APPLICATION SECURITY *FOR SAP SOLUTIONS*

Protecting SAP® Applications From Content-Based Cyber Threats

bowbridge Application Security protects mission-critical SAP applications from:

- Cross-site scripting
- SQL injections
- Command injections
- Directory traversal
- Malicious redirects

bowbridge

Your Internet-Facing SAP Applications Are Vulnerable to Malicious User Input.

SAP NetWeaver-based applications enable easy and convenient collaboration with external users, suppliers, and partners.

However, publishing SAP applications on the internet exposes them to a barrage of content-based cybersecurity threats, including cross-site scripting, SQL injections, command injections, directory traversal attacks, and malicious redirects.

How do you keep malicious user input from compromising your data — or even your entire SAP infrastructure?

bowbridge Application Security monitors any user input to SAP applications from external web users, transparently and in real time.

It integrates seamlessly into the SAP Internet Communication Manager (ICM), analyzing application page requests and related parameters before they reach the application.

The result is maximum, proactive protection against content-based threats.

Don't assume your SAP system is secure. Put bowbridge Application Security in place – and *know* it is.

Protecting You From Cyberattack

Cross-Site Scripting

- AntiXSS-module detects and blocks user-input or parameters aimed at mounting a cross-site scripting (XSS) attack.

Injection Attacks

- AntiSQLi module uses attack-signature-based algorithms and complex heuristics to ensure detection and blocking of SQL-injections.

Directory Traversal

- Application Security Bridge analyzes application parameters and user input, blocking attempts to access or tamper with resources outside the application context.

Open Redirect

- Identifies and prevents redirections to URLs outside of the application infrastructure, protecting the application and users against data-theft and drive-by malware installations.

Providing Reliable Support

Maximum Performance

- All security scans takes place in memory for optimum performance. And because it seamlessly plugs into SAP ICM, it does not need separate HTTP decoding.

End-to-End Encryption

- Sessions remain end-to-end encrypted from the user's browser to the SAP application server, helping meet data privacy requirements.

Automatic Updates

- bowbridge distributes updates to customers which are automatically downloaded and applied. Your application is always protected by the latest filters and threat detection capabilities.

Broad Platform Support

- Available on numerous operating system platforms supported by SAP, including Microsoft Windows Server, Linux, and several UNIX variants.

Made For SAP
bowbridge Application Security is built specifically for SAP, integrating seamlessly into SAP environments.

Quality Product and Service
bowbridge earns high praise not just for our results, but for our commitment to service.

SAP® Certified
Integration with SAP NetWeaver®

bowbridge Software GmbH.
Altrottstr. 31
D-69190 Walldorf
GERMANY

Tel: +49 (0) 6227-69899-50
Email: info@bowbridge.net

bowbridge Software USA
530 Lytton Ave, 2nd Floor
Palo Alto, CA 94301
USA

Tel: +1 650-617-3408
Email: us-sales@bowbridge.net

bowbridge