Microsoft

Protect your SAP systems with the Azure Sentinel threat monitoring solution for SAP

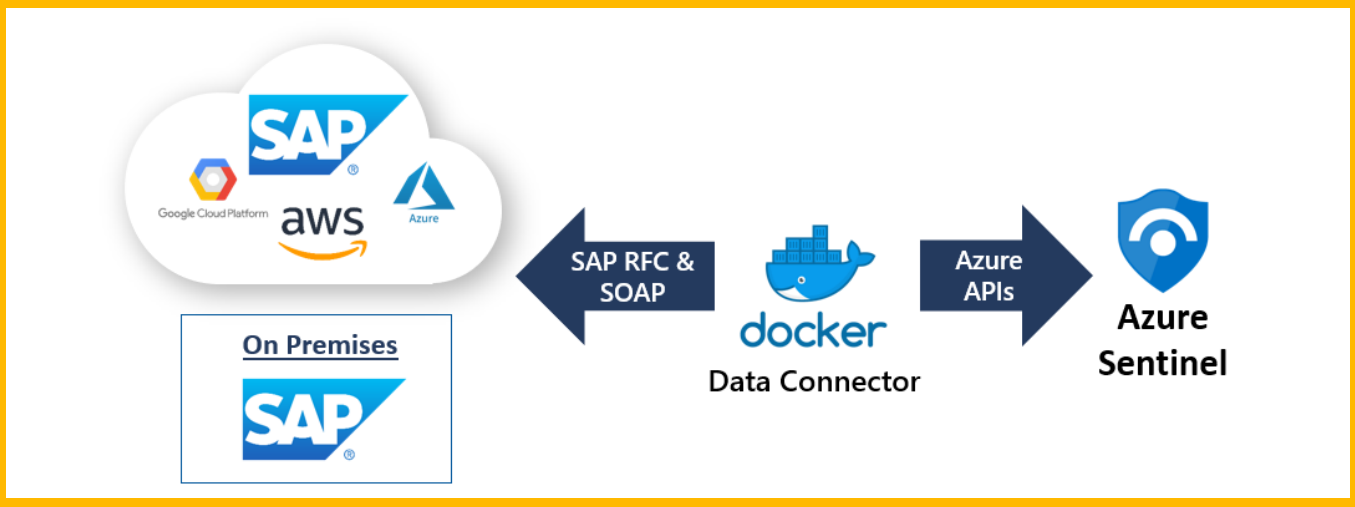
Your SAP systems and applications handle massive amounts of business-critical data, but protecting these systems is notoriously challenging. The complex nature of SAP systems means threats can emerge across multiple modules, requiring ongoing monitoring, advanced threat detection, and cross-correlation. However, since these ecosystems are so unique, it's traditionally been difficult for security operations (SecOps) teams to monitor SAP effectively for threats.

The Azure Sentinel threat monitoring solution for SAP cuts through the complexity of SAP systems to provide continuous threat detection and analytics for SAP systems hosted on Azure, other clouds, or on-premises.

- **Continuously monitor SAP systems for threats at all layers:** Gain visibility at business logic, application, database, and OS layers.
- **Detect common SAP threats:** Discover privilege escalation, unapproved changes, and more with out-of-the-box detections.
- **Correlate SAP activity with other signals:** Accurately detect SAP threats by cross-correlating across all your data sources.
- **Customize to your needs:** Build your own detections to monitor sensitive transactions and other business risks.

Deployment and content details:

- **NetWeaver data connector:** Delivered as a Docker container image that can be deployed anywhere in the network and integrate to SAP NetWeaver-capable systems, the data connector collects more than ten different log files for monitoring business and application risks.
- **SAP infrastructure data connector:** Use Azure Sentinel data connectors for your underlying infrastructure (virtual machines, storage, network, Azure Active Directory) while monitoring HANA database audit logs using Azure Sentinel Syslog integration.
- **Built-in security content:** Built-in detections help catch SAP threats, such as configuration changes, execution of sensitive function modules, and suspicious activity by privileged users. Plus, a workbook helps SecOps teams visualize the security health of their SAP systems.
- **SAP application logs:** Gain deep insights into SAP transactional activities with the SAP security audit log, job log, spool log, change documents, and more.
- **Simplified deployment:** Protect your SAP systems today with simplified deployment and integration via the Azure Marketplace.



Microsoft

The Azure Sentinel threat monitoring solution for SAP detects threats like:

Abuse of SAP privileges: An SAP user with developer privileges could exploit those rights to view sensitive documents, such as HR or financial data, or to gain elevated access. With Azure Sentinel threat monitoring solution for SAP, your SecOps team can define a granular set of sensitive modules—narrowing detection parameters for production environments or performing specific operations in a development or sandbox system. Pre-configured functions enable you to monitor a baseline from day one, all while retaining the freedom to modify any configuration via Azure Sentinel watchlists.

SAP break-glass users: In SAP environments where usage needs to be carefully monitored because of default "superman" users (DDIC) with elevated privileges, your team can monitor system access and automatically call a playbook that requests SAP basis permissions. Grant only the permissions needed to perform a specific operation using your designated Microsoft Teams channel.

.

Attempts to bypass SAP security mechanisms: Detect indicators that a user is trying to bypass SAP security mechanisms, such as disabling audit logging (HANA and SAP), executing sensitive function modules, unlocking blocked transactions, or debugging production systems.

Data exfiltration: SAP systems contain extremely sensitive data, making them a prime target for data exfiltration. Detect signs of malicious data exfiltration activity such as unusual file downloads, spool takeovers, access to insecure FTP servers, and connections from unauthorized hosts.

Malicious initial access: The Azure Sentinel threat monitoring solution for SAP detects signs that an attacker has made initial access to your SAP system, including brute force attacks, multiple logins from the same IP address, and privileged logins from unexpected networks.

Pro tip: Learn how to deploy continuous threat monitoring in your SAP system.

Get the flexible cloud solution that delivers comprehensive protection for SAP systems and helps enable your SAP cloud migration—**Azure Sentinel threat monitoring solution for SAP**.