APPSIAN

USE CASE

Mitigate SAP Data Exfiltration Risks

Prevent data leakage from both privileged accounts and normal end-users by ensuring data can only leave SAP in secure environments

The financial, reputational, and regulatory impact of a data breach can be catastrophic. Data exfiltration, whether malicious and accidental, typically originates from employees' legitimate access to ERP applications and can be hard to prevent or detect with existing SAP security capabilities.

SAP's security stature is inherently robust and secure. However, with the radical increase in insider threats, legacy access control and data protection features pose certain limitations:

Static rules – User privileges are governed by static roles and groups. The black and white approach often forces a compromise in security for the sake of usability.

Limited data masking – Preventive measures such as data masking are difficult to implement, and once implemented, can create user friction if data access is required.

Lack of contextual controls – User roles that require privileges to high-risk transactions / data can access this information freely, regardless of where access is coming from.

Limited visibility – Current logging and analytics capabilities are not actionable enough to decipher malicious user activity from normal usage.

Protect SAP Data with Appsian

Appsian Security Platform allows SAP customers to mitigate the risks of data exfiltration while still providing secure and productive user access. With native integration, Appsian's plugin extends SAP controls to account for real-world access and the risks that come with it. Advanced logging and analytics capabilities further enable organizations to quickly detect and remediate suspicious user activity.

Block Report Downloads

Prevent users from executing transactions that download SAP data in high-risk scenarios, such as: after business hours, from untrusted locations, networks, or devices.

Deploy Policy-based Data Masking

Reduce the exposure of high-risk data using a centrally managed policy that can adjust access based on context (e.g. mask field when user access is remote, show field when on corporate network).

Expedite Detection & Response

Gain real-time visibility into data access and download attempts by users. Trigger security event alerts for high-risk access (e.g. CXO salary was viewed) and anomalous activity (e.g. deviations from baselines).

8111 Lyndon B Johnson Fwy. Dallas, TX 75251 ☎ +1 (469) 906-2100 ✉ info@appsian.com