

Attachment G – Custom Cloud Services

AT&T offers a variety of cloud based solutions that are custom developed to your specific requirements. AT&T and your team will meet to assess your requirements and qualify the applications of these solutions to develop the Scope of Work for these services.

Cloud based Fax

AT&T can provide a full suite of cloud based fax services. We support our offer with live 24x7x365 engineering support. Our product services include:

- **Desktop Fax** – Fax-to-Email/Mail2Fax – send and receive faxes from your desktop
- **Fax for Notes/Exchange** – Integrated faxing solutions for your email client
- **Fax for SAP®** – Certified SAP® integration that requires no hardware or software
- **Fax for Applications** – send and receive faxes in production environments

Virtual Meeting Room

Virtual Meeting Room (VMR) Collaboration Services consolidate real-time conferencing tools (voice, video and web) into a single solution, allowing users to connect anytime, anywhere with virtually any device. The suite of vendor-agnostic VMR solutions are designed to meet unique consumption and architectural needs.

- Connect standards-based and software-based clients into one call
- No reservation needed; similar to making an audio call
- Available 24/7/365
- Interoperable with H.323, SIP, Microsoft Lync, WebRTC and audio

Whether in the office or on the go, join meetings anytime, anywhere from any device. Connect from virtually any device

- Video endpoint
- Desktop/laptop
- Tablet
- Smartphone
- Office phone

AT&T Synaptic Storage as a ServiceSM

A highly reliable, virtualized file-store that provides elastic data storage capacity on demand. It easily scales up and down to any size, allows customers to pay only for the storage used, requires no commitments, minimums or limits, and can be accessed by authorized users from virtually anywhere, anytime, via a web services interface via the EMC Atmos™ REST API. Developers can use this API to connect to virtually any internal or external web services application. Additionally, a variety of third-party software vendors called “Cloud Solution Providers” have created products that integrate the API and enable common IT “use cases” such as data backup, archival, image management, file shares and more.

AT&T Synaptic Storage as a Service with Enterprise File Sync and Share

AT&T Synaptic Storage with Enterprise File Sync and Share is an enterprise-grade file sync and share solution that gives users access to their files, on supported devices, online or offline. By combining a highly secure file sync with a mobile and web experience, users can access business files and automatically share inside or outside the organization.

AT&T Remote Back Up as a Service

AT&T Enterprise Remote Backup as a Service is an easy to use, easy to measure, backup service that you consume on a protected per GB cost basis. With AT&T Enterprise Remote Backup as a Service, backing up your company's data is simple. Just identify the computer systems you want to protect, choose how long the backup data should be retained, and AT&T does the rest. Ours is a cloud-based backup and recovery for business continuity and protection providing backup for desktop/laptop and remote Offices. This is a single, scalable solution from edge to data center

- Backup and recovery protection for VMware, Servers, NAS, Applications and Desktop/Laptop managed as a service in an on-demand OPEX model.
- Self-service options for IT managers and desktop/laptop file recovery.

AT&T Threat Manager – with Advanced Log Management

AT&T Threat Manager – with Advanced Log Management provides comprehensive threat identification and log management capabilities for our Enterprise customers. Threat Manager—with Advanced Log Management provides expert security incident and event management (SIEM) via the AT&T Security Operations Center (SOC), a state-of-the-art facility that identifies and works to resolve network security issues. The AT&T SOC uses advanced, industry-leading analysis tools, including an integrated data mining system developed at AT&T. This system provides an additional layer of anomaly detection algorithms to produce rich, correlated alerts. The SOC monitors your network 24x365 to help identify both active threats and precursors to network attacks. We notify you of incidents—depending on their severity—via phone, email, or the AT&T Security Center portal.

Threat Manager—with Advanced Log Management uses a proactive approach to help you identify, detect, and repel attacks and intrusions before they damage your business. We collect, correlate, analyze, interpret, and communicate information to you in near real time and according to your priorities. In addition, we look for traffic pattern anomalies to pinpoint possible attacks in the early stages.

Key features include:

- 24x7 access to Security Analysts in our Security Operations Center
- Customer-specific alerting strategies
- Broad vendor device support
- Three-way correlation of syslog data for threat identification
- Asset inventory feature to track devices reporting into the service
- Easy-to-use portal with:
 - Customizable dashboards
 - Comprehensive reporting
 - Hierarchical access

Web Security

This Web Security solution is a part of a scalable global Security as a Service platform that sits in-line between the Customer and the Internet, to assist in protecting your enterprise from cyber threats, stopping intellectual property leakage and providing a compliance avenue with corporate policies and statutory regulations. This Web Security solution scans incoming and outgoing Internet traffic irrespective of device or location, providing comprehensive security and compliance. Web Security protects from a broad range of web security threats including malicious URL requests, viruses, advanced persistent threats, adware, spyware, botnets, cross-site scripting and more. The features include:

- **URL Filtering** - Enables organizations to limit their exposure to liability by managing access to web content for users, groups and locations. URLs are filtered by global reputation – against more than 90 categories, 30 super categories, and 6 classes.
- **Cloud Application and Social Media Control** - Leverage the power of cloud applications and social media without compromising productivity or security. Now, IT teams can easily create granular global policies—based on users or groups—for webmail, streaming media, social networking and IM.
- **Bandwidth Control** - Easily and efficiently allocate bandwidth to prioritize business critical web applications over recreational usage.
- **Inline Threat Protection** - Context-aware security scans every byte of inbound/outbound traffic to secure devices, users, data and web applications against advanced security threats. Inline ByteScan™, full SSL scanning and Cloud Intelligence protects against botnets, malicious active content, phishing, XSS attacks and more.
- **Behavioral Analysis** - Provides non-signature based protection against zero day exploits. By executing suspicious binary files in a sandbox, malicious content can be identified even if the sample has never been previously observed. The cloud model ensures that when a file is identified, users across the entire network are immediately protected.
- **Unified Policy and Reporting** - Delivers one, unified console to create web policy across security, Internet access management and data loss prevention. Administrators manage their own policy—with changes instantly reflected across the entire cloud. The administrative portal also provides a single pane of glass to view and analyze all traffic across all devices and locations in real time.

Vulnerability Scanning Service (VSS-PRO)

The VSS-Pro service is used to conduct host discovery and/or vulnerability scans on external and/or internal IP-based systems and networks. A variety of scanning techniques are employed to survey the security posture of the target IP-based systems and networks. External scanning addresses all Internet-facing assets such as routers, firewalls, web servers, and e-mail servers for potential security weaknesses. Internal scanning addresses all internal assets such as workstations, intranet servers, and printers for Trojans, improper configurations, peer-to-peer (PTP) file sharing programs and more. The VSS-Pro service also provides workflow management, host-based risk assignments, and remediation progress reporting. In addition to the portal view, critical vulnerabilities that are identified are forwarded on a regular basis to the AT&T Threat Manager for correlation with other events within the network.

Security Education (SecurED)

SecurED is a security training package that will help organizations build a "Culture of Security." SecurED training modules which are brief, engaging and cost effective can be viewed the training modules on their PC, laptop, iPad/tablet or mobile device. Social Engineering, system issues and employee and third party negligence are all contributing factors to security breaches. In addition to the precautions that organizations take to protect their networks from attack, it is essential that they effectively educate their employees to fend off the attacks which target employee vulnerabilities. The modules you receive will address the following key concerns of every organization no matter how large or small:

- Onsite Social Engineering
- Password Development & Security
- Remote Social Engineering
- Social Media Dangers
- Acceptable use of Computer Systems
- Physical Security & Removable Media
- Mobile Device Security
- Installing Software from Unknown Sources
- Using Cloud Services Safely
- Preventing Virus & Malware Outbreaks
- Safe Web Browsing Habits
- Keeping Information Safe via Sensitivity Marking



AT&T Threat Manager—with Advanced Log Management

Protect your network with a cloud-based security solution that has a low cost of ownership.

Description

AT&T Threat Manager—with Advanced Log Management is a managed security service that helps you protect your business and reduce risks by analyzing data from your in-scope network devices and issuing alerts. Threat Manager—with Advanced Log Management provides expert security incident and event management (SIEM) via the AT&T Security Operations Center (SOC), a state-of-the-art facility that identifies and works to resolve network security issues.

The AT&T SOC uses advanced, industry-leading analysis tools, including an integrated data mining system developed at AT&T. This system provides an additional layer of anomaly detection algorithms to produce rich, correlated alerts. The SOC monitors your network 24x365 to help identify both active threats and precursors to network attacks. We notify you of incidents—depending on their severity—via phone, email, or the AT&T Security Center portal.

Threat Manager—with Advanced Log Management uses a proactive approach to help you identify, detect, and repel attacks and intrusions before they damage your business. We collect, correlate, analyze, interpret, and communicate information to you in near real time and according to your priorities. In addition, we look for traffic pattern anomalies to pinpoint possible attacks in the early stages.

How Does It Work?

AT&T offers several Threat Manager—with Advanced Log Management service options, so we can tailor the service to your needs. Options include premium or standard installation, host or security device types, ThreatWatch, compliance reports, additional collector pairs, deployment outside the U.S., and virtual collectors.



Needs

You've told us you have the following needs:

- **Security**—help protect sensitive data vital to the organization. You need to help strengthen your security posture by using a proactive approach against Internet-based attacks.

Features and Benefits

AT&T Threat Manager—with Advanced Log Management gives you these features:

- **Client Web Portal**—provides security event data, alerts, logs, scan vulnerabilities, and external threat intelligence that help you understand risks. Compliance-specific dashboards give you reports and information on compliance gaps and recommended actions. Portal access is encrypted and uses multi-factor security features, and you can define layered access roles. So, you get a highly secure, customizable portal that provides a centralized, holistic view of your organization's network security from multiple sources of potential risk.
- **Vulnerability Scanning**—uses NexPose Rapid 7 scanning technology and displays the results in the client portal. And, because it contributes to the correlation engine, the scan data increases the usefulness and accuracy of the service's security alerting and monitoring capabilities.
- **Threat Center (Alert Analysis)**—provides full, real-time alert monitoring. The service assigns a severity ranking to all alerts and prioritizes them on the client web portal. You can view alerts in table, chart, or trend graph format. And, security incident notifications are available for immediate viewing, so you can keep current on your security status.
- **Log Management**—lets you run standard reports, create custom reports, sift through log events based on trend graphs, and more. We use column-oriented database technology, so you can search records more quickly.
- **Custom Zones**—enable you to logically group data from the client web portal. Zones may include devices or systems like IP addresses, host names, system descriptions, locations, and asset profiles (in which you define asset importance level). Consequently, custom zones let you define and represent areas of your system that you'd like to collect information about, such as compliance requirements (e.g., PCI, GLBA, HIPAA, or SOX), network areas (e.g., external, perimeter, internal, or VLANs), or functional areas (e.g., bank tellers, POS systems/users, or accounting department staff).



- **Integrated Help Desk**—provides call ticket tracking, event and incident triage, technical support, escalations, and more. So, you can get instant status on all open issues and interact further with the technical staff assigned to your case.
- **Threat Research**—is available via the client web portal. You can view RSS feeds from top information sources on current security issues and news. In addition, you can research threats, obtain helpful information from the Common Vulnerabilities and Exposures (CVE) system and BUGTRAQ, and more. These resources help you stay up to date with current intelligence on security threats, events, and trends.
- **Change Management**—can track all configuration changes to the system. Depending on your requirements, we can track these changes via an IT service management (ITSM) system or a Tripwire configuration. In addition, the solution can provide asset management data from the monitoring system that can populate most asset management systems. This means that we support a formalized change management system that can track all change requests, change approval routing, and support audit tracking for compliance purposes.
- **Flexible Device Support**—is possible because we can easily define—via the Regular Expressions (RegEx) programming language—how the event correlation system receives and processes logs. As a result, we can collect log data from various databases, and we can support almost any device as long as it can produce log data in a file or another accessible output.

Customer Applications

Following are some ways you might use AT&T Threat Manager—with Advanced Log Management:

- **IT Services Protection**

You provide IT services to your customers throughout the state who want to take advantage of your advanced network and economies of scale. However, because your network is so large, it's a likely target for Internet-based attacks. You want to strengthen your network security for the sake of your customers and reduce risk.

To better protect your network and your customers' data, we suggest a proactive security approach using AT&T Threat Manager—with Advanced Log Management.



Threat Manager—with Advanced Log Management can help you to be more aggressive against threats. We correlate data collected from in-scope devices across your network so you get a broad, rich view into your environment.

This broader context and deeper insight helps strengthen your security posture, allowing you to identify more patterns, trends, anomalies, and threats. In addition, you get fast remediation when problems appear.

Diagrams

- **Client Web Portal Home Dashboard**



This screenshot depicts the home dashboard.

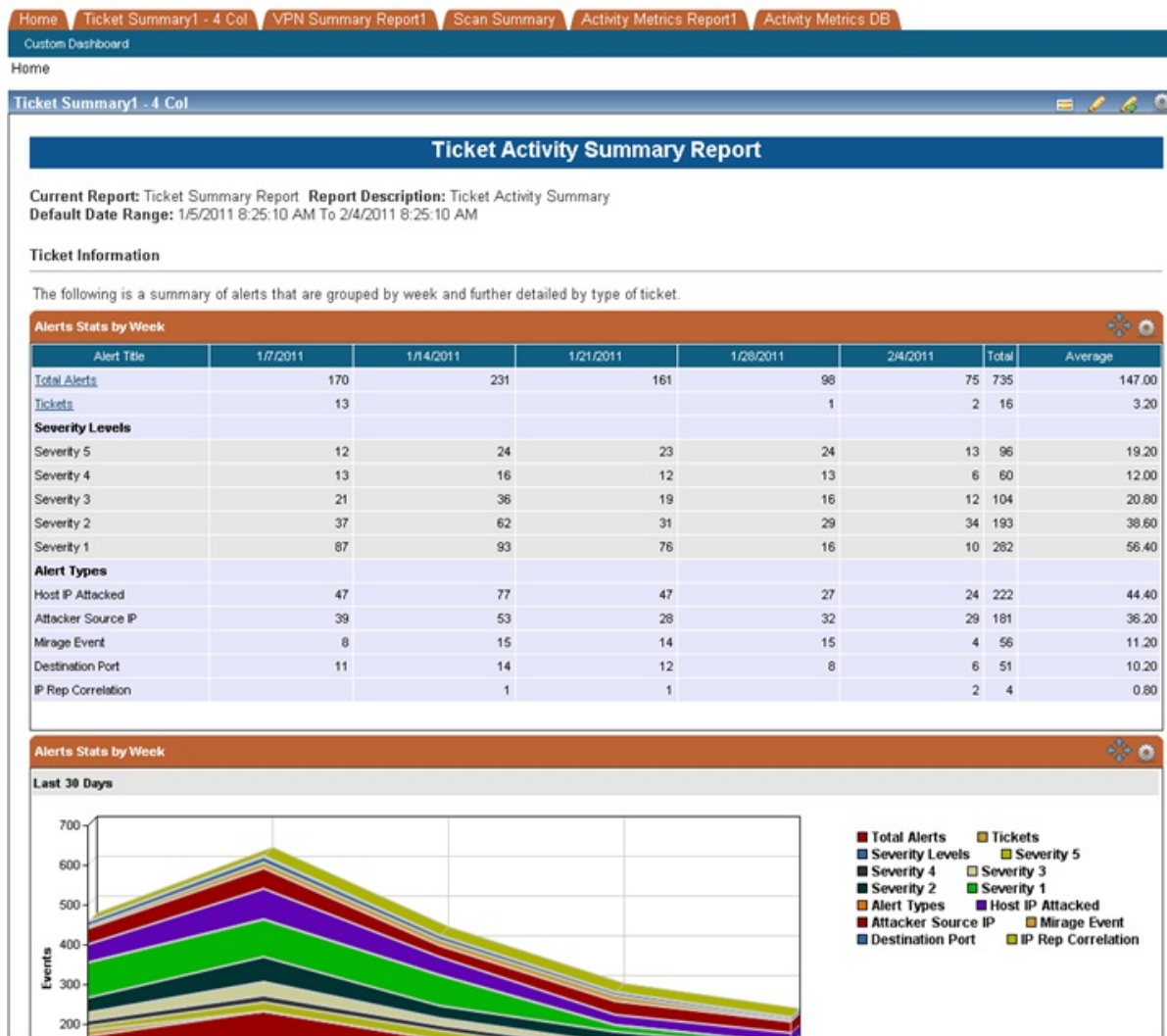


- Client Web Portal Seven Day Alert Trend Page



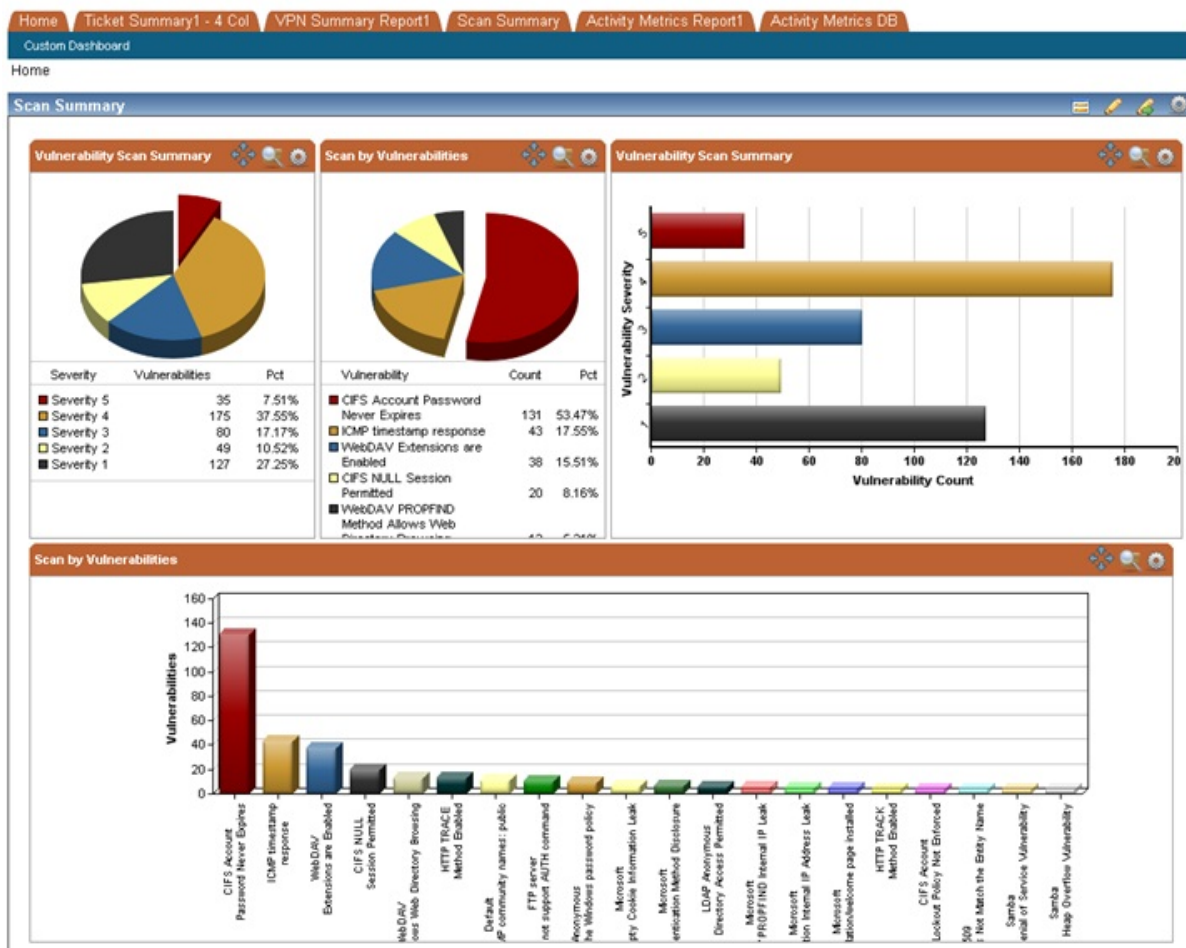
This screenshot depicts some of the alerts you can view on the portal.

- Client Web Portal Ticket Activity



This screenshot depicts how the portal summarizes all support calls and alerts during a time period that you specify.

- Client Web Portal Scan Summary Dashboard



This screenshot depicts scan results information on the portal.

Important Information

Subsidiaries and affiliates of AT&T Inc. provide products and services under the AT&T brand. © 2016 AT&T Intellectual Property. All rights reserved. AT&T, the Globe logo, and other marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. The contents of this document are proprietary and confidential and may not be copied, disclosed, or used, in whole or in part, without the express written permission of AT&T, except to the extent required by law and insofar as is reasonably necessary in order to review and evaluate the information contained herein.