Malware Protection and Content-Security — Made for SAP

Standard anti-virus solutions fail at protecting SAP applications. They cannot scan file transfers into and out of SAP applications, leaving mission-critical IT assets vulnerable to malware and other file-based threats.

bowbridge Anti-Virus is the only content-security solution explicitly created for SAP applications by leveraging SAP's Virus Scan Interface (NW-VSI). The solution scans file uploads and downloads in SAP applications, detecting and blocking malware, as well as SAP-specific non-malware threats embedded in files. Implementing bowbridge Anti-Virus does not require changes to your SAP applications, making the rollout easy and seamless.

Protecting Your SAP Cloud Journey

Due to its new modular architecture, bowbridge Anti-Virus supports a multitude of deployment options. Whether it's an "all-in-one" installation on on-premises application servers, centralized scalable scan servers on Kubernetes, or Cloud-based hybrid SaaS scanning and management for private-cloud deployments, all options are supported. And moving from one to another is merely a matter of configuration.

Malware Detection by Trellix® and SOPHOS®

bowbridge Anti-Virus includes two commercial enterprise-class malware detection engines to choose from. Whether you select Trellix or SOPHOS, you can rest assured files in your SAP applications are malware-free.

The built-in ICAP client allows the easy integration of network-based anti-malware solutions to substitute or complement your choice of built-in malware detection engines. High-availability and load-balancing options accommodate even the most demanding availability and performance requirements.

Protection from File-Based Cross-Site Scripting

By embedding executable content in files displayed in a web browser, such as PDF or image files, attackers can stage cross-site scripting attacks that may compromise your SAP application. bowbridge Anti-Virus detects and blocks such XSS attacks according to your security policy.

Active Content

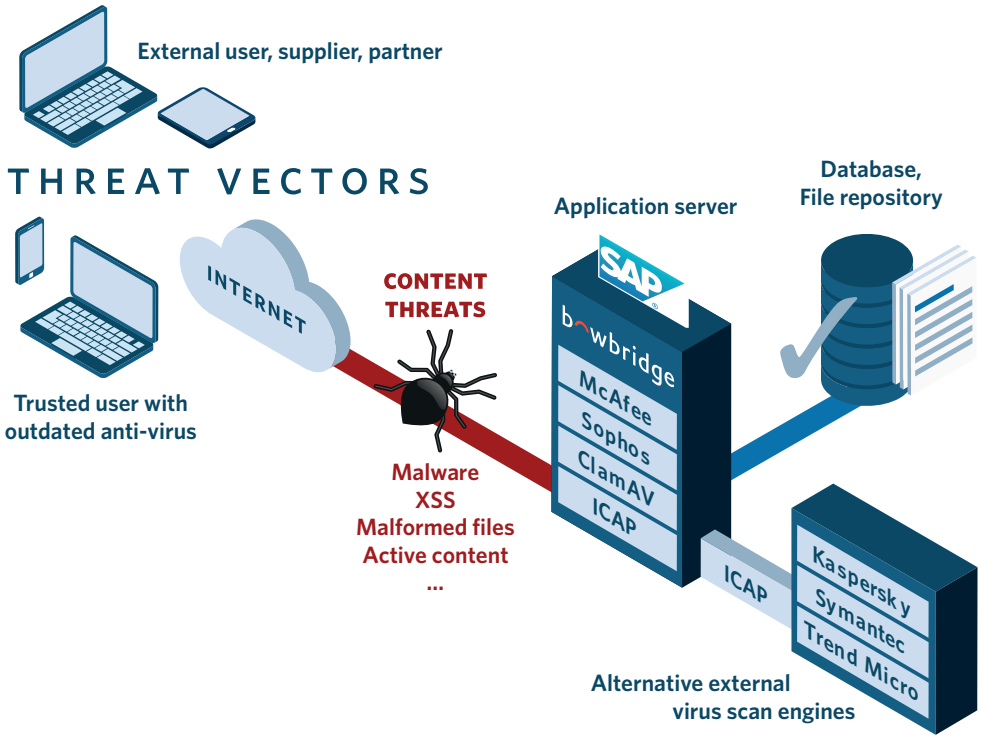
Active content, such as macros, JavaScript, OLE/DDE, etc. can be embedded in many seemingly benign file types. Such active content is not detected as malware and anti-virus engines don't block it. However, this active content, when executed automatically by web browsers or client applications can access the SAP application it was downloaded from and can potentially execute malicious tasks, unbeknownst to the user.

bowbridge Anti-Virus includes granular filters to detect and block active content in numerous file types.

bowbridge Anti-Virus at a Glance:

- Protection against viruses and malware
- Detection of file-based cross-site scripting (XSS)
- Blocking of embedded active content
- Content-based MIME-filters
- SAP-certified for NW-VSI 2.1
- No code-changes required

SAP® Certified
Integration with SAP NetWeaver®



Content-Based MIME-Filters

Out of the box, SAP applications can only filter files based on their extension. Bypassing these filters is as easy as renaming a file. Therefore, SAP introduced MIME-type based filters in VSI 2.1, permitting administrator to set up filters based on the MIME-type of files, determined by a thorough analysis of the file content.

Even without maintaining MIME-type filter lists, bowbridge Anti-Virus bolsters the protection of extension-based filters by checking and enforcing that the files' extension match their MIME-type.

SAP-Certified Compatibility

bowbridge products have been continuously certified by SAP since 2006, including certification for the latest generation of the Virus Scan Interface, VSI 2.1.

These demanding certification checks ensure the stability and performance of your mission-critical SAP application are never impacted.

For Any SAP Application – No Code Changes Needed

SAP's Virus Scan Interface is an SAP-kernel-level API. As such, once activated, all applications seamlessly benefit from bowbridge Anti-Virus' capabilities with no changes to the application code, be it ABAP or Java.

VSI is also integrated in several non-traditional SAP applications, such as Business Objects, Mobile Platform, etc., delivering the same level of protection to these applications' data store.

Seamless Integrations

bowbridge Anti-Virus is available natively on several operating systems and hardware platforms. Flexible scriptable event-handlers allow for the easy integration with your enterprise infrastructure, like proxies, network monitoring and SIEM solutions.

System Requirements

Operating Systems:

- Linux on x86_64 (SLES 12 or higher, RHEL 7 or higher)
- IBM AIX 6.1 or higher
- Microsoft Windows Server 2016 or higher

Memory:

- RAM: up to 2GB (all modules)
- Disk: 5GB

SAP:

- AS ABAP: SAP_BASIS 640 SP 11 or higher
- AS Java: SAP J2EE SP 13 or higher
- HANA XS: SP09 or higher
- Mobile Platform 3.0 or higher
- Business Objects 4.2 SP3 or higher

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