SAP Security Reimagined

SECUDE's Halocore platform is designed to simplify the task of securing sensitive information downloaded from SAP. In a modern enterprise where there is a rise of business collaboration, an explosion of storage locations, cloud computing, and an increased mobile workforce, traditional protection mechanisms are often left powerless. SECUDE's **Halocore for SAP NetWeaver** represents the next generation of information security solutions that enforce protection on the data/documents themselves.

Business Challenges

Today, business processes rely heavily on SAP applications that handle product lifecycle, finances, customer relationship, or human resource management. These applications store vast amounts of information about your business, products, finances, employees, partners, and customers.

Being among the elite of enterprise IT users worldwide, SAP clients have long realized that their business revolves around information. They fiercely protect and leverage that information for greater advantages in their industries. As a result, a wide range of security technologies is deployed to strengthen SAP servers and their perimeters to ensure proper access control.

However, there is an often-overlooked blind spot that can leave some of the most critical information vulnerable and exposed.

On a regular basis, users export sensitive data from SAP applications to generate reports, spreadsheets, PDFs, and other documents. The information is then downloaded and stored on devices such as USB thumb drives and local hard disks, or more increasingly on mobile devices and in cloud storage solutions, such as Dropbox and Microsoft OneDrive.

Sometimes the data is stored in a place where you have an ability to control access, such as a network file server or a Microsoft SharePoint portal. However, this data often ends up in a place beyond your control, such as on the file share of an untrustworthy partner or the inbox of a competitor. Even on trusted employee devices, with the increase in sophistication of malware and Trojans, the risk of data loss has never been higher.

The IT security industry has been attempting to tackle this problem for many years. Solutions such as Data Loss Prevention (DLP), application firewalls, or file storage encryption are often deployed. The problem with these approaches is that they are numerous steps away from the point where data leaves the secure perimeter of the application and its access control mechanisms.

How does a company ensure that data leaving applications is correctly classified and protected from unauthorized access?

Every month, there is an increase in the number of places where your exported SAP data can be saved.

Solution Overview

Halocore for SAP NetWeaver integrates directly with SAP. By ensuring data is secured right at the moment it leaves SAP applications, Halocore integrates persistent protection with advanced classification and auditing capabilities.

Instant Security

The Halocore NetWeaver Add-On 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. All of this is done before the content leaves SAP. Protection is immediate and applied directly to the downloaded file.

Permanent Protection with Microsoft Rights Management

Halocore utilizes the Microsoft Rights Management solution via Windows AD Rights Management (AD RMS) for on premise environments or Azure Rights Management (Azure RMS) for hybrid or full cloud environments to apply protection to downloaded data. Microsoft Rights Management is the industry leading document security solution and allows you to ensure only authorized users can open the protected content, while also controlling what they can do with it, such as print, edit or save.

Mobility

Downloaded files remain protected no matter where they may travel, inside or outside of the organization. Since the content is secured as soon as it leaves the application, risk of exposure is reduced when it ends up in emails, network shares, or even mobile devices and cloud services

Auditing & Reporting

Halocore has rich auditing capabilities, providing immediate visibility of how data is exported from SAP and is shared throughout your organization and beyond. Audit information can be aggregated through the Microsoft Rights Management technology and imported into your existing reporting and GRC systems. Now your CIO can see who is accessing sensitive SAP data, even when it's downloaded, emailed and sent to partners.

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

Technical Requirements

Halocore for SAP NetWeaver comprises of two main components:

- Halocore Server
- SAP Add-on

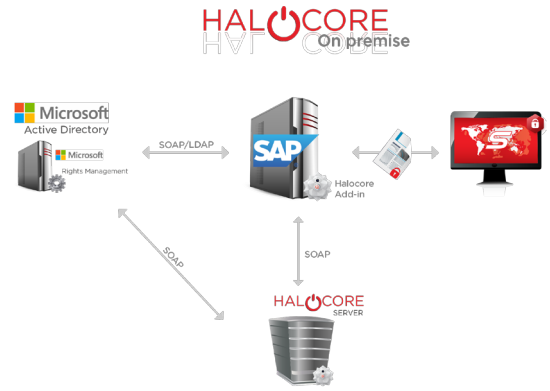
The Halocore Server runs as a service in a Microsoft Windows Server and the SAP Add-on is installed into the SAP NetWeaver application server. We also leverage the Microsoft Rights Management technology to provide the persistent document protection.

Component	Supported platforms
SAP Add-on	NetWeaver 7.00, 7.01, 7.02, 7.31, 7.40
Halocore Server	Windows Server 2008 R2, 2012, 2012 R2
Microsoft Rights Management	Windows Server 2008 R2, 2012, 2012 R2

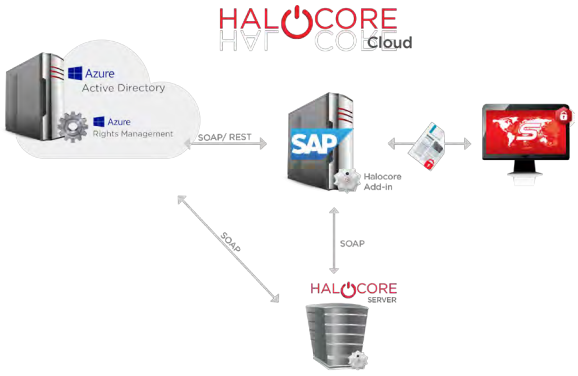
Deployment Options

Halocore for SAP NetWeaver is available in a variety of deployment options to allow enterprises to pick the scenario that best fits their information architecture and IT infrastructure.

- **On-premise:** A traditional on-premise approach might be most beneficial for companies with existing significant investments in on-premise systems.



- **Cloud:** A cloud-based option provides flexibility associated with licensing and scalability, without significant capital investment and incremental resources to support it.



- **Hybrid cloud:** A hybrid cloud approach enables the best of both worlds, delivering cloud-like flexibility, with the confidence of on-site hardware.