

Solution highlight: User Interface Logging and Field Masking Solutions by SAP

Erin Hughes, SAP

May 19, 2020

Your speakers today



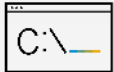


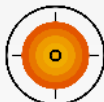








Erin Hughes
Cybersecurity Solution Advisor
SAP

Key Takeaways

- Understand why data masking plays a key part in an overall data security strategy.
- Discover how the UI masking solution can help protect data based on configurable attributes and rules.
- Learn how the UI logging solution complements the UI masking solution by providing a way to record and analyze data that has been displayed in SAP.

Security challenges are evolving

	Historical IT Security Perspectives	Today's Leading Cybersecurity Insights
Scope of the Challenge	 <p>Limited to your “four walls” and extended to the enterprise</p>	 <p>Spans your interconnected global and business ecosystem</p>
Ownership and Accountability	 <p>IT led and operated</p>	 <p>Business-aligned and owned; CEO and board driven</p>
Adversaries' Characteristics	 <p>One-off and opportunistic; motivated by notoriety, technical challenge and individual gain</p>	 <p>Organized, funded and targeted; motivated by economic, monetary and political gain</p>
Information Asset Protection	 <p>One-size-fits-all approach</p>	 <p>Prioritize and protect the “crown jewels”</p>
Defense Posture	 <p>Protect the perimeter; respond if attacked</p>	 <p>Protect the application and data yet plan for a breach, monitor and rapidly respond</p>
Security Intelligence and Information Sharing	 <p>Keep to yourself</p>	 <p>Public/private partnerships; collaboration with industry working groups</p>

Global data protection regulations are expanding

Data protection regulations vary globally and are extending their reach

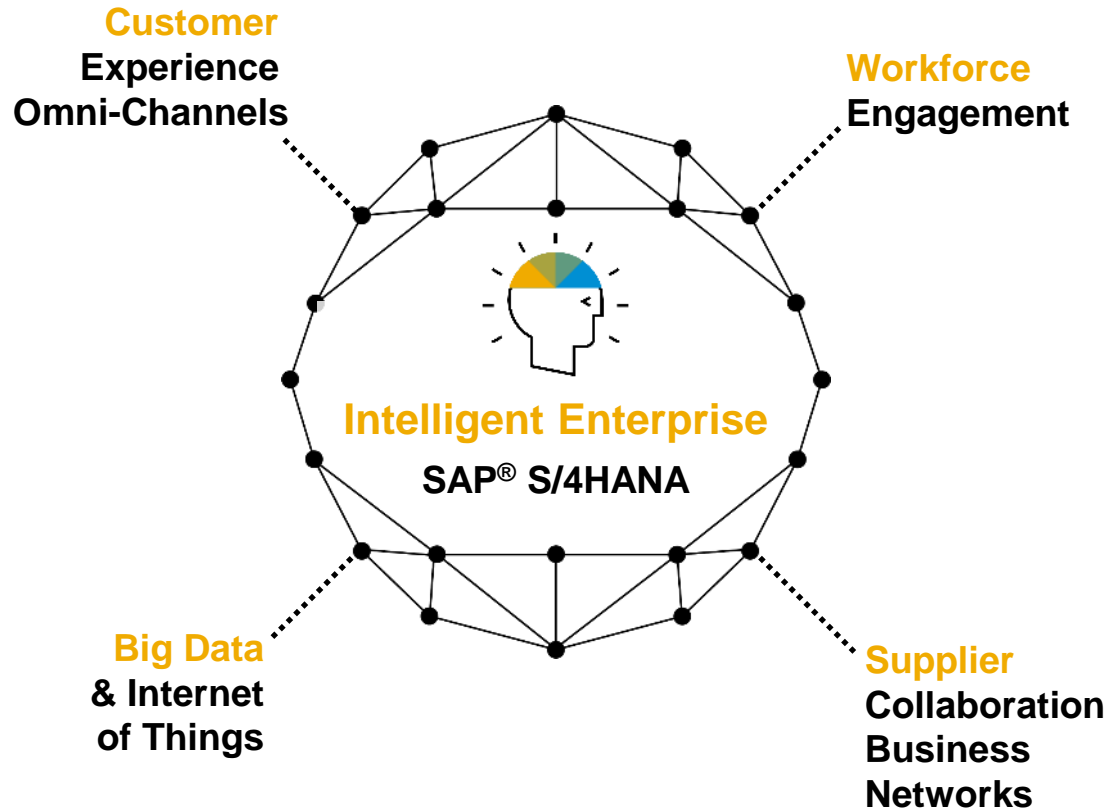
Global data protection regulations impact cloud vendors and customers

Country	Regulations
USA	USA Patriot Act, Stored Communications Act, EU-US Privacy Shield, California Consumer Privacy Act – 2020
EU	EU Data Protection Directive replaced in 2018 by the EU General Data Protection Regulation (GDPR) – privacy laws in 28 countries
Germany	Federal Data Protection Act (FDPA)
Brazil	General Data Protection Law (LGPD) – 2020
Australia	Privacy Act 1988, Australian state and territory legislation
Singapore	The Personal Data Protection Act (PDPA)
Canada	Personal Information Protection Act (PIPA), Personal Information Protection and Electronic Documents Act (PIPEDA), Freedom of Information and Protection of Privacy Act (FIPPA)
Russia	Federal Law No. 152-FZ on Personal Data



SAP helps build Digital Trust in digital transformation

Effectively manage cybersecurity and data protection risk



Digital transformation requires security to be smarter, automated, and embedded

- 1 Security role design and governance** must be considered early on to minimize cross-system risk and insider threats
- 2 Systems and applications** must be monitored and maintained to minimize vulnerabilities and protect against data loss
- 3 Manual controls and checks** must be replaced with smarter, AI-driven controls to identify anomalies and potential issues early on
- 4 Digital automation** requires even more reliable and effective monitoring of transactions and processes as human intervention is minimized

Data security: What it's all about

Privacy controls and security should be baked in



Privacy by design

- Include privacy risk in security risk assessments
- Incorporate data privacy in information security policies
- Maintain procedures to restrict access to personal data – segregation of duties and roles
- Enable identity management and customer identity management processes



Data security

- Maintain technical security measures
- Maintain measures to encrypt personal data
- Secure and track access to specific application fields



Data loss prevention

- Maintain a data loss prevention strategy
- Classify and distribute policies
- Conduct testing of security posture
- Maintain security certification
- Maintain business continuity plans

Agenda

1

What

Solution
overview

2

When

Use cases

3

Where

Architecture and
availability

4

Next Steps

Agenda

1

What

Solution
overview

2

When

Use cases

3

Where

Architecture and
availability

4

Next Steps

Key business requirements

1

Reliable control who gets sensitive information displayed in SAP transactions and applications, in a quick and low-effort fashion

2

Introduce a *dynamic* determination of data access authorizations based on the context, at runtime

3

Increase protection of sensitive data against theft and abuse where access must be provided to privileged insiders

4

Detect potentially problematic access to sensitive data rapidly (in near-real time), and conduct a meaningful analysis in order to take the right actions

5

Better comply with business or legal requirements for tracking who accessed sensitive data (PII, BOMs, prices, customer information)

UI Data Security: two step approach to protect data from insiders

UI Masking



to **conceal specific data** (values in fields/columns) – **unless required for tasks**

The solution masks sensitive (configured) values **per default**; unmasking requires **explicit access rights** (on top of existing role/authorization setup)

→ make **data elements unavailable** for data abuse (opportunistic and targeted)



“the speed limiter”

UI Logging



to **keep data accessible**, but **log & analyze access**, to identify adequate path of action

The solution provides a **detailed, structured data access log and allows for analysis** who exactly received which data (output), how (input), and in which context (IP...)?

→ **prevent illegitimate data access and theft** by inducing compliant behavior

→ **identify & prove** irregular data access



“the speed camera”

- awareness for data security (“human firewall”) → protect employees by decreasing inadvertent breaches
- top-of-class protection measures → **trust** (employees, customers, and investors)

Agenda

1

What

Solution
overview

2

When

Use cases

3

Where

Architecture and
availability

4

Next Steps

Sample use cases

- **Prevent theft of massive amounts of data** by masking mass access (e.g. from SE16n, and similar transactions, reports)
- **Protect IP in BOMs** (=recipes)
- **Mask specific fields in HR** to protect sensitive private data; specifically Social Security Number
- Mask **pricing/costing information** (conditions, end prices, resulting price list) to avoid leaking to customers/vendors
- **Mask customer data & pricing/costing information** (conditions, end prices, resulting price list) for 3rd parties (usually partners/vendors) working in the system
- “**Divestiture**” – company split or spin offs: virtually segregate data access until systems are physically separated/split
- **Mask data for external/temporary roles** (e.g. call center: show only what is required for the task; e.g. only last names, only parts of identifying numbers like bank accounts, telephone and customer numbers)

UI Masking



... conceal specific data (values in fields/columns) – unless required for tasks

Data masking at the UI layer on server side

- data pseudonymization and anonymization
- business and technical transactions
- restriction of data processing (display, change)
- Compliant data transfers (download, export, print)

Highly configurable – define:

- Which screen fields will appear masked to unauthorized users
- Which users should receive unmasked data for a given field
- When an access trace will be written on access
- Additional logic through BADIs provided by the solution

Based on **SAP NetWeaver** releases 7.00 – 7.50

Maintenance: planned until 31.12.2025

Role based masking



UI Masking

Example: Role based masking



1. Define fields to be masked, and rules

- Define which field are masked.
- Configure on field level how a field is displayed. Define on digit base whether and how data are masked.

The screenshot shows the 'Change View "Maintain Masking Configuration": Details' dialog. It includes a 'Dialog Structure' tree on the left with 'Maintain Masking Configu' expanded. The main area is divided into sections: 'General Details' with fields for 'Table Name' (FA0002) and 'Field Name' (ENDDA), a 'Role' dropdown set to '/UIM/PFCG_ROLE', and checkboxes for 'Masking Control Indicator' (checked) and 'Field Is HR Relevant' (unchecked). The 'Masking Approach' section has 'Hook Point Approach' selected. The 'Masking Pattern' section contains a table with columns 'Position' and 'Masking Character(s)', and three rows labeled 'Set 1', 'Set 2', and 'Set 3'. A 'Mask Override' checkbox is at the bottom.

2. Register authorized users per field

- In transaction PFCG, assign users to the UI Masking authorization a role.
- Users assigned to these roles will be able to see unmasked values for the applicable fields
- BAdIs available to introduce customized business logic determining who has access

The screenshot shows the 'Change Roles' dialog. The 'Role' field is set to 'ZKR_TAXID' with a description of 'KR TAXID Role'. Below this, there are tabs for 'Description', 'Menu', 'Authorizations', 'User', and 'Personalization'. The 'User' tab is active, showing a 'User Assignments' table. A red arrow points to the 'Role' field, and another red arrow points to the 'User Assignments' table.

User ID	User name	From	to	I
I804587	Ted Sohn	26.11.2011	31.12.9999	I

UI Masking

Example: Role based masking

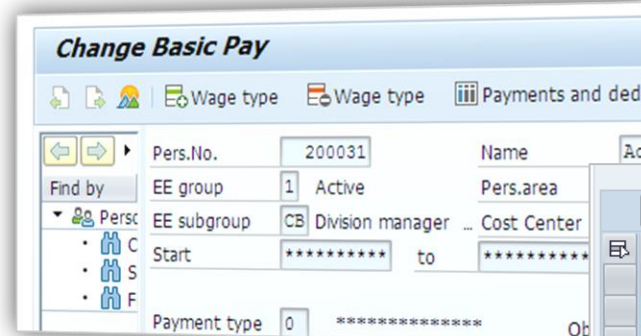


3. Result: data masking

Data is masked in GUI transaction display for un-authorized users.

This also affects high-level “admin” system users (in dynamic transactions, e.g. SE11, SE12, SE16, SE16n) – unless they are explicitly authorized for a field

UI Masking also protects data during download, export, and print



PersNo.	STY	ObjID	LI	End Date	Start Date	RNo	UtilLvl
10154	&			*****	*****		100,00
10155	&			*****	*****		100,00
10270	&			*****	*****		100,00
10271	&			*****	*****		100,00
10451	&			*****	*****		100,00
10451	&			*****	*****		100,00
10452	&			*****	*****		100,00
10452	&			*****	*****		100,00

Data Browser: Table PA0008 Select Entries 20

Table: PA0008
Displayed Fields: 34 of 284 Fixed Columns:

MANDT	PERNR	SUBTY	OBJPS	SPRPS	ENDDA	BEGDA	SEQNR	AEDTM
300	00010154	&			*****	*****	000	12.03.
300	00010155	&			*****	*****	000	12.03.
300	00010270	&			*****	*****	000	12.03.
300	00010271	&			*****	*****	000	12.03.
300	00010451	&			*****	*****	000	14.03.

pa0008.txt - Notepad

MANDT	PERNR	SUBTY	OBJPS	SPRPS	ENDDA	BEGDA	SEQNR	AEDTM	UNAME	HISTO	ITX
300	10154	&			*****	*****				12.03.2002	
300	10155	&			*****	*****				12.03.2002	
300	10270	&			*****	*****				12.03.2002	
300	10271	&			*****	*****				12.03.2002	
300	10451	&			*****	*****				14.03.2002	

C2

	A	B	C	D	E	F	G
	PERNR	SUBTY	ENDDA	BEGDA	AEDTM	DIVGV	ANSAL
2	10154	&	*****	*****	12.03.2002	86,67	*****
3	10155	&	*****	*****	12.03.2002	173,6	*****
4	10270	&	*****	*****	12.03.2002	86,65	*****
5	10271	&	*****	*****	12.03.2002	86,65	*****
6	10451	&	*****	*****	14.03.2002	81,25	*****
7	10451	&	*****	*****	15.03.2002	81,25	*****

UI Masking Access trace

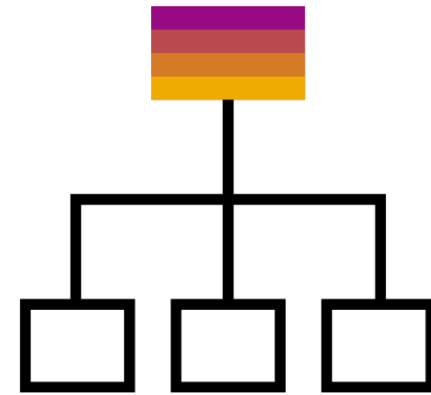


Display and Delete Field Access Trace

Date	Time	User Name	IP address	TCode	Program	Screen	Table	Field	Fld Value	Free Text	Auth Ind
10.01.2018	09:55:48	KELLERTO	10.18.161.164	PA30	MP000800	300	Q0008	BETRG			
10.01.2018	09:56:44	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	AEDTM			
10.01.2018	09:56:44	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	ANSAL			
10.01.2018	09:56:44	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	PERNR			
10.01.2018	09:57:18	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	AEDTM			
10.01.2018	09:57:18	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	ANSAL			
10.01.2018	09:57:18	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	PERNR			
10.01.2018	09:57:46	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	AEDTM			
10.01.2018	09:57:47	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	ANSAL			
10.01.2018	09:57:47	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	ENDDA			
10.01.2018	09:57:47	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	PERNR			
10.01.2018	10:30:57	KELLERTO	10.18.161.164	PA30	MP000800	300	Q0008	BETRG			
22.01.2018	10:36:25	KELLERTO	10.18.161.164	PA30	MP000800	300	Q0008	BETRG			
22.01.2018	10:47:26	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	AEDTM			
22.01.2018	10:47:26	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	ANSAL			
22.01.2018	10:47:26	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	ENDDA			
22.01.2018	10:47:26	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	PERNR			
23.01.2018	10:14:19	KELLERTO	10.88.6.151	PA30	MP000800	300	Q0008	BETRG			
24.01.2018	18:01:35	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	AEDTM			
24.01.2018	18:01:36	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	ANSAL			
24.01.2018	18:01:36	KELLERTO	10.18.161.164	SE16N	RK_SE16N	100	PA0008	PERNR			
24.01.2018	18:01:38	KELLERTO	10.18.161.164	SE16N	RK_SE16N	200	PA0008	ANSAL			
24.01.2018	18:01:38	KELLERTO	10.18.161.164	SE16N	RK_SE16N	200	PA0008	ANSAL			

- UI Masking trace functionality gives an overview which data were requested per user, and what information was actually displayed.
- Always, never, only if unmasked
- UIM trace functionality is not comparable to the UI Logging log file. UI Logging is far more detailed, contains context and meta data of the access, and thus is an excellent basis for meaningful analysis of data access.

Attribute based masking



UI Masking

Example: Attribute based

Change Personal Data

Pers.No. 69 Age 31
 EE group 1 Active Pers.area 200 Corporate - United Kingdom
 EE subgroup GC Salaried
 Start 31.05.2018 To 31.12.9999 Chng 26.04.2019 KELLERTO

HR data

Natl.ins.no. ***** Gender Male Female
 Language EN English
 Birth date ***** Birthplace *****
 Nationality IN Indian
 Mar.status Marrd. Since 01.01.2010 No. child. 1

Change Personal Data

Pers.No. 71 Age 51
 EE group 1 Active Pers.area 200 Corporate - United Kingdom
 EE subgroup GC Salaried
 Start 09.09.1967 To 31.12.9999 Chng 28.02.2019 KELLERTO

HR data

Natl.ins.no. ***** Gender Male Female
 Language EN English
 Birth date ***** Birthplace Atlan***
 Nationality AZ Azerbaijani
 Mar.status Divor. Since No. child.

The state of the attribute “marital status” (“family status”) determines whether and how the place of birth value is treated.

The logic is configured in “policies”, which are highly versatile and enable more differentiated treatment of field values based on additional attributes – pertaining to the user (e.g. HR employee associated to the company code), the data object ((e.g. employee older than 65 years), or other system-borne as well as external variables.

Data Browser: Table PA0002 Select Entries 500

MANDT	PERNR	BEGDA	ENDDA	SECNR	FAMST	GBORT	NACHN	VORNA	GBDAT
700	00000002	01.01.1970	31.12.9999	000			Jp	Test	19700101
700	00000010	22.05.1967	31.12.9999	000	0		Bond	James	19670522
700	00000069	01.01.1956	30.05.2018	000	1		Holder	XYZ	19450119
700	00000069	31.05.2018	31.12.9999	000	1	*****	Verma	Arun	19880418
700	00000070	01.01.1921	31.12.9999	000	0		Broughton	Beryl	19210101
700	00000071	09.09.1967	31.12.9999	000	3	*tiantis	Hil	Harry	19670909
700	00000072	08.09.1965	31.12.9999	000			Fish	Freda	19650908
700	00000073	09.09.1956	31.12.9999	000			Mustard	Colman	19560909
700	00001000	05.09.1960	04.10.2006	000		*****	Müller	Anja	19600905
700	00001000	05.10.2006	31.12.9999	000		*****	Müller	Anja	19600905
700	00001001	05.06.1960	31.12.9999	000		*****	Mäer	Michaela	19600705
700	00001002	05.09.1960	31.12.9999	000	7	*****	Zaucker	Ulrike	19600905
700	00001003	09.06.1970	31.12.9999	000	3	*rankfurt	Pfandili	Stefan	19600609
700	00001004	01.01.1994	31.12.9999	000	6	*****	Paulsen	Olaf	19651012

UI Masking

Example: Attribute based

The screenshot shows the SAP Shop interface. At the top, there's a navigation bar with 'Shop' and a search icon. Below it, a 'Standard' dropdown and a shopping cart icon with '2' items. The main content area is titled 'Products (123)' and includes buttons for 'Add to Cart', 'Show Items', and sorting options. A list of products is displayed with columns for Name, Description, Average Rating, and Price. Two product entries are highlighted with a blue box, showing their names, descriptions, ratings, and prices. The product names and descriptions are masked with asterisks.

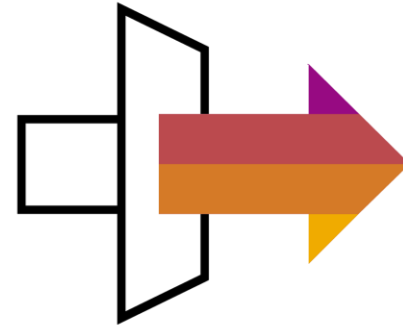
VBAK: Display of Entries Found

Sales Doc.	Created By	Net value	Curr.	Sold-To Pt	Cost Ct
4969	****	5.500,00	EUR	1390	
4970	****	32.838,00	EUR	1175	
4971	****	*****	EUR	1001	
4972	*****	28.604,00	EUR	2200	
4973	*****	*****	EUR	1033	
4974	*****	46.686,00	EUR	2140	
4975	*****	32.778,00	EUR	1002	
4976	*****	36.726,00	EUR	2004	
4977	*****	9.352,00	EUR	1360	
4978	*****	*****	EUR	2130	
4979	*****	*****	EUR	1360	
4980	*****	*****	EUR	2130	
4982	*****	43.004,00	EUR	1033	

T17

	A	B	C	D	E	F	G	H	I
	Sales Doc.	Created On	Created By	Net value	SOrg.	DChl	Dv	SGrp	Sold-To Pt
1									
2	4969	02.01.1997	****	5.500,00	1000	10	0	103	1390
3	4970	03.01.1997	****	32.838,00	1000	12	0	110	1175
4	4971	07.01.1997	****	*****	1000	12	0	101	1001
5	4972	21.01.1997	*****	28.604,00	1000	12	0	110	2200
6	4973	21.01.1997	*****	*****	1000	12	0	130	1033
7	4974	21.01.1997	*****	46.686,00	1000	12	0	101	2140
8	4975	21.01.1997	*****	32.778,00	1000	12	0	130	1002
9	4976	21.01.1997	*****	36.726,00	1000	12	0	130	2004
10	4977	21.01.1997	*****	9.352,00	1000	10	0	130	1360
11	4978	21.01.1997	*****	*****	1000	10	0	101	2130
12	4979	21.01.1997	*****	*****	1000	10	0	130	1360
13	4980	21.01.1997	*****	*****	1000	10	0	101	2130
14	4982	22.01.1997	*****	43.004,00	1000	12	0	130	1033

Reveal on Demand



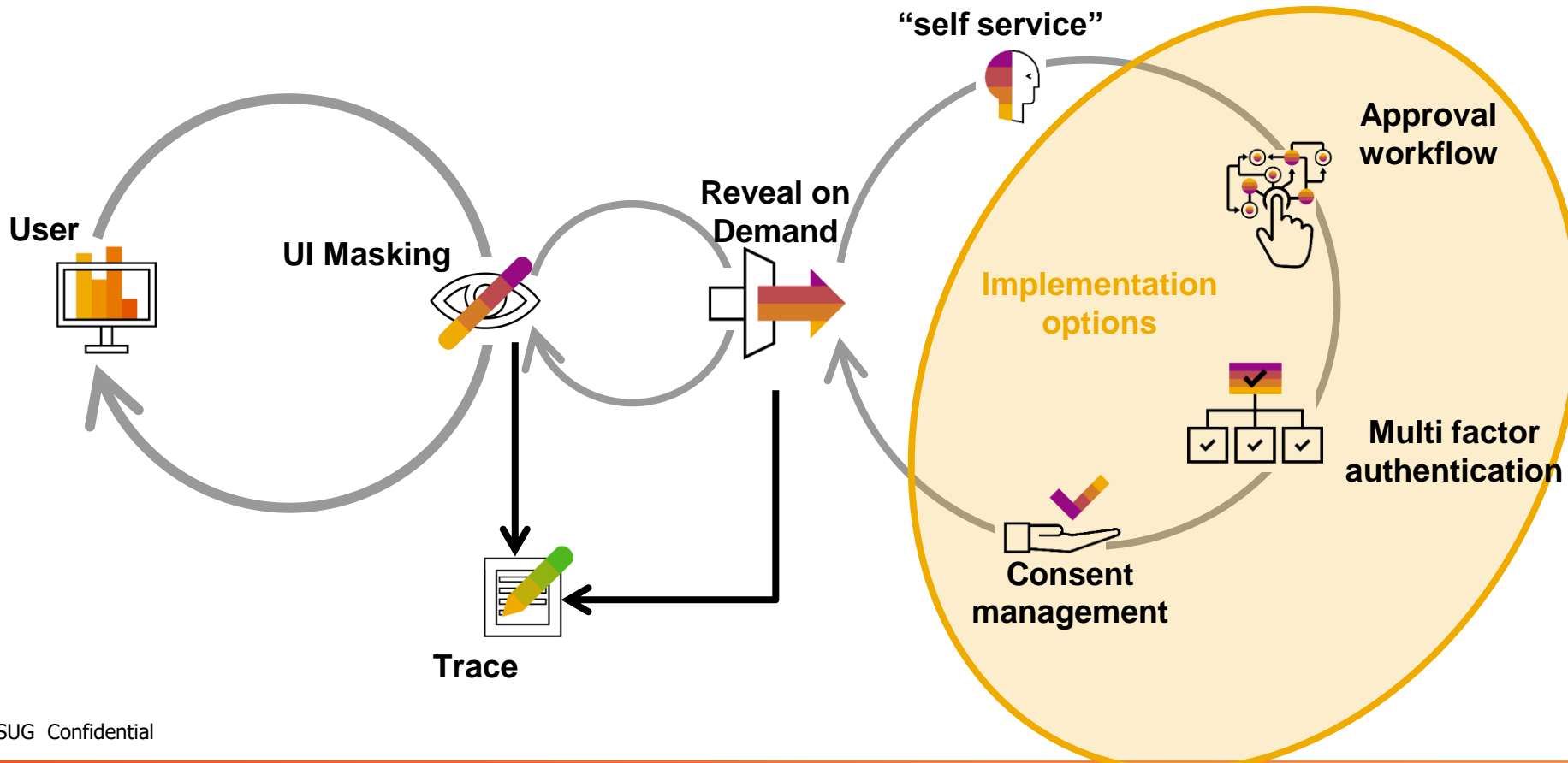
UI Masking: "Reveal on Demand"

UI Masking introduces an intercept point for a user's access to data based on a determination of authorization.

"Reveal on Demand" constitutes a second intercept, refining and basing authorization on additional conditions.

In an RoD scenario, data are always protected initially. A user action triggers an additional determination of authorization including a bespoke trace of the event and result.

RoD authorization could be based e.g. on approval, additional authentication or, in a case the data subject of PII has given her consent for her data to be used under the given conditions.



UI Masking: "Reveal on Demand"

Fiori app

The screenshot shows a Fiori app interface for 'UI Masking Demo'. It features a table with columns: Employee ID, First Name, Last Name, and Masked Last Name. The first name 'PARAG' is masked as '**RAG'. A 'Reveal on Demand' dialog is displayed, with the 'Reveal' option selected. Below the table, the 'Employee Details' section shows masked fields for First Name (**RAG) and Full Name (**RAG **RG). A blue arrow points from the 'Reveal' button in the dialog to the 'First Name' field in the details section.

Employee ID	First Name	Last Name	Masked Last Name
C5180792	**LVENDRA	**MAR	**MAR
C5244017	**EPAK	**PTA	**PTA
C5244018	**RAG	**RG	**RG
C5262600	**UN	**RMA	**RMA

SAP GUI

The screenshot shows the SAP GUI 'Display Basic Pay' screen for employee Mr. Arun Vezma. The 'Salary amount' field is masked with asterisks. A 'Reveal on Demand' dialog is open, asking 'Please confirm: Are you sure you want to view sensitive data?'. A blue arrow points from the 'Ok' button in the dialog to the 'Amount' field in the table below.

W...	Wage Type	Long Text	Amount	Curr.	I.	A.	Number/Unit	Unit
M110	S*****		*****	GBP	✓		0,00	

UI Logging



UI Logging: configurable logging of data access in SAP UIs



- configurable scope of data to be protected on transaction/application/service level
- configurable list of users subjected to logging
- configurable alerts on specific (critical) data accesses
- configurable log reasons and retention time
- Log Analyser UI for researching the log file
- Integration with SAP Enterprise Threat Detection

UI Logging: Log access, get notified, take action

1. Log data access



Change Basic Pay

Personnel No: 1 Name: Christian Schubert
 EE group: 1 Active Pers.area: DE01 Personnel area DE01
 EE subgroup: 00 Salaried employees
 Start: 01.01.2013 to 31.12.9999 Chng: 24.11.2016 EDEBALI

Payment type: 0 Basic contract Object ID:
 Reason:
 Next increase:
 Pay scale:
 Type: 40 Metal Capacity Util. Level: 100,00 % PER
 Area: 01 Baden-Wuerttemberg Work hours/period: 167,40 Monthly
 Group: M3 Level: Ann.salary: EUR

W...	Wage Type	Long Text	O. Amount	Curr...	I.	A.	Number/Unit	Unit
MA10	Standard salary		1.602,00	EUR		✓		
MA20	Standard bonus		153,40	EUR		✓		
MA30	Standard bonus (%)			EUR	I	✓		Percent

IV 25.01.2017 - 31.12.9999 1.755,40 EUR

2. Automatic alert



FROM: Voss, Martin SUBJECT: Serious Alert for System XPX/200 when accessing personal d... Do 26.01.2017

Alert ID: ##01717## Personal Information of Adam is getting displayed by MVOSS

Reply Reply All Forward

From: Voss, Martin

Serious Alert for System XPX/200 when accessing personal data

This message was sent with High importance.

Alert ID: ##01719##

Personal Information of Adam is getting displayed by MVOSS

system id: XPX
 client: 200
 user id: MVOSS
 system time: 12:45:08
 system date: 26.01.2017
 transaction: PA20

```

***** HEADER*****
GUID=B9F783586FB23949E1000000A60883B
TIMESTAMP=25.01.2017 16:38:28
TRX_NAME=PA30-Maintain HR Master Data
USERNAME=KELLERTO
CLIENT_ID=10.66.6.234
LOG_CLIENT=200
SYSID=YPX
HOST_NAME=WDFN33937027A
TECHNOLOGY=10
SUB_TECHNOLOGY=
TID=000000040
MODNO=000000000
SESSION_ID=00040255882FC3ED4F2697DE1000000A60883B
CONTEXT_ID=000400005882FC3ED4F2697DE1000000A60883B

***** INPUT*****

SAP_SYSTEM=YPX
SAP_CLIENT=200
TITLE=Maintain HR Master Data
Function code that PAI triggered=MOD
PA30.SAPMP50A.1100.SAPMP50A.1100.RP50G-PERNR[0]=1
Function code that PAI triggered=MOD
PA30.SAPMP50A.1100.SAPMP50A.0350.RP50G-CHOIC[0]=8
PA30.SAPMP50A.1100.SAPMP50A.0350.RP50G-SUBTY[0]=
PA30.SAPMP50A.1100.SAPMP50A.0350.SUBTY_TEXT[0]=

***** OUTPUT*****

SAP_SYSTEM=YPX
SAP_CLIENT=200
TITLE=Module Pool for Infotype 0008 (Basic Pay)
PA30.MP000800.1000.MP000800.1000.[1]=Person
PA30.MP000800.1000.MP000800.1000.[1]=Collective search help
PA30.MP000800.1000.MP000800.1000.[2]=Search Term
PA30.MP000800.1000.MP000800.1000.[3]=Free search
PA30.MP000800.2000./1PAPAXX/HR_20002A.0100.$_DG01_200A02_DAT_P0000_PERNR[0]=1
PA30.MP000800.2000./1PAPAXX/HR_20002A.0100.$_DG02_200A02_DAT_P0001_ENAME[0]=Christian Schubert
PA30.MP000800.2000./1PAPAXX/HR_20002A.0100.$_DG03_200A02_DAT_P0001_PERSG[0]=1
PA30.MP000800.2000./1PAPAXX/HR_20002A.0100.$_DG04_200A02_DTX_P0001_PERSG[0]=Active
PA30.MP000800.2000./1PAPAXX/HR_20002A.0100.$_DG05_200A02_DAT_P0001_WERKS[0]=DE01
PA30.MP000800.2000./1PAPAXX/HR_20002A.0100.$_DG06_200A02_DTX_P0001_WERKS[0]=Personnel area DE0
PA30.MP000800.2000./1PAPAXX/HR_20002A.0100.$_DG07_200A02_DAT_P0001_PERSK[0]=DU
PA30.MP000800.2000./1PAPAXX/HR_20002A.0100.$_DG08_200A02_DTX_P0001_PERSK[0]=Salaried employees
PA30.MP000800.2000.MP000800.2000.P0008-BEGDA[0]=01.01.2013
PA30.MP000800.2000.MP000800.2000.P0008-ENDDA[0]=31.12.9999
PA30.MP000800.2000.MP000800.2000.P0008-AEDTM[0]=24.11.2016
PA30.MP000800.2000.MP000800.2000.P0008-UNAME[0]=EDEBALI
PA30.MP000800.2000.MP000800.2000.RP50M-SPRTX[0]=
PA30.MP000800.2000.MP000800.2000.P0008-SUBTY[0]=0
PA30.MP000800.2000.MP000800.2000.T591S-STEXT[0]=Basic contract
PA30.MP000800.2000.MP000800.2000.P0008-OBJPS[0]=
PA30.MP000800.2000.MP000800.2000.P0008-PREAS[0]=
PA30.MP000800.2000.MP000800.2000.T530R-TEXT[0]=
PA30.MP000800.2000.MP000800.2000.P0008-STVOR[0]=
PA30.MP000800.2000.MP000800.2000.P0008-TRFAR[0]=40
PA30.MP000800.2000.MP000800.2000.T510A-TARTX[0]=Metall
PA30.MP000800.2000.MP000800.2000.P0008-BSGRD[0]=100,00
PA30.MP000800.2000.MP000800.2000.T546T-TEXT[0]=PER
PA30.MP000800.2000.MP000800.2000.P0008-TRFGR[0]=1
PA30.MP000800.2000.MP000800.2000.T510G-TGBTX[0]=Baden-Wuerttemberg
PA30.MP000800.2000.MP000800.2000.P0008-DIVGV[0]=167,40
PA30.MP000800.2000.MP000800.2000.Q0008-ZTEXT[0]=Monthly
PA30.MP000800.2000.MP000800.2000.P0008-TRFGR[0]=M3
    
```

3. in-depth analysis



4. Aggregate & detect (SAP ETD)

Analysis and Pattern Design

Forensic Lab Desktop Recommended | Anomaly Detection Lab | Patterns Active 73, All 86, Value Lists 52

SAP Enterprise Threat Detection: Forensic Lab

WORKSPACE

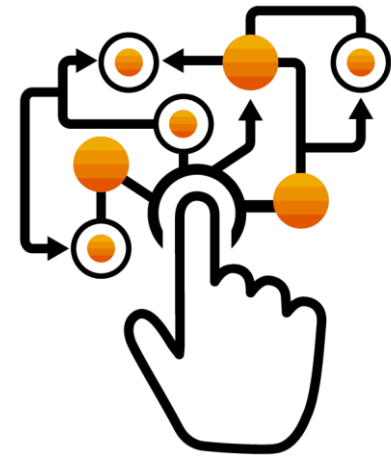
New Forensic Workspace | Refresh | Open | Save | Event, Log Type

Path1 | Events | 572 078 | Add new subset

Invert

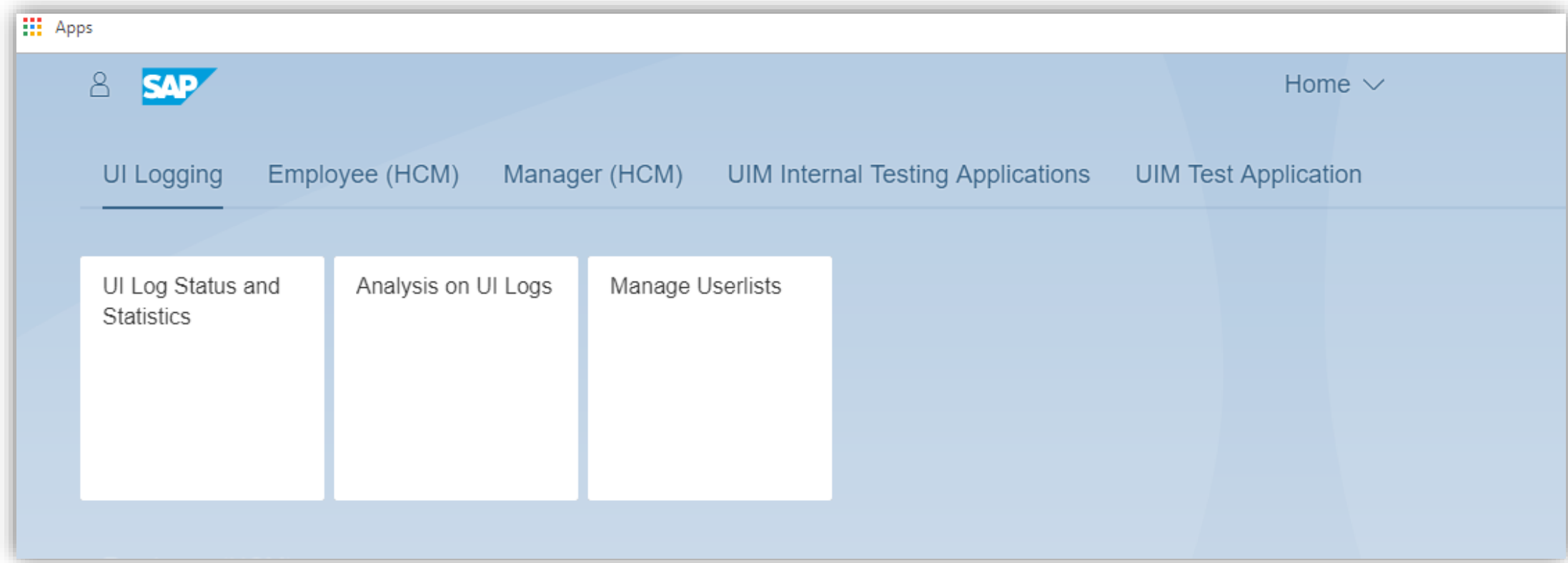
- BusinessTransactionLog
- SecurityAuditLog
- SystemLog
- HttpServerLog
- Indicator

UI Logging Analysis Apps Screen View



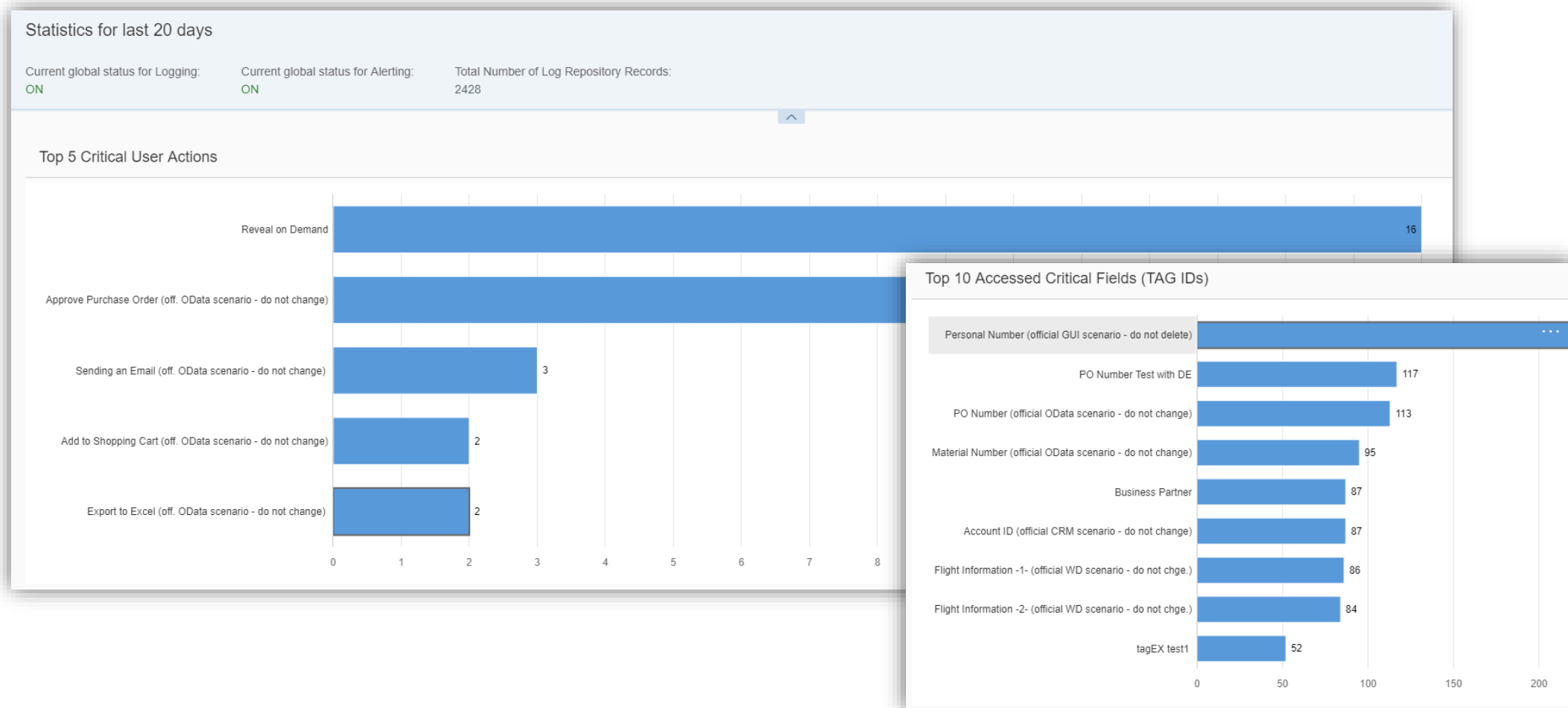
UI Logging: Fiori Applications for the DPO (Data Protection Officer)

“Security personnel” (e.g., security office, data protection officer running UI Logging and working on its logs) leverage Fiori apps for keeping an overview, conducting deep dive analysis into data usage, and managing lists of users whose data access they have identified as noteworthy.



UI Logging: Fiori Applications for the DPO (Data Protection Officer)

Security personnel can get an overview of system status as well as statistics concerning data usage (top n logged users, top n accessed critical data fields (data types), top n triggered actions, and more)



UI Logging: Fiori Applications for the DPO (Data Protection Officer)

Analysis of UI Logs

Security personnel can conduct exploratory analysis of access to data types.

They gain a comprehensive view on data usage as multiple screen fields of the same type (e.g., social security number) can be aggregated or grouped by “tags”. Filter criteria allow for a more granular display of accessed data objects, and accessing users.

Critical Field (TAG ID)

SELECT FROM LIST DEFINE CONDITIONS

Search Hide Advanced Search

*Logging Date:

Critical Field (TAG ID):

Items

<input checked="" type="checkbox"/>	Critical Field (TAG ID)	Number of Applications	Number of Users	Number of Logs	St
<input checked="" type="checkbox"/>	PERS_NUM	2	3	89	08

Define Conditions: Critical Field (TAG ID) Value

Include (1)

Critical Field (TAG ID) Value

Exclude

Define Conditions: User

Include (1)

User

UI Logging: Fiori Applications for the DPO (Data Protection Officer)

Analysis of UI Logs

Security personnel can analyze deeper into access and behavior of specific users, through a list of applications in which they accessed critical objects, and more in detail also into the sequence of activities.

For deeper research on more detailed level, jump points are provided into SAP GUI analysis applications.

The screenshot displays the 'Analysis on UI Logs' interface for user TESTUSER01. The interface is divided into three tabs: 'List of Applications', 'Statistics', and 'Sequence of Activities'. The 'Sequence of Activities' tab is active, showing a vertical timeline of activities. Each activity entry includes a date, time, and the number of logs. Below each activity, there is a table of TAGs and Values. The TAGs table lists 'PERS_NUM' with a 'multi' link. The Values table shows the corresponding values for 'PERS_NUM'. A dropdown menu is visible next to the 'multi' link in the third activity, showing the values '109820' and '1000'.

TAGs	Values
PERS_NUM	1001

TAGs	Values
PERS_NUM	multi

TAGs	Values
PERS_NUM	109820

TAGs	Values
PERS_NUM	multi

TAGs	Values
PERS_NUM	109820

UI Logging: Fiori Applications for the DPO (Data Protection Officer)

Analysis of UI Logs

Security personnel can identify users whose data access and actions are worth noting, and can add them to a list of “users of interest” which can be edited until it is “published” (for handing over to other departments who may take additional steps).

Standard * ▾ Hide Filter Bar Clear Filters (4) Go

*Logging Date: Critical Field (TAG ID): Application: Critical Field (TAG ID) Value: Critical Action: User:

Standard ▾ Add to Userlist ⚙️ 📄

User	Number of Critical Fields	Number of Applications	Number of Logs	Userlist of Interest
<input type="checkbox"/> Martin Voss	1	1	41	UT1

Standard * ▾ Hide Filter Bar Clear Filters (4) Go

*Logging Date: Critical Field (TAG ID): Application: Critical Field (TAG ID) Value: Critical Action:

User:

Standard ▾ Add to Userlist ⚙️ 📄

User	Number of Critical Fields	Number of Applications
<input checked="" type="checkbox"/> Martin Voss	1	1

General Information

*Title:

Description:

Users (1)

Remove all

Martin Voss	Filter Criteria	<input data-bbox="2229 1220 2267 1242" type="text" value="x"/>
-------------	-----------------	--

UI Logging

Classic Analysis: TagAnalyzing

In addition to the Fiori based analysis apps, analysis can be conducted through the classical tools if desired. Relevant roundtrips are grouped by user sessions (Extended Passport). Per roundtrip, the relevant log data is displayed in the bottom left section, and additional data fields that may be assigned to tags are specified in the top right section. Technical field names are enhanced by more telling labels where available.

Analyzing Logs based on TAG ID

Roundtrips	Personal N	Log.Entity	Platform	Host
50 Roundtrips Found				
09.10.2019 10:18:40.143 - 10:20:15.305 (6)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:18:40.143	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:18:43.962	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:18:45.948	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:18:47.673	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:18:47.957	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:20:15.305	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:20:19.070 - 10:20:28.230 (6)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:23:23.777 - 10:23:33.696 (5)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:26:03.432 - 10:26:15.380 (5)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 10:34:02.025 - 10:34:10.429 (5)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 14:27:33.973 - 14:27:43.624 (6)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 14:29:51.727 - 14:30:03.810 (5)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 14:41:03.528 - 14:41:18.669 (6)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 14:42:58.959 - 14:44:18.348 (5)	200031	PA20-Display HR Master Data	10	WDFN34717402A
09.10.2019 14:45:40.352 - 14:45:40.352 (1)	200031	PA20-Display HR Master Data	10	WDFN34717402A

TAG/Contex	Description	Value	Is Context
PERS_NUM	Personal Number (official GUI scenario - do not delete)	200031	
COSTCENTER	Cost Center	F1-FIN1000	X
NAME	Full Name	Ackermann Steffen	X

Name	Data Elem.	Value	Value Is Long	Screen Title	Short text
\$_DG01_700A60_DAT_P0001_ENAME	EMNAM	Ackermann Steffen		Display HR Master Data	Formatted Name of Employee or App
\$_DG02_700A60_DAT_P0001_PERSG	PERSG	1		Display HR Master Data	Employee Group
\$_DG03_700A60_DTX_P0001_PERSG	PGTXT	Active		Display HR Master Data	Name of Employee Group
\$_DG04_700A60_DAT_P0001_WERKS	PERSA	CH01		Display HR Master Data	Personnel Area
\$_DG05_700A60_DTX_P0001_WERKS	PBTXT	Switzerland Sub		Display HR Master Data	Personnel Area Text
\$_DG07_700A60_DAT_P0001_PERSK	PERSK	CB		Display HR Master Data	Employee Subgroup
\$_DG08_700A60_DTX_P0001_PERSK	PKTXT	Division manager G.		Display HR Master Data	Name of Employee Subgroup
\$_DG09_700A60_DAT_P0001_KOSTL	KOSTL	F1-FIN1000		Display HR Master Data	Cost Center
\$_DG10_700A60_DTX_P0001_KOSTL	KTEXT			Display HR Master Data	General Name
INF_EX	ICON_TEXT			Display HR Master Data	Carrier field for icons
INF_EX	ICON_TEXT			Display HR Master Data	Carrier field for icons
RP50G-BEGDA	BEGST			Display HR Master Data	From
RP50G-CHOIC	CHOIC			Display HR Master Data	Infotype selection for HR master data
RP50G-ENDDA	ENDST			Display HR Master Data	Valid To Date
RP50G-PERNR	PERNR_D	200031		Display HR Master Data	Personnel Number
RP50G-SELEC	SELEC			Display HR Master Data	Indicator for list screen
RP50G-SUBTY	SUBTY			Display HR Master Data	Subtype
RP50G-TIMR1	TIMR1			Display HR Master Data	Time Period Indicator: Today
RP50G-TIMR2	TIMR2			Display HR Master Data	Time period indicator: Current month

UI Logging

Classic Analysis: LogAnalyzing

On roundtrip basis, a report can be accessed that renders logged data in a more readable way, with non-technical labels where available.

```
*****
***** TRANSFER *****
*****
CREATED_AT=09.10.2019 10:18:53
CREATED_BY=MVOSS
CHANGED_AT=09.10.2019 10:18:53
CHANGED_BY=MVOSS

*****
***** HEADER *****
*****
GUID for Log=248A07FC62601EE9BACDAD3AC00BDBEF
Time Stamp=09.10.2019 10:18:46
Logged Entity=PA20-Display HR Master Data
User Name=MVOSS
Client IP=10.18.163.119
Client of Log=700
SAP System ID=Y1X
Host Name=WDFN34717402A
Platform=10
Sub Technology=
Reason ID=REASON_VOSS
Retention Date=20221009
Terminal ID=0000000142
Mode Number=0000000002
Session ID=00142255248A07FC62601EE9BACD9E98B88DBE2
Context ID=00142002248A07FC62601EE9BACDA95E8107DBEC

*****
***** INPUT *****
*****
SAP_SYSTEM=Y1XSAP_CLIENT=700
FUNCTIONCODE=
TITLE=Display HR Master Data
TAG ID PERS_NUM_FLD           = 200031
TAG ID PERS_NUM_DATAE        = 200031
TAG ID Personal Number (official GUI sce = 200031
Personnel Number              = 200031
Infotype selection for HR master data ma = 8
Subtype                        =
Name of Subtype                =

*****
***** OUTPUT *****
*****
SAP_SYSTEM=Y1XSAP_CLIENT=700
FUNCTIONCODE=
TITLE=Display HR Master Data
Formatted Name of Employee or Applicant = Ackermann Steffen
Employee Group                       = 1
Name of Employee Group                 = Active
Personnel Area                         = CH01
Personnel Area Text                     - Switzerland Sub
< >                                     "
```

Agenda

1

What

Solution
overview

2

When

Use cases

3

Where

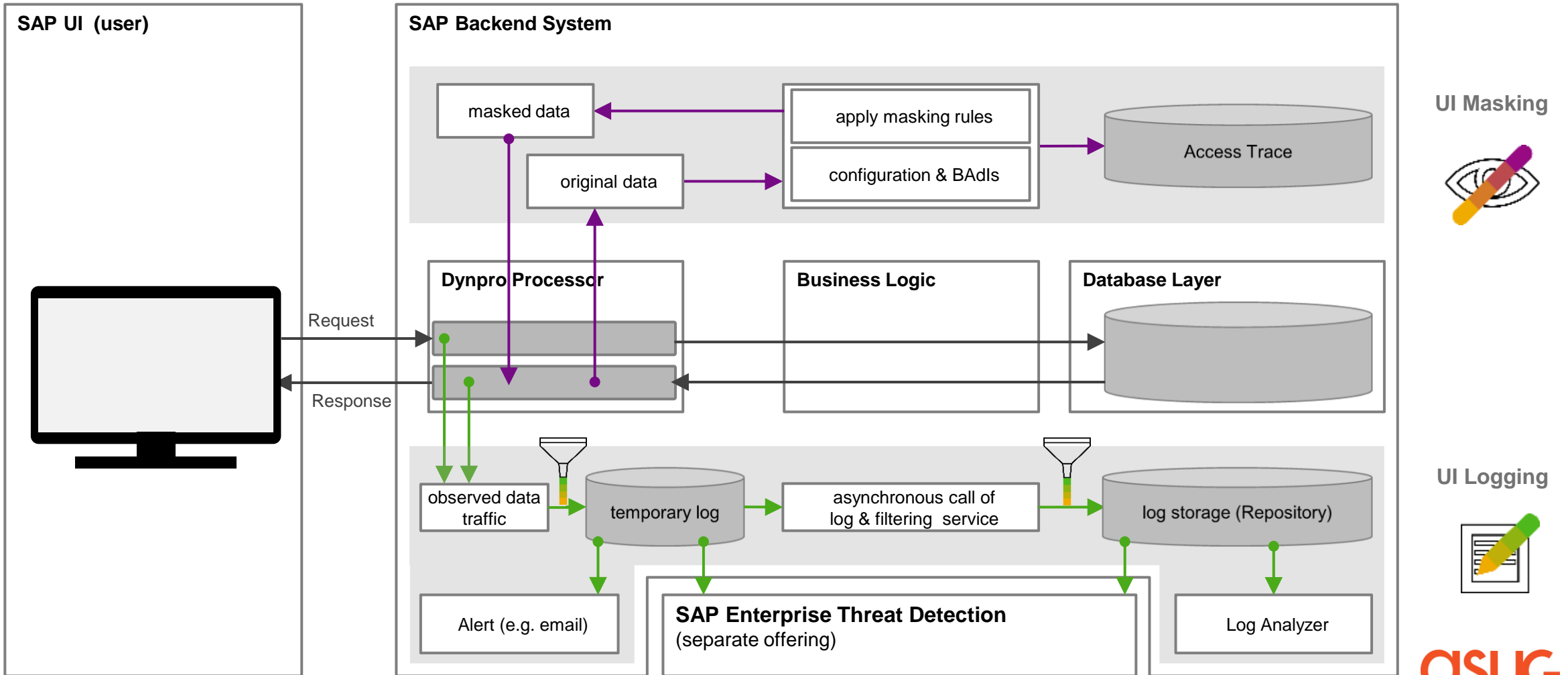
Architecture and
availability

4



Next Steps

High level solution architecture

- UI Masking and UI Logging can be **used individually or jointly**, depending on the required functionality
- add-ons to SAP NetWeaver – **modification free** installation, **secure** server-based functionality with **minimal performance impact**



Coverage is based on UI technologies

UI technology	UI Masking 	UI Logging 
SAP GUI for Windows / HTML / Java	✓	✓
WebDynpro ABAP	✓	✓
CRM Web Client UI	✓	✓
RFC/BAPI and Web Services	project based	✓
BW Access (BEx Web/Analyser, BW-IP, BICS, MDX)	project based	✓
UI5/Fiori	✓	✓

- **Available for ECC, HEC, Suite on HANA, S/4HANA**
- **Enhancements and adaptations** can be delivered on request

UI Masking: Classic vs. S/4HANA offering

	“classic” UI Masking solutions	S/4HANA “UI data protection masking”
Where to use	ECC, classic CRM scenarios, HEC, (S/4HANA as „compatible“ solutions, potential limitations)	S/4HANA
How to get	Separate installations per required UI technology	Unified technical installation
Configuration	Separate configurations per required UI technology	Unified config, automated with data elements ; consistent application of protective actions over all supported UI technologies.
Protective actions	Masking of values in fields	Masking of values in fields emptying/hiding/disabling fields/links suppression of lines in table displays data blocking
Authorization paradigm	Role based; attribute/rule based authorizations through BAdI implementation	Role based Policy based (attributes and rules)
Additional features		Reveal on Demand (2-step authorization)

Agenda

1

What

Solution
overview

2

When

Use cases

3

Where

Architecture and
availability

4

Next Steps

Reality and Vision: Protecting the Intelligent Enterprise: A Data Protection "Suite"

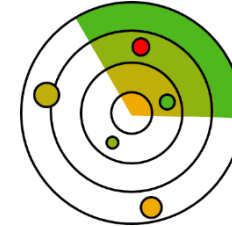
1) mask/obfuscate what
can be masked: with
UI Masking



2) Log what *can NOT*
be masked: with
UI Logging

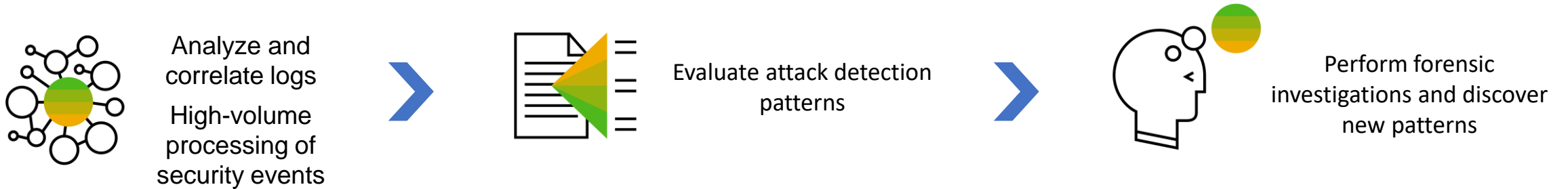


3) Automatically correlate and
analyze the log with
Enterprise Threat Detection

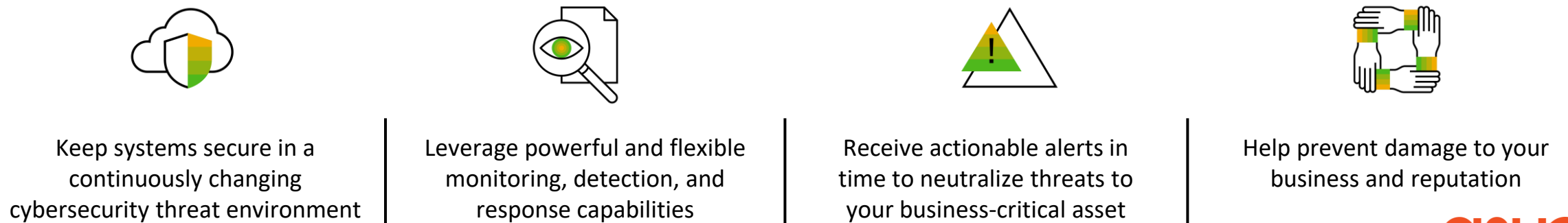


SAP Enterprise Threat Detection

Refine algorithms to better detect threats



Leverage machine learning to refine anomaly detection methods such as statistical methods, one-time behavior, and potential malicious sites



Summary

Where do we go from here?

Upcoming ASUG webinars

Solution deep dives

First Half Webinars

- March 24: What You Need to Know About SAP's Offerings for Data Protection and Privacy ([recording available](#))
- April 14: Solution highlight: SAP Privacy Management by BigID ([recording available](#))
- April 28: Solution highlight: SAP Privacy Governance ([recording available](#))
- May 19: Solution highlight: User interface logging and field masking solutions by SAP
- June 2: Solution highlight: SAP Enterprise Threat Detection

Second Half Webinars – dates to be confirmed

- Cloud Security Considerations
- Managing the identity lifecycle in hybrid landscapes
- Solution highlight: SAP Cloud Identity Access Governance
- Solution Highlight: Authentication scenarios
- Solution Highlight: Authorization scenarios
- Solution highlight: SAP Data Custodian

More information for SAP GRC and Security solutions

Select the area of interest below

SAP solutions for GRC & Security

Products Industries Support Training Community Developer Partner About

Home / Products / Data Platform

Cybersecurity and Governance, Risk, and Compliance (GRC)

International SAP Conference for Internal Controls, Compliance and Risk Management
Join us in Barcelona, Spain on March 12-13, 2019 to discover how next generation GRC solutions deliver connected and real-time operations to your teams. Hear first-hand from customers on the benefits of using SAP across the entire GRC value chain.

Register

Protect your business and bottom line with smart GRC and security tools

Quickly adapt to changes in technology, regulations, and the economy – with governance, risk, and compliance (GRC) solutions from SAP. Our automation-enabled, integrated GRC solutions are organized into four categories: Three Lines of Defense, Access Governance, International Trade, and Cybersecurity.

Practical Tools and Approach

SAP

Gain one view of risk with smart GRC and security tools

Improve your business and bottom line

Today's GRC professionals have tools and technology available that simply weren't available just a few short years ago. But expectations have also been raised. Stakeholders expect GRC to contribute to business performance. That requires integration, transformed professional practices, the use of powerful analytics and visualization. Road ahead: the opportunity and how smart GRC and security tools from SAP meet the challenge.

SAP Cloud as a Leader in The Forrester Wave™ Governance, Risk, and Compliance platforms, Q3 2018

Deloitte ranked their top 100 of the highest performing, well-organized GRC solutions the highest their ranked GRC software providers in 2018. SAP was ranked 1st and 2nd in the 2018 GRC software providers list.

SAP Cloud Trust Center

Products Industries Support Training Community Developer Partner About

About SAP

SAP Cloud Trust Center

Overview SAP Network Status Security Data Center Data Protection and Privacy Governance Regulatory

Security, privacy, and compliance in the cloud – we keep your data safe

Your business is built on trust, and you expect the same from your software provider. As a leading software provider and a cloud company, we're dedicated to building – and keeping – our customers' trust.

- Cloud Service Status**
Discover the uptime and availability of SAP's cloud services with access to real-time insights.
[Cloud Service Status](#)
- Security**
Rest assured that your data is protected with a cloud security foundation based on the highest security standards.
[Security](#)
- Data Center**
Visit our data centers and see state-of-the-art technologies and rigorous security methodologies.
[Data Center](#)
- Data Protection and Privacy**
- Compliance**
- Agreements**

[News Release: SAP Receives Global Certification of Data Protection and Privacy from British Standards Institution \(BSI\)](#)

Questions?

For questions after this session, contact us at:

Erin Hughes
Cybersecurity Solution Advisor
Erin.Hughes@sap.com

Thank you.

Stay connected. Share your SAP experiences anytime, anywhere.
Join the ASUG conversation on social media: **@ASUG365 #ASUG**

