

WHITE PAPER

A Guide To Implementing a Secure SAP System with Fortinet



Executive Summary

With today's rapidly changing market conditions and economic climate, organizations are using enterprise application software to manage their business functions with an integrated system. An integrated enterprise resource planning (ERP) system improves decision-making and integrates information from customers, supply chains, and vendors to gain competitive insights.

SAP is the world's largest enterprise application software provider, a leader on the Gartner Magic Quadrant helping organizations with their digital commerce platforms sales and operations planning systems, integrating, consolidating, and generating insights into its critical processes.

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 and increasing the attack surface area.

Fortinet's focused SAP security practice takes a holistic approach to securing the enterprise SAP landscape.

Fortinet leverages its extensive threat intelligence, a strong portfolio, and state-of-the-art artificial intelligence (AI) and machine learning (ML) security to provide a seamless security experience across your SAP landscapes. It automates security controls, making it easier to manage, respond, and automate the SecOps capabilities.

In this paper, we present best practices and recommendations for implementing a secure SAP environment, including SAP S/4HANA, a future-ready system with built-in intelligent technologies, including AI, ML, and advanced analytics. We highlight the most common attack vectors on SAP and how Fortinet's portfolio can address those vectors by taking a preventative and detecting role in SAP environments.

Business Innovation with SAP

Business leaders must stay on top of emerging trends and modern technology to remain relevant in the digital world. Organizations turn to SAP HANA for accessing real-time data across business units to make data-driven decisions, improve business outcomes, and drive innovation.

SAP S/4HANA transforms business processes with intelligent automation and runs on SAP HANA—a market-leading in-memory database that offers real-time processing speeds and a dramatically simplified data model. Many organizations embrace cloud providers to free budget and invest parts of that budget into more innovative tasks and projects.



SAP deployments turn to the cloud

- SAP customers will have to convert their SAP systems to SAP S/4HANA by 2027
- New implementations of SAP systems, SAP upgrades, and conversions to S/4HANA are being deployed with cloud providers, rather than on-premises



Protecting SAP solutions is top of mind

- Global cyber-crime damages to reach \$6 trillion annually by 2021¹
- SAP security updates are periodically released, and customers are encouraged to apply patches promptly
- SAP systems' uptime requirements create a burden to the SAP basis team to upload, test, and validate every SAP patch

Fortinet secures the Intelligent Enterprise running SAP—by protecting all SAP data generated by edge devices, endpoint systems, users, AI, applications, databases, third-party systems in multi-cloud environments, and on-premises.



Threat landscape for SAP software is shifting

- Enterprises shift their attack surface by adding cloud services or by managing hybrid environments
- SAP Fiori is a new web interface, which is HTML5-based and are targets for attacks
- Smart devices connecting to SAP are prone to security vulnerabilities



SAP security risks exist

- Currently SAP does not provide guidance on infrastructure security
- SAP does not provide any rules on how SAP systems can prevent security attacks with today's technologies available to cyber criminals

The Journey to SAP S/4HANA

CIOs and IT teams are planning their SAP system conversion to SAP S/4HANA with the 2027 deadline on the horizon.² The majority of SAP S/4HANA systems will be deployed in the cloud at one of the top global hyperscalers (cloud providers).³ SAP S/4HANA is the top SAP initiative, followed by agile adoption of SAP projects and moving SAP workloads to the cloud.⁴

SAP at a Glance

The world's largest provider of enterprise application software

- **92%** of the Forbes Global 2000 are SAP customers
- **77%** of the world's transaction revenue touches an SAP system
- **400,000** customers worldwide

SAP S/4HANA is SAP's successor of SAP BusinessSuite. SAP announced that standard support for SAP BusinessSuite would end by 2027. By that date, all customers will have to be converted to SAP S/4HANA unless they prefer to pay a premium for their SAP support fees. Converting old systems to S/4HANA is not necessarily straightforward. This type of project requires careful planning and consulting expertise, as well as a significant budget to execute in time.

The role of cloud providers

The majority of S/4HANA systems are expected to move to the cloud leveraging a cloud provider. Adding services to the cloud or managing hybrid environments shift an enterprise's attack surface. As organizations move to the cloud to deploy S/4HANA, their most critical business applications become vulnerable. As a result, every SAP organization must seriously rethink security to ensure customer data and enterprise information is protected, and data privacy policies in each country conducting business are respected.

Major cloud providers offer dedicated services for SAP users. SAP can be deployed in their clouds to offload costs of running on-premises systems into the cloud and pay by OPEX instead of CAPEX. However, many customers will prefer a hybrid model, where the majority of SAP systems will run in the cloud and where dedicated production systems remain on-premises. No matter which model is selected, the need for higher security for data of mission-critical systems is increasing as the attack surface shifts when moving to the cloud.⁵

SAP Enables Business Innovation

Organizations are planning for new implementations of SAP systems, SAP upgrades, and conversions to S/4HANA to embrace digital initiatives for improving operational efficiency and enabling new business models. SAP software is an integrated software suite that addresses needs from all areas and organizations within an enterprise. SAP enhances the competitiveness of enterprises by modernizing and transforming processes into digital solutions. Implementations of SAP software can take between four months to several years with dozens if not hundreds of SAP systems deployed. SAP systems are always business-critical, and most of the time, they also are mission-critical; thus, downtime is unacceptable.

SAP S/4 and the benefits of HANA

SAP S/4HANA is based on a simplified data model, and provides an immediate benefit to the line of business (LOB) by improving productivity. While S/4HANA offers faster and more flexible processes at significantly less IT costs, it sits at the core of enterprises to enable them to reach their next level of digital transformation by using embedded artificial intelligence, real-time analytics, and more.

S/4HANA is an architectural redesign of SAP's traditional application architecture based on SAP R/3 from 1992. Although S/4HANA is developed to achieve maximum benefit of SAP HANA—High-Performance Analytical Appliance—it also supports traditional database management systems (DBMS) like Oracle, DB/2, MSSQL, Sybase, etc.

SAP HANA is an in-memory, column-oriented DBMS that allows real-time OLTP and OLAP operations in a single system, thus avoiding the need for additional data warehouse systems that enable data mining on OLTP data. Such data warehouse systems are not capable of screening real-time data. SAP HANA has that capability due to its ability to store data in-memory and in columns. Scale-out systems of SAP HANA can span up to 16 nodes and hold up to 24 TB of data in-memory for a single SAP system.

Protecting SAP Against Cybersecurity

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

Two 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 be used to access SAP applications, which are HTML5-based, and is about to replace the traditional SAP fat client SAP GUI.

SAP is deploying more cloud or hybrid solutions. SAP does not limit itself to its SAP HANA Enterprise Cloud (HEC) and enables operations of SAP solutions in AWS, Microsoft Azure, and Google Cloud Platform. As a result, SAP systems are no longer available only internally within company boundaries but can also be externally accessed. Hybrid deployments are deployments where SAP is partly available in the cloud as well as on-premises. More emphasis must be placed on security-driven networking to avoid known attacks.

Fortinet Secures the Intelligent Enterprise

Fortinet, the number one cybersecurity leader with more than 20 years of history protecting assets, optimizing content delivery, detecting malicious actors, and mitigating threats, saw a rising in the attacks targeting SAP systems. As these systems are one of the critical assets of organizations, Fortinet decided to secure those landscapes.

By applying the Fortinet unified portfolio, organizations can have a consistent security framework for SAP across multiple locations and regions. Leveraging the Security Fabric, a broad, integrated, and automated cybersecurity framework, it weaves together all operational and technical security facets, creating a consistent structure to the SAP security landscape's needs.

As data is the new oil and SAP systems contain confidential data, Fortinet provides capabilities addressing the data's lineage, providing confidentiality, integrity, and availability. Fortinet capabilities in data loss prevention (DLP), preventing exfiltration of data, and integration with leading vendors as part of the Security Fabric create a unique value in data security, as it consolidates it in a single pane of glass.

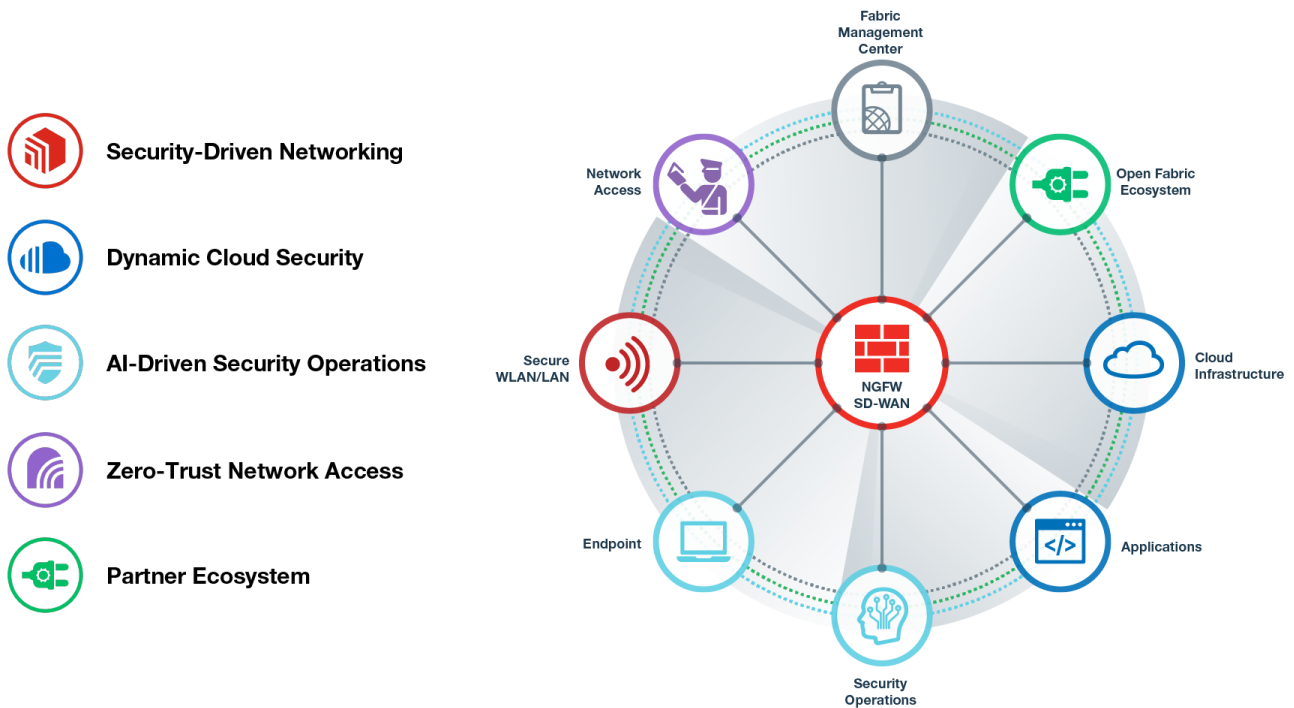


Figure 1 Fortinet Security Fabric Diagram

The single-pane-of-glass management enabled by the Fortinet portfolio provides a complete and consolidated view across various network edges. It simplifies operations and provides networkwide security, visibility, and analytics, in every environment, centralizing operations for complex landscapes such as SAP, delivering scale, performance, and resiliency for SAP.

As SAP systems are becoming more prevalent in the cloud, Fortinet has integrated next-generation firewalls (NGFWs) that can be deployed in cloud environments supporting the majority of the cloud providers. Customers can leverage consistent multi-layer security protection, automation, and deep integrations, no matter how many clouds they adopt, and provide protection to the SAP ecosystem and beyond.

Fortinet reduces the time to deploy S/4HANA with prepackaged Infrastructure-as-Code templates, enabling the organization to be more agile, adopt DevOps best practices, and provide 360 protection to the SAP landscape.

Fortinet wants to accelerate the security in your SAP ecosystem by protecting all SAP data generated by edge devices, endpoint systems, users, AI, applications, databases, third-party systems in multi-cloud environments, and on-premises. Fortinet will provide an integrated experience to ensure that your critical assets stay protected and empower you to focus on your core business.

SAP Systems Are Being Attacked

Securing SAP systems is becoming more and more relevant in today’s world. The threat landscape is constantly expanding, and it does not stop at SAP systems. It exposes companies of all sizes and industries to the risk of cyberattacks with severe consequences such as data leaks or damage to the company’s reputation.

Some of the vulnerabilities of SAP systems have been given well-known codenames such as **RECON** or **10KBLAZE**. Besides these known vulnerabilities, easy-to-use exploits are found on the internet and used by threat actors without much knowledge of SAP.

Every month SAP publishes security advisories about current vulnerabilities or bugs that could endanger the entire SAP landscape. These notes should be implemented in the SAP systems at regular intervals to ensure secure operation and often requires system downtime.

Overview of Published SAP Security Updates

Due to the size and complexity of SAP software, SAP carries out numerous tests, validations, and checks for compliance with programming guidelines before a new software component is released. Nevertheless, there are always vulnerabilities, without knowing where and which ones are currently in the SAP code. SAP closed a total of 182 vulnerabilities between May 2019 and May 2020.

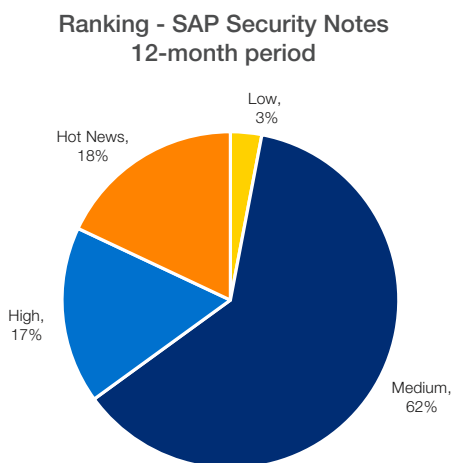


Figure 2 SAP Vulnerability Ranking May 2019 2020

Managing SAP Security Notes

SAP systems directly accessed from the internet must be patched with a higher priority due to its higher exposure to potential attacks.

Hot news: Imported immediately since they impose a serious threat to the system.

High: Evaluate advantages of applying them as quickly as possible versus importing them with the next SAP Support Package Stack, based on the system landscape and vulnerability exposure.

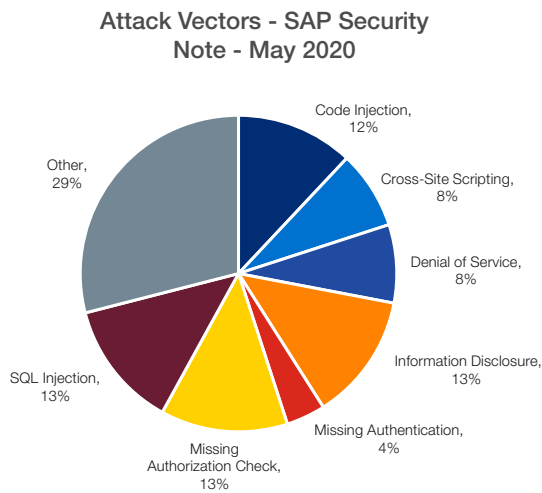


Figure 3 Attack Vectors SAP Security Note May 2020

SAP Attack Vectors

Disclosure of information: Helps an attacker find the right tool or attack point.

SQL injection: Allows an attacker to read parts of the database and view data that is not intended for that user.

Code injection: Injecting code into the SAP system could lead to a remote code execution.

How can we protect the SAP system from such attacks to avoid data exploits and a compromised system? Generic protection for threats such as, e.g., SQL injections or cross-site scripting is a **web application firewall (WAF)**.

How Fortinet Provides Higher Security for SAP

The modern SAP system, and its migration to the cloud, enable ever more interfaces—connections to other SAP and non-SAP systems that are internal and external to an organization. Defending what is typically a business's most vital application is as complex as it is critical. An SAP deployment may involve multiple landscapes spread across a hybrid premises and cloud footprint running on a variety of software-defined networks (SDNs). Front ends, application servers, and databases must be segmented against lateral infection and unauthorized access. With user connections and data largely encrypted by secure sockets layer (SSL), high-performing, in-line deep packet inspection is a necessity. At the same time, security must have no perceptible impact on the user experience and system performance.

With so many vectors to protect against, visibility can be a challenge across such a broad and diverse infrastructure as SAP. With respect to infrastructure, SAP's Security Baseline Template leaves these problems to the customer to solve. **The Fortinet Security Fabric** platform specifically addresses SAP's most common and emerging threats by providing a unified security context that is simultaneously integrated with, and independent of, the underlying infrastructure. Fortinet uniquely provides the high-performing network and content protection that an SAP deployment demands.

Segment SAP workloads with FortiGate

SAP's well-architected security starts with considering how SAP traffic will transit the infrastructure and where boundaries of trust reside. Segmenting SAP from other workloads ensures a minimum boundary of trust and inspection. Critically, this includes the internal segmentation of application servers, front ends, and databases to prevent lateral attacks through impersonation or privilege escalation. The best practice of segmentation enables the FortiGate to high-performance, low-latency SAP security through the deep packet and content inspection specific to SAP services.

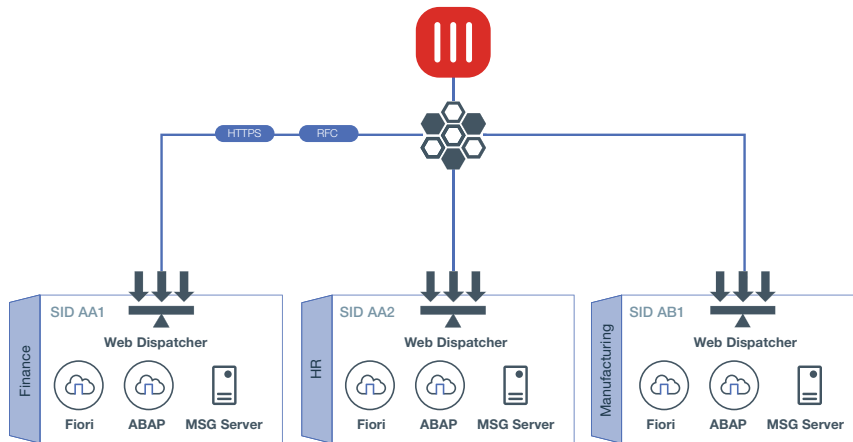


Figure 4 SAP East/West Segmentation

FortiGate delivers unmatched security with high performance

- Secures without impacting transaction times for users
- Doesn't impede database processes

High-Performance Intrusion Prevention and Content Inspection Using FortiGate NGFW

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 intrusion prevention system (IPS) technology.

Fortinet products are designed to protect SAP

- FortiGuard Labs provides SAP threat intelligence to the FortiGate's IPS engine to protect from well-known and emerging threats.
- Fortinet mitigates common SAP threats with microsecond latency.
- Configuration errors are minimized as SAP heuristics, and signatures are enabled in the default IPS policy.
- Compact pattern recognition language (CPRL) is a deep-inspection, proactive signature-detection technology developed through years of research by FortiGuard Labs. A single CPRL signature can catch 50,000 or more variants of a family of malware.
 - CPRL proactive signature detection helps cast a wider net over the attacks and methods of modern advanced persistent threats (APTs) and advanced evasion techniques (AETs), preserving full sandbox analysis for the most sophisticated threats.
- FortiSandbox is a rigorous inspection tool that can fully execute and analyze content and executable code to uncover APTs that pursue SAP systems by exploring all code execution paths.
 - Combining sandboxing with proactive signature detection minimizes the opportunity for APTs.
 - With Fortinet Security Fabric integration, threat intelligence is distributed across the network footprint in real time to elevate the security posture continually.

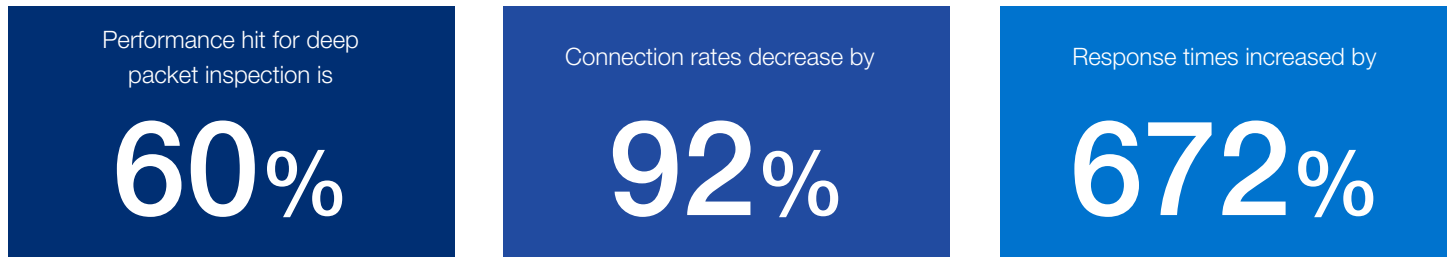
SSL Inspection with FortiGate NGFW

It's no secret that the majority of HTTP traffic is SSL encrypted for apparent reasons. As SAP has embraced HTTP as a protocol for a modern S/4 deployment and customers move away from the SAP GUI thick client, the guidance has been to "maintain end-to-end encryption."

Today more than 60% of malware is encrypted. Supporting localized SSL inspection (decrypt, inspect, re-encrypt) provides both the visibility into malicious traffic flows and maintains the best practice of "end-to-end encryption." However, there is a risk for performance impacts that can cause user experience and database lock times to suffer.

Speed matters for end-to-end encryption

NSA Labs has found, on average, the following⁶



Fortinet removes this compromise between security and performance in a variety of ways.

1. Physical FortiGate NGFWs proprietary hardware acceleration offloads encryption functions to a security processing unit boosting performance up to 20 times that of competitors.⁶
2. Virtual FortiGate implements the virtual security processing unit (vSPU) as a virtualized application-specific integrated circuit (ASIC) in conjunction with a unique decryption load-balancing service delivering up to 7 times the performance of competitors.

With Fortinet, SAP decision-makers can be assured that Fortinet provides the highest security catch rates with the most significant performance levels possible.

Hybrid Cloud Security Context

SAP S/4HANA is the core of SAP’s modern Intelligent Enterprise solution that extends line-of-business applications from the data center to the cloud. A hybrid cloud deployment permits flexibility between customization and speed to market but also increases cyber risks.

Security Challenge	Solution
Protect dynamic edges where SAP systems may federate across these platforms	The Fortinet Security Fabric provides real-time threat intelligence shared across the entire SAP security boundary
Multiple, continually evolving edges that require a single security context	Network segmentation is implemented as microsegmentation with FortiGate NGFW policies attached at each virtual network interface card (VNIC). Similarly, the cloud is deployed on the cloud provider’s SDN with subnet-level segmentation with east-west and north-south inspection between application tiers. Identity services are synchronized from the data center into cloud single sign-on (SSO).
Lack of a single-point truth and management for policies that are deployed in the cloud	Fortinet FortiManager and FortiAnalyzer coordinate the management and threat intelligence everywhere Fortinet network security is deployed. FortiManager and FortiAnalyzer can be deployed on-premises or in the cloud.
Managing security for next-generation software-defined data centers (SDDCs) and clouds run on SDNs that are application programming interface (API)-driven. The rich metadata of the SDN benefits security by providing information on the objects and networks in the SDN.	FortiGate NGFWs farm this metadata through Fabric Connectors to implement dynamic policies. As SAP workloads are pushed into production, metadata filters inform the FortiGate on how to apply policy. This automation drives business intent and non-blocking production security for new service deployments.

FortiWeb Web Application Firewall Protects the SAP Web Dispatcher

SAP S/4 shifts much of SAP’s user interaction from SAP GUI to a user’s browser and HTTP(s) protocol. As this encrypted web traffic grows, the opportunity to exploit common web vulnerabilities expands, creating a larger attack surface. Web Dispatchers are deployed for load balancing to SAP Fiori systems. Still, they lack any ability to protect back-end resources from cross-site scripting, SQL injection, JavaScript exploits, and other common Open Web Application Security Project (OWASP) attacks. SAP recommends maintaining end-to-end encryption along with appropriate patching. While this is a best practice, most malware is encrypted as well, which still leaves a gap in protection.

FortiWeb web application firewall (WAF) is a dedicated HTTP(s) protection platform that goes beyond protecting known OWASP Top 10 threats. FortiWeb provides the following advanced functionality:

- Auto tuning and machine learning while maintaining full-length encryption and only decrypting locally to support inspection
- Lifts the burden of cumbersome manual tuning and distracting false positives
- Looks for the user's habits and patterns to build security tailored to the sessions that should be permitted
- Provides virtual patching
- FortiWeb can be deployed as a physical or virtual instance or as Software-as-a-Service (SaaS) as the most effective way to protect your web services in SAP.

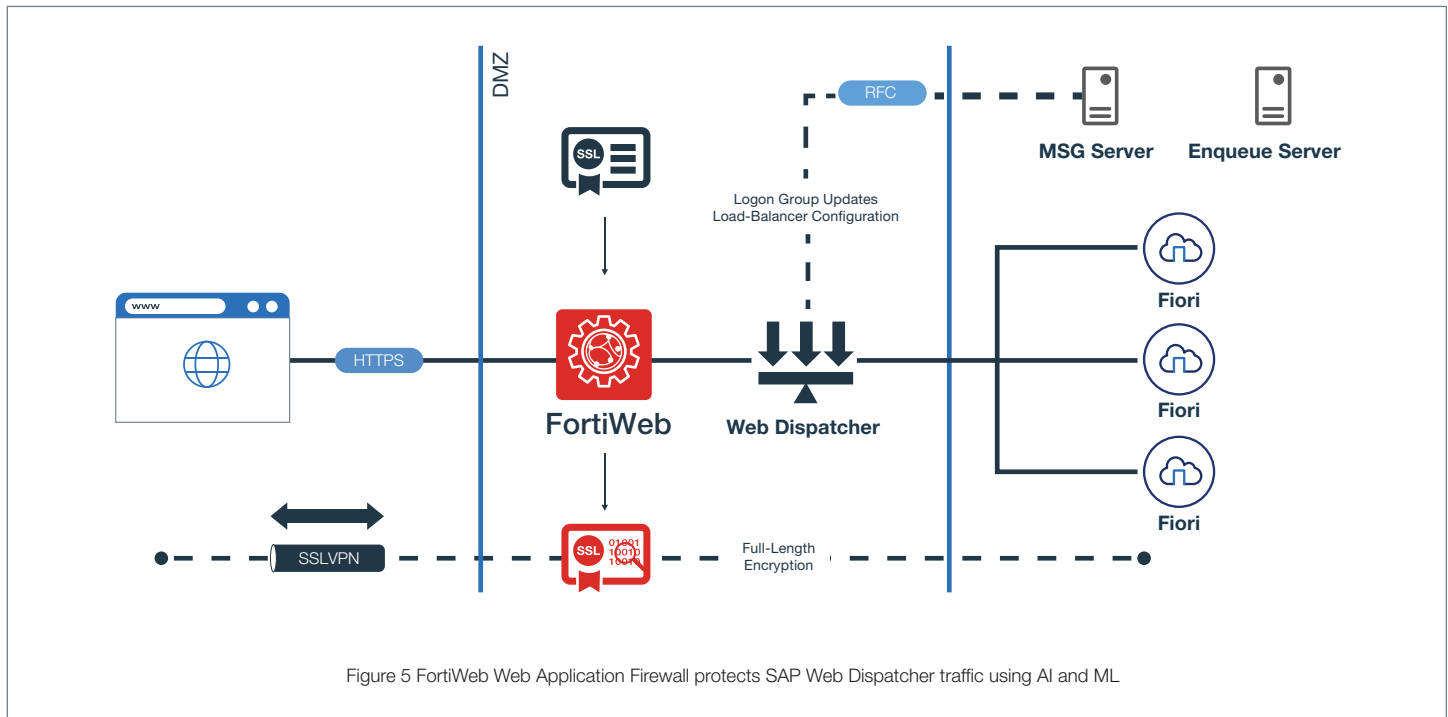


Figure 5 FortiWeb Web Application Firewall protects SAP Web Dispatcher traffic using AI and ML

Evaluate SAP Compliance

With the increase in hybrid architectures and cloud usage, userbase and resources have become perimeterless, in the sense that they are now distributed across landscapes and infrastructure, especially in the cloud world as organizations adopt multi-cloud environments to reduce concentration risk. Fortinet brings tools to security teams such as FortiCWP cloud workload protection (CWP).

Using FortiCWP, security teams can evaluate their cloud configuration security posture, detect potential threats originating from misconfiguration of cloud resources, analyze traffic across cloud resources (in and out of the cloud), and evaluate cloud configuration against best practices.

Fortinet enables a holistic understanding of the risk posture and compliance levels of SAP resources deployed in the cloud, considering the overall ecosystem and not only the SAP landscape, by providing:

- Automatic tracking of risk and compliance that is monitored continuously
- Reports are generated in a single centralized dashboard across your public cloud providers
- Manage risk throughout multi-cloud infrastructures
- Provide regulatory compliance reporting
- Integrates remediation into the cloud infrastructure life cycle automation framework

Integration with Cloud Providers

Fortinet integrates with all major cloud providers to provide deployment flexibility for organizations as they begin planning their SAP S/4HANA conversions. Fortinet reference architectures for SAP S/4HANA can be found for Microsoft Azure, Amazon Web Services (AWS), and Google Cloud in our Fortinet Security Solutions for SAP S/4HANA white paper.

Secure Your SAP System with Fortinet

SAP is a business's most critical business application in its ability to create value by organizing, operationalizing, and monetizing complex data. For these reasons, great care must be given to protect SAP's infrastructure and systems. This becomes especially difficult for migrations from traditional data centers to S/4HANA running in the cloud, creating the opportunity for blind spots in the security posture. While cloud providers have solutions for basic network filtering, they lack deep application visibility and have no effectiveness beyond their own edge.

Fortinet's holistic coverage ensures SAP systems are protected and that security policy and visibility remain unified across the hybrid and multi-cloud footprints. Fortinet eases skills gaps and correlates events through machine learning and workflow automation, multiplying the scale of SAP basis, network, and security administrators.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 450,000 customers trust Fortinet to protect their businesses.

Fortinet is the only security leader to develop and build custom security processing unit (SPU) technology to offer the best performance and cost value in the industry with a Security Compute Rating that ranges between 3 to 47x the performance of other software approaches. Each day Fortinet FortiGuard Labs uses one of the most effective and proven AI and ML systems in the industry to process and analyze more than 10 billion events, sending actionable real-time threat intelligence to customers. The combination of FortiOS, purpose-built SPU technology, and AI-powered threat intelligence showcases the Fortinet commitment to cybersecurity innovation and excellence.

The Fortinet flagship enterprise firewall platform, FortiGate, is available in a wide range of sizes and form factors to fit any environment and provides a broad array of next-generation security and networking functions. The Fortinet market position and solution effectiveness have been widely validated by industry analysts, independent testing labs, business organizations, and media outlets worldwide. Fortinet is proud to count the majority of Fortune 500 companies among its satisfied customers.

Fortinet is headquartered in Sunnyvale, California, owns a 200,000 square foot manufacturing assembly and operations center in Union City, California, and has offices around the globe. Founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen, Fortinet is led by a strong management team with deep experience in networking and security.

Fortinet technologies can secure the demanding needs of any organization and help drive digital innovation from within.

¹ Steve Morgan, "[Global Cybercrime Damages Predicted To Reach \\$6 Trillion Annually by 2021](#)", 2019 Official Cybercrime Report, Herjavec Group, December 7, 2018.

² "[Strategy - Extended Innovation Commitment for SAP S/4HANA Clarity and Choice on SAP Business Suite 7](#)," SAP, accessed March 10, 2020.

³ "[Make the move to SAP S/4HANA with Microsoft Azure](#)," SAP, accessed July 14, 2020.

⁴ Wayne Ariola, "[SAP Trends to Watch: S/4HANA, Agile, Cloud, and Testing Transformations](#)," CIO, June 19, 2019.

⁵ Steve Evans, "[Cloud Use Increases Attack Surface, But Security Not Keeping Up](#)," Infosecurity, August 22, 2016.

⁶ Omar Yaacoubi, "[The rise of encrypted malware](#)," ScienceDirect, Volume 2019, Issue 5, May 2019, Pages 6-9.