HALOCORE

Frequently Asked Questions

Welcome to HALOCORE FAQ. In this document, you will find answers to important questions regarding HALOCORE products, services, security, and infrastructure policies.

The purpose of this document is to provide quick guide to the frequently asked questions about our HALAOCORE product.

While this document contains answers to our most frequently answered questions, should you have any additional questions, please contact our sales representative or our support team.

TABLE OF CONTENTS:

GENERAL FAQs

Q: Does HALOCORE have a SAP certification?

A: Yes, HALOCORE is SAP Certified for deployment on SAP S/4HANA.

Q: Who are your reference customers?

A: Microsoft, MARS, Swisscom, Accenture & Infosys are some of our reference customers.

Q: Is it possible to run a proof of concept?

A: Yes. The customers can experience different use cases of HALOCORE with our remote PoC environment on SECUDE Garden4You. SECUDE's GARDEN4YOU is a remote standalone demo environment for performing a PoC with Microsoft Information Protection. The POC showcases the ability to handle sensitive data from SAP, CAD/PLM using SECUDE's flagship products HALOCORE and HALOCAD respectively.

To know more and schedule a PoC, visit https://secudegarden4you.com

Q: What are the commonly used sensitive data in an organization that needs protection?

A: The different types of sensitive data within an organization:

- Customer (CRM)
- Finance (FI/CO)
- HR (HCM)
- Material (MM/SRM)
- Production & Logistics (LO/EWM/WM)
- Pricing (SD/MM/SRM)
- Reports (BI/BW)

Q: Is there a way to modify the permissions on the data once the data is out of SAP?

A: By default, HALOCORE puts the "system" as the owner of the exported file. As a result, no user can change the permissions to the file, which ensures the highest security level. However, as a special case, HALOCORE can be configured to set the user, who downloaded the file, also as the owner of the file. The file owner can change the permissions of any file previously protected.

PRODUCT FAQs

Q: What are the different modules of HALOCORE?

A: HALOCORE has three different modules:

MONITOR – Monitor all SAP user data exports and downloads
BLOCK – Block unauthorized exports out of SAP
PROTECT – Access & privilege control for sensitive documents out of SAP

Q: What's the benefit of HALOCORE?

A: The data exports of the SAP users are automatically labeled and protected. The exported data are thus subject to the same protection and access restrictions as within the SAP environment. Every data export is logged and can be analyzed in real time.

Q: What SAP modules are typically protected by HALOCORE?

A: Downloads from any SAP module can be protected, and most commonly those with sensitive data such as FI-CO, HCM, ESS, IDM, IAM, Basis, GRC, etc. are protected. The definition of sensitive data may vary from business to business, consequently the modules and transactions to protect are selected by the HALOCORE administrator.

Q: What download file types are typically protected by HALOCORE?

A: Most commonly all files, but they also can be specified: Excel, Word, PowerPoint, txt, CAD, HTML, XML, email, PDF, PPT, ZIP, etc.

Q: Does the HALOCORE module 'MONITOR' provide real-time notification of data leaks?

A: Yes. HALOCORE reduces risk and helps users stay compliant by providing real-time alerts of sensitive data downloads. Also, all data downloads and extraction activities from SAP are aggregated into a fully customizable audit log, which can be extracted to powerful tools such as SAP Business Intelligence and Analytics solutions.

Q: Is it possible to implement the module 'MONITOR' alone without buying/implementing the complete HALOCORE suite?

A: Definitely. HALOCORE can be implemented as per the data security requirements of the end user. MONITOR can be installed to meet the client's data tracking and audit requirements. In fact, implementing MONITOR is often considered the first step in establishing a comprehensive data security system. As the MONITOR module of HALOCORE provides the vital visibility into what happens to downloaded data by tracking and analyzing access to sensitive SAP data exports for enhanced control and compliance, it forms the must-have foundation for subsequent deployment of BLOCK and PROTECT.

Q: SAP GRC detects unauthorized SAP data exports. How does HALOCORE add value and differentiate?

A: Typically, SAP GRC monitors unauthorized SAP data exports, which basically covers audit and classification of SAP 'user downloads. However, HALOCORE does not only do this for individual end users, but also monitors backend API data flows. In other words, it extends the audit and classification functionalities to applications as well. This is critical to the current complex SAP operations scenario as many protocol-based machine-to-machine communication (APIs) are legacy.

Q: Is it possible to implement HALOCORE BLOCK alone without buying/implementing the HALOCORE suite?

A: MONITOR is a prerequisite (foundation) on which BLOCK and PROTECT function. Thus, BLOCK cannot function without MONITOR. However, it does not require installation of PROTECT to function as these two modules function independently, but in parallel, depending upon the user's requirement.

Q: Is the security policy for HALOCORE BLOCK rigid? Can it be modified?

A: BLOCK is the only SAP integrated DLP solution for structured data. The classification determined by the MONITOR module from the SAP context information is used as input for corresponding blocking rules. Administrators can easily define, e.g. based on user, role, IP range, etc., in which cases the data export should be prevented.

Q: On what functions and on what interfaces does HALOCORE BLOCK perform?

A: The BLOCK function of HALOCORE prevents unauthorized exports out of SAP. It prevents data leakage through platforms such as file printing and emailing. It also prevents data leakage from unauthorized exports when using other SAP frontends, such as Business Object (BO) or BEx.

Q: Is it possible to implement HALOCORE PROTECT alone without buying/implementing the HALOCORE suite?

A: MONITOR is a prerequisite (foundation) on which PROTECT and BLOCK function. Thus, PROTECT cannot function without MONITOR. However, it does not require installation of BLOCK to function as these two modules function independently, but in parallel, depending upon the user's requirement.

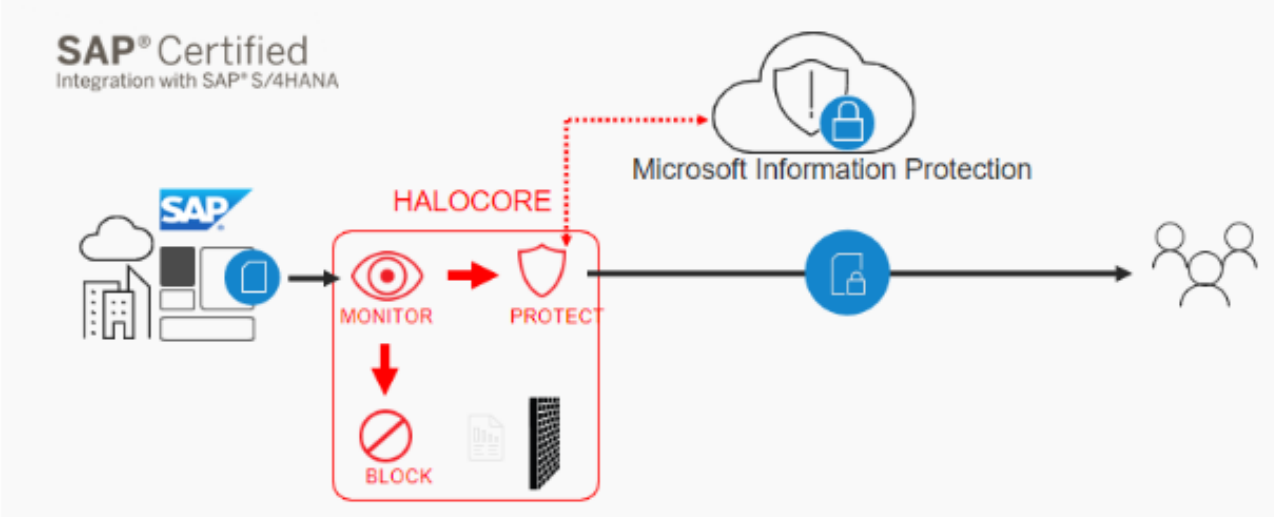
Q: How does HALOCORE address data leaks in SAP?

A: HALOCORE plugs the critical security hole in SAP environment by:

- Blocking data exports, which must not leave SAP
- Protecting sensitive data, which is needed outside of SAP

Q: What is the architecture of HALOCORE?

A: Here is the reference architecture of HALOCORE for SAP



SUPPORT FAQs

Q: Which team is required to install HALOCORE in a company?

A: HALOCORE is an infrastructure software and employees from the following teams are needed for the installation: SAP Basis Administrator, SAP ABAP Developer, Microsoft Information Protection Administrator, Network/Firewall Administrator, Windows Server Administrator.

Q: What are the supported SAP Releases?

A: SAP NetWeaver 7.00, 7.01, 7.02, 7.31, 7.40, 7.50 and S/4HANA 1511, 1610, 1709, 1809, 1909, 2020.

Q: What are the supported Servers to run the Halocore Central Server and the Halocore Service?

A: Microsoft Windows Server 64bit, 2012 2012 R2, 2016, Core 2019.

Q: Is it possible to send the HALOCORE log information to a SIEM system (like Splunk or QRadar)?

A: The HALOCORE log Information can be processed in real time in a SIEM system. A wide number of SIEM systems are supported.

Q: What are the various SIEM solutions supported?

A: The HALOCORE audit log can be forwarded automatically to all kind of SIEM solutions, like SAP ETD, HP ArcSight, IBM Security Qradar, Splunk, etc.

Q: What are the supported log formats?

A: Common event format (CEF), Log event extended format (LEEF) & JavaScript Object Notation (JSON).

Q: Does HALOCORE support custom programs and custom transaction codes (z tcodes)

A: Yes. You can monitor, block or protect downloads out of any custom program or transaction.

Q: Which UI technologies are supported by HALOCORE?

A: HALOCORE supports all SAP standard UI technologies, like SAP GUI, Web Dynpro, FIORI, etc.

Q: What versions of GRC does HALOCORE support?

A: Currently we support GRC Foundation ABAP 10.0 (component GRCFND_A, release V1000) or greater, and GRC NetWeaver Plug-In 10.0 (component GRCPINW, release V1000_700) or greater.

INFRASTRUCTURE & SECURITY FAQs

Q: What infrastructure components are part of the HALOCORE landscape?

A: SAP ABAP Server, SAP GUI Client, Windows Server to run the Halocore Central Server and Halocore Service, Microsoft Information Protection Service in the Microsoft Azure Cloud, Network and Firewall.

Q: What changes need to be made to my SAP system?

A: The HALOCORE ABAP Add-On must be installed. In addition to the ABAP Add-On a few ABAP Code-Changes need to be implemented.

Q: How long will it take to setup a HALOCORE Pilot?

A: The installation of the ABAP Add-On and the ABAP Code Changes will take 3 hours. The installation and configuration of the Halocore Central Server and Halocore Service will take 1 hour. The configuration will take 1 hours. The pure installation and configuration therefore take around 5 hours. .

Q: How long does it take to implement HALOCORE?

A: Implementation of HALOCORE is simple and does not require any major external support. Implementation support will be provided by SECUDE or by a channel partner through whom the end customer buys the solution. In terms of man days, HALOCORE can be installed within just four to eight days depending upon implementation size and other end-customer related factors.

Q: What is required for Azure/MIP configuration?

A: User login ID’s and passwords for the HALOCORE Central Server and for end users (individual or group). Azure labels specific to the security levels may be required. Typically, the default labels used with Microsoft Office can be applied.

Q: Does HALOCORE require additional hardware to implement?

A: No. HALOCORE’s technical components are running on a standard web server on any virtual machine or cloud environment. They scale like any other web server too.

Q: Is there a performance overhead by adding HALOCORE?

A: There is no performance impact when HALOCORE is monitoring or blocking SAP downloads. The performance overhead caused by HALOCORE while protecting the downloads is very minimal. SAP users will not recognize any impact by HALOCORE.

LICENSE RELATED FAQs

Q: What other products must be licensed in order to use HALOCORE in the SAP landscape?

A: Microsoft Information Protection (MIP) must be licensed.

Q: What Microsoft License is needed for HALOCORE?

A: The Microsoft 365 E5 license is required to implement automated processes based on Microsoft Information Protection (MIP) in the unstructured data domain. Our solutions extend and integrate this automated MIP approach into the structured data domains of SAP.

About SECUDE

SECUDE is an established global security solutions provider offering innovative IT data protection for users of SAP software.

Founded as a joint venture between SAP and Fraunhofer Institute in 1996, SECUDE maintained a close SAP technology partnership and became a reliable resource for security solutions for the SAP market with 'Single Sign-On' for SAP, which was acquired by SAP in 2011. With a focus on making business process for data protection efficient and automated with little or no user interference,SECUDE's goal is to provide ease of use while minimizing cost of rollout and operations.

Leveraging its 20-plus years of experience in SAP security and business process know-how in protecting enterprise IP and data, SECUDE launched HALOCORE® as a holistic approach to protect SAP data exports.

SECUDE's solutions are trusted by many Fortune 500 and DAX listed companies. With branches in Europe, North America and Asia, SECUDE supports customers with the implementation of IT security strategies through a global network.

For more information, visit www.secude.com and follow our social media channels: LinkedIn, Twitter, and YouTube.

SWITZERLAND
SECUDE International AG
Werfestrasse 4 A
6005 Lucerne
Tel: +41 61 366 30 00

INDIA
SECUDE Solutions Pvt. Ltd.
No. T2/6, Dr. VSI Estate
Thiruvanmiyur
Chennai – 600 041
Tel: +91 44 4297 5600

USA
SECUDE IT Security, LLC
5F, 160 East 84th Street
New York, NY 10028
Tel: +1 646 944 6944