildFire® cloud-based threat analysis service, Threat Prevention, and URL Filtering. Term-based license offerings are not considered to be attached subscriptions.



Policy Requirements:



* Shipment from Palo Alto Networks or a Palo Alto Networks authorized dealer.

Summary of the grace period policy, where North America covers the U.S. and Canada.

Grace Periods for Prisma SD-WAN Subscriptions ends after 30 days.

Overview

- Support contracts start either (i) at the time hardware is registered or (ii) 30 days after hardware is shipped when shipped to North America and 90 days after hardware is shipped when it is shipped outside North America, whichever is earlier.
Japan only: support contracts start either (i) at the time the authorization code is activated or (ii) 90 days after hardware is shipped, whichever is earlier.
- Attached subscriptions start when subscriptions are activated or 90 days after the delivery of the authorization code, whichever is earlier. Grace Periods for Prisma SD-WAN Subscriptions is 30 days.
- Lab subscription and support bundles for end users as well as not-for-resale (NFR) subscription and support bundles for partners follow the support policy defined herein, which means support contracts and applicable attached subscriptions start on the same day.

Warranty

The warranty start date for hardware is the same as the ship date. For software, the warranty start date is the same as the email delivery date of the authorization code. For additional information, refer to the Palo Alto Networks Product Warranty document located at <https://www.paloaltonetworks.com/services/support/product-warranty> (/services/support/product-warranty).

Support Contracts

The support contract start date is determined by the timing of the applicable hardware or software shipment but we provide a grace period—30 days in North America and 90 days outside North

America—to allow for in-transit shipment time and end-user setup time. Support is similar to *insurance* in that, when active, it is in place to help if something goes wrong and, thus, it is important that support contracts start on the hardware or software shipment date. For details about support options, refer to the Global Customer Support Services Terms and Conditions at https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/support/global-customer-support-services-terms-conditions.pdf (/content/dam/pan/en_US/assets/pdf/datasheets/support/global-customer-support-services-terms-conditions.pdf).

Important: The grace period for support contracts is based on the hardware ship date, not the delivery date of the support authorization code. For example, if a hardware appliance was shipped on January 1, 2011, and a support contract was purchased and applied to this appliance on May 1, 2011, the start date for support would be January 31, 2011 (30 days after the ship date). The start date would be earlier if the appliance was activated prior to January 31, 2011.

Attached Subscriptions

Attached subscriptions start either (i) at the time they are activated or (ii) 90 days after delivery of the authorization code, whichever is earlier, and they expire at the end of their subscription term even if you never activate the subscription. For example, a one-year attached subscription purchased on January 1, 2012, but never activated would still expire on March 31, 2013 (at the end of the 90-day grace period plus one year).

Additionally, attached subscription grace periods are determined by the delivery date of the authorization code(s)—not by the hardware ship date—and are 90 days long because attached subscriptions are product services that provide functionality only after they are activated. For example, if an appliance was shipped on January 1, 2018, and a Threat Prevention subscription was purchased on May 1, 2018, and activated on June 15, 2018, then the start date for the attached Threat Prevention subscription would be June 15, 2018 (because it is within the 90-day grace period that started on May 1, 2018, for the attached subscription). Grace Periods for Prisma SD-WAN Subscriptions is 30 days.

Bundles—Excluding VM-Series Firewall

The support contract start date for support and subscription bundles, including lab and NFR bundles, follows the support contracts grace period model defined above, which means that support starts either (i) at the time the hardware or software appliance is registered or (ii) either 30 days after the hardware or software appliances is shipped within North America or 90 days after the hardware or software appliance is shipped outside North America, whichever is earlier.

Term-Based Licensed Offerings

Term-based licensed offerings (such as Endpoint Protection, AutoFocus™, Strata Logging Service (formerly known as Cortex Data Lake), Prisma Access, and Prisma SaaS) do not have grace periods. Terms for term-based licenses start on the email delivery date of authorization codes.

VM-Series Firewall Perpetual Bundles

All VM-Series firewall perpetual bundles do not have a grace period: support contracts and applicable attached subscriptions start on the email delivery date of authorization codes. This policy applies to VM-50, VM-100, VM-300, VM-1000-HV, VM-500, and VM-700 firewall perpetual bundles. Each bundle includes a VM-Series firewall perpetual capacity license, support contract, and zero or more attached subscriptions. All renewals of VM-Series firewall bundles start at the end of the previous bundle term regardless of any gap between the end of that previous term and the date that the bundle is renewed.

VM/CN-Series Software Credits

All Software NGFW Credits do not have a grace period: Credits Pools start on the email delivery date of activation Link.

All renewals of Software NGFW Credits start at the end of the previous term regardless of any gap between the end of that previous term and the date that the Credit Pool is renewed.

Enterprise Agreements

Enterprise Agreements do not have a grace period. Enterprise Agreements start (i) on the email delivery date of authorization codes or (ii) on the start date requested by the customer, whichever is later.

**paloalto®**
NETWORKS

Support Policies

RMA PROCESS and POLICY

RMA (Return Merchandise Authorization) Process

Palo Alto Networks provides warranty repair and return services, as well as advanced replacement services as described in more specificity below. Please follow the steps below to request an RMA service.

1. Open a technical support case by visiting <https://support.paloaltonetworks.com> or [contact TAC by phone](#). You must obtain a valid RMA number before returning any failed device to Palo Alto Networks.
2. A technical support engineer will assist you to troubleshoot the device and verify if an RMA is required.
3. Should a replacement device be required, the technical support engineer will initiate the RMA process by obtaining the following information from you:
 - Company name
 - Shipping address
 - Contact name
 - Contact phone number
 - Contact email address
 - Problem description
 - Product model number
 - Product serial number
4. Palo Alto Networks will notify you via email upon shipment of the replacement device and will also provide you with instructions on how to return the failed device.
5. Palo Alto Networks may contact you at varying intervals until the failed device is returned to a local or regional Palo Alto Networks service location. If you have any questions regarding the return of a device, please contact rmareturns@paloaltonetworks.com.
6. European Union RMAs: All defective parts or failed devices must be returned to Palo Alto Networks according to the return instructions that are included with the replacement part or device. These return instructions will help you comply with the Waste Electrical and Electronic Equipment (WEEE) directive. If you have any questions regarding the return of a device, please contact rmareturns@paloaltonetworks.com.

Software and Hardware Warranty

All Palo Alto Networks products are covered by a 90-day software and 12-month hardware warranty.

STANDARD SUPPORT PLAN: Repair and Return Service

You must obtain a valid RMA number before returning a failed device (refer to the RMA Process above). You are responsible for all shipping costs incurred to return the failed device to Palo Alto Networks, including duties and taxes, where applicable. Palo Alto Networks will pay all shipping costs related to shipping replacement devices to you, except for duties or taxes required to clear customs. Within 10 days of receipt of the failed device, Palo Alto Networks will, at its discretion, repair or replace the failed device with a new or like-new device. However, if repair or replace is not feasible, an upgraded device will be provided. It is



your responsibility to ensure that the failed device is packaged in a manner that will withstand the rigors of return shipment to one of Palo Alto Networks' designated repair facilities.

PREMIUM OR PLATINUM SUPPORT PLAN: Advanced Replacement Service - Next Business Day Service

Once the Technical Assistance Center confirms the validity of the hardware defect, an RMA will be created. If you have purchased Premium or Platinum Support for your device, Palo Alto Networks will ship a new or like-new replacement device. However, if providing you with a new or like-new replacement is not feasible at the discretion of Palo Alto Networks, an upgraded device will be provided, subject to the RMA Shipping Cut-off Times listed below. Palo Alto Networks will use commercially reasonable efforts to attempt to deliver the replacement device by the following business day.

Requests received after the RMA Shipping Cut-off Times listed below will ship the following business day. Shipments will be made Monday through Friday during normal business hours. You are responsible for returning the failed device to Palo Alto Networks within 10 business days of receipt of the replacement device. While you may retain and destroy: (a) any failed Hard Disk Drives (HDD) that are externally separable from the failed device, and (b) appliances or chassis blades with non-removable HDDs, you must return the remaining component(s) to Palo Alto Networks within 10 business days of receipt of the replacement device.

OPTIONAL ADD-ON TO PREMIUM & PLATINUM PLANS:

4 Hour Replacement - Same Day Service

If you have purchased 4-Hour Premium Support or 4-Hour Platinum Support for your device, Palo Alto Networks will use commercially reasonable efforts to aim to deliver, at its discretion, a new or like-new replacement. However, if providing you with a new or like-new replacement is not feasible at the discretion of Palo Alto Networks, an upgraded device will be provided to you the same day within 4 hours from RMA order submittal and approval. Once the Technical Assistance Center confirms the validity of the hardware defect, an RMA will be created and submitted for shipment. This hardware delivery service is available 24/7/365. You must have an authorized representative available to accept delivery of the replacement device. You are responsible for returning the failed device to Palo Alto Networks within 10 business days of receipt of the replacement device. While you may retain and destroy: (a) any failed Hard Disk Drives (HDD) that are externally separable from the failed device, and (b) appliances or chassis blades with non-removable HDDs, you must return the remaining component(s) to Palo Alto Networks within 10 business days of receipt of the replacement device.

IMPORTANT: You are responsible for promptly notifying Palo Alto Networks if or when a device is physically moved from one location to another, in order for Palo Alto Networks to determine if the new device location remains within the range of at least one of our 4-hour servicing depots. If you move the device to a new location without informing Palo Alto Networks, then Palo Alto Networks cannot be held responsible for meeting the 4-Hour service commitment. Instead, Palo Alto Networks will use commercially reasonable efforts to deliver replacement devices promptly. Please notify Order Fulfillment at [of-
orders@paloaltonetworks.com](mailto:orders@paloaltonetworks.com) when moving a device from one location to another.



**United States Government (USG) Next Business Day or 4 Hour Premium Service*
(Limited to Federal US customers only)**

If you have purchased USG Next Business Day or 4-Hour Premium Service for your device, Palo Alto Networks will aim to deliver, at its discretion, a new or like-new replacement; however, if not feasible at the discretion of Palo Alto Networks, an upgraded device will be provided to you either the same day or next business day, depending on the level of service purchased. Once the Technical Assistance Center confirms the validity of the hardware defect, an RMA will be created to facilitate shipment of the replacement unit. While you may retain and destroy: (a) any failed Hard Disk Drives (HDD) that are externally separable from the failed device, and (b) appliances or chassis blades with non-removable HDDs, you must return the remaining component(s) to Palo Alto Networks within 10 business days of receipt of the replacement device. To the extent you retain a failed device, you must send to Palo Alto Networks a signed Certificate of Decommission for that device.

Dead on Arrival (DOA)

Hardware will be considered DOA if it fails: (a) within 30 days from the shipment date to destinations within the United States, or (b) 45 days from the shipment date to destinations outside the U.S. If newly purchased hardware is deemed DOA by the Technical Assistance Center, a **NEW** replacement device will be sent from one of our regional distribution centers. For quicker service, you have the option to accept a like-new replacement device from a local depot, provided one is available in that country. All efforts will be made to ship the replacement device by the following business day, provided the request is made prior to the RMA Shipping Cut-off Times listed below. Please allow for customs clearance delays for locations outside the United States. You are responsible for returning the failed device to Palo Alto Networks within 10 business days of receipt of the replacement device.

Your Data Removal Obligations for RMA Returns

You acknowledge and agree that it is your responsibility to remove any and all data from devices prior to shipment to Palo Alto Networks. Palo Alto Networks will not be responsible for the security, safeguarding or return of any data left on devices that have been shipped to Palo Alto Networks.

RMA Shipping Cut-off Times

Americas	Mon to Fri, 15:00 Pacific Time Zone
EMEA	Mon to Fri, 15:00 Local Depot Time ¹
Asia Pacific	Mon to Fri, 15:00 Local Depot Time ¹
Japan	Mon to Fri, 15:00 Local Depot Time ¹
¹ Palo Alto Networks maintains regional depots around the world. Thus, you will benefit from being serviced by the depot closest in proximity to you.	

RMA Return Instructions

When returning devices to Palo Alto Networks, follow the return instructions provided with the RMA replacement shipment. Palo Alto Networks devices must be returned within 10 business days from the date of receipt of the replacement device. You agree to receive follow-up phone calls and/or emails from Palo Alto Networks to remind you and ensure that the failed device is returned. Devices returned to Palo Alto Networks must abide by the return instructions to ensure proper credit for the return of the failed device and to close out



the RMA. Palo Alto Networks may charge you the list price as stated in the most current Palo Alto Networks price list if you do not return the failed device. For any questions regarding a RMA return, please contact rmareturns@paloaltonetworks.com.

Registering Replacement Units (Licensing)

Please follow these RMA licensing procedures to properly register your replacement unit: [How to Transfer Licenses to a Spare Device](#). If you have any questions regarding this licensing procedure, please contact your support provider (i.e., Palo Alto Networks Support or your designated Authorized Support Center).

Your Operating System (OS) Environment

Field Replacement Units (FRUs) in depots are stocked with pre-defined OS versions, which may not coincide with the OS version that you are running. For this reason, you may need to downgrade or upgrade the replacement device upon receipt. For further assistance, contact your support provider (i.e., Palo Alto Networks Support or your designated Authorized Support Center).

RMA Shipping Cost Responsibilities

Support Plan	RMA Type	Who Pays Shipping Costs Incurred for Returning Failed Devices to Palo Alto Networks	Who Pays Shipping Costs Incurred for Shipping Replacement Devices to You
Standard Support: Return and Repair Service	You return a failed device to Palo Alto Networks. Unit is repaired or replaced with new, like-new, or upgraded device.	You	Palo Alto Networks
Premium or Platinum Support: Next Business Day	New, like-new, or upgraded device	Palo Alto Networks	Palo Alto Networks
4 Hour Premium or Platinum Support: 4 Hour Replacement	New, like-new unit, or upgraded device	Palo Alto Networks	Palo Alto Networks
DOA	New	Palo Alto Networks	Palo Alto Networks

Requesting Status on Existing RMA's

For any questions regarding the status of your RMA, please contact your regional support center or navigate to <https://support.paloaltonetworks.com> and log into your case to view updated RMA information.

*** IMPORTANT:** Next Business Day Service and 4 Hour Service are subject to certain limitations outside of the control of Palo Alto Networks. Palo Alto Networks is not responsible for delivery delays due to the customs clearance process where shipment requires the crossing of international borders, supply chain constraints, unavailability of transportation carrier, natural disaster, act of God, war, labor strike or other similar causes beyond our reasonable control.



CYBERSECURITY
PARTNER OF CHOICE

Palo Alto Networks Global Customer Services Support Resource Guide

Contact Information

Corporate Headquarters:

3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal: www.paloaltonetworks.com/documentation.
- To search for a specific topic, go to our search page: www.paloaltonetworks.com/documentation/document-search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

© 2025 Palo Alto Networks, Inc. Palo Alto Networks and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

March 2025

Table of Contents

Contact Information	2	4.8 Report a Beta Release Issue.....	10
About the Documentation	2	4.9 Request a Feature Enhancement	11
1. Overview of Support Resources	4	4.10 Reopen a Closed Case.....	11
1.1 Self-Service Tools.....	4	5. Return Materials Authorization	
1.2 Technical Support	4	(RMA) Workflow	11
1.3 Customer Service	5	5.1 Request an RMA.....	11
1.4 Hardware Services.....	5	5.2 RMA Delivery Times	11
2. Support Plan	5	5.3 RMA License Transfers	12
2.1 Service Deliverables	5	5.4 Returning the Defective Device	12
3. Technical Case Workflow	6	5.5 Failure Analysis Reports	13
3.1 How to Open a Case.....	6	6. Security Vulnerability Workflow	13
3.2 Case Owner Responsibilities	7	6.1 Definition of a Security Vulnerability.....	13
3.3 Customer Support Summary.....	7	6.2 How to Report a Security Vulnerability	13
3.4 Case Resolution Process	7	6.3 Acknowledgment and Analysis of a	
3.5 Customer Best Practices for Engaging Support... 8		Vulnerability Report	13
3.6 Software Defect Case Resolution Process	8	6.4 Fix or Corrective Action.....	13
3.7 Case Closure Policy	8	6.5 Notification of Product Security Information	
4. Access Support Resources	9	and Software Updates.....	14
4.1 Customer Support Portal Login	9	6.6 Publication of Security Advisories	14
4.2 Open a Noncritical Case	9	6.7 Security Assurance.....	14
4.3 Open a Critical Case.....	9	7. End-of-Life Announcements	15
4.4 Update Case.....	9	8. Appendix: Quick Reference to	
4.5 Case Severity Definitions	10	Support Resources	15
4.6 Report a Software Defect (Bug)	10	8.1 Overview	15
4.7 Request RMA	10	8.2 Online Self-Help	15
		8.3 How to Open a Case.....	15

1. Overview of Support Resources

Palo Alto Networks Support provides timely access to the expertise needed to protect your business. Digital resources such as knowledge base, LIVEcommunity, Beacon, TechDocs, and other self-service tools are available 24/7, year-round.

The Global Customer Support teams, composed of Technical Support, Customer Service, and Hardware Services, provide around-the-clock [web](#) or [phone](#) support for customers with valid entitlements.

1.1 Self-Service Tools

We encourage you to use our self-service tools to help you quickly and efficiently find answers to your questions.

- [Knowledge base](#)—knowledge-centered support to answer questions and resolve issues
- [LIVEcommunity](#)—where authorized users can connect, share, and learn with other cybersecurity professionals through posts, blogs, and discussions
- [Beacon](#)—Palo Alto Networks education portal that gathers all Palo Alto Networks resources in one location
- [TechDocs](#)—technical guides to all products, [best practices](#), and resources, such as [Release Notes](#) and [Compatibility Matrix](#)
- [Applopedia](#)—application database used along with App-ID™ technology to identify applications traveling through your Palo Alto Networks Next-Generation Firewall
- [Security Advisories](#)—lists all security vulnerabilities identified in currently supported Palo Alto Networks products
- [Threat Vault](#)—enables authorized users to research the latest threats (vulnerabilities/exploits, viruses, and spyware) that Palo Alto Networks Next-Generation Firewalls can detect and prevent
- [URL Filtering categorization](#)—test URL Filtering categories
- [Updates](#)—software and dynamic (content) updates available to authorized users in the Updates section of the Customer Support Portal (CSP)

1.2 Technical Support

Technical Support is available for Palo Alto Networks products 24/7/365. Standard Support provides customers with Technical Support through the CSP.

Phone support is available to customers with Platinum and Premium Support after opening a case online. If an issue becomes critical, log in to the CSP and increase the priority before contacting TAC. Customers with [Partner Enabled Premium Support](#) will open cases through their Authorized Support Center (ASC).

Technical Support handles:

- All technical inquiries
- Product software or feature problems (bugs)
- Defective returns (return merchandise authorization or RMAs)

To engage Technical Support, select **Tech Support** in the **Type** field when creating a web case.

1.3 Customer Service

Customer Service assists with nontechnical administrative cases 24/7/365, including:

- [Login assistance](#) for the Customer Support Portal
- Password resets and email address changes
- Product registration and license activation
- License management (expiration dates, grace period, bundles)
- Product and license transfers

Select **Admin** in the **Type** field when creating a [web](#) case or when prompted by the automated phone system. (Note: Select **Tech Support** for product login administration issues.)

1.4 Hardware Services

Technical Support determines that if a product is defective, they'll assign a subcase to the Hardware Services team for the logistics follow-up. Hardware Services will:

- Obtain the delivery address.
- Verify trade compliance for international deliveries.
- Submit an RMA to logistics provider.
- Provide delivery updates.

View the [RMA Process Policy](#).

2. Support Plan

With business-critical [customer support options](#) and 24/7 availability, as well as a global network of support centers and parts-replacement depots, Palo Alto Networks provides a range of support, customer guidance, and maintenance options designed to meet all business needs:

- [Premium Support](#)
- [Platinum Support](#)
- [Focused Services](#)

2.1 Service Deliverables

Table 1: Service Deliverables						
		Required Support Tiers (Asset)		Optional Focused Services (Account)		
		Premium	Platinum	Focused	Focused PLUS	Focused ELITE
Technical Support	Telephone Support	24/7	24/7			
	Response Time (critical issue)	1 hour	15 minutes			
	Support Specialist Type	Support Engineer	Senior Engineer	Support Engineer	Designated Engineer	Designated Engineers
	RMA	NBD 4 hours	NBD 4 hours			
Security Assurance	Assisted Security Investigations	•	•			
	Advanced Log & IoC Analysis	•	•			
	Recommended Next Steps	•	•			
Expert Assistance	Planned Event Support		•			•
	On-Site Assistance (critical issue)		•			•
	Failure Analysis (HW)		•			•

Table 1: Service Deliverables (continued)

		Required Support Tiers (Asset)		Optional Focused Services (Account)		
		Premium	Platinum	Focused	Focused PLUS	Focused ELITE
Personalized Experience (Focused Services)	Designated SAM			•	•	•
	Case Management/Escalation			•	•	•
	Weekly Reviews (cases, planning)			•	•	•
	Root Cause Analysis (HW + SW)			•	•	•
	Best Practice Reviews			•	•	•
	Focused Services Webinars			•	•	•
	Proactive Threat Notifications			•	•	•
	Release Reviews			•	•	•
	Designated Engineers				•	24/7
	Tailored Release Strategy				•	•
	Access to Engineering				•	•
	Proactive Performance Sweep				1	2
	SecOps Optimization Service				1	2
Customer Surround	Designated Service Delivery Leader				(Tier 3)	(Tier 2 and 3)
	Orchestrate All Services Delivered				•	•
	Coordinate All Designated Resources				•	•
	Report Activities and Milestones				•	•

3. Technical Case Workflow

When a case is opened, a Technical Support Engineer will review the issue and data presented. The engineer will update the case either via **Case Comments** or call the customer at the phone number provided when opening the case.

If a live troubleshooting call is required, the TAC engineer will coordinate with the customer at an appropriate time.

3.1 How to Open a Case

Web cases may be created by authorized users from the CSP. These options are available to customers with Platinum, Premium, or Standard Support. Customers with [Partner Enabled Premium Support](#) will contact their Authorized Support Center.

CSP: <https://support.paloaltonetworks.com> > **Support Cases > Get Help**

Knowledge base articles will be suggested throughout the case creation process based on subject and [description](#).

Recommended for critical cases: Create a web case through the CSP. Set the severity as critical.

If you would like to speak with the case owner, call Technical Support and enter the case number into the automated system.

If unable to create a login or access the **Support Cases** section of the CSP, request [Login Assistance](#). If unable to locate the product serial number, select the option to have Customer Service submit the technical case. Customer Service will investigate and provide the serial number.

New cases aren't [accepted via](#) email, but once a case is created, email may be used to view and reply to case updates.

3.2 Case Owner Responsibilities

Once a support case is opened with Palo Alto Networks TAC, depending upon product technology and service entitlements, the case is routed to an appropriate engineer. The engineer is responsible for the following:

- Take ownership of the Palo Alto Networks support case.
- Provide an initial response time and perform troubleshooting, diagnostics, or undertake any remediation steps.
- TAC will document all activity in Case Comments.
- Engage additional resources as needed to address issues.
- Follow up and close the support case upon confirmation from the customer.

3.3 Customer Support Summary

Customers can request an event if they have purchased Premium/Platinum entitlement. An event is a scheduled session with a Support Engineer where all parties will join a bridge at a predetermined time to conduct whatever troubleshooting or maintenance has been agreed upon.

An event may be requested for:

- Failed upgrade attempts
- Maintenance windows associated to a support case with an existing technical issue
- Troubleshooting session to resolve an ongoing technical issue

If requesting a Support Event, review the Support Event Guidelines: Request a Support Event in the Customer Support Portal knowledge base. The [Customer Support Program Summary](#) explains which entitlements include [Planned Event](#) assistance.

If you're seeking help migrating or upgrading to a newer version, engage with your Palo Alto Networks account manager or Professional Services.

3.4 Case Resolution Process

Palo Alto Networks Support Engineers will take ownership of the support case and work toward providing a resolution. If a resolution can't be provided, the Support Engineer will make the best effort to provide a workaround or mitigation plan. The Support Engineer may perform any or all of the following steps:

- Review network topology, firewall configuration, and analyze logs to provide the next steps or debug issues.
- Perform live troubleshooting on customer devices or replicate issues in a Palo Alto Networks lab.
- If the issue is determined to be a hardware failure, proceed with an RMA.
- If the issue is determined to be a software defect, raise an issue report with Engineering.
- Guide customers to correct resources if an issue falls outside the scope of Support.

3.5 Customer Best Practices for Engaging Support

We understand your business needs to resolve Support issues in a timely manner. To help provide you with a quality support experience and resolve your issues quickly, we encourage our customers to follow these best practices when engaging with Palo Alto Networks Support:

- Search for help online. See section 1.1 for self-help tools.
- If you choose to open a web case, check the articles offered as you enter the subject and description to see if they'll resolve the issue.
- When opening a case, fill in all fields to the best of your knowledge and provide a brief summary and detailed description of the issue with as much information as possible.
- Set the appropriate severity of the support case. Raise or lower the severity of the case online through the CSP if the situation changes.
- For faster resolution, upload all relevant support files and logs to the case when opening it.
- Contact [Support](#) if you need assistance outside of your case owner's working hours.
- When we update a case online, an email is generated. To add additional comments, enter them using **Case Comments**. Update a case via the email generated each time a comment is made online through **Case Comments** or contact [Support](#) for urgent issues. There's no option to email Support directly.
- If you're unable to log in or create a case, request [assistance](#).
- During case creation, we may ask you to provide additional information for certain product types. We strongly encourage you to spend a few more minutes and answer these questions as they help to speed up the resolution time.

3.6 Software Defect Case Resolution Process

During the course of the investigation of a Support issue, if we determine the issue is due to a software failure, the assigned Support Case Engineer will follow the process below:

- Open an issue report with Palo Alto Networks engineering team.
- Share the Issue Report ID with the customer and provide updates on the resolution status.
- Share with the customer any available workarounds or mitigation steps in the interim.
- Once a fix is identified and we have a targeted software release version, we'll share the release info and estimated time for the fix.

3.7 Case Closure Policy

Customers are to provide the logs and/or live troubleshooting sessions to troubleshoot the issue and ensure prompt resolution. Once the TAC/Support Engineer requests additional details or a troubleshooting session, customers have 5 days to respond, with 2 automated follow-ups. If more time is needed, the customer can inform the TAC/Support Engineer via the support **Case Comments** or by calling the [Support](#) line. If no response is received from the customer within 5 days, the case will be autoclosed.

After the TAC/Support Engineer provides a resolution, customers have 6 days to confirm the resolution and will receive two automated follow-ups. If more time is needed to validate the resolution, the customer can inform the TAC/Support Engineer via the support **Case Comments** or by calling the [Support](#) line. If the customer doesn't respond within 6 days, the case will be autoclosed.

In the event the issue persists or recurs after the case is closed, the case can be reopened within 14 days. After the 14-day window, customers can open a new case and reference the previous case number to continue working on the issue.

4. Access Support Resources

4.1 Customer Support Portal Login

Create a [CSP account and user login](#) to securely access Support resources. Once the CSP account is created, you'll be able to [register products and auth codes](#). Among [other features offered on the portal](#), you'll be able to manage memberships, connect to knowledge resources, and log Support cases for products with valid Platinum, Premium, or Standard Support.

4.2 Open a Noncritical Case

Support cases may be created by [authorized](#) users from the [CSP](#) or through [LIVEcommunity](#) for technical (Tech Support) and nontechnical (Admin) issues. These options are available to customers with Platinum, Premium, or Standard Support. Customers with [Partner Enabled Premium Support](#) will contact their Authorized Support Center (ASC).

Be sure the case **Subject** and **Description** are complete and provide a clear explanation of the issue, including:

- A serial number of the product or auth code.
- Cluster peer if HA.
- Date and time of the issue (if possible).
- Explain changes made to the network or any new traffic introduced.
- Products in question upgraded or downgraded.
- Any logs, screenshots, or ACC output that can help further analyze the issue.
- Upload relevant product support files.

Knowledge articles that may resolve your issue will be suggested throughout the case creation process based on subject and description.

If unable to create a login or access **Support Cases**, request [login assistance](#). If a serial number isn't found when creating a case, select the option to have Customer Service create and route the technical case. The team will then investigate and resolve the issue with the missing serial number.

New cases aren't accepted via email, but once a case is created, email may be used to view and reply to case updates.

4.3 Open a Critical Case

- Open a web case through the CSP and set the severity as critical. Confirm that the product is down and critically affecting a production environment with no workaround available.
- Then contact [Support](#) and enter the case number in the automated system.

We'll work on the issue around the clock until a resolution or workaround is available. If we're unable to contact you, the severity of the case will be lowered. See table 2 for initial response times based on severity.

4.4 Update Case

Update an existing case by replying to the email generated when a new comment is entered or by logging in to the [CSP](#), selecting **Support Cases**, filtering by **My Cases**, **My Company's Cases**, or entering the case serial number. Enter the comment and click the **Post Comment** button.

Contact [Support](#) for urgent updates. Enter the case number when prompted by the phone system, and your case will be routed to the assigned case owner or the next available engineer.

4.5 Case Severity Definitions

Table 2 provides case initial response times.

Table 2: Initial Response Times		
Severity	Premium Support/Focused Services Initial Response	Platinum Support Initial Response
Critical	< 1 Hour	< 15 Minutes
High	< 2 Hours	< 30 Minutes
Medium	< 4 Hours	< 2 Hours
Low	< 8 Hours	< 4 Hours

Severity Definitions

- **Severity 1—Critical:** Product is down and critically affecting the customer production environment. A workaround isn't yet available.
- **Severity 2—High:** Product is impaired and customer production is up but impacted. No workaround is yet available.
- **Severity 3—Medium:** A product function has failed and customer production isn't affected. Support is aware of the issue and there's a workaround available.
- **Severity 4—Low:** Product function isn't impaired and has no impact on customer business. Includes features, information, documentation, how-to, and enhancement requests from the customer.

If the impact of the issue has increased since initially reported, increase the severity online. The system will generate a notification to the case owner or available team member.

If the issue has become critical, update the case online and contact [Support](#). Once the case number is entered into the system, the call will route to the assigned case owner or the next available team member.

Recommended for critical cases: Create a web case through the CSP and set the severity as critical. If you want to speak with the case owner, contact [Support](#) and enter the case number into the automated system.

4.6 Report a Software Defect (Bug)

Open a Technical Support case to confirm a software defect. Providing the additional details below will lead to a faster resolution:

- Detailed problem description.
- If any upgrades/downgrades were performed, including release versions.
- How the issue is observed (if under specific circumstances/traffic patterns).
- Any logs, screenshots, or ACC output that can help further analyze the issue.
- Tech Support files.

4.7 Request RMA

To report defective hardware, select **Platform/Hardware > Technical Issue** when creating a [web](#) case or Technical Support when prompted by the automated [phone](#) system. See section 6 for more details.

4.8 Report a Beta Release Issue

Invitation-only beta releases are supported through the Beta Forum on [LIVEcommunity](#). The forum is the place for authorized beta participants to engage in discussions, ask questions, report issues, and provide feedback about the product.

Contact BetaSupport@paloaltonetworks.com or your System Engineer for information about beta programs.

4.9 Request a Feature Enhancement

To submit a feature enhancement, reach out to your local sales team to create a new request or add your vote to an existing one. For a new feature enhancement, it helps to have as many details as possible to support the request, including:

- Use cases
- Business needs
- Comparable features
- Existing examples

A business justification will help the product teams and engineers decide which features merit the most priority for the next or subsequent releases.

4.10 Reopen a Closed Case

In the event the issue persists or recurs after the case is closed, the case can be reopened within 14 days. In the [Customer Support Portal](#), go to your **Support Cases** and click the specific case under the **Closed** filter tab or enter the case number in the search box. For the specific case, click the **Manage Your Case** tab, fill out the required fields, and click the **Submit Request To Reopen Case** button to complete the reopen request. The case will be routed to the next available engineer. Please contact the [Support](#) hotline if the issue is urgent after reopening the case. After the 14-day window, customers can open a new case and reference the previous case number to continue working on the issue.

5. Return Materials Authorization (RMA) Workflow

5.1 Request an RMA

To request an RMA, the defective device must be [registered](#) in the CSP with [active support auth code](#), and a technical case must be submitted.

Select **Platform/Hardware > Technical Issue** when creating [a web](#) case or Technical Support when prompted by the automated [phone](#) system. The Technical Support Engineer will troubleshoot the device to diagnose the defect.

After determining that an RMA is necessary, the engineer will route the case to the Hardware Services team, which will act immediately to:

- Obtain the delivery address.
- Verify trade compliance for international deliveries.
- Submit RMA to the logistics provider.
- Provide delivery updates.

5.2 RMA Delivery Times

RMAs must be delivered to a physical address (not a P.O. box), and a recipient signature is required.

Customers with a **4-Hour Support** contract will receive the replacement within 4 hours of submission of the RMA to the logistics provider by the Hardware Services team. The replacement will be delivered by private courier, and no RMA tracking information will be available in the **RMA Tracking** section of the case. Contact your case owner for delivery updates. A specific delivery time may be requested if delivery within 4 hours isn't convenient. Palo Alto Networks will pay for all shipping costs associated with the advance replacement and defective return.

Customers with **Platinum**, **Premium**, or **Partner Enabled Premium Support** receive Next Business Day (NBD) delivery if the order is received by the logistics provider by 3 p.m. local time at the depot,

which is shipping it. With the exception of some countries where local couriers are used, the tracking information (generally from FedEx or DHL) will appear in the RMA Tracking section of the case. If there's no tracking information in your case, the case owner should be able to obtain an update for you. Palo Alto Networks will pay for all shipping costs associated with the advance replacement and defective return.

Customers with **Standard Support** must return the defective unit at their own expense to the address provided in the case by the Hardware Services team. A replacement unit will be shipped upon receipt. Replacement shipping costs will be paid by Palo Alto Networks. (Note: LAB and NFR units have **Standard Support**; however, RMAs are processed with all NBD shipping rules.)

An Importer of Record (IOR) must be identified if shipping to a country that doesn't have a local depot. The IOR will facilitate customs clearance of the device. The device will remain in customs and eventually be returned to Palo Alto Networks or destroyed if no IOR is provided. Palo Alto Networks will reimburse any shipping and duty costs incurred if the device is under **Platinum, Premium, or Partner Enabled Premium Support**. Your account team will provide information about depot locations. Shipping times will vary depending on the trade rules in these countries.

The [RMA Process and Policy](#) document provides additional detailed RMA information.

5.3 RMA License Transfers

The replacement device uses the SKU "spare" to permit the [license transfer from defective to replacement](#).

Customers with an On-Site Spare (OSS) device will be able to transfer licenses from the defective device to the OSS using the steps in the above link. There are two replacement options with an OSS:

- Leave the OSS in the production network and use the RMA replacement as the new spare.
- Transfer the licenses from the OSS to the replacement spare and open an Admin case to have the OSS returned to the spares inventory.

Once the license transfer is complete, the spare device will have all of the attributes of the defective unit. The defective device will have valid licensing for 30 days from the date of the transfer to allow time to remove the unit from a production network.

Be sure to transfer licenses prior to returning the defective device. If the defective serial number is no longer visible in the CSP account, license recovery may still be possible using the **Can't Find Defective Serial Number** option. If still unable to find the serial number, create an Admin case, and Customer Service will assist.

5.4 Returning the Defective Device

A defective device should be returned to Palo Alto Networks within 10 days of receipt of the replacement unit. Return instructions and a prepaid return airway bill will be provided with the replacement unit.

Customers are asked to provide information for the Asset Recovery Contact in the RMA form. This is the person the Asset Recovery team will communicate with should the unit not be returned within 10 days.

Here are some additional RMA instructions and details:

- Click the **Missing Return Instructions** button in your RMA case if unable to locate your return instructions. The **Asset Recovery Contact** should receive new instructions within one business day.
- If the device won't be returned within 10 days, request an extension via Case Comments and provide an estimated return date. The Hardware Services team will notify Logistics.
- If returning the replacement or realizing that the serial number reported defective is incorrect, update the **Case Comments** with the serial number being returned. The Hardware Services team will notify Logistics.
- Failure to return a defective device will result in the decommissioning of that serial number. Failure to notify Palo Alto Networks of a change to the returned serial number may also result in the decommissioning of the original serial number reported.

- Many defective parts don't need to be returned. The Hardware Service team will advise via **Case Comments** if the defective part can be recycled. No prepaid airway bill will be provided with the replacement for parts that don't need to be returned.

5.5 Failure Analysis Reports

A detailed Failure Analysis Report may only be requested for devices entitled with Platinum Support. When submitting the case for such serial numbers, indicate in the **Case Comments** that a Failure Analysis Report is needed. The Hardware Services team will include the request when submitting the RMA to Logistics. Failure analysis may be requested after the RMA has been submitted up until the returned unit has been scrubbed of all customer data. The Hardware Services team will be able to advise the status of the defective serial number.

Failure analysis for devices with Premium Support will only be provided on an exception basis with a Technical Support Manager's approval. Failure analysis isn't available for devices with Standard Support.

6. Security Vulnerability Workflow

6.1 Definition of a Security Vulnerability

Palo Alto Networks defines a security vulnerability as a weakness or flaw in a product or service that could allow an attacker to compromise the integrity, availability, or confidentiality of the product or service.

Note: This specifically excludes network security-related functionality of the product or service (e.g., intrusion prevention, application, or file identification, antivirus, malware analysis) which pertains to the function and efficacy of the product or service. Issues pertaining to the security-related functionality of a product or service will be handled via [Palo Alto Networks Customer Support](#).

6.2 How to Report a Security Vulnerability

Contact the Palo Alto Networks Product Security Incident Response Team (PSIRT) by completing the [Palo Alto Networks Report a Security Vulnerability form](#) or submitting an email to **psirt@paloaltonetworks.com**. We encourage the submission of vulnerabilities via encrypted email. Our PGP public key is available [here](#).

Please include details on the software and hardware configuration, reproduction steps, potential impact, and a proof of concept (if possible). This will enable us to duplicate the issue and respond to your report more quickly. In order to avoid reporting a known issue that has already been resolved, we recommend all testing be performed on the [Customer Support Portal](#).

6.3 Acknowledgment and Analysis of a Vulnerability Report

PSIRT will acknowledge the receipt of the report within two (2) business days. A tracking number will be provided in the acknowledgment email. Please include this tracking number in the subject of all further email communications relating to the submission. Upon receiving all relevant information, we'll endeavor to provide a response with our analysis within five (5) business days. Some issues may be more complex and require more time to investigate.

6.4 Fix or Corrective Action

Palo Alto Networks will provide a fix for a security vulnerability that affects our products or services that aren't end-of-life. Our end-of-life policy can be viewed [at End-of-Life Summary](#).

The fix may take one or more of the following forms:

- For customer-delivered software (such as PAN-OS® or Panorama®), a software fix included in a subsequent major or minor release of the affected product
- For cloud-based services (such as SaaS Security and AutoFocus®), a software fix applied to the cloud-delivered service
- A corrective procedure or workaround to mitigate the impact of the vulnerability

6.5 Notification of Product Security Information and Software Updates

Information relating to addressed vulnerabilities are published in Security Advisories on our website at [Palo Alto Networks Product Vulnerability—Security Advisories](#).

6.6 Publication of Security Advisories

Security Advisories are published under the following situations:

- A security issue that is specific to our software or that affects open-source software, which can reasonably be assumed to affect our software is publicly reported and widely available, and a fix is available in one or more supported software versions.
- A security issue that affects our software is privately reported to Palo Alto Networks, and a fix is available in all currently supported software versions.

Security Advisories will contain a Description, Common Vulnerability Enumerator (CVE), Impact, Severity, Affected Products, Available Updates, and Acknowledgment of the reporter (if applicable).

We may publish blog posts or knowledge base articles for issues that drive high volumes of support requests or generate media attention, or in cases where additional information is useful to support our customers after the release of a Security Advisory.

Customers can sign up for email notifications of new or updated [Security Advisories on our support website](#).

6.7 Security Assurance

If you detect suspicious activity in your network, Security Assurance provides extra help from Palo Alto Networks when you need it the most. Security Assurance provides the following:

- Access to Palo Alto Networks security experts and their specialized threat intelligence tools and threat hunting practices
- Advanced log and indicators of compromise (IoC) analysis
- Configuration assessment that includes customized product security recommendations
- Next-step recommendations to expedite the transition to your incident response (IR) vendor to help manage and resolve the incident

To take advantage of Security Assurance, you must subscribe to the Premium Support Contract (on or after November 1, 2019) or to the Platinum Support Contract. The first step toward Security Assurance is to run the [AIOps for NGFW](#) (formerly [Best Practice Assessment](#) [BPA]) to measure your adoption of seven key security capabilities.

If you experience suspicious activity, when you engage Security Assurance, you must provide a specific set of data about the suspected incident so Palo Alto Networks experts can investigate the activity. After you collect data about suspicious activity to ensure the timely analysis of the relevant information, you're ready to engage Security Assistance. You can engage Security Assistance by:

- Logging in to the CSP. Click **Create a Case** to open a support case. When you fill out the form, select **Threat**. Your sales engineer (SE) can open a support case on your behalf.

For further information on Security Assurance, please [visit this best practices document](#).

7. End-of-Life Announcements

Products eventually reach their natural end-of-life for various reasons, including new and better technologies becoming available, marketplace changes, or source parts and technologies being unavailable. This is part of any technology product's lifecycle. It's the goal of Palo Alto Networks to make this process as seamless as possible for you and our partners as well as to provide as much visibility into what you can expect during the process:

- [End-of-Life \(EoL\) Policy](#)
- [End-of-Sale Announcement](#)
- [Software End-of-Life Dates](#)
- [Hardware End-of-Life Dates](#)

8. Appendix: Quick Reference to Support Resources

8.1 Overview

Palo Alto Networks offers a variety of online resources to answer product questions, resolve issues, and provide configuration help.

Support is available for product issues 24/7, year-round with current Platinum or Premium entitlements. [Partner Enabled Premium Support](#) will be provided by the contracted Authorized Service Center.

8.2 Online Self-Help

- **Knowledge base**—knowledge-centered support to answer questions and resolve issues
- **TechDocs**—technical guides to all products, [best practices](#), and resources such as [Release Notes](#) and [Compatibility Matrix](#).
- **Beacon**—a one-stop education portal that gathers all Palo Alto Networks resources in one location
- **Applopedia**—application database used along with App-ID to identify applications traveling through your Palo Alto Networks Next-Generation Firewall
- **Security Advisories**—listing of all security vulnerabilities identified in currently supported Palo Alto Networks products
- **Threat Vault**—enables authorized users to research the latest threats (e.g., vulnerabilities/exploits, viruses, spyware) that Palo Alto Networks Next-Generation Firewalls can detect and prevent
- **URL Filtering categorization**—test URL Filtering categories
- **Updates**—software and dynamic (content) updates available to authorized users in the Updates section of the CSP.

8.3 How to Open a Case

Web cases may be created by [authorized](#) users from the CSP or through LIVEcommunity for technical (Tech Support) and nontechnical (Admin) issues. These options are available to customers with Platinum, Premium, or Standard Support. Customers with [Partner Enabled Premium Support](#) will contact their Authorized Support Center.

CSP: <https://support.paloaltonetworks.com> > **Support Cases** > **Get Help**

Knowledge base articles will be suggested throughout the case creation process based on subject and description.

Recommended for critical cases: Create a web case through the CSP. Set the severity as critical. If you'd like to speak with the case owner, contact [Support](#) and enter the case number in the automated system.

If unable to create a login or access the **Support Cases** section of the CSP, request [Login Assistance](#).

If unable to locate the product serial number, select the option to have Customer Service submit the technical case. Customer Service will then investigate and resolve the issue with the serial number.

New cases aren't accepted via email, but once a case is created, email may be used to view and reply to case updates.

8
YEARS



2015 • 2016 • 2017 • 2018 •
2019 • 2020 • 2021 • 2023



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
parent_global-customer-services-support-resource-guide_030425

Discover what's really driving the shift toward unified security

(/)

Third-Party Components Support

Palo Alto Networks, Inc. has the following policy regarding the use of third-party transceivers, power supplies, hard drives, or other components used within the Palo Alto Networks devices.

- If a customer uses a third-party component in a Palo Alto Networks device, and a fault is traced to the use of this third-party component, then at Palo Alto Networks' discretion, support and warranty service may be withheld.
- If a product fault is determined to not be related to the use of third-party components, then Palo Alto Networks will continue to support the customer per our standard support policies.
- At no time will hardware RMA support be provided on third-party components. If hardware is replaced and the fault is determined to have been caused by the installation of a third-party component, Palo Alto Networks reserves the right to charge for reasonable time and material rates for the service provided.

Get the latest news, invites to events, and threat alerts

Enter your email now to subscribe!

By submitting this form, you agree to our [Terms of Use \(/legal-notices/terms-of-use\)](/legal-notices/terms-of-use) and acknowledge our [Privacy Statement \(/legal-notices/privacy\)](/legal-notices/privacy)

Sign Up

Products and Services

Company

Popular Links



Privacy (/legal-notices/privacy)

Trust Center (/legal-notices/trust-center)

Terms of Use (/legal-notices/terms-of-use)

Documents (/legal)

Copyright © 2025 Palo Alto Networks. All Rights Reserved

(https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector) (https://www.paloaltonetworks.com/pan-os/pan-os-9-1-vector)

EN



Cloud NGFW for Azure Service-Level Agreement

Palo Alto Networks will use commercially reasonable efforts to make its Cloud NGFW for Azure service (“Service”) available at least 99.99% of the time during any calendar month. In the event that Palo Alto Networks does not meet this service-level commitment, customers will be eligible to receive a Service Credit as described below.

Service-Level Commitment

The following service levels and Service Credits apply to the customer’s use of the Service. If, during any calendar month, the Service availability falls below 99.99%, the customer will be eligible to request a Service Credit. Customers must submit such a request (“claim”) for credit. If a customer makes such a claim, Service Credits owed will be calculated as follows:

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.99% but greater than or equal to 99%	10%
Less than 99% but greater than or equal to 95%	25%
Less than 95%	100%

Definitions

“**Cloud NGFW for Azure service**” is Palo Alto Networks ML-Powered Next-Generation Firewall delivered as a service on the Azure® platform.

“**Cloud NGFW tenant**” is an instantiation of the Cloud NGFW service associated with an Azure customer account. The tenant is created when a user associated with the Azure customer account subscribes to the Cloud NGFW service. The user can create NGFW resources within the tenant.

“**NGFW resource**” refers to a logical resource that provides NGFW capabilities to customers’ Azure Virtual Network (VNet). This resource has built-in resiliency, scalability, and lifecycle management. The NGFW resource spans multiple Azure availability zones.

“**Deployment Minutes**” is the total number of minutes a given NGFW resource is provisioned during a billing month in a given Azure region.

“**Maximum Available Minutes**” is the sum of all Deployment Minutes across all NGFW resources provisioned in a Cloud NGFW tenant during a billing month.

“**Downtime**” is the total accumulated Deployment Minutes across all NGFW resources in a Cloud NGFW tenant provisioned during a month in which the NGFW resource is Unavailable. An NGFW resource is considered “**Unavailable**” during a given minute if packets are routed to the NGFW resource and the NGFW resource processes none of the packets routed to it within the minute. If no packets are routed to the NGFW resource during the minute, the NGFW resource is considered available during the minute.

“**Excluded Downtime**” is Downtime resulting directly or indirectly from any “Cloud NGFW for Azure” SLA Exclusion.

“**Monthly Uptime Percentage**” is calculated as Maximum Available Minutes less Downtime less Excluded Downtime, divided by Maximum Available Minutes less Excluded Downtime, in a billing month for a given Cloud NGFW tenant. The following formula represents Monthly Uptime Percentage:

$$\text{Monthly Uptime Percentage} = \frac{(\text{Maximum Available Minutes} - \text{Downtime} - \text{Excluded Downtime})}{\text{Maximum Available Minutes} - \text{Excluded Downtime}} \times 100$$

Administration

Service Credit

A “Service Credit” is a dollar credit, calculated as set forth in the table above, that Palo Alto Networks credits back to your Azure account using the [Azure Marketplace refund process](#). Service Credits are calculated as a percentage of the Cloud NGFW hourly charges paid by you for the Cloud NGFW for Azure service during the month, **excluding traffic-secured GB charges**.

- In any month, the maximum amount of Service Credits that Palo Alto Networks shall be liable for is 100% of the monthly service fee paid by the customer.
- In the case of multiyear contracts, Palo Alto Networks may calculate the monthly service fee by dividing the service fee by the number of months of the contract duration.
- The Service Credits will be based on the estimated retail price for the applicable Service, as determined by us at our reasonable discretion.

Eligibility

To qualify to claim and receive credits under this Service-Level Agreement, the customer must be in good standing and the customer shall not be or have been delinquent in paying Service fees. This Service-Level Agreement does not apply to beta, trials, and evaluations of the Service provided at no cost to the customer.

Notifications

The customer may, at any time, obtain Service status at <https://status.paloaltonetworks.com>, which provides region-specific status information and an alerts feature from which customers may subscribe to receive service notifications. Palo Alto Networks will use commercially reasonable efforts to provide advance notice of Service events.

Claims Process

Customers must have enrolled for an account on the Customer Support Portal in order to open a case and submit a claim.

If the customer believes they are entitled to a Service Credit, they must:

- Report the outage within 24 hours of an incident using the [Cloud NGFW LIVEcommunity](#).
- Submit a claim on the Claim Dashboard (https://supportcases.paloaltonetworks.com/apex/Communities_Claims) within five business days of the outage.

Customers must include the following information in their claim:

1. The words “SLA Credit Request” in the subject line.
2. The dates and times of each unavailability incident that you are claiming.
3. The affected Cloud NGFW resources.
4. The email address associated with your Azure account.
5. Azure account number of your account used to subscribe to your product.
6. The billing periods for which the customer would like a Service Credit.
7. Logs that document the errors and corroborate your claimed outage. (Any confidential or sensitive information in these logs should be removed or replaced with asterisks.)

When properly submitted, Palo Alto Networks will evaluate all information available and make a good faith determination of whether you are owed a Service Credit. Palo Alto Networks shall use commercially reasonable efforts to promptly adjudicate the claim after determining the outage’s root cause and closing the case, confirming your request. Palo Alto Networks shall be the final arbiter of whether any Service Credits are due. Adjudicated claims shall be deemed final and may not be resubmitted for reconsideration.

The customer’s failure to properly submit a claim for a Service Credit or respond to or provide any other information necessary to validate the request will disqualify the customer from receiving a Service Credit.

If Palo Alto Networks determines that a Service Credit is owed to the customer, it will use the [Azure Marketplace refund process](#) to apply the Service Credit to the customer's Azure account. Service Credits will not entitle the customer to any refund or other payment from Palo Alto Networks. The Service Credits awarded in any billing month for the Cloud NGFW for Azure service will not exceed your monthly service fees as applicable in the billing month. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar (\$1 USD). Service Credits may not be transferred or applied to any other Cloud NGFW tenant.

Exclusions

This Service-Level Agreement does not apply to any unavailability, suspension, or termination of Cloud NGFW for Azure, or any other performance issues that result from:

1. Any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties and beyond the control of Palo Alto Networks, including, but not limited to, force majeure events or internet access.
2. Factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to Azure, including at your site or between your site and Azure).
3. Failure of the customer's internet service provider, utility companies, or another vendor(s) the customer relies on to access the internet.
4. Use of services or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services (other than third-party equipment, software, or technology under Palo Alto Networks control).
5. Any actions or inactions by you or any third party, including the improper configuration of your NGFW resources, Azure routing tables, or other Azure resources.
6. Your failure to follow the guidelines or adhere to any required configurations described in the Cloud NGFW documentation, use supported platforms, follow any policies for acceptable use; failure to modify your use of a Service as advised, or your use of the Service in a manner inconsistent with the Service's features and functionality.
7. Your attempts to perform operations exceeding prescribed quotas or use features outside of associated support, or from our throttling of suspected abusive behavior.
8. Your failure to purchase an adequate license to meet the volume or capacity at which you use the Service if the Service commitment would have been met if not for such failure.
9. Your unauthorized action or lack of action when required, or from your employees, agents, contractors, vendors, or anyone gaining access to our network using your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices.
10. Planned and unplanned maintenance windows.
11. Rightful suspension and/or termination by Palo Alto Networks of the Service according to the Palo Alto Networks End-User Agreement.

Sole and Exclusive Remedy

The foregoing terms state Palo Alto Networks sole and exclusive liability and your sole and exclusive remedy for any claim of noncompliance with service-level commitment.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. Palo Alto Networks and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
strata_ds_cloud-ngfw-for-azure-sla_080823

CLOUD NGFW FOR AWS SUPPLEMENTAL END USER SUPPORT AGREEMENT

THIS CLOUD NGFW FOR AWS SUPPLEMENTAL END USER SUPPORT AGREEMENT (THIS “SEUSA”) SUPPLEMENTS AND AMENDS THE PALO ALTO NETWORKS END USER SUPPORT AGREEMENT AVAILABLE AT THE FOLLOWING WEB ADDRESS: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-global-customer-support-services-terms-and-conditions-eusa.pdf (THE “EUSA”). THIS SEUSA FORMS A LEGALLY BINDING AGREEMENT BETWEEN YOU AND PALO ALTO NETWORKS, INC., INCLUDING ITS AFFILIATES.

This SEUSA sets forth the supplemental terms and conditions under which Palo Alto Networks will provide technical support services for the Cloud NGFW for AWS products sold and/or licensed pursuant to the End User Agreement. In the event of a conflict between this SEUSA and the EUSA or End User Agreement, this SEUSA shall take precedence, but only with respect to the subject matter described below.

1. SUPPORT PLANS AND SERVICES OFFERED

		Standard Digital	Premium Digital Plus
	Digital Experience Product Documentation Proactive Notifications Access to communities		
	Digital Force Chat Support ¹ Community Support Customer Support Portal Phone Support ² Premium SLO		SL: 1hr, S2:4hr
	Digital Training Access to online training		

¹Community Support will be moderated by Palo Alto Networks on a commercially reasonable effort basis
²For Premium, phone support will be through callback provided by TAC



Service Level Agreement

Cortex Products

Palo Alto Networks will make Cortex Cloud, XSIAM, XDR, XSOAR, and Xpanse Software-as-a-Service products (each being a "Cortex Product", collectively "Cortex Products") available to meet a **99.9% Monthly Uptime Availability**, as set forth in this document ("Service Level").

All capitalized terms not defined herein shall have the same meaning as set forth in the Palo Alto Networks [End User License Agreement](#).

1. Service Level Commitment Calculation Formula

The Monthly Uptime Availability will be calculated as follows:

$$\text{Monthly Uptime Availability percentage} = \left(\frac{\text{Total Time} - \text{Downtime}}{\text{Total Time}} \right) \times 100\%$$

Total Time: Total number of minutes in a calendar month.

Downtime: Total number of minutes the Cortex Product was down in a calendar month, excluding the number of minutes that meet the criteria under Section 2 (Exclusions).¹

2. Exclusions

Unavailability of the Cortex Product due to the following reasons shall be excluded from the Downtime:

- 2.1 Issues related with Customer's equipment, networks, software, or technology, or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);
- 2.2 Failure of Customer's internet service provider, utility companies, or other vendors Customer utilizes or relies on to access the Cortex Product or to access the internet;
- 2.3 Any reasonably unforeseeable interruption or degradation in the Cortex Product due to actions or inactions caused by third parties or by activities outside of Palo Alto Networks' control, including, but not limited to, force majeure events;
- 2.4 Customer's failure to purchase adequate licenses to meet the volume or capacity at which it uses the Cortex Product, if the Service Level would have been met if not for such failure;
- 2.5 Rightful suspension or termination by Palo Alto Networks of Customer's access to or use of the Cortex Product pursuant to the Palo Alto Networks End User Licensing Agreement (www.paloaltonetworks.com/legal/eula), unless Customer and Palo Alto Networks have entered into a separate written agreement that specifically overrides such End User Licensing Agreement;
- 2.6 Any feature or portion of the Cortex Product marked or licensed to Customer as "Beta," "Test," "Preview," or the like, indicating that the feature has not been made generally available (aka in production);
- 2.7 Scheduled or emergency maintenance windows;
- 2.8 High Availability events and scaling events; or
- 2.9 Blocking of data communications or other software-as-a-service (SaaS) by Palo Alto Networks, due to security reasons, in accordance with its Information Security policies.

3. SLA Credit Claim

- 3.1 **SLA Credit.** In the event that Customer reasonably believes that the Service Level is not met in any calendar month, Customer may file a claim pursuant to the process described in Section 3.2 below. Once verified by Palo Alto Networks, Downtime shall begin to accrue from the time Customer notifies Palo Alto Networks pursuant to Section 3.2 and will continue to accrue until the Cortex Product is restored. Subject to the terms and conditions herein, for a qualified claim, Palo Alto Networks will issue a credit equivalent to 2% of Customer's monthly fees for the applicable Cortex Product when there is a period of at least sixty consecutive minutes where Monthly Uptime Availability is not met, provided that: (1) no more than one SLA Credit will be issued in any calendar day; and (2) for each calendar month, the maximum amount

¹ Delays in data log ingestion are not considered Downtime.

of SLA Credit that Palo Alto Networks shall be liable for is one week of the monthly fees received by Palo Alto Networks for the applicable Cortex Product ("SLA Credit").

- 3.2 **Claims Process.** In order to receive an SLA Credit, Customer must notify Palo Alto Networks within 24 hours of the Cortex Product's unavailability by opening a case on the Customer Support Portal ("CSP") at <http://support.paloaltonetworks.com>. When properly submitted, Palo Alto Networks will use commercially reasonable efforts to adjudicate the Customer's claim promptly and in good faith, based on its technical records and the information provided by the Customer. The Customer may check on the claim status at any time through the CSP and may sign up to receive notifications from the CSP when the claim status changes. Adjudicated claims shall be deemed final and may not be submitted again for reconsideration.
- 3.3 **Claim Eligibility.** To qualify to receive benefits under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying the applicable Cortex Product fees; and (b) have onboarded the Cortex Product for at least sixty days. This Service Level Agreement does not apply to Cortex Product Evaluations.

4. Miscellaneous

- 4.1 **Cortex Product Status.** Customers may, at any time, verify Cortex Product's operational status at <https://status.paloaltonetworks.com>, which also provides region-specific status information and an alerts feature from which the Customer may subscribe to receive notifications.
- 4.2 **Applicability.** The Cortex Product monthly fee excludes fees arising from additional services Customers may have purchased, such as Professional Services, consulting or managed services, if any. Where applicable, the Cortex Product monthly fee will be calculated by dividing a one-year fee by 12, a three-year fee by 36, etc.
- 4.3 **Distributor & Reseller Orders.** If the Customer has purchased the Cortex Product through an authorized Palo Alto Networks distributor or reseller, the SLA Credit will be made to the distributor which placed the order for the Cortex Product. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer. If a Customer purchased the Cortex Product directly from Palo Alto Networks, then Palo Alto Networks shall issue the SLA Credit towards the Customer's next renewal of the Cortex Product.
- 4.4 **Entire Liability.** The terms in this document state Palo Alto Networks' sole and exclusive liability and the Customer's sole and exclusive remedy for any claim of non-compliance of this Service Level Agreement.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks.
A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>.
All other marks mentioned herein may be trademarks of their respective companies.

SERVICE LEVEL AGREEMENT

IoT Security Service

For its IoT Security service ("Service"), Palo Alto Networks commits to using commercially reasonable efforts to achieve certain service metrics described below. In the unlikely event that Palo Alto Networks does not meet these commitments, Customers will be eligible to receive a service credit.

1. Definitions

1.1 **"Available"** means that the Service is capable of processing and presenting Customer's data in accordance with Service documentation.

1.2 **"Available Time,"** in minutes, is when the Service is Available during a calendar month.

1.3 **"Total Time"** is the total number of minutes in a calendar month.

1.4 **"Excluded Time"** means the time, in minutes, described in the section entitled "Exclusions" below.

1.5 **"Uptime Percentage"** is calculated by subtracting from 100% the percentage of minutes during a given rolling six-month period during which the Service was not Available. The Uptime Percentage measurements exclude Exclusions. It is formulated as,

$$\text{Uptime Percentage} = \frac{\text{Available Time}}{(\text{Total Time} - \text{Excluded Time})}$$

2. Service Level Commitments

Palo Alto Networks will use commercially reasonable efforts to make the Service Available with an Uptime Percentage of at least 99% during any given rolling six-month period ("Service Level"). In the event that the Service does not meet the Service Level, Customer will be eligible to request a Service credit. Service credits are calculated as a percentage of the total charges paid by Customer for the monthly billing cycle in which the Service fell below the Service Level.

Uptime Percentage	Service Credit
Less than 99% but equal to or greater than 98%	5%
Less than 98%	10%

3. Exclusions

Customer agrees and acknowledges that the IoT Security service is a tool that monitors network traffic used by certain IoT devices and is not capable of detecting intrusions or other security issues outside the normal parameters defined by Palo Alto Networks in the Service documentation. Palo Alto Networks will attempt to monitor as much network activity as possible, but it may not be possible to monitor certain devices that are obscured behind a different intranet environment such as a layered network address table or other obstacle to intranet TCP/IP communication. Network latency and throughput may also affect the responsiveness of the Service. Palo Alto Networks is unable to monitor network traffic that is encrypted, encapsulated, tunneled, compressed or otherwise obfuscated. This Service Level Agreement shall not apply and the Service shall be deemed Available where the loss of Service results from:

- (i) Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);
- (ii) Failure of Customer's Internet Service Provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet;
- (iii) Any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties including, but not limited to, force majeure events;
- (iv) Any actions or inactions of Customer or any third party, including failure to assist in Palo Alto Networks' efforts to provide support;
- (v) Planned and unplanned maintenance windows;
- (vi) High Availability events and scaling events;
- (vii) Fetching of logs from Cortex Data Lake service;
- (viii) Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Agreement (www.paloaltonetworks.com/legal/eula).

4. Administration

4.1 Customer may, at any time, obtain Service status [here](https://status.paloaltonetworks.com) (<https://status.paloaltonetworks.com>).

4.2 To qualify to receive Service credit under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to beta, trials and evaluations of the Service provided at no cost to the Customer.

4.3. Customer must submit a claim by opening a ticket on the Palo Alto Networks Customer Support Portal. To be eligible, the credit request must be received by Palo Alto Networks within 24 hours of an outage or an incident. Customer's failure to request and to respond to other information as required will disqualify Customer from receiving a Service credit.

4.4 When the claim is confirmed by Palo Alto Networks to be less than the Service Level, then Palo Alto Networks will issue a service credit by applying it against future Service payments due from Customer. Service credits will not entitle Customer to any refund or other payment from Palo Alto Networks.

4.5 If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the service credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer.

4.6 The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any claim of breach of this Service Level Agreement.

SERVICE LEVEL AGREEMENT
For Prisma Access service (“Service”)

Palo Alto Networks commits to using commercially reasonable efforts to achieve certain service metrics described in sections 1.1, 1.2, and 1.3 below for Prisma Access. In the unlikely event that Palo Alto Networks does not meet these commitments, Customers will be eligible to receive a service credit. Customers must follow the Prisma Access configuration guidance in the product datasheet, deployment guides and technical documents (<https://docs.paloaltonetworks.com/prisma/prisma-access>).

This Service Level Agreement applies solely to Prisma Access core services, other Palo Alto Networks products and add-ons have separate service level agreements or service level objectives.

1. Service Level Commitments

1.1 Uptime Availability SLA. If, during any calendar month, the Service availability falls below 99.999%, Customer can submit a claim for credit, calculated as follows:

Monthly Uptime Availability	Service Credit Percentage
Less than 99.999% but equal or greater than 99.99% **not applicable to Prisma Access for Clean Pipe**	5
Less than 99.99% but equal to or greater than 99.9%	10
Less than 99.9% but equal to or greater than 99%	15
Less than 99% but equal to or greater than 98%	25
Less than 98%	100

“**Monthly Uptime Availability**” is calculated as follows:

$$\text{Monthly Uptime Availability (\%)} = \frac{(\text{Total} - \text{Downtime})}{(\text{Total})}$$

Total = Total number of minutes in a calendar month.
Downtime = Time the Service was down, excluding Excluded).
Excluded = time the Service was down due to exclusions set forth in section 1.4 below.

1.2 Security Processing Latency SLA. The latency of a transaction is measured from when the Prisma Access security engine receives the network data packets for a particular transaction

to the point when the same Prisma Access security engine component attempts to transmit the same data packet. For any given minute, if 1% or more packets spend more than 10ms in latency, this is considered as exceeding the Security Processing Latency threshold, except when due to the exclusions in section 1.4 below. If, during any month, the “Monthly Security Processing Latency Percentage” (calculated as set out below) falls below 99.99%, Customer can submit a claim for credit.

“**Monthly Security Processing Latency Percentage**” is calculated as follows:

Monthly Security Processing Latency (%) =
$$\frac{(\text{Total} - \text{Exceeded})}{(\text{Total})}$$

Total = Total number of minutes in a month.
Exceeded = Total number of minutes exceeding latency threshold, excluding Excluded.
Excluded = time exceeding the latency threshold due to exclusions set forth in section 1.4 below.

Monthly Security Processing Latency Percentage	Service Credit Percentage
Less than 99.99% but equal or greater than 99.9%	5
Less than 99.9% but equal to or greater than 99%	15
Less than 99% but equal to or greater than 98%	25
Less than 98%	100

1.3 Third-party SaaS Application Latency SLA. The latency of a transaction is measured as round trip time elapsed between when the Prisma Access regional security engine transmits the network data packets to the third-party SaaS application and receives the same packet response by the third-party SaaS application, less any response and loading times by the third-party SaaS application. The following SaaS applications are supported: Microsoft O365, Google G Suite, Salesforce, Box and Slack. If, during any calendar month, “Monthly SaaS Application Latency Percentage” falls below 99.99%, Customer can submit a claim for credit, calculated as follows:

“**Monthly SaaS Application Latency Percentage**” is the percentage of minutes during one month that the third-party SaaS application latency exceeds 35 ms for Americas and EMEA or 75 ms for APAC, except when due to the Exclusions set forth in section 1.4:

Monthly SaaS Application Latency (%) =
$$\frac{(\text{Total} - \text{Exceeded})}{(\text{Total})}$$

Total = Total number of minutes in a month.
Exceeded = Number of minutes SaaS Application Latency exceeded 35 ms in Americas & EMEA or 75 ms in APAC, but excluding Excluded.

Excluded = time where latency exceeded the criteria due to exclusions set forth in section 1.4 below.

Monthly Third Party SaaS Application Latency Percentage	Service Credit Percentage
Less than 99.99% but equal or greater than 99.9%	5
Less than 99.9% but equal to or greater than 99%	15
Less than 99% but equal to or greater than 98%	25
Less than 98%	100

1.4 Exclusions. This Service Level Agreement shall not apply and the Service shall be deemed available where the loss of Service results from:

1.4.1 Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);

1.4.2 Failure of Customer's Internet Service Provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet; And any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties or by activities outside Palo Alto Networks control, including, but not limited to, force majeure events;

1.4.3 Customer's failure to purchase adequate licenses to meet the volume or capacity at which it uses the Service, if the SLA would have been met if not for such failure; Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Agreement (www.paloaltonetworks.com/legal/eula)

1.4.4 Any feature or portion of the Service marked as "Beta," "Test," "Preview," or the like, indicating that the feature has not been made generally available (aka production);

1.4.5 Scheduled maintenance and scaling events, including switchover time during high availability events;

1.4.6 Route convergence time if using BGP (Border Gateway Protocol);

1.4.7 For purposes of the Security Processing Latency SLA, packets which have been given a QOS (Quality of Service) policy by the Customer are excluded;

1.4.8 For purposes of the Third-party SaaS Application Latency SLA: Downtime at the SaaS provider or SaaS service degradation events are excluded, and latency caused by traffic redirection via a non cloud default path due to a customer's configuration are excluded.

2. Administration

2.1 Notifications. Customers may, at any time, obtain Service status here (<https://status.paloaltonetworks.com>), which also provides region-specific status information and

an alerts feature from which Customers may subscribe to receive service notifications. Detailed information regarding service maintenance notifications are published here (<https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/release-definitions>).

2.2 Eligibility. To qualify to receive benefits under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to trials and evaluations of the Service provided at no cost to the Customer.

2.3 Claims Process. Customers must have enrolled for an account on the Customer Support Portal in order to open a case and submit a claim. If Customer believes it is entitled to a service credit, it must: (a) open a case on the Customer Support Portal (<http://support.paloaltonetworks.com>) within 24 hours of an outage or an incident; and (b) submit a claim on the Claim Dashboard (https://supportcases.paloaltonetworks.com/apex/Communities_Claims) within 5 business days of the outage. When properly submitted, Palo Alto Networks will use commercially reasonable efforts to adjudicate claims promptly: no later than 15 days after the root cause of the outage has been determined and the case closed. Customers may check on the claim status at any time and may sign up to receive notification when the claim status changes. Adjudicated claims shall be deemed final and may not be submitted again for re-consideration.

2.4 Service Credit Calculation.

2.4.1 Service credits are calculated by multiplying the Service Credit Percentage by the proportional monthly Service fee, and further prorated by the part of the Service affected by the outage: Service Credit = Service Credit Percentage x Monthly Service fee x Service Outage (see table in section 1) (see 2.4.2) Total Service (see 2.4.4)

Service Credit =

Service Credit Percentage x

(see table in section 1)

Monthly Service fee x

(see 2.4.2)

Service Outage

Total Service (see 2.4.4)

2.4.2 The monthly service fee attributable to the applicable Service excludes fees arising from collateral services Customers may have purchased such as Professional or Consulting Services, if any. The monthly service fee may be calculated by dividing one-year service fee by 12, three-year service fee by 36, etc.

2.4.3 For each month, the maximum amount of service credit that Palo Alto Networks shall be liable for is 100% of the monthly service fee paid to Palo Alto Networks.

2.4.4 Service Outage and Total Service are measured in users or bandwidth depending on the Service employed (i.e., For Prisma Access for Users, the outage impact is measured based on the number of users affected; for Prisma Access for Networks and Prisma Access for Clean Pipe, the outage impact is measured in Mbps affected).

2.4.5 If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the service credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer. If a Customer has purchased the Service directly

from Palo Alto Networks, then Palo Alto Networks shall issue the service credit towards the renewal of the Service.

2.4.6 Where an outage gives rise to liability arising from sections 1.1, 1.2, and/or 1.3 above, Customer shall not be entitled to double-dip by claiming service credits for such overlap.

2.4.7 The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any claim of non-compliance of this Service Level Agreement.

SERVICE LEVEL AGREEMENT

Prisma Cloud Subscription Service

Palo Alto Networks will use commercially reasonable efforts to make its Prisma Cloud SaaS Subscription service ("Service") meet 99.9% Monthly Uptime Availability as set forth herein ("Service Level"). In the unlikely event that Palo Alto Networks does not meet this Service Level commitment, Customers will be eligible to claim a service credit as described below ("Service Credit").

1. Service Level Commitment

Palo Alto Networks will use commercially reasonable efforts for the Service to maintain a Monthly Uptime Availability of at least 99.9%, which is calculated as follows:

$$\text{Monthly Uptime Availability Percentage} = \left(\frac{\text{Total Time} - \text{Downtime}}{\text{Total Time}} \right) \times 100\%$$

Total Time: Total number of minutes in a calendar month.

Downtime: Total number of minutes Customer lost external connectivity to the Prisma Cloud Console in a calendar month, excluding the number of minutes that meet the criteria under Section 2 - Exclusions.

2. Exclusions

Unavailability of the Service due to the following reasons shall be excluded from the Downtime, as provided for above:

- 2.1 Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);
- 2.2 Failure of Customer's internet service provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet;
- 2.3 Any reasonably unforeseeable interruption or degradation in Service due to actions or inactions caused by third parties or by activities outside Palo Alto Networks control, including, but not limited to, force majeure events;
- 2.4 Customer's failure to purchase adequate licenses to meet the volume or capacity at which it uses the Service, if the SLA would have been met if not for such failure;
- 2.5 Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Licensing Agreement (www.paloaltonetworks.com/legal/eula), unless Customer and Palo Alto Networks have entered into a separate written agreement that specifically overrides such End User Licensing Agreement;
- 2.6 Any feature or portion of the Service marked or licensed to Customer as "Beta," "Test," "Preview," or the like, indicating that the feature has not been made generally available (aka production);
- 2.7 Scheduled and unplanned maintenance windows;

2.8 High Availability events and scaling events.

2.9 Blocking of data communications or other software as a service (SaaS) by Palo Alto Networks in accordance with its Information Security policies shall not constitute a failure to provide adequate Service under this Service-Level Agreement.

3. Service Credit Claim

3.1 Service Credits. In the event that a Customer reasonably believes that the Service Level in connection with Customer's use of the Service is not met in any calendar month, Customer may file a claim for Service Credit pursuant to Section 3.2 below. Once verified by Palo Alto Networks, Downtime shall begin to accrue from the time Customer notifies Palo Alto Networks pursuant to Section 3.2 and will continue to accrue until the Service is restored. Subject to the terms and conditions herein, for a qualified Claim, Palo Alto Networks will issue a Service Credit which equals to 2% of monthly Service fees when there is a period of at least sixty (60) consecutive minutes where Monthly Uptime Availability is not met, provided that: (1) no more than one Service Credit will be issued in any calendar day; and (2) for each calendar month, the maximum amount of Service Credit that Palo Alto Networks shall be liable for is one (1) week of the monthly Service Fee received by Palo Alto Networks.

3.2 Claims Process. Customers must have enrolled for an account on the Customer Support Portal in order to open a case and submit a Claim. If Customer believes it is entitled to a Service Credit, it must open a case on the Customer Support Portal (<http://support.paloaltonetworks.com>) within 24 hours of the start of the outage. When properly submitted, Palo Alto Networks will use commercially reasonable efforts to adjudicate claims promptly and in good faith based on its technical records and the information provided by the Customer. Customers may check on the Claim status at any time and may sign up to receive notifications when the Claim status changes. Adjudicated Claims shall be deemed final and may not be submitted again for re-consideration.

3.3 Claim Eligibility. To qualify to receive benefits under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to trials or evaluations of the Service that are provided at no cost to the Customer.

4. Miscellaneous

4.1 Notifications. Customers may, at any time, obtain Service status updates at <https://status.paloaltonetworks.com>, which also provides region-specific status information and an alerts feature from which Customers may subscribe to receive Service notifications.

4.2 Applicability. The monthly Service fee attributable to the applicable Service excludes fees arising from additional services Customers may have purchased, such as Professional Services or consulting services, if any. The monthly Service fee may be calculated by dividing one-year Service fee by 12, three-year Service fee by 36, etc.

4.3 Distributor & Reseller Orders. If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the Service Credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer. If a Customer purchased the Service directly from Palo Alto Networks, then Palo Alto Networks shall issue the Service Credit towards the next renewal of the Service.

4.4 Entire Liability. The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any Claim of non-compliance of this Service Level Agreement.



SERVICE LEVEL AGREEMENT

Prisma SD-WAN

For its Prisma® SD-WAN SaaS Subscription Service, Palo Alto Networks commits to using commercially reasonable efforts to achieve a 99.99% level of dataplane availability due to Prisma SD-WAN portal outages. "Dataplane" means all physical or virtual components through which the Customer's data traffic flows. Any disruption of the Prisma SD-WAN portal should not impact the functionality of the Customer's dataplane.

Service Level Commitment: Dataplane Monthly Uptime Availability	Service Credit Percentage
Less than 99.99% but equal to or greater than 99.9%	5
Less than 99.9% but equal to or greater than 99%	15
Less than 99%	25

1. Service Level Commitments

1.1 Uptime Availability SLA. Service availability is calculated for each location of the CloudGenix-supplied or Prisma SD-WAN-supplied hardware ("Branch"). If, during any calendar month, the service availability falls below 99.99%, the Customer must submit a claim for credit, calculated as follows:

Monthly Uptime Availability is calculated by subtracting from 100% the percentage of minutes during any calendar month the dataplane is not available. This calculation excludes downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice and taking into account the Exclusions set forth in section 1.2:

$$\text{Availability} = \frac{(\text{Total} - \text{Downtime} - \text{Excluded})}{100 (\text{Total} - \text{Excluded})} \times 100$$

Total = Total number of minutes in a calendar month.

Downtime = Time for which a Branch experiences a complete loss of capability due to Prisma SD-WAN portal outage or malfunction.

Excluded = Excluded time, including criteria specified in section 1.2 ("Exclusions").

1.2 Exclusions. This Service Level Agreement shall not apply, and the service shall be deemed available, where the loss of service results from:

- 1.2.1 Customer's equipment, software, technology, and/or third-party equipment, software, or technology (other than third-party equipment, software, or technology under the control of Palo Alto Networks);
- 1.2.2 Failure of the Customer's internet service provider, utility companies, or other vendor(s) the Customer relied on to access the internet;
- 1.2.3 Failure of the Customer to monitor system faults and alarms available in the management portal or via API or SNMP-based monitoring tools;
- 1.2.4 Customer's misconfiguration of service features or settings that are wholly under the Customer's control;
- 1.2.5 Customer's failure to purchase adequate licenses to meet the volume or capacity at which it uses the service, if the SLA would have been met if not for such failure;
- 1.2.6 Any feature or portion of the service marked as "Beta," "Test," "Preview," or the like, indicating that the feature has not been made generally available (a.k.a. "production");
- 1.2.7 Any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties including, but not limited to, force majeure events;
- 1.2.8 Planned and emergency maintenance windows. Palo Alto Networks conducts emergency maintenance to address and mitigate an outage or degradation of service;
- 1.2.9 Scheduled maintenance, high availability, and scaling events;
- 1.2.10 Portal defects and failures (e.g., ION element software, network routing protocol convergence events) that are not based on Prisma SD-WAN;
- 1.2.11 Rightful suspension and/or termination by Palo Alto Networks in accordance with the service agreement.

2. Administration

- 2.1 Notifications.** Customers may, at any time, obtain service status at the Prisma SASE updates page (sase.status.paloaltonetworks.com), which provides region-specific status information, and an alerts feature from which Customers may subscribe to receive service notifications. Palo Alto Networks will use commercially reasonable efforts to provide advance notice of service events.
- 2.2 Eligibility.** To qualify to receive benefits under this Service Level Agreement, the Customer must (a) be in good standing, i.e., the Customer shall not be or have been delinquent in paying service fees; and (b) have onboarded the service for at least fifteen (15) days. This Service Level Agreement does not apply to any trials and/or evaluations provided at no cost to the Customer.
- 2.3 Claims Process.** Customers must have enrolled for an account on the Customer Support Portal in order to open a case and submit a claim. If the Customer believes it is entitled to a service credit, they must open a case on the Customer Support Portal (support.paloaltonetworks.com) within 24 hours of an outage or an incident and request a claim within 5 business days of the outage. When properly submitted, Palo Alto Networks will use commercially reasonable efforts to adjudicate claims promptly. The Customer's failure to request and to respond to other information as required will disqualify the Customer from receiving a service credit. When Palo Alto Networks confirms the claim to be less than the Service Level, then Palo Alto Networks will issue a service credit by applying it against future Service payments due from the Customer. Service credits will not entitle the Customer to any refund or other payment from Palo Alto Networks. When properly submitted, Palo Alto Networks will use commercially reasonable efforts to adjudicate claims promptly: no later than 15 days after the root cause of the outage has been determined and the case closed. Adjudicated claims shall be deemed final and may not be submitted again for reconsideration.

2.4 Service Credit Calculation.

- 2.4.1 Service credits are calculated by multiplying the Service Credit Percentage by the proportional monthly service fee, and further prorated by the part of the service affected by the outage:

Service Credit = $\frac{\text{Service Credit Percentage} \times \text{Monthly Service Fee} \times \text{Service Outage}}{\text{(see table in section 1)} \quad \text{(see 2.4.2)} \quad \text{Total Service (see 2.4.4)}}$

- 2.4.2 The monthly service fee attributable to the service excludes fees arising from collateral services Customers may have purchased such as Professional or Consulting Services, if any. The monthly service fee may be calculated by dividing the one-year service fee by 12, the three-year service fee by 36, etc.
- 2.4.3 For each month, the maximum amount of service credit that Palo Alto Networks shall be liable for is 100% of the monthly service fee paid to Palo Alto Networks.
- 2.4.4 Service Outage and Total Service are measured on a per-Branch basis as experienced by the outage.
- 2.4.5 The service credit will be applied by extending the service subscription term in proportion to the amount of the service credit due to the Customer.
- 2.4.6 The foregoing terms state the sole and exclusive liability of Palo Alto Networks and the Customer's sole and exclusive remedy for any claim of breach of this Service Level Agreement.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
prisma_prisma-sd-wan-service-level-agreement_041425

SERVICE LEVEL AGREEMENT

STRATA LOGGING SERVICE

Palo Alto Networks will use commercially reasonable efforts to make its Strata Logging Service (“Service”) available at least 99% during any calendar month. In the unlikely event that Palo Alto Networks does not meet this service level commitment, Customer will be eligible to receive a service credit as described below.

1. Uptime SLA. If, during any calendar month, the Service availability falls below 99.9%, Customer must submit a claim for credit, calculated as follows:

Strata Logging Service Monthly Uptime Availability	Service Credit Percentage:
Less than 99.9% but equal to or greater than 99%	5
Less than 99% but equal to or greater than 98%	15
Less than 98% but equal to or greater than 97%	25
Less than 97%	100

2. Data Freshness SLA. If, during any calendar month, the average data freshness for the month is greater than 60 minutes, Customer must submit a claim for credit, calculated as follows:

Strata Logging Service Data Freshness	Service Credit Percentage:
Greater than 60 min but less than or equal to 90 min	5
Greater than 90 min but less than or equal to 120 min	15
Greater than 120 min but less than or equal to 150 min	25
Greater than 150 min	100

3. Calculation.

(a) “Monthly Uptime Availability” is calculated by subtracting from 100% the percentage of minutes during any calendar month that the Service is not available, excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice, and taking into account the Exclusions set forth in section 8 below:

$$\text{Availability} = \frac{(\text{Total-Downtime-Excluded})}{(\text{Total-Excluded})} \times 100$$

Total = Total # of minutes in a calendar month.

Downtime* = Time the service was down.

Excluded = Excluded time as specified in section 8 (“Exclusions”).

*Downtime occurs when: (i) the Service is unavailable for ingestion or access and (ii) the Service is unable to forward data to external syslog collectors due to factors caused by the Service infrastructure.

(b) “Data Freshness” is calculated by measuring the average time it takes for ingested data to be available to be viewed or accessed by Customer.

Data Freshness = Total – Excluded

Total = Average time for the month for ingested data to made available

Excluded = Excluded as specified in section 8 (“Exclusions”)

(c) Where an outage gives rise to liability arising from both 3(a) and 3(b) above, Customer shall not be entitled to “double dip” by claiming service credits for such overlap.

4. Eligibility. To qualify to receive benefits under this Service Level Agreement: (a) Customer must be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) Customer must have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to beta, trials and evaluations of the Service provided at no cost to the Customer.

5. Notifications. Customers may, at any time, obtain Service status [here](https://status.paloaltonetworks.com), (<https://status.paloaltonetworks.com>) which provides region-specific status information, and an alerts feature from which customers may subscribe to receive service notifications. Palo Alto Networks will use commercially reasonable efforts to provide advance notice of Service events: (a) three weeks in advance of a planned maintenance; and (b) six hours in advance of an unplanned maintenance.

6. Claims Process. If Customer believes it is entitled to a service credit, it must open a case on the [Customer Support Portal](http://support.paloaltonetworks.com) (<http://support.paloaltonetworks.com>) within 24 hours of an outage; When properly submitted, Palo Alto Networks shall use

commercially reasonable efforts to adjudicate the claim promptly, no later than within 15 days after root cause of the outage has been determined and the case closed. Adjudicated claims shall be deemed final and may be not re-submitted for re-consideration. Note that Customer must have enrolled for an account on the [Customer Support Portal](#) in order to open a case and submit a claim. Customer's failure to request and to respond to other information as required will disqualify Customer from receiving a Service credit.

7. Service Credit. Service credits are calculated as a percentage of the monthly service fees attributable to the applicable Service (excluding fees arising from collateral services Customer may have purchased such as Professional or Consulting Services, if any) and further pro-rated based on the portion of the Service impacted by the outage. For each month, the maximum amount of service credit that Palo Alto Networks shall be liable for is 100% of the monthly service fee paid by Customer; monthly service fee may be calculated by dividing the one-year service fee by 12 or the three-year service fee by 36. If Customer had purchased the Service through an authorized Palo Alto Networks reseller partner, the service credit will be made to the distributor which placed the order for the service. Distributors are responsible for reimbursing the reseller partner which in turn will credit the Customer. If Customer had purchased the Service directly from Palo Alto Networks, then Palo Alto Networks shall issue the service credit towards the renewal of the Service.

8. Exclusions. This Service Level Agreement shall not apply and the Service shall be deemed available where the loss of Service results from:

- a. Customer's equipment, software, technology and/or third-party equipment, software or technology (other than third-party equipment, software or technology under Palo Alto Networks' control);
- b. Failure of Customer's Internet Service Provider, utility companies, or other vendor(s) Customer relies on to access the internet;
- c. Customer mis-configuration of Service features or settings wholly under Customer's control;
- d. Customer's failure to purchase an adequate license to meet the volume or capacity at which it uses the Service, if the Service commitment would have been met if not for such failure;
- e. Planned and unplanned maintenance windows;
- f. High Availability events and scaling events;
- g. Any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties and beyond the control of Palo Alto Networks including, but not limited to, force majeure events;
- h. Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the [Palo Alto Networks End User Agreement](#).

9. Sole and Exclusive Remedy. The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any claim of non-compliance of service level commitment.



CYBERSECURITY
PARTNER OF CHOICE

Service Level Objectives

Last Updated January 25, 2025

Prisma SD-WAN

Palo Alto Networks commits to using commercially reasonable efforts to make the Prisma® SD-WAN portal available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99.9% for the SD-WAN portal service, measured over the calendar month.

SaaS Security

Palo Alto Networks commits to using commercially reasonable efforts to make SaaS Security available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). SaaS Security includes SaaS Inline, SaaS API, DLP Inline, and SSPM. Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99.9%, measured over the calendar month.

WildFire

Palo Alto Networks commits to using commercially reasonable efforts to make the WildFire® malware prevention service available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99.9%, measured over the calendar month.

Cloud Identity Engine

Palo Alto Networks commits to using commercially reasonable efforts to make the Cloud Identity Engine service available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99.9%, measured over the calendar month.

Data Loss Prevention (DLP)

Palo Alto Networks commits to using commercially reasonable efforts to make cloud DLP services available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99.9%, measured over the calendar month.

Remote Browser Isolation (RBI)

Palo Alto Networks commits to using commercially reasonable efforts to make cloud RBI services available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99.9%, measured over the calendar month.

Application Acceleration

Palo Alto Networks commits to using commercially reasonable efforts to make cloud Application Acceleration services available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99.9%, measured over the calendar month.

Strata Cloud Manager

Palo Alto Networks commits to using commercially reasonable efforts to make the Strata Cloud Manager portal available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99% for the Strata Cloud Manager portal service, measured over the calendar month. Note: A customer's data traffic flows to Palo Alto Networks security products is unaffected by Strata Cloud Manager unavailability.

Prisma Access Browser

Palo Alto Networks commits to using commercially reasonable efforts to make Prisma Access Browser services available 24 hours a day, 7 days a week (excluding downtime resulting from any planned outage wherein Palo Alto Networks had provided prior notice or any emergency outage making it impracticable for Palo Alto Networks to issue advance notice). Palo Alto Networks commits to using commercially reasonable efforts to achieve uptime availability of 99.999% for the browser and 99.99% for the management console, measured over the calendar month.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
parent_sb_service-level-objectives_091324

CLOUD NGFW FOR AWS SUPPLEMENTAL END USER SUPPORT AGREEMENT

THIS CLOUD NGFW FOR AWS SUPPLEMENTAL END USER SUPPORT AGREEMENT (THIS “SEUSA”) SUPPLEMENTS AND AMENDS THE PALO ALTO NETWORKS END USER SUPPORT AGREEMENT AVAILABLE AT THE FOLLOWING WEB ADDRESS: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-global-customer-support-services-terms-and-conditions-eusa.pdf (THE “EUSA”). THIS SEUSA FORMS A LEGALLY BINDING AGREEMENT BETWEEN YOU AND PALO ALTO NETWORKS, INC., INCLUDING ITS AFFILIATES.

This SEUSA sets forth the supplemental terms and conditions under which Palo Alto Networks will provide technical support services for the Cloud NGFW for AWS products sold and/or licensed pursuant to the End User Agreement. In the event of a conflict between this SEUSA and the EUSA or End User Agreement, this SEUSA shall take precedence, but only with respect to the subject matter described below.

1. SUPPORT PLANS AND SERVICES OFFERED

		Standard Digital	Premium Digital Plus
	Digital Experience Product Documentation Proactive Notifications Access to communities		
	Digital Force Chat Support ¹ Community Support Customer Support Portal Phone Support ² Premium SLO		SL: 1hr, S2:4hr
	Digital Training Access to online training		

¹Community Support will be moderated by Palo Alto Networks on a commercially reasonable effort basis
²For Premium, phone support will be through callback provided by TAC

AIOps for NGFW Supplemental End User Support Agreement

THIS AIOps for NGFW Supplemental End User Support Agreement (THIS “SEUSA”) SUPPLEMENTS AND AMENDS THE PALO ALTO NETWORKS [END USER SUPPORT AGREEMENT](#) (THE “EUSA”). THIS SEUSA FORMS A LEGALLY BINDING AGREEMENT BETWEEN YOU AND PALO ALTO NETWORKS, INC., INCLUDING ITS AFFILIATES.

This SEUSA sets forth the supplemental terms and conditions under which Palo Alto Networks will provide technical support services for AIOps for NGFW products sold and/or licensed pursuant to the End User Agreement. In the event of a conflict between this SEUSA and the EUSA or End User Agreement, this SEUSA shall take precedence, but only with respect to the subject matter described below.

1. SUPPORT PLANS AND SERVICES OFFERED

		Standard
	Digital Experience	Product Documentation Access to communities
	Digital Support	Community Support ¹
	Digital Training	Access to online training

¹ Community support will be moderated by Palo Alto Networks on a commercially reasonable efforts basis.



PREMIUM / PLATINUM WITH AUTOMATION SUPPORT SUPPLEMENTAL END USER SUPPORT AGREEMENT (“SEUSA”)

THIS PREMIUM / PLATINUM WITH AUTOMATION SUPPORT SEUSA SUPPLEMENTS AND AMENDS THE PALO ALTO NETWORKS [END USER SUPPORT AGREEMENT](#) (THE “EUSA”). THIS SEUSA FORMS A LEGALLY BINDING AGREEMENT BETWEEN YOU AND THE APPLICABLE PALO ALTO NETWORKS ENTITY PURSUANT TO THE EUSA. This SEUSA sets forth the supplemental terms and conditions under which Palo Alto Networks will provide technical support for issues related to Software Firewall Orchestration Hub used for Palo Alto Networks VM-Series firewalls. If Your issue is related to the Palo Alto Networks VM-Series firewalls but not the automation scripts, this SEUSA does not apply to You. Capitalized terms not otherwise defined herein shall have the meaning set forth in the EUSA. In the event of a conflict between this SEUSA and the EUSA, this SEUSA shall take precedence, but only with respect to the subject matter described below.

1. Sections 1 and 2 of the EUSA are replaced with the following:

	PREMIUM WITH AUTOMATION SUPPORT	PLATINUM WITH AUTOMATION SUPPORT
Online Support	Yes	Yes
Telephone support	No	No
Initial Response Time	PREMIUM WITH AUTOMATION SUPPORT	PLATINUM WITH AUTOMATION SUPPORT
Severity 1 – Critical Product is down, critically affects Customer production environment. No workaround available yet.	24 Business Hours	24 Business Hours
Severity 2 – High Product is impaired, Customer production up, but impacted. No workaround available yet.	48 Business Hours	48 Business Hours
Severity 3 – Medium A Product function has failed, Customer production not affected. Support is aware of the issue and a workaround is available.	48 Business Hours	48 Business Hours
Severity 4 – Low Non-critical issue. Does not impact Customer business. Feature, information, documentation, how-to and enhancement requests from Customer.	48 Business Hours	48 Business Hours

2. “Business Hours” mean Mondays through Fridays, 9:00 am - 6:00 pm CET (GMT-2), excluding local holidays.