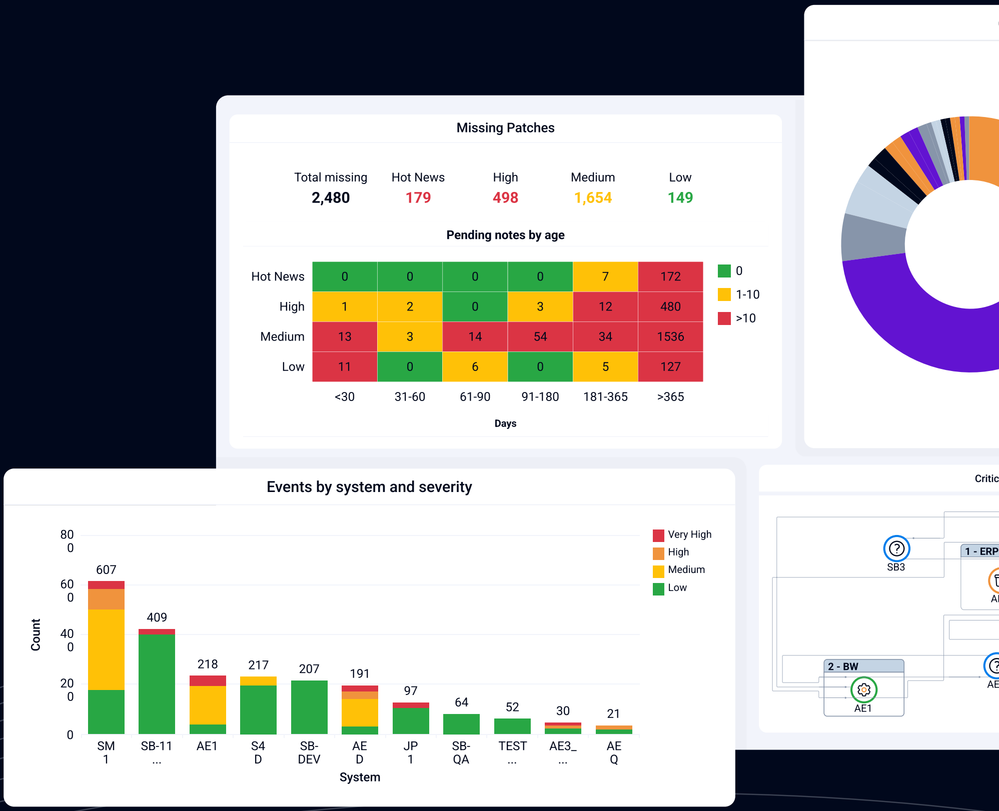
Security Bridge

SecurityBridge:

Buyer’s Guide to SAP Security



Missing Patches

Total missing	Hot News	High	Medium	Low
2,480	179	498	1,654	149

Pending notes by age

	<30	31-60	61-90	91-180	181-365	>365
Hot News	0	0	0	0	7	172
High	1	2	0	3	12	480
Medium	13	3	14	54	34	1536
Low	11	0	6	0	5	127

Days

🟩 0
🟨 1-10
🟥 >10

Events by system and severity

Index

Buyer’s Guide to SAP Security

The SecurityBridge Buyer’s Guide to SAP Security empowers organizations with the knowledge needed to protect their SAP systems from evolving cybersecurity threats. It provides insights into evaluating SAP security solutions, understanding the risks of inaction, and implementing best practices to safeguard critical business data and systems.

Introduction

SAP systems are the backbone of many organizations, supporting critical business functions and storing sensitive data. These systems are integral to business operations, encompassing everything from financial records and supply chain management to HR data. However, protecting SAP environments is essential as cyber threats become more sophisticated and frequent. This buyer’s guide is designed to help you understand the various aspects of SAP security solutions and make informed decisions about effectively safeguarding SAP systems.

Why Implement an SAP Security Solution?

As part of companies’ digital transformation initiatives, SAP systems with sensitive data such as financial records, employee details, and intellectual property become increasingly valuable to malicious actors. Because cybercriminals target this data, organizations must implement robust security measures to protect their “crown jewels.”

Implementing a robust SAP security solution and processes ensures:

- **Data Integrity and Confidentiality:** A robust security solution ensures that critical business data remains intact and accessible only to authorized users, preventing unauthorized access and tampering.
- **Compliance:** Many industries are subject to strict regulations, such as NIS2, NIST, SOX, and PCI-DSS. An SAP security solution helps ensure efficient compliance with these regulations, avoiding fines and legal consequences while limiting the manual work associated with audits.
- **Operational Resilience:** Effective security measures prevent disruptions caused by cyberattacks or malicious insiders, ensuring business operations continue smoothly.

By prioritizing SAP security, organizations protect their data and operations, ensure regulatory compliance, and build trust with customers and partners.

The Risk of Doing Nothing

Neglecting SAP security can lead to critical consequences beyond monetary losses:

Data Breaches:

Sensitive information, including personal and financial data, could be exposed, leading to reputational damage and regulatory fines.

Operational Disruptions:

Cyberattacks, human errors, insecure configurations, missing patches, or malicious insiders can cause downtime in SAP systems.

Increased Costs:

The financial impact of a security breach often far outweighs the cost of implementing preventative measures, as recovery efforts involve significant time and resources.

Inefficient Use of Resources:

Manual tasks such as keeping up with SAP notes or patching are a massive strain on your SAP team.

Why Native SAP Security Isn’t Enough

While SAP offers built-in security features, they often do not adequately support and enable efficient and (semi-)automated processes. Here’s why:

Limited Threat Detection:

Native SAP security tools lack advanced features like behavioral analytics, which are crucial for identifying sophisticated attacks. There are also limitations on integrating SAP with the broader cybersecurity team, making SAP a black box and making it difficult to grasp the context of specific threats.

Manual Processes:

Tasks such as patch management and vulnerability assessments are too complex and comprehensive to be performed manually, increasing the risk of human error and leaving gaps in the security posture.

Integration Challenges:

Built-in tools may not easily integrate with enterprise-wide security solutions, limiting the organization’s ability to establish unified security frameworks and processes.

To achieve comprehensive protection, organizations need solutions that complement native SAP features while addressing modern security requirements.

Shared Responsibility on RISE with SAP

The shift to RISE with SAP brings new opportunities **and** responsibilities for organizations. While SAP handles some security aspects, organizations remain accountable for safeguarding their data and applications. Key areas of responsibility include:

- **Data Protection and Compliance:** Organizations must implement measures to secure sensitive data and adhere to compliance regulations.
- **Access Management:** Proper control over user access and privileged accounts is essential to prevent unauthorized activities.
- **Security Enhancements:** Adding extra layers of protection, such as advanced security monitoring and threat detection, is critical to address cloud-specific risks.

A shared responsibility model requires collaboration between organizations and SAP to ensure a robust security posture across the entire SAP environment.

Monitoring your data

SAP ECS is responsible for managing client 000. Other clients, those containing your business data, are to be monitored by the customer. Many attack vectors, e.g. roles and authorizations, are client-dependent.

Maintain 360° Security

Standard monitoring tools provides a limited number of use cases and comes at additional cost. SecurityBridge covers many more scenarios, consumes more data sources, and remains fully configurable by the customer.

Centralized Security Monitoring

SecurityBridge enables plug-and-play and contextualized security event integration with a wide range of SIEM and SOAR solutions to ensure full SAP security visibility in the company’s security operations.

Don’t rely on manual processes

SecurityBridge has built-in automation capabilities for incident tracking and response, up to remediation.

Ensure a proactive patching strategy

SecurityBridge monitors SAP security notes and verifies if your system is properly patched. Since immediate patching isn't always feasible, Virtual Patching helps detect potential exploits and track events linked to missing security updates

Fast to implement, easy to learn

SecurityBridge is the only SAP security solution with platform capabilities natively built into the SAP technology stack.

- Enable DevSecOps for secure coding practices
- Streamline privileged or elevated access control processes
- Ensure robust data loss prevention
- Protect identities with anomaly detection

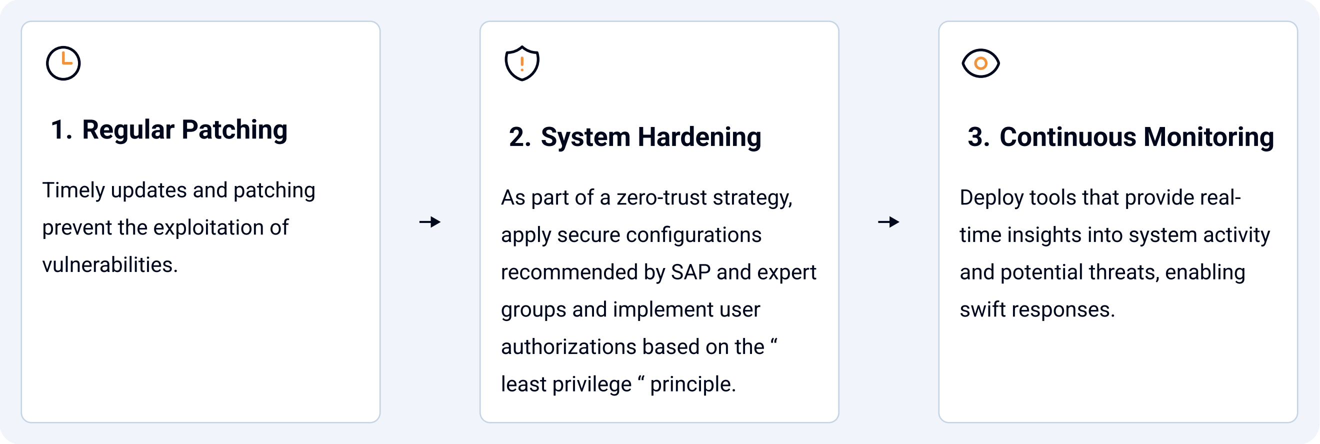
Key Considerations When Evaluating SAP Security Vendors

Selecting the appropriate SAP security vendor can be a complicated decision. Here are some factors to consider during the evaluation:

1. **Security Coverage:** Ensure the solution covers critical areas like threat detection, patch management, compliance monitoring, and vulnerability assessments. A holistic approach is essential for ensuring a robust security posture.
2. **Ease of Integration:** To provide a unified security monitoring and response program, look for solutions that integrate seamlessly with existing enterprise systems, such as SOC (SIEM) and ServiceDesk (ITSM) tools.
3. **Automation Capabilities:** (Semi-)Automated patching, monitoring, and reporting processes reduce manual effort and minimize human error, enhancing overall security.
4. **Real-Time Threat Detection:** A good solution should identify zero-day vulnerabilities and unusual behavior in real-time, enabling swift response to potential threats.
5. **Regulatory Compliance:** Ensure the vendor supports compliance with global standards like NIS2 or NIST to avoid regulatory penalties.
6. **Vendor Expertise:** Evaluate the vendor's track record, industry expertise, security research capabilities, and customer feedback to ensure they can meet your organization's unique needs.

Best Practices for SAP Security and How to Get Started

Beginning with SAP security doesn't need to be a daunting task. A solid SAP security platform offers a clear roadmap that identifies the lowest-hanging fruits that will significantly enhance your SAP security posture with minimal effort. Usually, these three steps are a strong starting point:



1. Regular Patching

Timely updates and patching prevent the exploitation of vulnerabilities.

→

2. System Hardening

As part of a zero-trust strategy, apply secure configurations recommended by SAP and expert groups and implement user authorizations based on the " least privilege " principle.

→

3. Continuous Monitoring

Deploy tools that provide real-time insights into system activity and potential threats, enabling swift responses.

While a mature SAP security approach contains several disciplines, with the limited resources typically available, the above will get you off to a great start with SAP security.

Total Cost of Ownership (TCO)

Understanding the total cost of ownership is critical when selecting an SAP security solution. Consider the following factors:

- **Hardware Requirements:** On-premises solutions often require additional infrastructure, which imposes hidden upfront- and maintenance costs.
- **Licensing Costs:** Evaluate pricing models and levels to ensure an adequate initial budget, while also considering the costs involved in expanding the solution’s coverage.
- **Maintenance and Updates:** Ongoing support, updates, and system maintenance should be factored into the overall cost.
- **Training and Adoption:** Implementation and user training can also impact the total cost. To minimize training efforts, opt for solutions with intuitive interfaces.

Calculate your SecurityBridge ROI →

Getting Started

Step 1:

The first step in improving your SAP security posture is gaining transparency into your current security posture covering, system configurations, implemented patches and monitoring capabilities.

Step 2:

Conduct a comprehensive audit to identify vulnerabilities, gaps, and areas for improvement. Running a POV with an SAP security vendor can often accelerate this manual process.

Step 3:

Engage key stakeholders across IT, security, and business units to align priorities.

Step 4:

Develop a roadmap with milestones for patch management, access control, and real-time monitoring.

Step 5:

Partnering with a trusted vendor, such as SecurityBridge or your SAP partner consultant, can streamline this process and ensure rapid implementation.

What Others Are Doing

Organizations worldwide are prioritizing SAP security to combat escalating threats. Leading companies invest in advanced threat detection, implement Zero Trust frameworks, and integrate SAP security with broader enterprise cybersecurity and risk management strategies. They also automate routine processes like patch management to enhance efficiency and reduce human error.

Read SecurityBridge's Customer Stories →

Top SAP Security Use Cases

Use Case	Description	
Real-Time Threat Detection	Identifying threats in real-time including behavioral analytics	Read More
Patch Management Automation	Automating the identification and deployment of critical security updates	Read More
Compliance Automation	Ensuring continuous adherence to regulatory requirements and making audits less resource intensive	Read More
Vulnerability Management	Proactively scan for and address system weaknesses to enable hardening	Read More
Custom Code Security	Ensure vulnerabilities are not deployed into production via custom code	Read More
Incident Response	Respond to threat immediately either directly in the platform or via the company SOC	Read More
Identify the attack surface	Gain visibility into potential entry points within your SAP landscape, for precise identification and mitigation of vulnerabilities	Read More

Essential Capabilities in an SAP Security Platform

Modern SAP security solutions offer a range of features, including:

- Advanced threat detection with AI and ML capabilities
- Comprehensive compliance monitoring and reporting
- Automated patch management
- Automated vulnerability management
- Privileged Access Management
- Seamless integration with SIEM and ITSM tools
- Custom code security
- Interface traffic monitoring
- SAP Security Roadmaps
- SAP Security Management Dashboards
- Identity Protection
- Data Loss Prevention

Building the Business Case

Building a strong business case involves quantifying the value of SAP security. Highlight potential cost savings from breach prevention, compliance, and operational efficiency. Use tools like **SecurityBridge's Business Case Calculator** to showcase the return on investment for implementing a robust SAP security solution.

Benefits of Choosing SecurityBridge

SecurityBridge is The Cybersecurity Command Center for SAP, offering unique advantages that set it apart:

360° Security:

A complete SAP security platform with threat detection, vulnerability management, user monitoring, and compliance automation.

Native SAP Add-on:

The only SAP security platform fully integrated and embedded within SAP.

Prebuilt Content:

Includes prebuilt content and use cases, enabling quick implementation and improved security posture within 48 hours.

Automation and Efficiency:

(Semi-)automated patch management, continuous monitoring, and advanced analytics enhance operational efficiency.

Real-Time Protection:

With real-time threat detection and response capabilities, SecurityBridge minimizes the risk of cyberattacks.

Regulatory Alignment:

The solution helps organizations achieve compliance with regulations such as PCI-DSS, GDPR, NIS2, NIST, and SOX.

Integrations:

To connect SAP data to the company-wide security operations, including SIEM, SOAR, ITSMs, and more.

Example Use Case: Sanofi, a global healthcare leader, implemented SecurityBridge to secure over 500 SAP systems. The solution covers real-time threat detection, seamless integration, and significant improvements in operational efficiency, allowing the company to safeguard its critical systems effectively.

Let us show you how to dramatically improve your SAP security posture by leveraging The Cybersecurity Command Center for SAP by SecurityBridge. Contact us here.

You should choose SecurityBridge if you care about:

Connecting your SAP systems to the SOC

Easily integrate SAP security data with your existing tech stack and SOC team to gain complete visibility of the threat landscape and understand SAP observations in a broader cybersecurity context.

SIEM Integration for SAP →

Navigating SAP security with a clear roadmap

Get a tailored step-by-step guide to identify and prioritize security risks, enabling immediate action on low-hanging fruits and continuous recommendations to harden your SAP systems.

Security Roadmap →

Protecting your SAP systems from threats

Get centralized, 360° monitoring and management of SAP vulnerabilities, access management, fraud attempts, compliance checks, events, logs, policy violations, behavioral anomalies, and more.

Threat Detection →

Limiting configuration and maintenance tasks

With low configuration needed and out-of-the-box security content, resources are freed up to focus on what matters in keeping the organization secure while limiting manual work.

How it Works →

Certifications:

SAP Silver Partner

Information Security Management ISO 27001 Certified

About SecurityBridge

SecurityBridge is the leading provider of a comprehensive, SAP-native cybersecurity platform. Trusted by organizations worldwide to safeguard their most critical business systems. Our platform seamlessly integrates real-time threat monitoring, vulnerability management, and compliance capabilities directly into the SAP environment, empowering organizations to protect their data's integrity, confidentiality, and availability with minimal manual effort. With a proven track record, including a stellar customer success rating and over 5,000 SAP systems secured globally. SecurityBridge stands out for its ability to accurately provide a 360° view of the SAP security posture, ease of use, rapid implementation, and transparent licensing. We are committed to innovation, transparency, and customer-centricity, ensuring businesses can confidently navigate the evolving landscape of SAP security threats.

Locations

Germany (Headquarters)

Münchener Str. 49, 85051 Ingolstadt

☎ +49 (841) 93914840

United States

228 Park Ave S, New York, New York

☎ +1 416 821 0850

Netherlands

Kraijenhoffstraat 137A, 1018RG Amsterdam

☎ +31 647 100 101

Singapore

4 Battery Road, Bank Of China Building, #25-01,
Singapore (049908)

☎ +65 9126 6097

See SecurityBridge in Action

Reach out to us if you are ready to talk SAP security or want to see SecurityBridge in action.

Request a demo

Contact Us

Certifications:

SAP Silver Partner

Information Security Management ISO 27001 Certified

Security Bridge

www.securitybridge.com