Logpoint BCS for SAP

A breach of an SAP system can severely impact your daily operations, leading to financial losses, productivity deficiencies, and damage your brand authority and customer trust.

Your SAP operations should be secured with a holistic security platform that covers all aspects of cybersecurity and is equipped with advanced detection, powerful analytics, and actionable intelligence. Detect threats early - before they impact your business and revenue.

f IDM Accounts

	System ID	Client	User	Message	Access Type	Authenticati
022 11:30:48	A4H	1	RFC_IDM	Logon successful (type=A, method=P)	Dialog logon (SAP GUI)	Password
022 11:28:51	A4H	1	RFC_IDM	Logon successful (type=A, method=P)	Dialog logon (SAP GUI)	Password
022 11:24:02	A4H	1	RFC_IDM	Logon successful (type=A, method=P)	Dialog logon (SAP GUI)	Password

ccounts

	System ID	Client	User	Changed U	Message	count
022 11:53:46	A4H	1	RFC_IDM	SAP*	User SAP* locked.	1
			RFC_IDM	SAP*	User SAP* locked.	1
			RFC_IDM	SAP*	User SAP* unlocked.	1
			RFC_IDM	SAP*	User SAP* locked.	1

Changes to accounts performed by accounts other than IDM accou

System ID	Client	User	Action
A4H	001	ADMIN_SMITH	User SAP* unlocked.
A4H	001	RFC_IDM	User SAP* unlocked.
A4H	000	ADMIN_MILLER	User SAP* unlocked.

/logpoint

A breach is detrimental to your business, reputation, and overall compliance

Vulnerable SAP systems are an extremely attractive target for cybercriminals. Breaking into an SAP system, the attacker can bypass all access and authorization controls, gaining full control of the SAP system, its underlying business data, and processes. This can then result in malicious activities severely impacting business operations and causing unprecedented reputational damage.

As data stored in the SAP system is subjected to various industry, financial and governmental regulations, securing it against attacks is essential to meet compliance requirements.

Successful exploitation of a vulnerable SAP system could allow an attacker to perform several malicious activities, including:

- Steal Personally Identifiable and Personally Sensitive Information (PII and PSI) from employees, customers, and suppliers
- Read, modify, or delete financial records
- Change banking details (account number, IBAN number, etc.)
- Administer purchasing processes
- Disrupt critical business operations, such as supply chain management, by corrupting data, shutting processes down completely, or deploying ransomware
- Perform unrestricted actions through operating system command execution
- Delete or modify traces, logs, and other files
- Steal intellectual property and other confidential data stored in the SAP system

The average cost of an SAP security breach is [$5 million per attack.]

Improve your defense against threats with BCS for SAP

Boost your resilience with holistic monitoring

Onboard your SAP data into a SIEM for better security robustness and improved threat detection. Our solution is agnostic and integrates with any SIEM.

With end-to-end visibility throughout your entire infrastructure, strengthen your monitoring capabilities and detect threats earlier and faster – way before they impact your business.

Go from visibility to action – all in one platform

Get real-time monitoring, powerful analytics, and automated incident response in a unified security operations platform. Monitor, analyze, and act based on a single source of truth. All of this helps reduce MTTR (Mean Time to Restore) because you can respond to threats more effectively in an integrated security platform as well as boosting your operational efficiency to successfully mitigate risk and combat threats.

Easily navigate and utilize your data

Get a complete overview of your SAP's security exposure with pre-built dashboards and customizable visualizations. Harness the data at your disposal and drill down to retrieve greater context and granular information on specific events. Use multiple filtering options and search templates to easily navigate data. Act faster, with greater efficiency, and improve performance with actionable intelligence.

To improve protection of your SAP operations, we are introducing four distinct solutions. Now you can tailor and adjust your security coverage to match your exact needs.

Boost your SAP security and effectively respond to threats with Security & Audit Compliance Monitoring

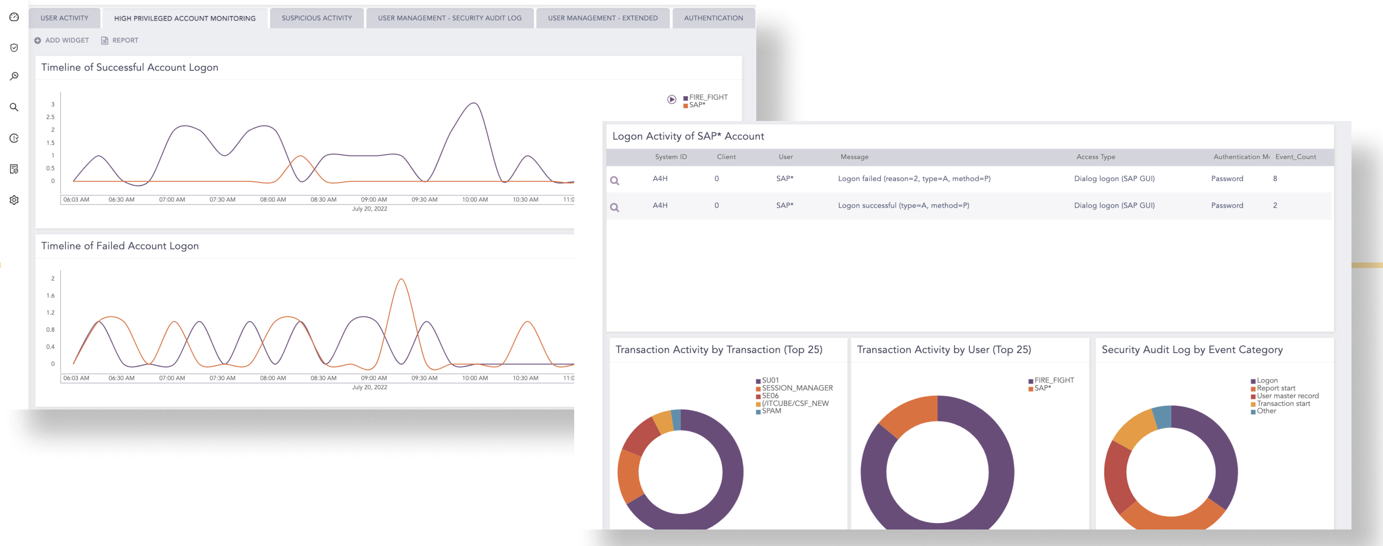
Did you know that 64% of the SAP systems have been breached during the past 24 months?

As it stands, SAP security is disconnected from the central security strategy hampering the ability to sufficiently monitor, patch and spot malicious activity. A security gap like this leaves businesses and organizations more exposed and subsequently vulnerable to attacks.

Elevate your SAP security to the next level
Strengthen your threat visibility and combat incidents more successfully with holistic end-to-end security operations capabilities. Let us bridge your security gap by onboarding your SAP into SIEM.

Advanced security insights across your entire infrastructure, enable you to identify threats earlier and respond faster – before they impact your business, compliance, and reputation.

Save time with automation
With pre-defined use cases- ready-to-use alerts, and checks, we automate your SAP security and compliance monitoring. Save time and effectively identify, mitigate, and manage threats.



Logon Activity of SAP* Account

	System ID	Client	User	Message	Access Type	Authentication M	Event_Count
🔍	A4H	0	SAP*	Logon failed (reason=2, type=A, method=P)	Dialog logon (SAP GUI)	Password	8
🔍	A4H	0	SAP*	Logon successful (type=A, method=P)	Dialog logon (SAP GUI)	Password	2

Secure your intellectual property and critical data against theft and misuse

Use-case: Security & Audit Compliance Monitoring

Business challenge:

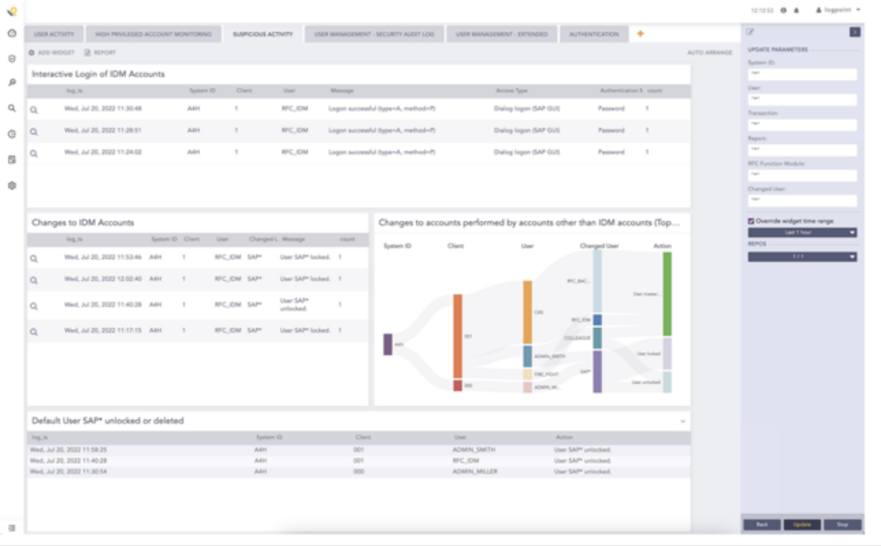
SAP systems store your intellectual property and govern your business secrets. A security breach to your business-critical data can have devastating consequences, crippling your competitive advantage, and threatening the entire existence of your business. Securing your SAP system against exposure is pivotal to safeguarding the foundation of your business.

Use-case:

Theft of confidential product information

Product Lifecycle Management enables the storage of product-specific information, technical details, and even an overview of all components comprising a product. For example, an airplane manufacturer's details regarding their newly introduced airplane were illegally accessed and downloaded on a USB stick.

If leaked or shared with competitors, this could easily have jeopardized years of research, compromise their competitive edge, and lead to unpreceded losses.



Interactive Login of IDM Accounts

	log_ts	System ID	Client	User	Message	Access Type	Authentication	count
	Wed, Jul 20, 2022 11:30:48	A4H	1	RFC_IDM	Logon successful (type=A, method=P)	Dialog logon (SAP GUI)	Password	1
	Wed, Jul 20, 2022 11:28:51	A4H	1	RFC_IDM	Logon successful (type=A, method=P)	Dialog logon (SAP GUI)	Password	1
	Wed, Jul 20, 2022 11:24:02	A4H	1	RFC_IDM	Logon successful (type=A, method=P)	Dialog logon (SAP GUI)	Password	1

Changes to IDM Accounts

	log_ts	System ID	Client	User	Changed U	Message	count
	Wed, Jul 20, 2022 11:53:46	A4H	1	RFC_IDM	SAP*	User SAP* locked.	1
	Wed, Jul 20, 2022 12:02:40	A4H	1	RFC_IDM	SAP*	User SAP* locked.	1
	Wed, Jul 20, 2022 11:40:28	A4H	1	RFC_IDM	SAP*	User SAP* unlocked.	1
	Wed, Jul 20, 2022 11:17:15	A4H	1	RFC_IDM	SAP*	User SAP* locked.	1

Changes to accounts performed by accounts other than IDM accounts (Top...

System ID	Client	User	Changed User	Action

Default User SAP* unlocked or deleted

log_ts	System ID	Client	User	Action
Wed, Jul 20, 2022 11:58:25	A4H	001	ADMIN_SMITH	User SAP* unlocked.
Wed, Jul 20, 2022 11:40:28	A4H	001	RFC_IDM	User SAP* unlocked.
Wed, Jul 20, 2022 11:30:54	A4H	000	ADMIN_MILLER	User SAP* unlocked.

Automated monitoring of suspicious activity

Logpoint solution:

We provide monitoring and end-to-end security for your SAP system in correlation with the wider IT network, in real-time. With pre-defined alert rules and comprehensive monitoring of your logs, access controls, and changes to accounts, we can automatically detect and flag suspicious activity, so you quickly can put an end to malicious acts.

Securing your SAP system is the first step in protecting your business from existential threats.

Identify advanced attacks early and defend efficiently against fraud with Business Integrity Monitoring

Insider threat incidents have risen by 44% over the past two years, costing $15.38 million per incident.

Reduce fraud-induced losses with improved detection of anomalies in business standards. We help you uncover potential fraud patterns, so you can take the necessary steps to mitigate risks of fraud.

Easier and cheaper management of errors and fraud

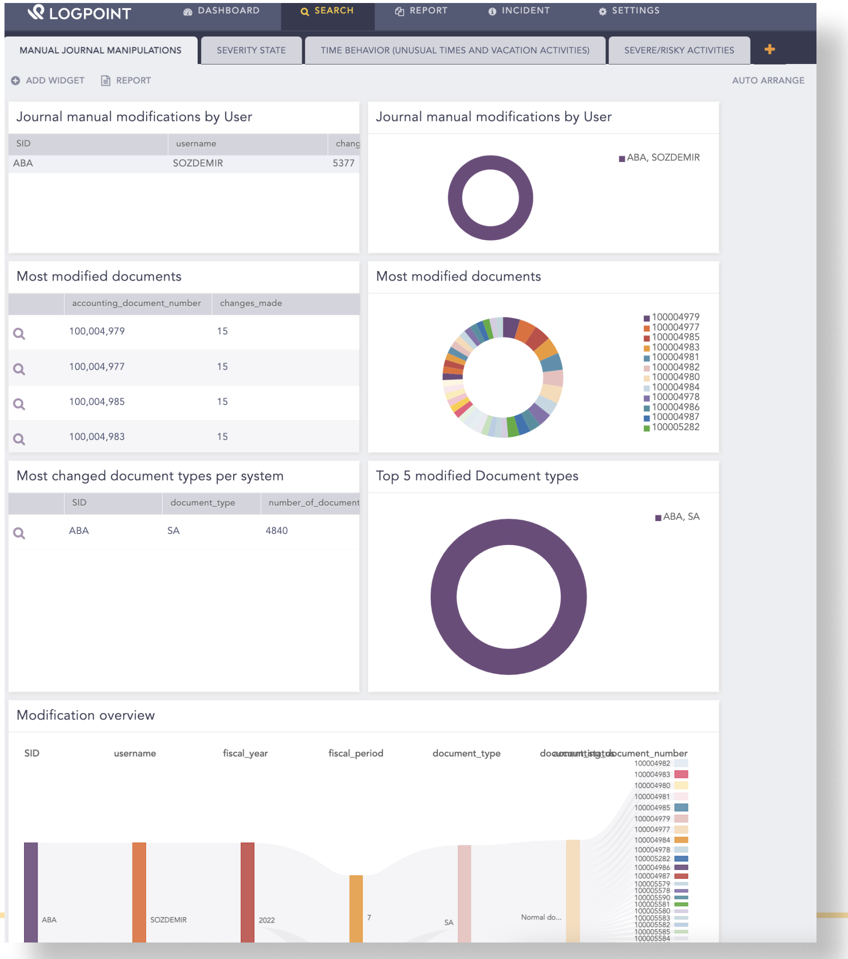
Insider threats are among the most common causes of data breaches worldwide. Coming from inside the organization, detection can be difficult. With pre-defined use cases and behavioral analytics, we identify deviations in your SAP business processes, so you quickly can put an end to employee theft, corruption, incorrect transactions, or warranty fraud.

Simple and inexpensive implementation

Get full functionality with minimal configuration efforts. No need to spend time and funds on implementation, when you can have an out-of-the-box solution that works in an instant.

Analysis at business run time

React quickly to mitigate risks effectively. Spot fraudulent activity immediately with monitoring and automated controls, at the speed of the business.



Journal manual modifications by User

SID	username	chang
ABA	SOZDEMIR	5377

Journal manual modifications by User

Most modified documents

	accounting_document_number	changes_made
🔍	100,004,979	15
🔍	100,004,977	15
🔍	100,004,985	15
🔍	100,004,983	15

Most modified documents

Most changed document types per system

	SID	document_type	number_of_document
🔍	ABA	SA	4840

Top 5 modified Document types

Modification overview

Efficiently detect and respond to fraud coming from inside the organization

- to protect your revenue and the integrity of your business

Use-case: Business Integrity Monitoring

Business challenge:

Inability to secure the integrity of a business can hurt and cripple the most robust of businesses. In 61% of all security breaches, valid credentials were involved. Insider attacks can be difficult to identify as established security controls do not apply or easily can be circumvented.

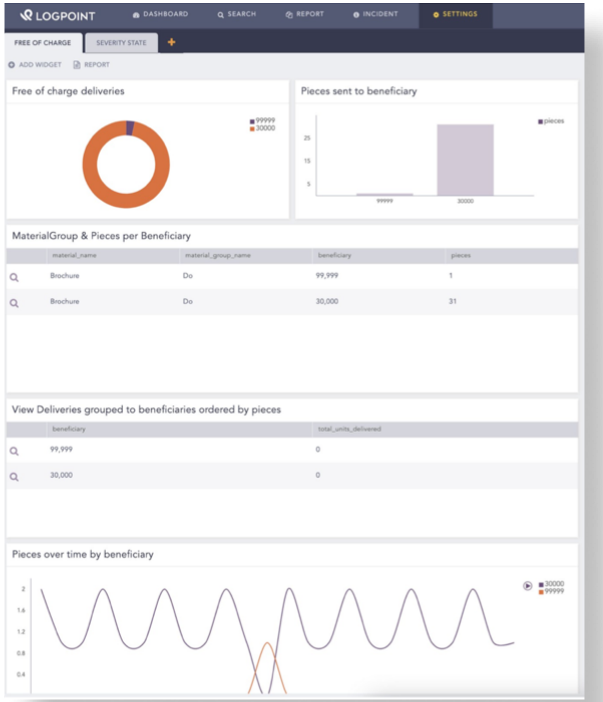
Use-case:

Detecting financial fraud within supply management

An employee in a healthcare organization creates a 'free of charge delivery' in the SAP system, then releases the order, and sends a large quantity of samples to a beneficiary. Despite being unusual behavior, traditional security tools fall short of detecting such compromising transactions, due to lacking investigative capabilities.

Logpoint solution:

With advanced behavioral analytics, Business Integrity Monitoring solution can detect deviations from standard business processes, in near real-time. In this case, anomalous transactions would be detected early, so you can intervene and circumvent financial losses.



MaterialGroup & Pieces per Beneficiary

	material_name	material_group_name	beneficiary	pieces
	Brochure	Do	99,999	1
	Brochure	Do	30,000	31

View Deliveries grouped to beneficiaries ordered by pieces

	beneficiary	total_units_delivered
	99,999	0
	30,000	0

Free of charge deliver monitors 'material groups and number of pieces sent to beneficiaries

Below are a few capabilities and examples that are delivered with Logpoint:

- Identification of critical combinations of authorizations in business processes (Segregation of duties; violations of 4-eyes-principles)
- Detection of violations against standards and policies like ISO27001, SOX, etc.
- Monitoring of current SAP activity and identification of fraud or human error
- Detection of Manual Journal entries
- Free of charge delivery
- Release strategies in the ordering process
- Duplicate invoice entries
- Multiple uses of a one-time vendor
- Monitoring of User and Business partner tolerance groups
- HR self-maintenance

Strengthen your compliance with full control of your sensitive data with Personal Identifiable Information (PII) Access Monitoring

Can you afford to lose control of your sensitive assets?

Personal Identifiable Information and corporate data are protected by regulatory standards. The inability to comply with regulation imposes sanctions and hefty penalties. For example, in the case of GDPR, entities can be fined up to 4% of their annual turnover. And if third-party data is compromised, the Copyright Act expressly provides cause for potentially massive claims for imposed damages.

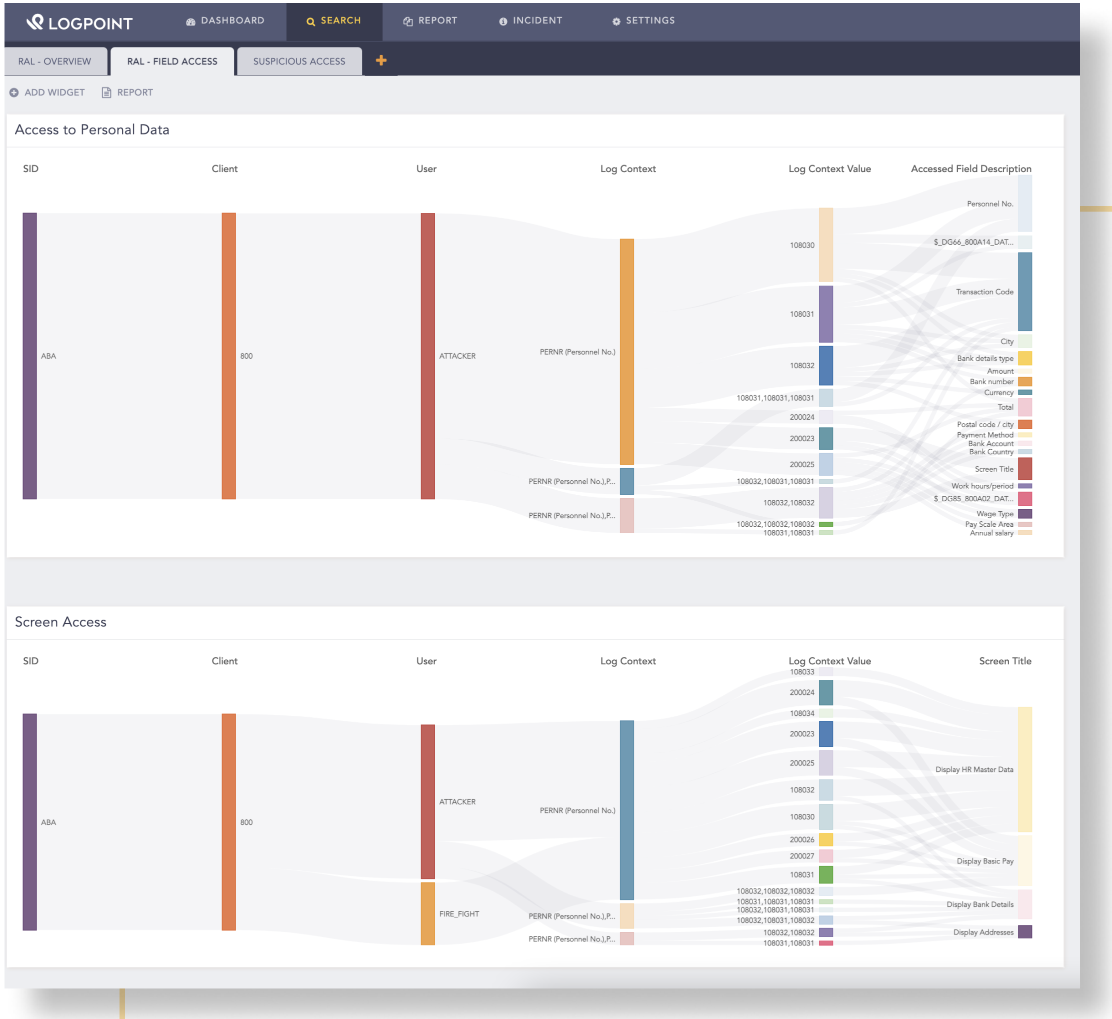
To protect this data, organizations need to understand where it resides, who has access to it, and how to monitor what is happening to it.

Meet compliance regulations

Automatically configure and extract SAP Read Access Log into SIEM for comprehensive security of your sensitive data. Monitor user authorizations in your SAP systems to detect access to critical transactions, disclosed corporate information, and personal data. Secure your sensitive data with a powerful and centralized logging solution.

Centralize the monitoring of PII and PSI into one platform

Instead of monitoring system by system, BCS for SAP enables all monitoring on a central platform. Manage access violations quickly and more effectively with a comprehensive, all-in-one overview.



Safeguard your sensitive data against theft

- to ensure compliance and avert misuse of personal data

Use-case: Personal Identifiable Information (PII) Access Monitoring

Business challenge

GDPR aims to protect personal sensitive data from misuse. To operate within EU or sell goods to EU citizens, companies must comply with the GDPR standards for collecting, storing, and managing personal data. A breach must be reported within 72 hours to a supervisory authority. Non-compliance will impose severe fines and penalties.

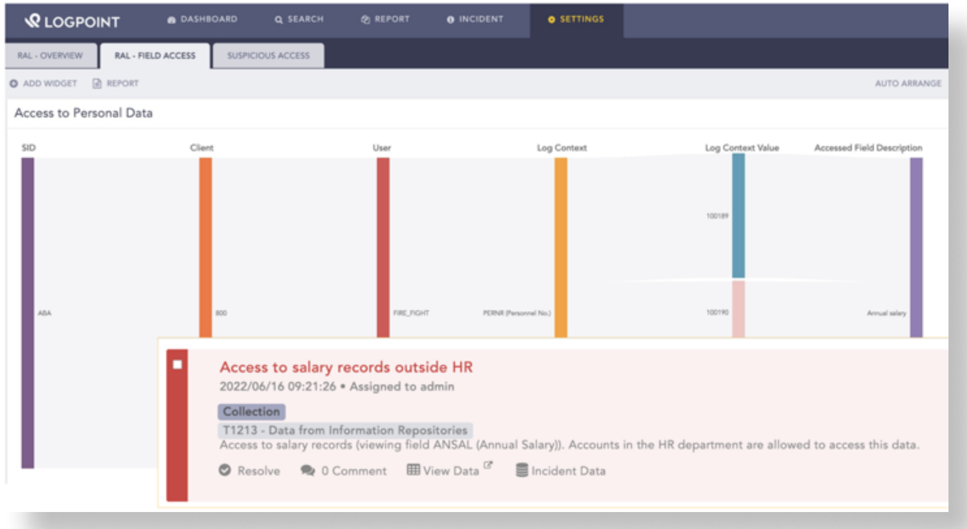
Securing your SAP system is an important step in ensuring GDPR compliance, as it stores huge amounts of sensitive data. Here are some examples of data stored in your SAP system and how it can be misused:

- Social Security/National Insurance Number
- Tax evaders
- Salaries and pensions
- Role specific authorizations

Use case:

Sensitive data is compromised by an employee

Through the transaction code PA20, an insider in a supply industry organization gained access to salary and pension payment information. This data was downloaded, sent to a private email, and subsequently distributed via mail to employees in the organization. Disclosing such sensitive data is an abuse and a clear violation of the GDPR regulations. Figuring out who had access, which accounts were accessed, and who distributed the data can be difficult.



Access to salary records outside HR

2022/06/16 09:21:26 • Assigned to admin

Collection

T1213 - Data from Information Repositories

Access to salary records (viewing field ANSAL (Annual Salary)). Accounts in the HR department are allowed to access this data.

Monitoring access to salary information

PII Access Monitoring is a powerful solution providing log access to more than 450 fields, stored in 200+ database tables, and accessible via 70 + transaction codes. We log the dialog access via SAPGUI and technical accounts' access (e.g. RFC, OData, Web UI). E.g. accessing employee data in SAP ERP HR from SAP SaaS solution Successfactors.

Logpoint solution

With the PII Access Monitoring solution, your SAP logs are continually cross correlated with logs from the e-mail, VPN access, etc. so you quickly can detect if your sensitive data has been displayed, downloaded, or sent to a private email. With our comprehensive out-of-the-box logging solution, you can effortlessly access, extract, centrally collect and automatically monitor RAL with appropriate rules.

Secure smooth operations and reduce the risks of costly outages with IT Service Intelligence

Outages are expensive - 1 in 3 cost over $1 million. Yet, during the past three years, 75% of all businesses have suffered from an outage.

Our IT-SI solution helps organizations identify an operations problem very quickly – before it impacts their revenue, customers, or internal teams.

Full-stack monitoring of your operational capabilities

Why operate in the dark and waste time searching for issues that impede your operational capabilities, when you can get full visibility with a click of a finger?

Monitor the application, integration, and technical layer to effectively detect the root causes and quickly respond to issues threatening the stability of your SAP system. Ensure smooth operations, eliminate downtime, and avoid costly outages with complete insight into your landscape.

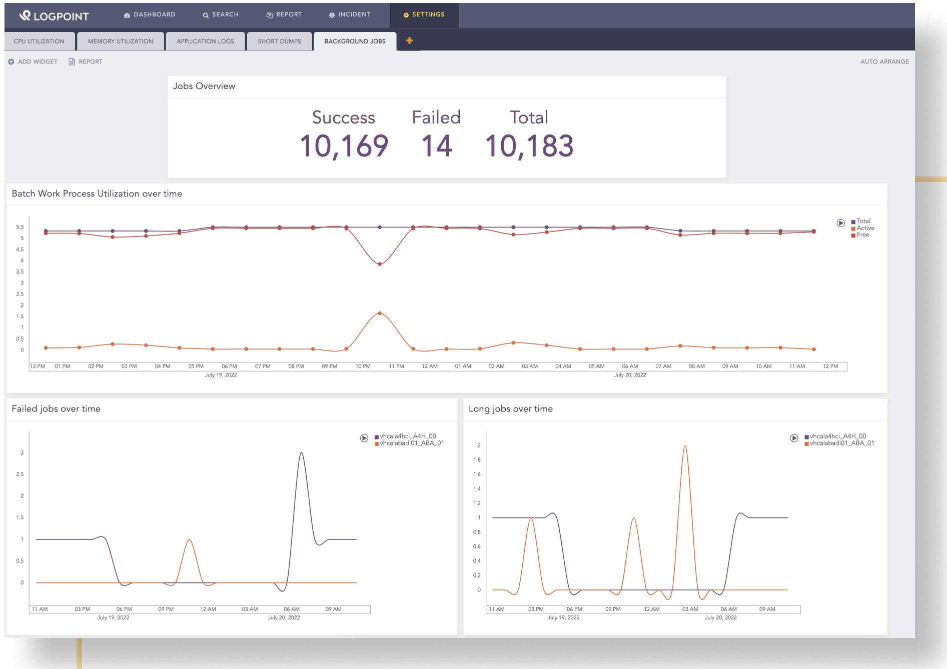
Combat degradations successfully with unified infrastructure monitoring

Work smarter, not harder. Through pre-configured KPIs, we help you monitor what matters the most. To increase efficiency, we cluster alerts into larger events and remove the unnecessary noise to help shorten your MTTR.

Effectively identify the root causes instigating service degradations and pinpoint areas of impact to make operations run more efficiently.

Act proactively with an early warning system and trend analysis

Detect future service degradations in advance based on historic data and trend analysis. Be proactive and circumvent incidents before they even happen with our early-warning system.



Jobs Overview

Success	Failed	Total
10,169	14	10,183

Secure your SAP systems against costly outages with early warning systems

Business challenge

An unexpected outage in an SAP system costs approximately $10,000 a minute. Being the primary operating system, downtime can lead to production disasters, induce delays, impact the revenue and harm your brand authority and customer trust. Due to the growing complexity of SAP systems the number of outages is rising, and subsequently recovery time objective (RTO) is increasing. 50% of SAP Basis Engineers perceive unpredictable issues in the operating system as their most significant challenge.

Use case:

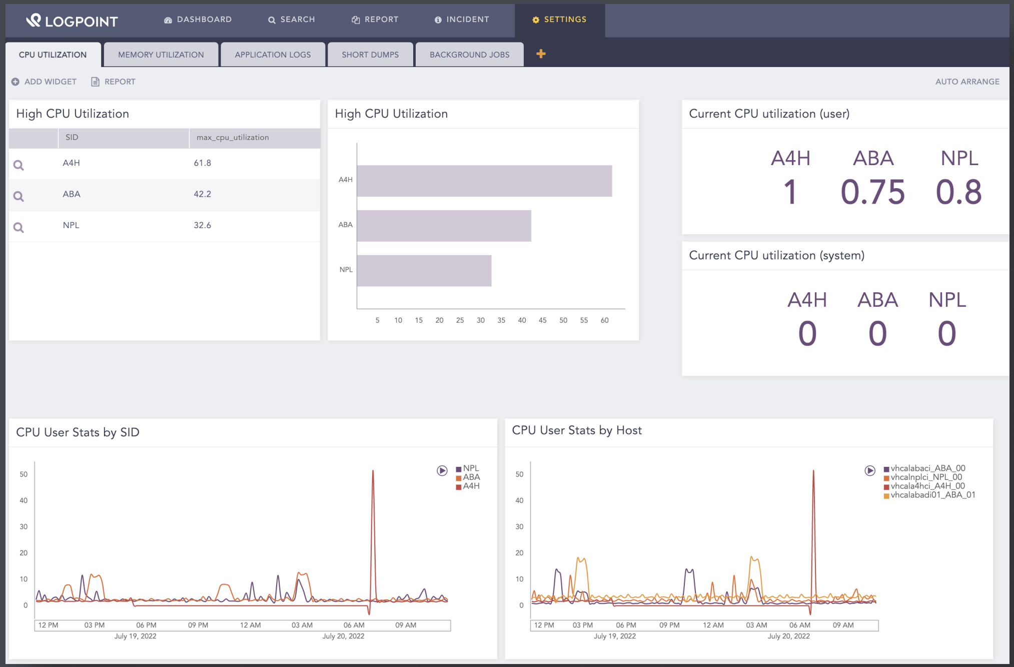
System downtime disrupting entire business processes

Due to system overload, critical SAP components suffered downtime. For this manufacturing company, SAP's inability to process data led to disruptions in business operations, fueling a chain reaction of delays throughout the entire production. This led to customer outcry, hurt the brand's reputation, and induced substantial losses in gross sales. Without historical data, predicting such downtime is an impossible task.

Logpoint solution

Detect performance issues before they affect your business processes

With full insight into the CPU usage and availability, run-time errors, background jobs, etc. SAP Basis Engineers can effectively monitor and respond to issues threatening the stability of the SAP system, in near real-time. This improves MTTR and secures operations from costly outages and unnecessary disruptions. Historical data analysis and trend graphs help you proactively circumvent future operational degradations and avoid situations of managing issues once the damage is done.



High CPU Utilization

	SID	max_cpu_utilization
	A4H	61.8
	ABA	42.2
	NPL	32.6

High CPU Utilization

Current CPU utilization (user)

A4H	ABA	NPL
1	0.75	0.8

Current CPU utilization (system)

A4H	ABA	NPL
0	0	0

CPU User Stats by SID

CPU User Stats by Host

Continuous, automated extrications of CPU and memory utilization

Proactively fix operational issues before they become an outage with the IT-SI solution.

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit www.logpoint.com

Trusted by more than 1,000 enterprises

KONICA MINOLTA CAPTIVATE BOEING GOSECURE RÉMY COINTREAU

Awards and honors

Gartner peerinsights customers' choice 2021

Gartner Peer Insights

Gartner

Gartner Magic Quadrant

Software Reviews GOLD MEDAL 2021 SECURITY INCIDENT AND EVENT MANAGEMENT