PRODUCT COMPARISON

SAP Cybersecurity Solutions

Compare leading solutions and choose with confidence

LAYER SEVEN SECURITY

PRODUCT COMPARISON

SAP Cybersecurity Solutions

Compare leading solutions and choose with confidence

Introduction

Securing SAP solutions is a priority for many organizations in today's heightened threat landscape. Breaches in mission-critical SAP systems can expose highly confidential information, disrupt business continuity, impact regulatory compliance, and lead to financial losses and reputational harm.

The risk is intensified by the shift towards cloud computing, digital transformation, and hybrid architectures that have evolved SAP systems from on-premise solutions isolated within internal networks to highly interconnected and accessible platforms. Modern SAP landscapes now integrate with a wide range of third-party applications, APIs, and external services. Users can access SAP solutions from anywhere and any device. While this drives innovation and efficiency, it also expands the attack surface. The same integrations and remote access that empower organizations also create more entry points for cyber threats, making security and continuous monitoring more critical than ever. Organizations today have access to a wide range of solutions designed to help them manage and reduce cyber risks in their SAP environments. This includes tools offered by SAP such as Enterprise Threat Detection (ETD) and Code Vulnerability Analyzer (CVA). It also includes platforms from third party vendors such as Layer Seven Security, Onapsis, Pathlock and SecurityBridge. These tools and platforms address different aspects of security, from system configuration and access control to threat detection and compliance management.

Some solutions focus on vulnerability management, ensuring SAP systems are securely configured and regularly patched. Others provide continuous monitoring to detect suspicious activities, unauthorized changes, or data exfiltration attempts in real time.

In addition, compliance and audit tools assist organizations in aligning with SAP's security baselines and industry regulations, while threat intelligence platforms deliver insights into emerging risks targeting SAP landscapes.

By adopting these technologies, organizations can create a comprehensive defense strategy that strengthens their SAP security posture and reduces exposure to cyber threats.

This guide helps organizations navigate the complex landscape of SAP security solutions and identify the tools best suited to their specific needs based on 20 specific criteria. It provides a clear framework for evaluating vendors and selecting solutions that align with their industry, regulatory requirements, budgets, and security maturity.

1. Vulnerability Analysis

Vulnerability analysis is the process of hardening SAP solutions by identifying, evaluating, and removing security weaknesses that could be exploited by threat actors to compromise systems. SAP is the only vendor in this evaluation that does not provide a commercial solution with coverage for system vulnerability analysis. SAP ETD supports primarily threat detection, SAP CVA is specifically for custom code vulnerability management. Limited support for system vulnerability analysis is provided by SAP through Cloud ALM. However, the coverage is restricted to basic health checks in the SAP Security Baseline. Solutions from third party vendors perform a greater volume of vulnerability checks and therefore provide a higher level of protection. For example, the Cybersecurity Extension for SAP from Layer Seven Security includes more than 5000 checks for vulnerabilities in SAP solutions.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✗	✗	✓

2. Security Patch Management

Security patch management is the process of reviewing, prioritizing, and applying SAP's official security updates - known as SAP Security Notes - to fix vulnerabilities and strengthen system protection.

Each month, SAP releases Security Notes that address newly discovered weaknesses or misconfigurations in its software. Organizations must analyze these notes to determine which are relevant to their systems, assess the risk and impact, and then implement the necessary patches or configuration changes.

Security Notes are reported by to customers SAP via the SAP Support Portal. Third party security solutions automate the discovery and lifecycle management of Security Notes, The Cybersecurity Extension for SAP calculates relevant notes for each SAP solution based on installed software components and versions and the implementation status of existing notes. Layer Seven Security also provide workarounds for many critical hot news and high priority security notes when official patches cannot be applied.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✗	✗	✓

3. Compliance Management

Security compliance management for SAP solutions is the process of ensuring that SAP systems meet internal security policies, industry standards, and regulatory requirements. It involves continuously auditing, assessing, and documenting SAP security controls to demonstrate that the environment is configured and operating securely.

SAP ETD and SAP CVA do not support compliance management for SAP solutions. Third-party solutions provide varying degrees of coverage. The Cybersecurity Extension for SAP performs automated compliance monitoring for 15 frameworks including GDPR, NIST, PCI-DSS, and SOX, as well as SAP standards such as the SAP Security Baseline, Security Guide for S/4HANA and Mandatory Security and Hardening Requirements for SAP RISE.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✗	✗	✓

4. Custom Code Security

SAP systems often include custom code such as ABAP programs and UI5 applications that extend standard SAP functionality. Insecure custom code can provide an entry point for attackers, even in SAP systems that are fully hardened and patched. Common risks include SQL injection, authorization bypass, malicious command execution, and sensitive data exposure. Manual code review is time-consuming and error-prone. Automated static and dynamic scanning for custom code in SAP systems can detect vulnerabilities more effectively and efficiently, and enforce consistent standards for secure development.

The Cybersecurity Extension for SAP integrates with SAP development tools such as the ABAP Test Cockpit (ATC) to detect 500+ vulnerabilities in custom ABAP and UI5 code. It also integrates with the SAP Transport Management System (TMS) to automatically scan and block transports with security errors and warnings. Periodic scans can be scheduled to detect and assess changes in custom code deployed in productive systems.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✗	✓	✓

5. Access Risk Analysis for S/4HANA & SAP ECC

Enterprise Resource Planning (ERP) solutions such as SAP ECC and SAP S/4HANA automate and integrate core business processes such as finance, HR, manufacturing, and supply chain management into single unified systems. Controlling end-user access across multiple integrated modules and large user bases in such solutions is a complex and continuous challenge. Access must be granted to end users in accordance with business needs and the principles of least privilege and Segregation of Duties (SoD).

The Cybersecurity Extension for SAP is the only solution in the evaluation that detects users with critical permissions and SoD violations across both SAP ECC and SAP S/4HANA. Coverage spans key business modules including Finance (FI), Controlling (CO), Sales and Distribution (SD), Materials Management (MM), Production Planning (PP), and Human Capital Management (HCM). The solution also supports periodic access reviews for SAP to maintain compliance with audit standards.

The functionality is included in the standard license for the Cybersecurity Extension for SAP. In contrast, SAP and Pathlock require separate tools for access risk analysis. This capability is absent from the cybersecurity offerings from Onapsis and SecurityBridge.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✗	✗	✗	✗	✗

6. Threat Detection

Malicious activity targeting SAP systems leaves identifiable traces in system and user logs. By continuously monitoring these logs and applying effective threat detection and response, organizations can identify and contain attacks early, preventing them from spreading and compromising critical SAP systems.

With the exception of SAP CVA, the solutions in this evaluation support real or near time log collection and analysis with predefined rules for detecting Indicators of Compromise (IoC). The Cybersecurity Extension for SAP stands-out with the highest number of predefined rules and coverage for application, database and OS logs for cross-stack monitoring in SAP systems. This includes 1200+ patterns for the Gateway Server Log, Message Server Log, HTTP Log, Read Access Log, System Log, and STAD in ABAP systems, the Security Log in SAP Java, and logs for the SAProuter, Web Dispatcher, Cloud Connector, and SAP BTP. For database monitoring, the Cybersecurity Extension supports the Audit Log in SAP HANA, and security logs for SAP ASE, Oracle, IBM DB2 and Microsoft SQL Server. Supported OS logs include Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise (SLES), and Microsoft Server.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

7. Anomaly Detection

Anomaly detection can identify unusual or abnormal behavior in systems that may indicate a security threat or compromise. The majority of the solutions in this class use analytics or machine learning to detect anomalies that deviate from established baselines for systems and users. For example, the Cybersecurity Extension for SAP analyzes event data against normalized patterns of behavior to calculate security-related anomalies.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

8. Anti-Ransomware

The impact of ransomware in SAP solutions can be devastating. Compromised solutions can paralyze business processes, disrupt supply chains, and lead to significant financial losses. Effective anti-ransomware for SAP combines application, database and OS hardening, continuous monitoring of SAP application and infrastructure logs, and anomaly detection to identify early signs of malicious activity.

The Cybersecurity Extension for SAP supports system hardening for anti-ransomware by identifying vulnerable settings and services that may be exploited to perform ransomware attacks. It also identifies users with privileges to download, install and execute programs in SAP applications. The Cybersecurity Extension for SAP detects and alerts for the execution of OS commands associated with ransomware exploits, suspicious HTTP and RFC calls, root commands and Sudo actions in SAP hosts, and changes in file systems that may indicate successful or unsuccessful attempts to install malware.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

9. Incident Response

Effective incident response can dramatically reduce the impact of cyber attacks by containing security threats, limiting data loss and minimizing system downtimes. Early containment prevents threat actors from escalating attacks, moving laterally and compromising sensitive data. It also ensures SAP systems supporting critical business processes remain resilient and recover quickly.

Cybersecurity solutions for SAP support effective response by detecting and alerting for security incidents. Often the solutions trigger notifications such as alarms and emails for alerts. They also support forensic investigation of security incidents. However, few of the solutions provide structured workflows for investigating, documenting and reporting on incidents. The Cybersecurity Extension for SAP provides automated workflows and best practices for investigating security alerts and support Security Orchestration, Automation, and Response (SOAR). It empowers non-technical and non-experts to effectively investigate security incidents for SAP solutions with predefined step-by-step instructions to analyze, respond, report, and close security alerts.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

10. Security Forensics

Investigating suspicious or malicious activity is critical to support effective incident response and identify the source and impact of security events in SAP systems. Cybersecurity solutions enable forensic analysis by collecting, standardizing and centralizing event data from SAP logs for review. This supports root cause analysis, event reconstruction and impact assessment. Users can apply complex queries to analyze events across multiple logs and systems.

Some solutions, such as the Cybersecurity Extension for SAP, also support the creation of custom alarms for events during forensic investigations. The Cybersecurity Extension for SAP also enables users to maintain exclusions for events to customize and tune security alerts and prevent alert flooding. It also archives event data in a separate system to protect against anti-forensics performed by threat actors in compromised systems. Anti-forensics can obscure, hide, or remove traces of malicious activity in monitored systems.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

11. SIEM Integration

Integrating SAP security logs with SIEM (Security Information and Event Management) solutions improves visibility, detection, and response capabilities. It also enables organizations to correlate events in SAP systems with events from other assets and endpoints. This supports end-to-end monitoring and reconstruction of incidents for IT landscapes.

Direct integration of SAP logs with SIEM solutions presents several challenges. SAP systems generate numerous logs, each with its own format and event structure. The logs often produce a high volume of Events Per Second (EPS), and many lack key information needed to support event correlation in SIEM platforms.

Solutions such as the Cybersecurity Extension for SAP enable organizations to address these challenges by providing a single integration point between SAP environments and SIEM platforms. This allows customers to maintain just one data source in their SIEM to collect information from all SAP logs and systems, simplifying both initial setup and ongoing maintenance. Additionally, the Cybersecurity Extension filters and enriches SAP events before they are sent to SIEM platforms, reducing event volume and improving correlation. The Cybersecurity Extension for SAP supports integration with any SIEM solution that ingests file-based logs and syslog. This includes Splunk, Logpoint, Sentinel, AlienVault, LogRhythm, QRadar and ArcSight.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

12. Interface Monitoring

SAP systems rarely operate in isolation. They continuously exchange data with other applications, databases, third-party systems, and external partners. The exchange is performed using numerous interfaces including RFC, IDoc, BAPI, OData, web service, and other protocols. Threat actors can exploit insecure connections for interfaces configured with missing or weak authentication and encryption.

The Cybersecurity Extension for SAP detects insecure interfaces in SAP systems including RFC destinations configured with privileged users and inadequate encryption. It also identifies systems using weak encryption algorithms or with insufficient restrictions for accessing Remote Function Modules (RFM). This includes settings for Unified Connectivity (UCON). The solution also detects misconfigurations in the gateway server,

message server and Internet Communication Manager (ICM) and alerts for successful and unsuccessful calls to vulnerable programs, reports, ICF services and RFMs.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

13. Configuration Drift

SAP environments are highly dynamic, undergoing continuous changes to align with evolving business needs. These changes may involve applying patches and updates to deliver enhancements and fixes, modifying or introducing custom developments, implementing new interfaces to enable cross-system integration, and adjusting user roles and permissions. Uncontrolled changes can undermine security hardening and expose SAP systems to hidden risks.

Solutions such as the Cybersecurity Extension for SAP mitigate the risk by detecting, reporting and alerting for changes that impact security hardening. This includes changes to security-related dynamic and static parameters in ABAP systems and database changes in SAP HANA. It also includes changes to custom code, system interfaces, and roles, profiles and authorizations assigned to SAP users.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

14. Transport Monitoring

Change control in SAP landscapes is managed using the SAP Transport Management System (TMS). The TMS ensures that configuration, code, and other changes are migrated in a controlled, consistent, and auditable manner through transport requests, reducing the risk of errors or inconsistencies between environments.

The Cybersecurity Extension for SAP enforces TMS-based change control by continuously monitoring SAP systems for unauthorized modifications, including dynamic changes to code in production systems. It analyzes transport requests for security vulnerabilities and automatically blocks any request containing errors or warnings, supporting change governance and system integrity across the SAP landscape.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✗	✓	✓

15. Database & OS Monitoring

SAP systems are not standalone applications. They are ecosystems comprised of application, database and host layers. The application layer supports the business logic. The database layer stores transactional and master data, system tables, logs, and configuration data. The host or operating system layer provides the runtime environment for SAP applications and the database. The layers are tightly integrated with trust relationships that can be exploited by threat actors to move laterally from compromised databases and hosts to applications or in reverse.

The Cybersecurity Extension for SAP is the only solution that secures the entire SAP system stack including application, database and host layers. The solution supports vulnerability scanning and threat detection for SAP applications, database and hosts.

The Cybersecurity Extension for SAP is the only solution that protects the full SAP system stack, including application, database, and host layers. It provides comprehensive vulnerability scanning and threat detection for both SAP and underlying infrastructure, ensuring no area is left exposed.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✗	✗	✗	✗	✗

16. User Experience

The user experience is important for SAP cybersecurity solutions since even the most powerful platforms can fail if they are difficult to use or unresponsive. Security tools with intuitive interfaces and clear workflows are more likely to be used consistently by employees. Complex or confusing tools may be bypassed, ignored, or misconfigured, leaving organizations vulnerable. Clear dashboards, alerts, and guidance help security teams quickly identify and remediate risks. An effective user experience ensures that critical actions are simple and unambiguous, minimizing mistakes, improving response times and reducing the need for extensive training.

Solutions such as the Cybersecurity Extension for SAP provide a responsive, intuitive, and user-friendly design using an SAP Fiori interface. Fiori applications are web-based and mobile-friendly. They emphasize clarity, consistency, and ease of use. Fiori tiles,

dashboards and apps deliver a roles-based user experience that can be customized for each user. Custom Fiori applications in the Cybersecurity Extension for SAP integrate seamlessly with standard SAP applications since they share the same platform and user framework. Fiori applications are more intuitive for SAP users, leading to quicker onboarding.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✗	✓

17. Support for SAP RISE/ SAP Cloud ERP

There is a shared model of responsibility between SAP and customers for RISE with SAP/ SAP Cloud ERP Private Edition. Infrastructure security is managed by SAP, whereas customers are responsible for the application and data layer. Unless customers purchase additional packages and services from SAP Enterprise Cloud Services (ECS) that are not included in standard RISE/ Cloud ERP contracts, organizations are accountable for managing user access, system settings, custom code, application security notes, and security incidents.

All cybersecurity solutions in the evaluation can be effectively implemented by SAP RISE / Cloud ERP customers, even within the software and system constraints imposed by SAP ECS. For example, the Cybersecurity Extension for SAP can be deployed as an SAP-certified addon in RISE / Cloud ERP solutions, including SAP S/4HANA. The Cybersecurity Extension for SAP enables organizations to automate compliance audits for security requirements mandated by SAP Enterprise Cloud Services.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✓	✓	✓	✓

18. SAP Certification

SAP certification for third-party solutions provides assurance that solutions are compatible, secure, and fully supported within SAP environments. Certification indicates that vendor have met SAP standards for integration, reliability, and best practices. SAP-certified products are tested to integrate seamlessly with SAP solutions and reduce the risk of system conflicts, errors, or performance issues. Certification also includes security assessments for adherence to SAP development standards.

With one notable exception, the third-party cybersecurity solutions in the evaluation are certified by SAP. Certification is not relevant for the SAP solutions ETD and CVA. The Cybersecurity Extension for SAP has been SAP-certified since March 2021.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✓	✗	✓	✓	✓

19. Rapid Deployment

Shorter deployment times for SAP cybersecurity solutions leads directly to lower installation costs and faster adoption, reducing the window of vulnerability. Easier maintenance can also reduce the window of vulnerability by supporting more rapid updates with minimal system downtime.

Products such as Onapsis and SAP ETD require additional servers and infrastructure. This can lead to longer deployments and more extensive maintenance. Updates for SAP ETD, for example, often require OS upgrades and HANA updates before ETD itself can be updated.

Solutions such as the Cybersecurity Extension for SAP are lightweight addons for SAP. Consequently, they do not require additional servers and infrastructure and can be deployed within a few hours. They are also relatively easy to maintain since they are updated using SAP standard tools for addon updates.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✗	✓	✗	✓	✓

20. Licensing Cost

Licensing cost is a key factor when evaluating SAP cybersecurity solutions since it directly impacts both the total cost of ownership (TCO) and the sustainability of cybersecurity programs. Costly solutions are difficult to sustain and scale in organizations, regardless of their technical strength. Software vendors often divide their products into separate modules or units tailored for different use cases to make them appear more affordable and accessible. However, this approach can cause cost-conscious customers to compromise on coverage and functionality in favor of a lower price.

The Cybersecurity Extension for SAP is an integrated solution that combines SAP vulnerability management, compliance reporting, access risk analysis, patch management, custom code security, and threat detection and response within a single, unified, and competitively priced platform. This enables organizations to minimize costs without compromising on coverage.

LAYER SEVEN SECURITY	ONAPSIS	PATHLOCK	SAP ETD	SAP CVA	SECURITYBRIDGE
✓	✗	✗	✗	✗	✗

Conclusion

The Cybersecurity Extension for SAP from Layer Seven Security is the only option that satisfies all 20 of the criteria for SAP cybersecurity solutions. Other SAP or third-party tools often fall short in one or more area. SAP ETD and Onapsis demand significant infrastructure, resulting in complex and time-consuming deployments, along with high licensing costs. Pathlock and SecurityBridge offer simpler, lower-cost options but require licensing of multiple software units to achieve complete coverage.

For customers looking for a comprehensive, lightweight, and cost-effective SAP security solution, the Cybersecurity Extension for SAP stands out as the optimal option. It combines an intuitive, user-friendly design with robust protection, rapid deployment, ease of maintenance, and the lowest total cost of ownership in its class based on unified licensing.

LAYER SEVEN SECURITY

Layer Seven Security is an industry leading provider of security solutions and services for SAP systems. It's SAP-certified Cybersecurity Extension for SAP delivers advanced vulnerability management, threat detection and custom code security, enabling organizations worldwide to secure SAP systems from cyber threats.

CONTACT US

Westbury Corporate Centre
Suite 101, 2275 Upper Middle Road
Oakville, Ontario, L6H 0C3
Canada
Tel. +1 647-964-7370

www.layersevensecurity.com
info@layersevensecurity.com

SAP Partner

SAP® Certified
Integration with SAP S/4HANA®