



SAP Security Comparison Report



Probably the world's most complete threat detection and vulnerability monitoring system, designed to bridge the gap between traditional IT security and SAP security. SecurityBridge guards SAP systems with its real-time intrusion detection system, powered by machine learning to protect your systems from hackers and malicious behavior. No false positives, just factual real-time SAP security monitoring to detect breaches and, if required, integrate SAP with SIEM



SAP regards cyber-security as being of the utmost importance, and when it comes to securing its own landscape, SAP uses technology based on Real Time Threat detection that detects threats in real time so that they can be remediated before any harm is done. This top-down approach is defined as the most effective in providing bullet-proof security, backed up in conjunction with patching and hardening.

SecurityBridge and SAP share the philosophy that you will be infiltrated and have therefore created technology to detect actual attacks as they occur because no amount of patching will provide complete security, additionally there are no off-the-shelf patches for custom code, and the majority of successful hacks exploit that vulnerability.

To react in Real Time, you must have Actionable Intelligence, and this is where SecurityBridge and SAP stand out from other products that produce misleading false positives that are unreliable.

SAP and SecurityBridge both use Machine Learning to detect patterns of behavior to perform forensic analysis and identify new patterns so that you are always one step ahead of any attack.

Where SecurityBridge differs is the complexity in execution, providing a much simpler to deploy architecture that installs in days and is almost entirely self-maintaining. Compliance Reporting adds to the Holistic Security by detecting vulnerabilities and providing guidance for hardening, while providing proof as to whether those vulnerabilities are being concurrently exploited.

Functionality	SAP-ETD	SecurityBridge	Others
Realtime threat detection of actual attacks	✓	✓	✗ Most security vendors and SAP auditors run static validations.
Detection of threats in custom code	✓	✓ Static and real time	✗ or separate product required
Ability to triage actual threats in real time	✓	✓ Native triaging capabilities, convert events into security incidents	✗
Ability to accurately identify false positives	✓	✓ Known and validated risks can be marked as accepted not to cloud further findings	✗
Vulnerability monitoring in real time	✓	✓	✗
Link automated actions to security events	❓ No information available	✓ Fully configurable action framework	❓ No information available
Compliance reporting in real time	✓	✓	✗
Live dashboard reporting	✓	✓	✗
Remediation knowledgebase	✓ The SAP online support system	✓ Dedicated SecurityBridge KB	❓ No information available
SIEM integration	✓ Needs customization	✓ Plug & Play	✓ Needs customization
SPLUNK integration	✗	✓ Native Splunk app	✓ Some vendors
Support for HANA and S/4	✓	✓	✓
On premise / Cloud / Hybrid	✓	✓	✓
Patching and hardening management	✓ Solution Manager capabilities	✓	✓
No raw log extraction	✓ Big Data	✓ Smart data vs big data	❓ No information available
Minimal Installation efforts	✗ Full blown project	✓ Days only	❓ No information available
Regular maintenance effort	🔄 Continuous project	🔄 Continuous effortless updates	❓ No information available
Additional license requirements	€ € €	€ Subscription license	❓ No information available
Additional hardware requirements	Requires dedicated HANA hardware	Runs within existing infrastructure, small footprint	Most vendors require dedicated hardware and OS licenses.

What do I need to test drive SecurityBridge?

To deploy SecurityBridge within your SAP environment you only need to import our installation package. Since all of our software is contained within its own namespace and no SAP modifications are applied, it is safe to import, also allowing a full uninstall. Once the package is imported some basic steps are required in order to activate the Intrusion Detection System (IDS). Out-of-the-box SecurityBridge comes pre-configured, with a large set of detection patterns, which allow you to immediately test drive our software.

After running the test drive, if you want to convert to a live setup, you just need a license key. Configuration applied during an evaluation phase can be used as a starting base for your production implementation.

Do I need a SIEM solution?

No. SecurityBridge was designed to bridge the gap between SAP and leading security information and event management systems (SIEM). You do not need SIEM connectivity as the tool itself is also equipped with a powerful monitoring application.

Which SIEM solutions are supported?

SecurityBridge connects to a wide range of SIEM vendors (all magical quadrant leaders are supported), through the use of files or a REST service, both are based on the Common Event Format (CEF). SecurityBridge is Micro Focus ArcSight certified and a SecurityBridge Splunk application can be downloaded from splunkbase.



Can't I just retrieve similar security alerts using the SAP security audit log?

SAP security audit logging (SAL) has grown up quite a bit. SecurityBridge uses the SAL as one of its sources to identify potential threats. However, SAL logging is by far not the only source of valuable security information. Given the massive number of events recorded in SAL, it's not practical to simply run an extract from all systems. Check this blog article.

Can I use filters in my Security Audit Logging?

Our recommendation, supported by many security experts, is this: no SAL filter should be applied! Beware of introducing blind spots in your security monitoring! Check this blog article.

Some tools provide a full extract of SAP data sources. Is that what SecurityBridge does?

No, which is why this platform is so highly trusted and relied upon by major organizations. Our security solution does not move raw security logs into SIEM or any external log analyzer. SAP logs are massive, even just moving them may become an expensive and technically challenging exercise. SecurityBridge evaluates logs in real-time and alerts/exports only the relevant events messages. Smart data versus big data.

Can I trigger actions based on threat detection?

SecurityBridge has an action framework which allows the linking of security events with actions. Using a ruleset you can easily assign real-time actions to singular events. For example: show a popup to the event originator warning security monitoring has been triggered, activate SAP trace functions, apply an admin lock, generate an email, instantly kill the user session, generate a support ticket and more...



What kind of detection patterns are applied?

SecurityBridge specializes in SAP Basis and SAP application security monitoring. Detection patterns come predefined as configurable SecurityBridge "Listeners". Each specific vulnerability has a dedicated component which may cover a variety of event patterns. For example:

- *all vulnerabilities dealing with RFC destinations such as hard-coded passwords, insecure context users, ... are combined in a "RFC-destination" listener*
- *vulnerabilities triggered using debugging rights (bypassing authorization checks, debug jumping or altering the program flow, debug overwrite, ...) are combined within an "ABAP-Debug" listener*

At the time of publishing this FAQ over 70 listeners have been released, covering 250+ attack patterns. Contact us for the full list of available listeners.

Running SecurityBridge makes me GDPR compliant?

Unfortunately, nothing will do that, but it will help. The General Data Protection Regulation defines requirements which are not in the scope of a vulnerability monitoring tool. However, SecurityBridge is a very important enabler for GDPR-compliance. The regulation, which includes mandatory data breach notifications, unavoidably means you need to monitor your SAP systems. From 25th May 2018 GDPR-compliance was obligatory for all organizations doing business with European based firms.

Does SecurityBridge put an additional load onto the SAP system?

The Intrusion Detection System (IDS) continuously scans your systems, without any noticeable impact. In a typical environment, SecurityBridge consumes one single background process. For very large environments, having a large number of application servers and consecutive users, up to a maximum of 3 processes are required, all load balanced by one single IDS engine.

Compared to typical raw log extractors SecurityBridge does not process log sources sequentially, listeners are designed to work in delta mode, having real-time correlation capabilities.

What does a typical implementation look like?

SecurityBridge can be operational within one single day. Out-of-the-box configuration means it only requires activation, without the need for expert SAP security knowledge.

Since each environment is unique, the IDS initially protects your systems without customer specific rules being configured. During a predefined ramp-up period, ranging from a day to a few weeks, you will gain experience by exploring the alerts raised. Using customer rules and listener configuration, you can ensure that only the relevant security alerts are raised, zero severity events like false positives will no longer clutter your monitoring.

Security monitoring as a service?

For organizations not having the expertise or bandwidth, a fully managed security monitoring is also available. We not only provide the required tooling for continuous monitoring, we also offer security operation center services. This service can range from regular management reports to 24/7 surveillance.

Does SecurityBridge provide penetration test capabilities?

SecurityBridge is mainly a vulnerability scanner, to instantly report security- and data breaches. If e.g. someone gains unauthorized production access through an insecurely configured RFC destination this would be alerted in real-time.

The SecurityBridge suite however is being continuously expanded, and an RFC penetration testing module has been added, with further development on the Roadmap.

What is the relationship between the SecurityBridge code scanner and the SAP Code Vulnerability Analyzer?

SAP-CVA is a commercially available SAP product (requiring a dedicated license) used to QA your custom development process. The SecurityBridge code scanner is a fully independent ABEX product. SecurityBridge and SAP-CVA are complementary to each other.

The SecurityBridge code check runs as an embedded component within the intrusion detection system. When a developer produces code, SAP basis performs a transport, ... SecurityBridge is always on guard.

SAP-CVA is a code inspector plug-in, which facilitates developers with writing better and secure code (bottom-up).

The SecurityBridge code scanner focuses on security gatekeeping for your system, and only optionally involves developers (top-down).

Pricing scheme

All products are available through a yearly subscription model. SecurityBridge licensing is very straightforward and transparent. License fees are based on the number of SID's and landscapes, independent from the number of users, business revenue or the number of application servers. A subscription includes product support, and there are no hidden costs.



CONTACT US

Europe (Headquarters)
+49 911 4902 1918

Munchenerstr. 49
85051 Ingolstadt, Germany

United States
+1 416 821 0850

Info@SecurityBridge.com
SecurityBridge.com