History of SAP Solutions: UI Logging and UI Masking

"Protecting an organisation's data has never been more challenging. The cost of a data leak goes far beyond fines – impacting both investor and consumer confidence, causing potentially catastrophic harm to brand and reputation. Proactively addressing risk through logging what a user sees on screen, and the functions executed, coupled with masking sensitive or confidential data provides much needed tracking, auditability and safeguarding."

Steve Hewison
CEO, Winterhawk

About Winterhawk

Winterhawk is a leading global consulting practice, supporting organisations in SAP Security, SAP GRC services and solutions (more than 20) across a variety of SAP environments including SAP R/3, S/4HANA, ARIBA, Fieldglass, Concur and SuccessFactors.

Winterhawk is the Global Solution Partner for the United VARs Alliance (Platinum SAP Partners) servicing over 8,000 clients worldwide.

As part of a new SAP solution spotlight series, Winterhawk spoke with SAP's Tobias Keller (Data Security at SAP Innovative Business Solutions) about the ongoing development of SAP UI Logging and UI Masking.

What are SAP UI Logging and UI Masking?

UI Logging and UI Masking are two separate solutions which are often purchased and used together to provide organisations with increased user interface data security. They support organisational cyber security and data protection by reducing the risk of data breaches.

UI Logging is a cyber security product which provides organisations with the means to record and analyse data for atypical access. Every access event of a database is logged and identifiable by activity type, with real-time, configurable alerts and notifications which can be used to detect and act upon the misuse of data. The solution provides both the contextual visibility and transparency for businesses to ensure data privacy at a satisfactory level for regulatory and internal requirements.

UI Masking is a data protection product that restricts access to legally protected or business critical data, on a configurable basis. The solution provides an additional layer of security on top of current business roles, without making any unwanted disruptions, helping organisations comply with internal and legal requirements concerning restriction of data access across their enterprise application portfolio.

Why are they important?

On the most basic level, these solutions protect critical data and minimise the impact of data breaches. UI Logging is used to keep data accessible as needed and on a controlled basis by logging and analysing access throughout organisational systems. The solution's detailed data access log allows for analysis of exactly who received which data (output), how and when they accessed it (input), and in which context (IP) – information which is crucial for the CIO and Data Protection Officer (DPO). It prevents illegitimate data access and theft by inducing compliant behaviour and identifying irregular data access.

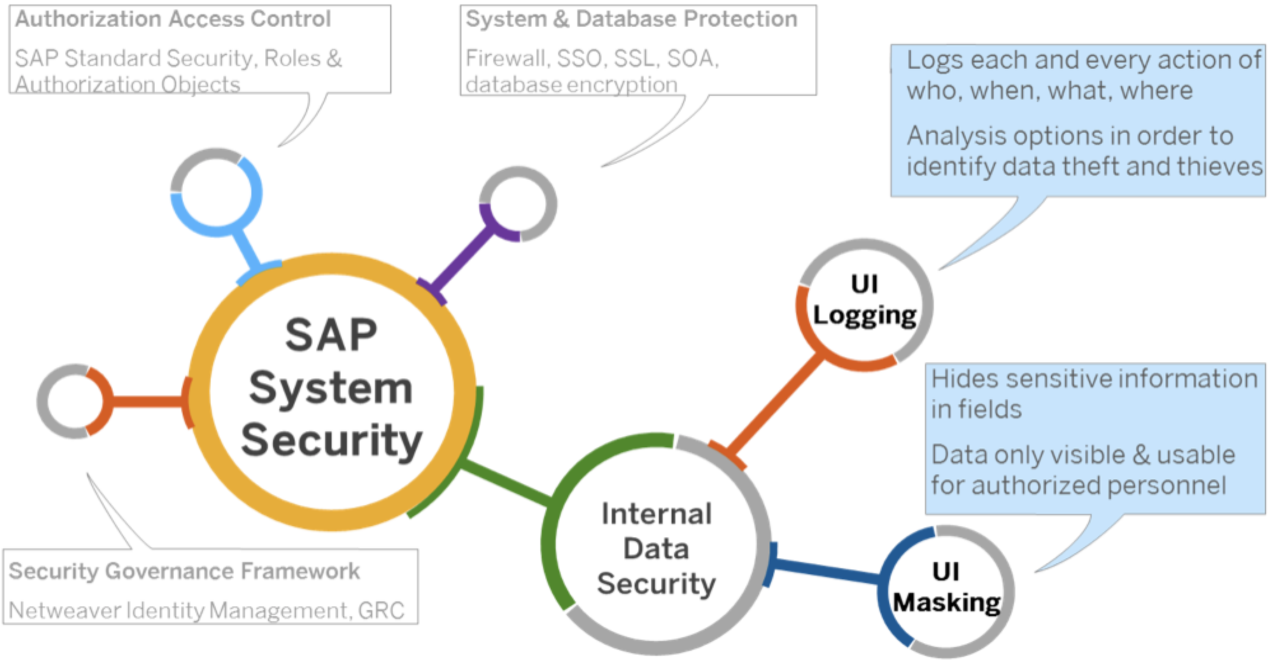
UI Masking is used to conceal specific data (values in fields or columns). These parameters are configurable based on organisational needs or as required for specific tasks. The solution masks sensitive values as default; unmasking requires explicit access rights (on top of existing role/authorisation setup) therefore making data elements unavailable for data abuse (opportunistic and targeted).

Origins of SAP UI Logging and UI Masking

UI Logging and UI Masking were originally created in 2015 by the SAP innovative business solutions department. Driven by customer demand for increased data privacy and cyber security, there was an internal push to develop robust technology to protect a company's data throughout their enterprise applications. SAP development teams worked directly with customers to understand the fundamentals of relevant data masking and access logging, based on regulatory or internal corporate requirements. With the advent of SAP S/4HANA, SAP amalgamated UI Logging and UI Masking for the first time as one commercial product.

Who were the first customers?

CF Industries (Manufacturing and Distribution), bought UI Masking to improve their data security and prevent large-scale data leaks. The solution helped to ensure compliance with data security regulations by restricting access to sensitive information to those who actually needed it and preventing data leaks caused by the mass download or export of data. For example, a large Healthcare company purchased UI Logging to detect unauthorised access to sensitive data and patient information, thereby preventing fraud and enabling them to react to anomalous activity. The company was able to fulfil its legal and internal data security objective by ensuring the confidentiality of all patient data.


Authorization Access Control
SAP Standard Security, Roles & Authorization Objects
System & Database Protection
Firewall, SSO, SSL, SOA, database encryption
Logs each and every action of who, when, what, where
Analysis options in order to identify data theft and thieves
SAP System Security
UI Logging
Hides sensitive information in fields
Data only visible & usable for authorized personnel
Internal Data Security
UI Masking
Security Governance Framework
Netweaver Identity Management, GRC

What's the relevance for C-Suite Executives?

For **CIOs**, **CISOs**, and **Data Protection Officers (DPOs)** in particular, these solutions are technical tools which protect critical information and data; however, as the responsibilities of organisational data protection evolve, they're increasingly relevant to the **CFO** as they provide a means to reduce the risk of, and/or damage from, data breaches.

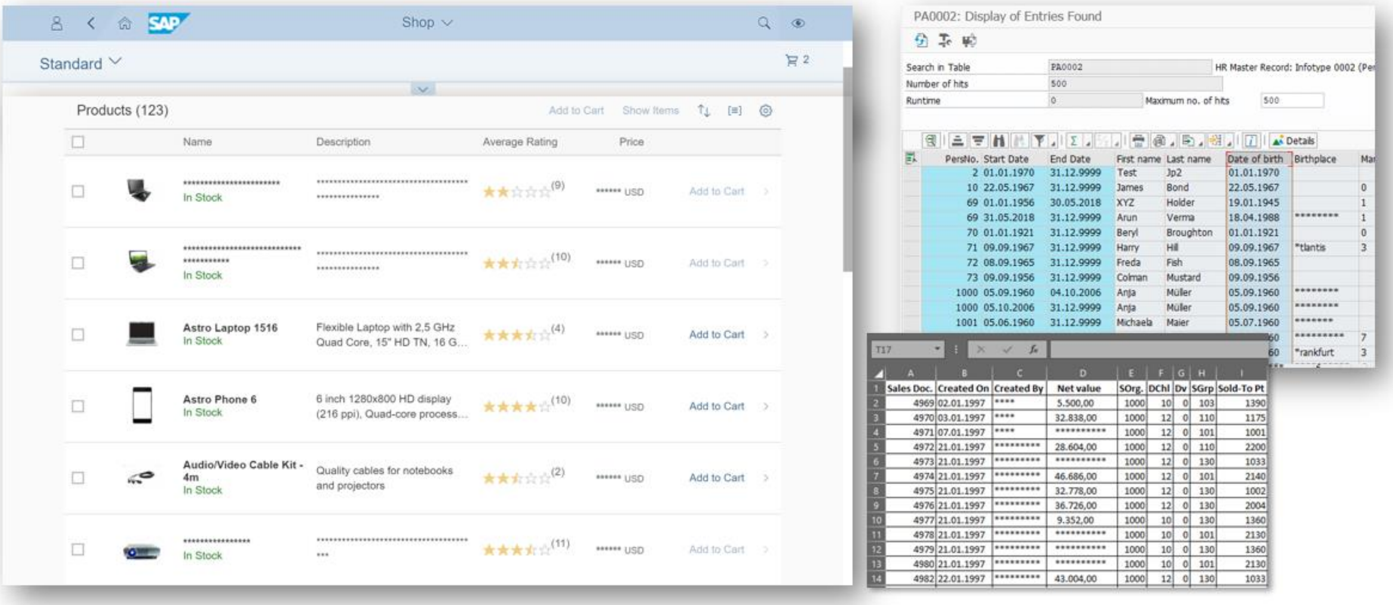
UI Logging and UI Masking serve the office of CFO to better protect data and improve corporate risk strategies. With these tools, roles and access are governed better, and human error in handling data is significantly reduced; they offer innovative and specific coverage of "insider" risk compliance and reduce total risk exposure. Because the tools log everything that is accessed, it is easy to determine what was exposed and when. This would be invaluable in cases of social engineering or where wrongdoing has gone undetected; the scale of a breach could be determined quickly, allowing for a rapid response to data breaches and compliance with regulatory requirements.

What's New with SAP UI Logging and UI Masking?

A new feature of note is integration with SAP Enterprise Threat Detection (ETD). With UI Logging, this enables the solutions to identify threats that would otherwise be invisible. SAP ETD feeds data into UI Masking to help determine whether or not to mask a specific field or block a particular transaction, on an automated basis. The tools give additional context to areas of data protection otherwise unachievable. Furthermore, in UI Masking, there is a new reveal-on-demand feature – in order to access data the user must complete an additional action. This produces a feedback loop to further protect data and inform systems and machine learning capabilities. Increased integration of SAP ETD with UI Masking will enable increased visibility of transactions enterprise-wide, safeguarding data throughout an entire enterprise and enabling organisations to react quickly to data breaches and reach successful conclusions faster.

How do SAP UI Logging and UI Masking support the Intelligent Enterprise?

The Intelligent Enterprise is a complex construct and these solutions support ongoing success through data protection and cyber security. With these tools, the CFO, CIO, CISO and DPO will be able to determine on an ongoing basis the status of critical data and systems and realise a reduced risk position. As integration with the rest of the SAP Suite is achieved, UI Logging and UI Masking will provide visibility and transparency of data access enterprise-wide and will also be able to protect critical data wherever they are linked. Sensitive data will be protected globally throughout rules and workflows, along all lines of business.



Products (123)

□	Name	Description	Average Rating	Price	
□	************************ In Stock	************************************* ****************	★★☆☆☆ (9)	****** USD	Add to Cart
□	***************************** *********** In Stock	************************************* ****************	★★½☆☆ (10)	****** USD	Add to Cart
□	Astro Laptop 1516 In Stock	Flexible Laptop with 2,5 GHz Quad Core, 15" HD TN, 16 G…	★★★½☆ (4)	****** USD	Add to Cart
□	Astro Phone 6 In Stock	6 inch 1280x800 HD display (216 ppi), Quad-core process…	★★★★☆ (10)	****** USD	Add to Cart
□	Audio/Video Cable Kit - 4m In Stock	Quality cables for notebooks and projectors	★★½☆☆ (2)	****** USD	Add to Cart
□	***************** In Stock	************************************* ***	★★★½☆ (11)	****** USD	Add to Cart

PA0002: Display of Entries Found

Search in Table: PA0002 HR Master Record: Infotype 0002 (Pe
Number of hits: 500
Runtime: 0 Maximum no. of hits: 500

PersNo.	Start Date	End Date	First name	Last name	Date of birth	Birthplace	Mar
2	01.01.1970	31.12.9999	Test	Jp2	01.01.1970		
10	22.05.1967	31.12.9999	James	Bond	22.05.1967		0
69	01.01.1956	30.05.2018	XYZ	Holder	19.01.1945		1
69	31.05.2018	31.12.9999	Arun	Verma	18.04.1988	*********	1
70	01.01.1921	31.12.9999	Beryl	Broughton	01.01.1921		0
71	09.09.1967	31.12.9999	Harry	Hill	09.09.1967	*tlantis	3
72	08.09.1965	31.12.9999	Freda	Fish	08.09.1965		
73	09.09.1956	31.12.9999	Colman	Mustard	09.09.1956		
1000	05.09.1960	04.10.2006	Anja	Müller	05.09.1960	*********	
1000	05.10.2006	31.12.9999	Anja	Müller	05.09.1960	*********	
1001	05.06.1960	31.12.9999	Michaela	Maier	05.07.1960	********	
					60	**********	7
					60	*rankfurt	3

T17

	A	B	C	D	E	F	G	H	I
1	Sales Doc.	Created On	Created By	Net value	SOrg.	DChl	Dv	SGrp	Sold-To Pt
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

Data Protection and GDPR

The solutions can be configured to fit GDPR requirements or other industry-specific data protection regulations. Rulesets within the systems are entirely configurable and are already in use by customers for GDPR compliance. UI Masking safeguards specific data as per GDPR requirements and Winterhawk can implement these safeguards quickly leveraging best practices.

Data breaches are often instigated internally; in the event that an employee maliciously or inadvertently leaks accesses or data, UI Logging will produce a digital trail linking the actor to the crime. UI Logging keeps data access transparent, preventing wrongdoers from accessing or abusing important data. These solutions serve to block data leaks, identify potentially malicious behaviour, and resolve any attacks or leaks by establishing a data trail that can be quickly investigated.

Looking ahead with SAP UI Logging and UI Masking

In the medium-run, SAP wants to fully integrate UI Logging and UI Masking with the entire SAP suite to optimise the solutions' capabilities in protecting sensitive data. This will also tie in with increased automation, moving towards an AI influenced, rule-based function that will also be utilised on an ad hoc basis. UI Logging and UI Masking are fully automated, however researching or reviewing data is currently manual; the understanding and analysis can be automated in the future.

Integration with SAP Data Custodian is also in development and it is apparent they want to strongly structure and automate protection of cloud data. SAP Data Custodian helps to structure data in a manner for UI Logging and UI Masking to automatically determine what to protect and in which context.

UI Logging and UI Masking are often overlooked in the SAP solution suite, but their relevance to SAP customers should be clear. Winterhawk can deliver UI Logging and UI Masking rapidly without disruption to your business operations.

Winterhawk has broad, cross-industry experience with implementing SAP solutions in large, multi-national corporations with global footprints. If you have any questions, or interest in discussing SAP UI Logging & UI Masking please visit us at www.winterhawk.com, email us at info@winterhawk.com or call us at +44 1233 877 290.