WHITE PAPER

Fortinet Secures the Enterprise SAP Landscape on Alibaba Cloud

Authors
Chen Dong, Senior Solution Architect, Alibaba Cloud
Andy Wang, SAP System Engineer, Fortinet
Julian Petersohn, Global SAP System Engineer, Fortinet
Matthias Czwikla, Head of Global SAP Sales, Fortinet
Executive summary
Disruptions are challenging every industry with rapidly changing market conditions and increasing demand uncertainty. This is leading to an emphasis on using Enterprise Application Software to manage business functions with an integrated system. An integrated ERP system, such as SAP, improves decision making and integrates information from customers, supply chains, and vendors to gain agility and competitive insights.

SAP is the world's largest enterprise application software provider and a leader in the Gartner Magic Quadrant for ERP and Cloud Database Management Systems. SAP helps companies and organizations of all sizes and industries run their businesses profitably, adapt continuously, and grow sustainably.

SAP systems contain data from finance, human resources, and proprietary information. Security of this highly sensitive data is paramount, especially as cloud, mobile, and hyper-scale technologies come into play, exposing more services to the Internet, increasing the attack surface area.

Alibaba Cloud provides SAP-certified, cloud-native instance types to give SAP customers the flexibility to lift and shift their SAP landscapes to reduce costs or modernize on SAP S/4HANA. For years, Alibaba Cloud has been a trusted global technology partner for SAP solutions. Companies have deployed SAP systems including SAP S/4HANA, SAP NetWeaver, HANA, MaxDB, MSSQL, ASE, DB2, SAP Business One, and Data Hub in Alibaba Cloud. The Fortinet/Alibaba Cloud partnership brings enterprise-class security to SAP deployments on Alibaba Cloud.

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 AI/ML (Artificial Intelligence/Machine Learning) security to provide a seamless security experience across SAP landscapes. It automates security controls making it easier to manage, respond, and automate SecOps capabilities.

In this paper, we highlight the most common attack vectors faced by organizations as they upgrade or move to SAP S/4HANA. Whether it’s a new implementations of SAP systems in the cloud, performing an SAP upgrade, or converting to SAP S/4HANA, cyber security risk looms in the background of every CISO, IT leader, and SAP technical and operational professional.

Introduction
With the rise of cloud technologies, artificial intelligence, machine learning, and other advances, every industry is digitizing business processes to remain competitive, adapt to market changes, and improve efficiency. Efforts to transform are impacting value chains and supply chains, changing how customers and employees interact with data, and forcing companies to fully adopt the concept of the intelligent enterprise meaning to weave together formerly siloed processes, intelligent technologies, and real-world data threads from customer and employee experiences.

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 hyperscalers, such as Alibaba Cloud, to free up budget and invest more in innovative tasks and projects.

Trends driving the adoption of the Intelligent Enterprise
Forward-looking companies recognize trends as an opportunity to invest in digitization and automation and build new capabilities rather than get left behind. Becoming an intelligent enterprise is about rethinking business processes and using innovation and technology to improve every aspect of the business.

These trends span across industries from manufacturing to retail, health care, and automotive. Rising customer expectations, the need to develop new digital skills and processes, competition from unexpected challengers, and the need for flexibility are forcing organizations to innovate.
SAP software is an integrated software suite that addresses needs from all areas of the business within an enterprise. SAP enhances the competitiveness of enterprises by modernizing and transforming processes into digital solutions. SAP transforms organizations into an intelligent enterprise.

**Manufacturing**

With SAP, manufacturers can implement a just-in-time digital supply chain, create seamless omnichannel experiences, achieve excellence in procurement, and deliver customer-centered merchandising.

**Retail**

Retailers are becoming increasingly customer-centric and offer highly personalized omnichannel customer experiences and use data to build a 360-degree view of the customer.

**Healthcare**

Rising patient expectations are driving organizations to modernize their infrastructure and become more automated, increasing the efficiency and effectiveness of delivering modern patient care capabilities.

**Automotive**

The automotive industry is being reshaped by the shift from combustion engines to electric, the rise of autonomous vehicles, and the digitization of the supply chain.

**SAP is on the IT agenda**

To remain relevant, organizations are either upgrading to SAP S/4HANA or planning their SAP system conversion to SAP S/4HANA. CIOs and IT leaders are keenly aware of the 2027 deadline to convert their SAP systems to SAP S/4HANA.\(^1\) SAP S/4HANA is the top SAP initiative, followed by agile adoption of modern SAP solutions, and moving SAP workloads to the cloud.\(^2\)

Most of the SAP S/4HANA systems will be deployed in the cloud at one of the top global hyperscalers. Alibaba Cloud is a trusted global technology partner for SAP that provides a flexible cloud computing infrastructure and platform services with the following benefits:

- Great scalability: Seamlessly expand your IT infrastructure to meet growing business demands.
- Rapid deployment: Easily prepare your SAP environment and deploy it within minutes.
- Cost effectiveness: Reduce your CapEx by paying only for what you use, with no requirements for any additional IT infrastructure.
- High availability: Run your IT infrastructure with unparalleled stability thanks to our extensive network and comprehensive suite of cloud-based solutions.
Protecting SAP is top of mind
The threat landscape for SAP software is shifting as organizations upgrade or deploy SAP to the cloud. SAP is creating new security risks with SAP Fiori, a new web interface, which is HTML5-based and a target for cyber-attacks. Additionally, smart devices connecting to SAP are prone to security vulnerabilities. Global cyber-crime damages are forecasted to reach $10.5 trillion annually by 2025.¹

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 cybercriminals.
- SAP security updates are periodically released and customers are encouraged to apply the updates.
- SAP systems' uptime requirements create a burden to the SAP Basis team to upload, test, and validate every SAP patch across all SAP landscapes.

Becoming an Intelligent Enterprise
The majority of SAP 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 SAP 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.

Most cloud providers offer dedicated services for SAP users. SAP can be deployed in their clouds to offload costs of running on-premises systems and pay by OpEx instead of CapEx. However, many customers will prefer a hybrid model, where many 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.

Getting your SAP to Alibaba Cloud
A range of certified SAP solutions are available on Alibaba Cloud, supporting SAP S/4HANA, SAP Business Suite, and SAP Business Warehouse. Organizations deploying SAP systems in Alibaba Cloud reduce costs, improve efficiencies, and simplify operation and maintenance (O&M) across their IT infrastructures.

The global partnership between Alibaba Cloud and SAP provides many benefits including:

Certified solutions
An extensive range of certified SAP solutions are available on Alibaba Cloud, including SAP NetWeaver, SAP HANA, MaxDB, MSSQL, ASE, DB2, SAP Business One, and SAP Data Hub.

Low total cost of ownership (TCO)
Enterprises are able to enjoy a lower TCO than with an on-premises solution thanks to a range of cost-effective options including stable pricing and the ability to save costs by using Express Connect, compared to a lease line connection.

High performance
Alibaba Cloud's Enhanced SSD (ESSD) Cloud Disks deliver a maximum random IOPS of 1 million per disk and low one-way latency. Users can also benefit from enhanced performance provided by next gen CPUs.

Customized solutions
The range of customized solutions available for users include Alibaba Cloud's security suite, cloud backup, auto deployment and monitoring, on top of access to Alibaba Cloud's interconnected network.
Protecting SAP against Cybersecurity Threats

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 customers are deploying more cloud or hybrid solutions.** SAP does not limit itself to its SAP HANA Enterprise Cloud (HEC), and it enables operations of SAP solutions in a hyperscaler, like Alibaba Cloud. 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 partially available in the cloud as well as on-premises. More emphasis must be placed on security-driven networking to avoid known attacks.

Fortinet secures SAP solutions

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 rise 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. Fortinet identifies SAP network packets to gain SAP network traffic visibility. 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 secure 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.

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 network wide security, visibility, and analytics, in every environment, centralizing operations for complex landscapes such as SAP, delivering scale, performance, and resiliency.

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

**Run SAP on Alibaba Cloud securely with Fortinet**

Cloud security is maintained through a shared responsibility model, where Alibaba is responsible for protecting the cloud infrastructure that runs the services offered—**security of the cloud**. Customers are responsible for all the services, SAP workloads, applications, and data they use—**security in the cloud**. Fortinet natively integrates its Fortinet Security Fabric into Alibaba Cloud, enabling customers to deploy SAP workloads with full security visibility while maintaining centralized management and security automation. By protecting all the data generated within the SAP ecosystem regardless of its location—whether on-premises or in Alibaba Cloud—Fortinet centralizes and automates security controls and analytics, making it easier to manage, respond, and automate security for SAP workloads.

**Focused SAP practice**

A consistent security framework protects all SAP workloads. An organization’s SAP security posture is strengthened using Fortinet’s extensive threat intelligence, a comprehensive portfolio, and AI/ML security to provide a seamless security experience across the entire SAP landscape.

**Fortinet reference architecture for SAP S/4HANA**

![Fortinet Reference Architecture for SAP S/4HANA on Alibaba Cloud](image)
How 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 231 vulnerabilities between March 2020 and March 2021.

How can we protect the SAP system from such attacks to avoid data exploits and a compromised system? Generic protection for threats like, e.g., SQL injections or Cross-Site Scripting is a Web Application Firewall (WAF).

Ranking – SAP Security Notes

12 months period

Managing SAP Security Notes

SAP system 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.
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 systems within SAP landscapes and 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.
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. FortiGate, combined with Fortinet's world-famous FortiGuard Labs delivers FortiGuard Threat Intelligence, validated industry-leading intrusion prevention system (IPS) technology. FortiGuard Labs employs hundreds of skilled security researchers supported by machine intelligence and AI, all relying on data from millions of sensors around the world to stay ahead of the latest threats.

Fortinet solutions 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 continually elevate the security posture.

Fortinet solutions for SAP include:

FortiGate Next Generation Firewall: Fortinet NGFWs enhance security and reduce cost and complexity by eliminating point products and consolidating industry-leading security capabilities such as secure sockets layer (SSL) inspection including the latest TLS1.3, web filtering, and intrusion prevention system (IPS) to provide full visibility and protect any edge.

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. FortiGate NGFWs provide SSL inspection to protect SAP.

**FortiWeb Web Application Firewall:** FortiWeb provides advanced security for your web applications and APIs from bot known and zero-day threats. Using an advanced multi-layered approach, FortiWeb utilizes artificial intelligence driven threat feeds and machine learning as well as feeds of known vulnerabilities and attacks such as the OWASP Top 10 to provide industry-leading protection to your applications. FortiWeb's multi-stage machine learning distinguishes between normal and abnormal application traffic, providing robust protection without requiring the time-consuming manual tuning required by other solutions. With ML, FortiWeb identifies anomalous behavior and, more importantly, distinguishes between malicious and benign anomalies. The solution also features powerful bot mitigation capabilities, allowing benign bots to connect (e.g. search engines) while blocking malicious bot activity.

**FortiADC:** To provide more advance SAP protection, an SAP connector can be created when configuring the FortiADC. The SAP connector pulls information from the SAP Message Server in real-time, with automated configuration gathering from SAP ICM configuration (HTTP/HTTPS Ports, virtual hosts). As soon as the FortiADC detects any changes with SAP application, it will update the configuration to match the new state. The FortiADC is an Enterprise-class layer 4-7 ADC that secures applications with a full-featured web application firewall. It provides DDoS application, web filtering, IPS, Geo-IP, and IP reputation for enhanced security. The FortiADC offers protection for SAP APIs (JSON, SOAP and XML) and content delivery optimization for web pages. Disaster recovery with global server load balancing provides organizations with additional functionality.

**FortiSandbox Cloud:** A cloud-based security tool that can analyze attached files and URLs for previously unknown threats. FortiSandbox utilizes AI and advanced Machine Learning (ML)-based analysis, as well as the MITRE ATT&CK framework and advanced threat feeds to detect threats both known and unknown.

**Speed matters for end-to-end encryption**

NSA labs have found that, on average, the following:

- **Performance hit for deep packet inspection is 60%**
- **Connection rates decrease by 92%**
- **Response times increased by 672%**

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

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

1. Physical FortiGate NGFWs proprietary hardware acceleration offloads encryption functions to a security processing unit boosting performance up to 20 times that of competitors.

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.
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.

<table>
<thead>
<tr>
<th>Security Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect dynamic edges where SAP systems may federate across these platforms.</td>
<td>Fortinet’s Security Fabric provides real-time threat intelligence shared across the entire SAP security boundary.</td>
</tr>
<tr>
<td>Multiple, continually evolving edges that require a single security context.</td>
<td>Network segmentation is implemented as micro-segmentation 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).</td>
</tr>
<tr>
<td>Lack of a single point of truth and management for policies that are deployed in the cloud.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>The SAP Web Dispatcher is limited in functionality and lacks Web Application Security features like OWASP Top 10 protection. It lacks content delivery optimization and API protection.</td>
<td>The SAP connector provides advance security features like native Web Application Firewall, SSL Services, Antivirus and SSL, DDoS protection, L7 scripting, and content delivery is optimized for web pages. It protects SAP APIs (JSON, SOAP &amp; XML). FortiADC can replace the expensive SAP Web Dispatcher.</td>
</tr>
</tbody>
</table>

FortiWeb web application firewall protects the SAP web dispatcher

SAP S/4 shifts much of SAP’s user interaction from the 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.
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 lifecycle automation framework.

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, landscapes and systems. This becomes especially difficult for migrations from traditional data centers to SAP 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.