

SOLUTION BRIEF

Fortinet Secures the Intelligent Enterprise Running SAP

Executive Summary

Business leaders embrace SAP HANA functionality to stay on top of emerging trends and evolving business requirements. As SAP transforms business processes with intelligent automation, it also increases security risk. New implementations of SAP systems, SAP upgrades, and conversions to S/4HANA are now in the cloud rather than on-premises, and the threat landscape is shifting. Fortinet takes a holistic approach to secure SAP systems by protecting all SAP data generated by edge devices, endpoint systems, users, applications, databases, and third-party systems in on-premises, hybrid, and multi-cloud environments.

The SAP Threat Landscape Is Shifting

SAP systems contain data from finance, human resources, and proprietary information. Their security is paramount, especially as cloud, mobile, and hyperscale technologies come into play, exposing more services to the internet. The key factors listed below are responsible for the shifting SAP threat matrix.

Fiori, the new user web interface, opens the door for web-based threats. Fiori will access SAP applications, which are HTML5-based and are replacing the traditional SAP fat client.

SAP is connecting to smart devices. Smart devices connecting to SAP are prone to security vulnerabilities.

Managing hybrid and multi-cloud environments increases complexity. Customers are deploying more and more SAP systems in hybrid or multi-cloud solutions, and most S/4HANA systems are expected to move to the cloud. Adding point products to extend to the perimeter of the attack surface creates silos and added complexity.

Protecting Critical Business Applications Is a Top Priority

Sensitive data lives in SAP systems, and as organizations embark on their SAP projects, their threat landscape quickly shifts as applications and data are exposed to cybersecurity threats. One security breach can cost an organization millions of dollars and destroy their reputation.

Secure Your SAP System With Holistic Coverage

A focused SAP security practice is necessary to protect all the data generated by SAP. Using a holistic approach, Fortinet secures the entire enterprise SAP landscape to protect against security threats. By leveraging its extensive threat intelligence, a strong portfolio, and state-of-the-art AI/ML security, Fortinet provides comprehensive security across the entire SAP ecosystem.

Fortinet Secures the Intelligent Enterprise

Enterprise security

Simplify operations and provide consolidated security, visibility, and analytics with Fortinet to centralize operations across complex computing landscapes such as SAP.

Built-in intelligent technologies

Combat modern threats using artificial intelligence (AI), machine learning (ML), and advanced analytics with Fortinet to expedite threat prevention, detection, and response.

High-performance and end-to-end encryption

Gain visibility into malicious traffic flows that do not impact the user experience or system performance using Fortinet's localized secure sockets layer (SSL) inspection (decrypt, inspect, re-encrypt).

Accelerate SAP deployments

Deploy S/4HANA faster with Fortinet's prepackaged Infrastructure-as-Code templates to improve agility, adopt DevOps best practices, and provide broad protection to your entire SAP deployment.

The single-pane-of-glass management enabled by the Fortinet portfolio provides a complete and consolidated view of security events across on-premises, hybrid, and multi-cloud environments. A consistent security framework protects SAP workloads and all SAP-generated data. Fortinet applies AI for faster threat prevention, detection, and response. The Fortinet security solution for SAP centralizes and automates security controls and analytics—making it easier to manage, respond, and automate the SecOps capabilities.

How Fortinet Secures the Intelligent Enterprise

The different solutions that comprise the Fortinet Security Fabric protect data generated in SAP against common and emerging threats. Fortinet ensures all critical assets stay protected as IT teams embark on their SAP projects. SAP data generated at the edge, endpoint, users, apps, data, and third-party systems across multiple locations and regions are protected with the Fortinet Security Fabric.

The Fortinet Security Fabric, a broad, integrated, and automated cybersecurity framework, extends security policies from on-premises to the cloud and weaves together all operational and technical security facets, creating a consistent structure for the needs of the SAP security landscape.

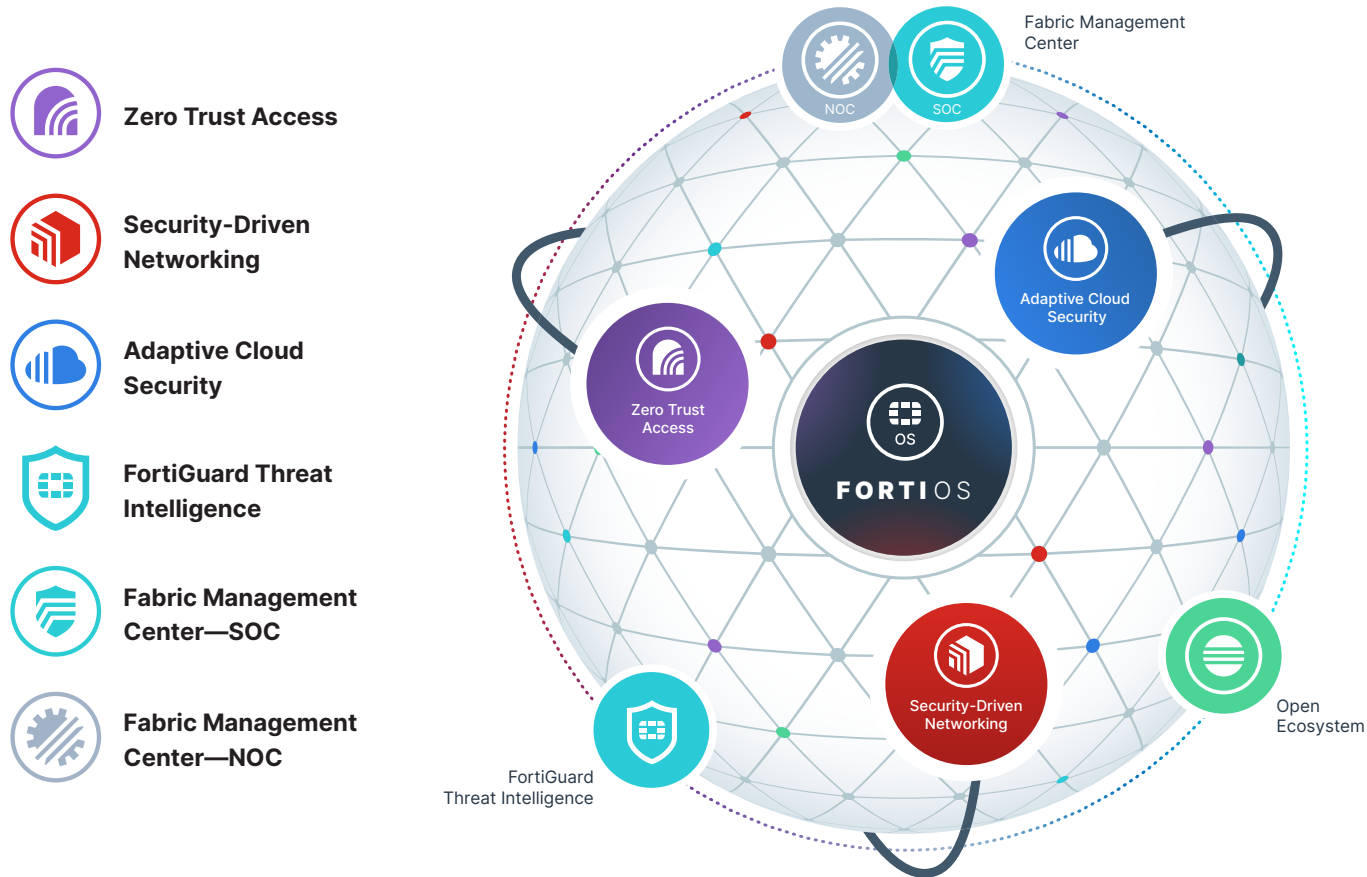


Figure 1: Fortinet Security Fabric diagram.

Securing the Intelligent Enterprise

The modern SAP system and its migration to the cloud are shifting the threat landscape and creating a more complex environment to defending mission-critical applications. An SAP deployment may involve multiple landscapes spread across hybrid premises and a cloud footprint running on various software-defined networks (SDNs). Security visibility is a challenge across such a broad and diverse infrastructure as SAP. Front ends, application servers, and databases must be segmented against lateral infection and unauthorized access. With user connections and data encrypted mainly by SSL, high-performing, in-line deep packet inspection is necessary. At the same time, security must have no perceptible impact on the user experience and system performance.

SAP deployments demand high performance while all SAP data is secured and protected. The **Fortinet Security Fabric** platform specifically addresses SAP's most common and emerging threats by providing a comprehensive and unified security solution. With over 20 years of history, Fortinet is the #1 cybersecurity leader protecting assets, optimizing content delivery, detecting malicious actors, and mitigating threats to secure the entire SAP landscape.

Fortinet Provides Comprehensive Security for SAP

Advanced application delivery controller

FortiADC enhances SAP applications' security, scalability, and performance. In one solution, **FortiADC** provides WAF, intrusion prevention system (IPS), SSLi, link load balancing, and user authentication whether SAP applications run on-premises or in the cloud.

Dynamic SAP integration

FortiADC secures SAP both with **SAP connector** and by integrating application delivery into the Fortinet Security Fabric. The **SAP connector** gets changes from the SAP Message Server. All SAP web traffic to the SAP Application Servers is protected with end-to-end encryption using the **FortiADC**.

Simplify setup and management

An intuitive user interface streamlines the configuration of CLI and APIs. Automated configuration gathers information from the SAP ICM configuration (HTTP/HTTPs Ports, virtual hosts, etc.) and additional application server instances. The **SAP connector** provides a topology view of the SAP landscape within the network for easier management and unified visibility for multi-cloud or on-premises SAP deployments.

Advanced Security

Policy-based insights into users, behaviors, and data stored in major SaaS applications

FortiCASB is a Fortinet-developed cloud-native Cloud Access Security Broker (CASB) solution designed to provide visibility, compliance, data security, and threat protection for cloud-based services employed by an organization. For organizations that comply with regulatory requirements and industry mandates, **FortiCASB** has predefined policies for common regulatory standards to detect violations with actionable recommendations to remediate, along with reports for auditing and tracking. **FortiCASB** monitors malicious traffic, malware and sensitive data, suspicious user activity, and compliance violation with predefined out-of-the-box security policies.

Monitor and track user activity

FortiCASB uses RESTful APIs to integrate directly with SAP Identity Authentication Service (IAS) to monitor and track SAP IAS user activities such as logins, user assignments, updates, etc. **FortiCASB** also integrates with SAP Success Factors using an API-based approach, pulling data directly from SAP Success Factors via RESTful API. Documents are uploaded to determine if malicious and log files reviewed to verify the traffic is valid.

Traffic Analysis and Investigation

FortiCWP uses User Entity Behavior Analytics (UEBA) to look for suspicious or irregular user behavior and sends alerts for malicious behavior. A centralized dashboard displays security events and user activity in real-time to shorten the time to insight.



Segment SAP workloads with low latency

Segmenting SAP from other workloads ensures a minimum boundary of trust and inspection. The internal segmentation of application servers, front ends, and databases prevents lateral attacks through impersonation or privilege escalation.

FortiGate delivers high-performance, low-latency SAP security through the deep packet and content inspection specific to SAP services.

Protect threats targeting SAP with intrusion prevention system (IPS) and content inspection

Addressing targeted SAP threats requires the security apparatus to be application-aware of the SAP systems running within the security boundary.

The **FortiGate**, combined with **FortiGuard Threat Intelligence**, delivers validated industry-leading IPS technology. FortiGuard Labs provides SAP threat intelligence to the FortiGate's IPS engine to protect from well-known and emerging threats.

Provide high-performance SSL inspection

Most Hypertext Transfer Protocol (HTTP) traffic is SSL encrypted, and SAP has embraced HTTP as a modern protocol for users to access SAP S/4 applications. Today more than 60% of malware is encrypted.¹ FortiGate next-generation firewalls (NGFWs) protect against encrypted malware without user or database performance degradation.

Physical **FortiGate NGFWs** use proprietary hardware acceleration that offloads encryption functions to a security processing unit. This Fortinet-only capability boasts performance advantages of up to 20x that of competitors in the latest-generation devices.

Protect SAP Web Dispatchers

Web Dispatchers are used by SAP to load balance SAP's Fiori systems. The Web Dispatchers create a larger attack surface and vulnerabilities for common Open Web Application Security Project (OWASP) attacks. The **FortiWeb web application firewall (WAF)** delivers end-to-end encryption. It is a dedicated HTTP(s) protection platform to protect against OWASP threats and provide virtual patching and auto tuning, and uses AI and ML to detect threats faster.

Evaluate SAP compliance

A holistic understanding of SAP resources' risk posture and compliance levels is critical as SAP is deployed across multiple cloud providers. To reduce security risk, Fortinet brings tools such as **FortiCWP** to assess cloud configuration security posture. It detects potential threats originating from misconfiguration of cloud resources, monitors user behaviors and cloud network traffic, and provides comprehensive compliance reports and alerts.

Provide deployment flexibility

All major cloud providers are natively integrated with Fortinet allowing organizations to support SAP deployments and plan SAP S/4HANA projects across major cloud providers. Support for older versions of SAP including SAP ECC, SAP NetWeaver, and SAP Business Suite is also provided.

Secure Your SAP System With Fortinet

Organizations run their mission-critical applications on SAP. These SAP deployments span across clouds and generate data in many locations that create the opportunity for blind spots in the security posture. Holistic security coverage with Fortinet ensures SAP systems are protected and that security policy and visibility remain unified across the hybrid and multi-cloud footprints. Protecting the entire SAP ecosystem frees IT to focus on other high-value projects.

¹ ["Fortinet Threat Report Reveals an Evolution of Malware to Exploit Cryptocurrencies,"](#) FortiGuard SE Team, May 16, 2018.

