Protect SAP systems with LogPoint for SAP

To detect and respond to fraud and cyberattacks, organizations need to monitor the entire network, including IT infrastructure, cloud applications and business-critical SAP® systems. SAP is one of the most critical applications in an organization, and it is often not part of the security monitoring solution.

LogPoint for SAP bridges the gap between SAP and SIEM solutions. With LogPoint for SAP, organizations can continuously monitor their SAP data to detect threats and maintain compliance within SAP.

LOGPOINT

Benefits of LogPoint for SAP

One central security monitoring solution

Organizations can monitor and track SAP events in near real-time throughout the entire IT environment, increasing cybersecurity posture.

Reduce the impact of cyberthreats

Receive alerts for any suspicious activity, making it easy to detect potential issues and quickly put a stop to any cyberattack.

Save time by automating tasks

Ready-to-use controls, checks, dashboards and reports automate the monitoring of SAP system compliance or maintenance.

Automated audits and compliance

Analyze and monitor SAP information and events to continuously audit the system and automatically create reports. Automated audits help identify system vulnerabilities and maintain compliance.

Works with any SIEM

LogPoint for SAP makes it possible to integrate SAP with any of the leading SIEM providers, including LogPoint, Splunk, ArcSight, LogRhythm and QRadar.

What is SIEM?

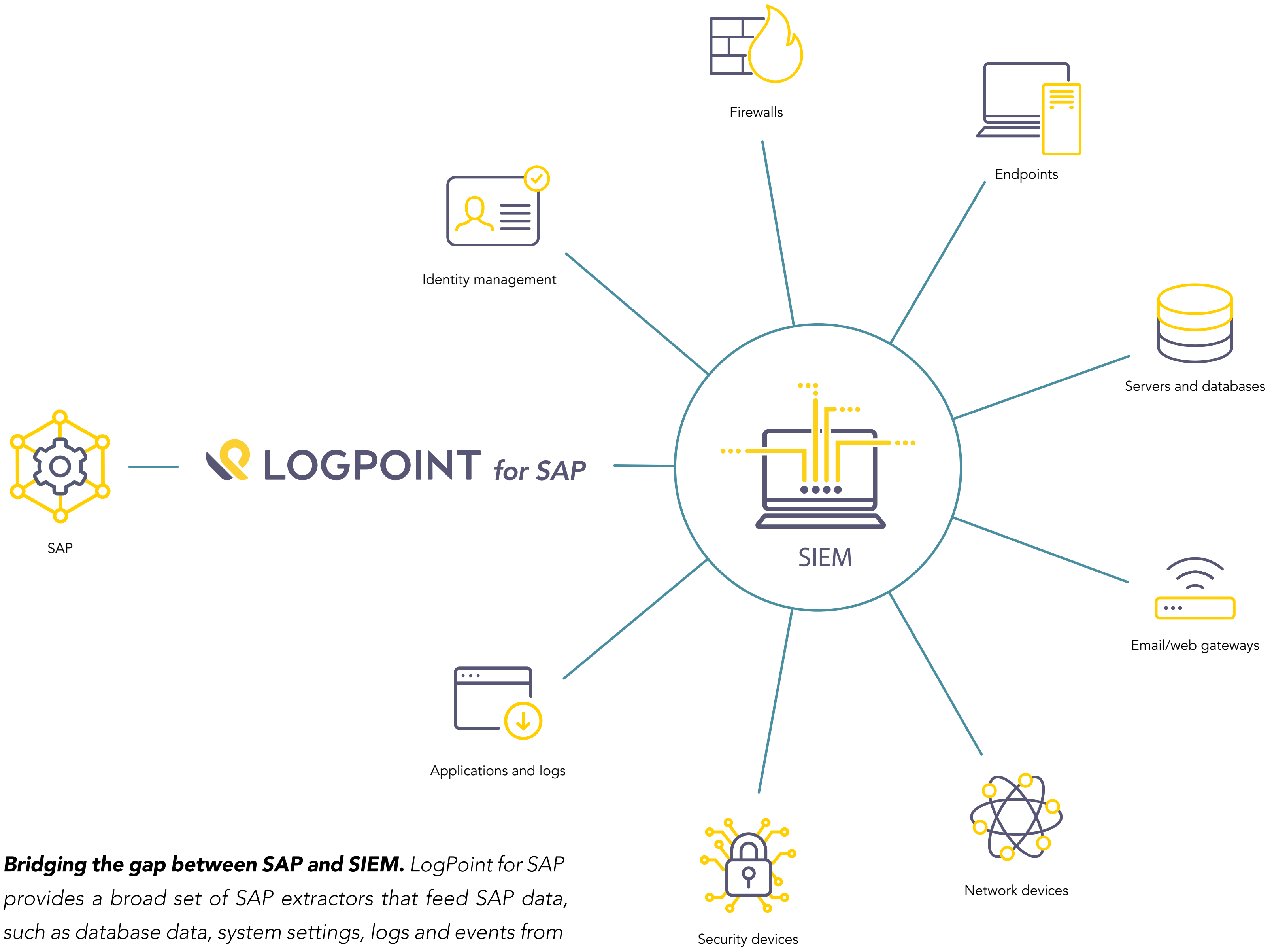
Security information and event management, or SIEM, aggregates data from multiple systems and analyzes it to detect abnormal behavior or potential cyberattacks. SIEM tools provide a central place to collect events and alerts making it easier to monitor and troubleshoot your IT infrastructure in real time.

How it works

LogPoint for SAP is a bridging technology that integrates SAP landscapes and different types of SAP data into SIEM.

LogPoint for SAP is based on a three-tier architecture model with a collection, administration and analysis layer. An extended security analytics pack categorizes events and has a large set of predefined SAP-specific event correlations for different security domains.

LogPoint for SAP also has an SAP-specific security intelligence pack that provides detection scenarios, visualization and notification, and delivers alerting rules, reports and dashboards.



Bridging the gap between SAP and SIEM. *LogPoint for SAP provides a broad set of SAP extractors that feed SAP data, such as database data, system settings, logs and events from various SAP security sources into SIEM.*

How businesses can use LogPoint for SAP

LogPoint for SAP is used to supervise security-critical activity and events, access control checks, monitoring of audit-relevant information, and compliance of system settings and authorizations.

SAP operations

Integrating SAP Basis information and events improves the efficiency of processes and remediation cycles. It also makes it possible to provide ad-hoc reports of system metrics data.

Any SAP data

Get any SAP data with the help of flexible and configurable LogPoint for SAP data extractors. The extractors help create any use case and integrate any SAP-based applications.

SAP log management

LogPoint for SAP extractors retrieve all kinds of security-relevant information of SAP NW and ABAP-based SAP systems. LogPoint for SAP adds SAP security intelligence to any SIEM solution.

For more information about LogPoint for SAP:

www.logpoint.com/LogPointforSAP

sales@logpoint.com

Ready to use

LogPoint for SAP has a large number of detection use cases, including dashboards, searches, reports and search forms. With LogPoint for SAP organizations can fully integrate SAP information into SIEM for continuous, automated monitoring and automated incident response.

LOGPOINT *for SAP*