Maximize Your SAP Access Control Investment with Flexible Use-Cases

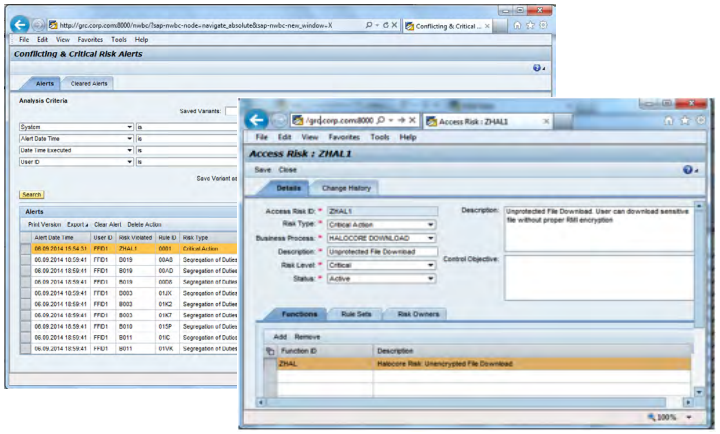
SECUDE's Halocore for SAP NetWeaver can complement your efforts to strategically manage your organizations risk with our integration into SAP Access Control, part of the Governance, Risk, and Compliance (GRC) portfolio. Alongside Halocore's core capability of protecting sensitive data that leaves SAP in an unstructured form (such as a spreadsheet), Halocore also captures real-time logs pertaining to these downloads. Learn the Who, What, and Where of all activity surrounding confidential information downloaded from your SAP systems for simple, functional, and secure monitoring.

- Extract data for more powerful analysis
- Identify who downloads what by name and file
- View where data is going by path, terminal and IP address

The comprehensive information within these download logs can seamlessly integrate into your SAP Access Control landscape to aid in detection and prevention of risk via real time reporting.

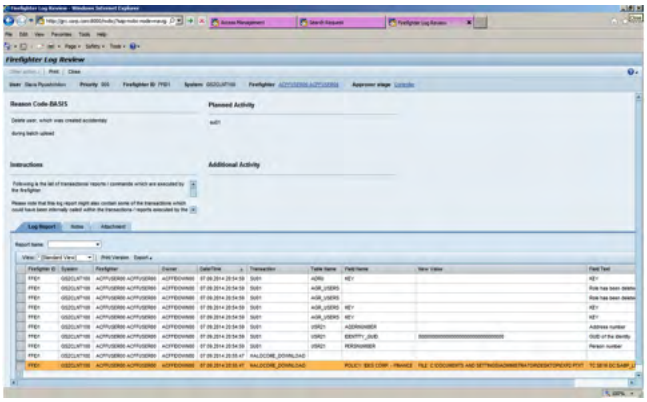
Trigger Alerts

You can trigger alerts when something unexpected or potentially damaging for the enterprise occurs. Leverage your existing SAP Access Control infrastructure to track the download activity of SAP users and trigger alerts if the system deems the combination of access attributes risky. Get notified anytime unprotected unstructured data leaves SAP by continual monitoring of the Halocore logs with SAP Access Control. Know when your sensitive company information is leaving the secure boundaries of SAP. Customize what you want to be notified about, for example you can trigger alerts by certain transaction types, file types, or users. Detect latest security and compliance risks before it's too late.



Enhance Firefighter Activity Review

Ever wonder if Firefighters could download any sensitive information during their sessions? Controllers are challenged to review numerous Firefighter logs daily that often fail to inform them about potentially risky download behavior. Don't leave your company at risk by failing to monitor the usage of sensitive information during Firefighter sessions. Gain more control over the highly versatile Firefighter user access by capturing information pertaining to data downloads occurring in these sessions. Controllers now have more information on Firefighter activity to ensure compliance and to mitigate any potential risky behavior.



SAP® Certified
Powered by SAP NetWeaver®

Halocore for SAP NetWeaver

Companies around the world rely on SAP to collect, analyze, and report data crucial to the success of their business. This data is considered secure while inside the protected boundaries of SAP, but data exists to be consumed and shared. To perform their jobs, employees download countless documents and reports every day, containing some of the most sensitive information an enterprise has. Documents with personally identifiable information (PII), social security and credit card numbers, customer data, product specs, and trade secrets travel freely without any protection to employees' computers and mobile devices, cloud, partner mailboxes, and beyond. How can an enterprise make sure its most sensitive data is persistently protected, while maintaining control and enabling secure collaboration?

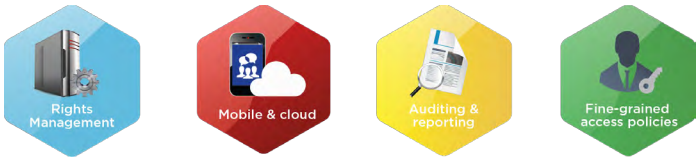
Data-Centric Security of Sensitive Data Leaving SAP

Applying protection to the information at a file level solves this problem by allowing downloaded information to travel safely in and out of SAP systems. Halocore for SAP NetWeaver, SECUDE's one-of-a-kind data protection solution for SAP data, delivers instant and permanent information protection, while facilitating compliance and productivity.

Unlike traditional data protection solutions that are focused on securing the network perimeter or data storage locations, ranging from Data Loss Prevention (DLP) and firewalls to antimalware and encryption, Halocore protects the information itself. Halocore is directly integrated with SAP. The solution intercepts each data download, classifies the information, and applies strong encryption, while controlling what users can do with sensitive data through easy-to-setup protection policies. Halocore is powered by a data classification mechanism that is based on SAP's existing roles and authorization scheme to protect files of any type and extension coming out of SAP.

Powerful Protection

Halocore for SAP NetWeaver is powered by Microsoft Rights Management (RMS), the industry leading document security technology that allows only authorized users to access sensitive data inside and outside the enterprise boundaries. Halocore is available in several deployment options: on-premise using AD RMS, in the cloud using Azure RMS, or as a combination of both in a hybrid scenario.



Perimeter Security is Failing

- 43% of U.S. businesses suffered at least one cyber incident this year*
- Average cost of a data breach in U.S. is $5.85 million*
- Attackers spend on the network an average of 243 days before being detected**
- 47.9% of the reported breaches involved the exposure of SSNs and 15.6% exposed credit card information***

* Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2014
** Threat Landscape Study, Mandiant, 2013
*** ITRC Breach Report, Identity Theft Resource Center, 2013

Key Benefits

- Provides end-to-end protection of sensitive SAP data that extends to mobile and cloud platforms
- Minimizes the risk of breaches, data theft and accidental loss
- Controls who has access to sensitive information and what they can do with it (view, edit, save, print, forward, etc.)
- Boosts secure collaboration within the organization and with partners and suppliers
- Enables compliance, while addressing the challenges of an increasingly complex regulatory landscape
- Offers advanced auditing capabilities, aimed at simplifying internal audit processes