Top 5 Reasons to Implement SAP-Application-Layer Malware Protection

Attacks on SAP applications are ramping up.

The United States Computer Emergency Readiness Team (US-CERT) and even the United States Department of Homeland Security (US-DHS) are warning SAP customers about targeted attacks on mission-critical SAP systems. Reportedly, more and more internet-exposed SAP applications are being targeted by malicious actors — with an increasing SAP-specific skillset.
If your SAP system has not been attacked yet, it will be, sooner or later.
As attackers grow more proficient on ways how to attack an SAP system, protecting it and its users from content-based attacks is imperative.

Here are the top 5 reasons why your organization needs to implement virus and content scanning at the application layer using SAP VSI:

Reason No.1 – SAP strongly recommends it

Ever since the first Security Guide for S/4 HANA was published by SAP in 2016, it has always contained an entire chapter on virus scanning. The guide states:

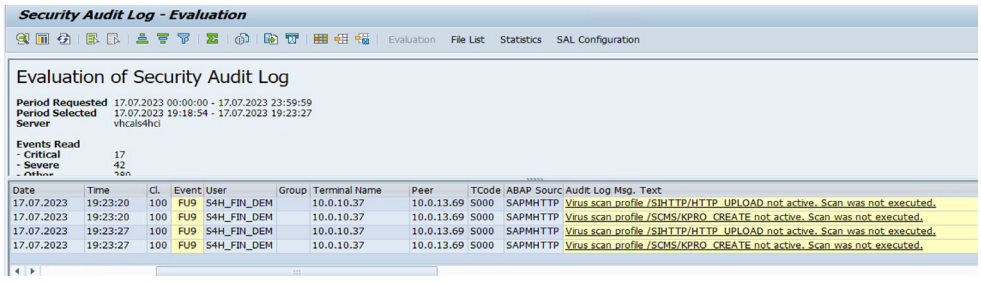
„We recommend installing and running a VSI 2.x-compliant virus scanner in your landscape. The SAP S/4HANA code calls this scanner using a dedicated interface during different stages of processing - during upload, download, and passage through the Gateway, and so on. You can customize the interface with the help of scan profiles.
We recommend running VSI scans for:

- *Signature scans*
  All files should be checked against an up-to-date list of known virus signatures.
- *MIME-type detection*
  Only trusted file types should be allowed.
- *Active content detection*
  Files with active content should be blocked (for example, PDF files containing JavaScript).“

Check-out the latest version of the Security Guide for S/4 HANA

Reason No.2 - Your auditor is checking for it

For the longest time, accepting uploads into SAP applications and not scanning them would not even be on the map for an auditor. However, with SAP_BASIS 757 and SAP note 3165706 and 3165707, your SAP stack will generate warnings in the Security Audit Log,



anytime a file transfer occurs that was not scanned by a VSI-compliant security solution.
Auditors who are commonly examining SAP's security audit log will flag this a business risk that needs to be mitigated.

Reason No.3 – Your Red Team or Penetration Tester will test it as a vulnerability

Mission-critical applications are a prime target for attackers. Hence, penetration testers or your organization's red team will also test that your SAP applications are configured in a secure way.
When evaluating the security of applications, probing the application's file-upload functionalities for vulnerabilities is a basic requirement. For example, the Open Web Application Security Project (OWASP), requires testers to attempt to upload malicious files, such as the EICAR test file or malicious archives (a.k.a. "ZIP-bombs") or to bypass simple file type filters — like the ones SAP provides without a VSI-compliant security solution.
If successful, the Pen-Test report will include findings of "Unrestricted File Upload" application-layer (CWE-434) and "Reliance on File Name or Extension of Externally-Supplied File" (CWE-646) vulnerabilities.

Reason No.4 - Your OS-level AV does not protect your SAP application

Many assume that the latest OS-level malware protection also secures file transfers into and out of SAP applications.
Unfortunately, that is not true. Here's why:

- Most OS-level anti-malware solutions monitor read and write access to the file system, so they catch malware when it is accessed.
- In an SAP application, files uploaded by application users are never written to the file system. They are processed by the SAP application server or the SAP Gateway, and then stored in the database, or a Document Management System like SAP Content Server — neither of which can be scanned by the OS-level anti-malware either.

And even highly advanced anti-malware solutions that monitor memory, resources and running processes cannot detect malware in an upload into an SAP application. These advanced solutions will detect malware as soon as it executes — but that also does not happen when a file is uploaded into your SAP application.

Reason No.5 - Your organization may be liable if you don't do it

Most cybersecurity regulations in the US and the EU require organizations to implement malware protection.
Standards and frameworks (like ISO 27002:2022, Control 8.7., the UK's "Cyber Essentials Scheme" and Security Standard SS-015, PCI DSS, HIPPAA, or the German BSI's Cloud Computing Compliance Catalogue – C5:2020) all require the implementation of state-of-the art malware protection.
SAP's Virus Scan Interface VSI is included in all SAP products since 2005 and is considered "state-of-the-art," by those standards.
Hence, failure to implement VSI-based protection is seen as negligence. In turn this could entitle persons or organizations to compensation for damages if they downloaded a malware-infected file from your SAP application, for example.

Conclusion:

SAP has long been an attractive, but difficult target for cyberattackers. But, as these attackers get smarter, better, and faster at finding the vulnerabilities in your SAP system, you too must become smarter, better and faster at protecting your organization's mission-critical systems and data. It starts with putting the right solution in place, which monitors SAP applications and provides real-time, in-memory protection from multiple types of attacks.

bowbridge Software GmbH
Altrottstraße 31 ⌒ 69190 Walldorf ⌒ Germany

t +49-6227-69899-50
e sales@bowbridge.net
w www.bowbridge.net

SAP Silver Partner

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig