SOLUTION BRIEF

Fortinet Secures SAP on Microsoft Azure

Executive Summary

The digital economy is disrupting every industry. Business leaders look to SAP to transform business processes using the latest technologies and intelligent automation. SAP enables organizations to adopt best practices while attaining operational excellence. As organizations upgrade their existing SAP system or convert to S/4HANA, many leverage Microsoft Azure for agility and scale on-demand.

Microsoft Azure is a cloud platform optimized for SAP workloads. The Embrace initiative deepens the Microsoft and SAP strategic partnership to help customers accelerate the migration of SAP ERP and SAP S/4HANA workloads to Azure. A focused SAP security practice is necessary to protect all the data generated by SAP. Fortinet utilizes a holistic approach to secure the entire SAP landscape. By leveraging its extensive threat intelligence, a comprehensive portfolio, and state-of-the-art artificial intelligence (AI)/machine learning (ML) security, Fortinet strengthens an organization's SAP security posture.

Microsoft Azure Delivers SAP Cloud Services and Challenges

Organizations deploying SAP workloads on Azure want to take advantage of the public cloud benefits without compromising security. Microsoft Azure supports various security solutions and technologies to protect applications and data in the cloud. But Azure does not provide complete, enterprise-class protection across the SAP ecosystem.

Secure SAP With Holistic Coverage

Azure customers gain the confidence to deploy SAP while maintaining a consistent operational model and managing risks using Fortinet to secure the Intelligent Enterprise running SAP. The Fortinet security solution for SAP centralizes and automates security controls and analytics—making it easier to manage, respond, and automate the SecOps capabilities.

Focused SAP security practice

A consistent security framework protects all SAP workloads. Fortinet applies AI for faster threat prevention, detection, and response. It protects all SAP data generated by edge devices, endpoint systems, users, applications, databases, third-party systems on Azure, on-premises or across multi-cloud environments.

Protecting SAP landscapes is top of mind

Threat actors target SAP systems. With cybercrime expected to cost $10.5 Trillion by 2025 and SAP security updates unable to provide sufficient protection, protected SAP is crucial.[1]

Fortinet protects SAP workloads on Azure

- FortiGate adds Application Control, Intrusion Prevention and segmentation
- FortiADC protects SAP web applications and SAP APIs from malicious web attacks
- FortiWeb WAF protects the SAP Web Dispatcher and adds ML and AI to increase security of SAP landscapes

Support for older versions of SAP

SAP ECC, SAP NetWeaver, SAP Business Suite, ERP, CRM, SCM, Solution Manager and SRM.

Accelerate SAP deployments

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

Enterprisewide security

Hybrid cloud footprints bring additional complexity and increase the level of effort to manage an extended security domain. Such complexity is resolved through the Fortinet single-pane-of-glass and consistent operating system approach to managing infrastructure, regardless of where and on what platform it is deployed. Provide consolidated security, visibility, and analytics with Fortinet to centralize operations across complex computing landscapes such as SAP.

74% of companies are moving apps back and forth between the cloud and on-premises—thus, consistent security across clouds and data centers is critical for ensuring SAP workloads are protected.[2]

Built-in intelligent technologies

Combat modern threats using AI, ML, and advanced analytics with Fortinet to expedite threat prevention, detection, and response.

Public cloud deployment flexibility

Organizations are using multiple cloud providers to use best-in-class cloud services, and to avoid vendor lock-in. Using a multi-cloud approach protects organizations from potential constraints or substantial costs if they switch cloud providers. 74% of companies are moving apps back and forth between the cloud and on-premises—thus, consistent security across clouds and data centers is critical for ensuring SAP workloads are protected.

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. The Fortinet Security Fabric protects all SAP-generated data across multiple locations and regions and extends security policies from on-premises to the cloud.

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

- Zero Trust Access
- Security-Driven Networking
- Adaptive Cloud Security
- FortiGuard Threat Intelligence
- Fabric Management Center—SOC
- Fabric Management Center—NOC
- Open Ecosystem

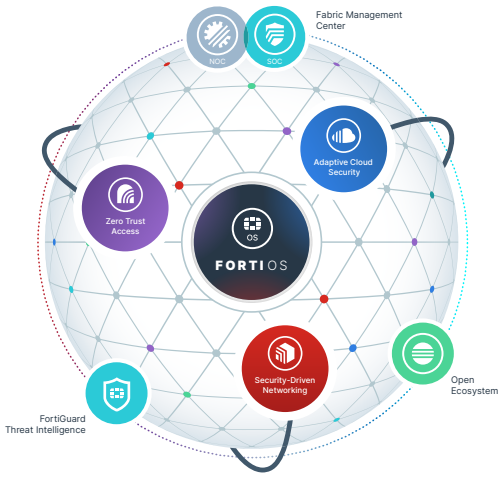

Figure 1: Fortinet Security Fabric diagram.

Fortinet Ensures SAP Workloads Running on Azure Are Protected

The Fortinet Security Fabric was designed to complement Microsoft Azure security solutions. Fortinet solutions not only run seamlessly in Azure but they also integrate with Azure security services, including Azure Sentinel and the Azure Security Center, to provide transparency of security policies and events across the cloud infrastructure. Further, Fortinet's native integration with Microsoft Azure enables seamless, automated, and centralized management across all clouds to support SAP deployments that span cloud environments.

How FortiADC provides advanced services for SAP

FortiADC is an advanced application delivery controller that enhances SAP applications' security, scalability, and performance. **FortiADC** provides WAF, intrusion prevention system (IPS), SSLi, link load balancing, and user authentication in one solution, whether SAP applications are hosted 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.

Advance 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.

Fortinet Use Cases for SAP

Segment SAP workloads with low latency

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

Fortinet Reference Architecture for SAP S/4HANA

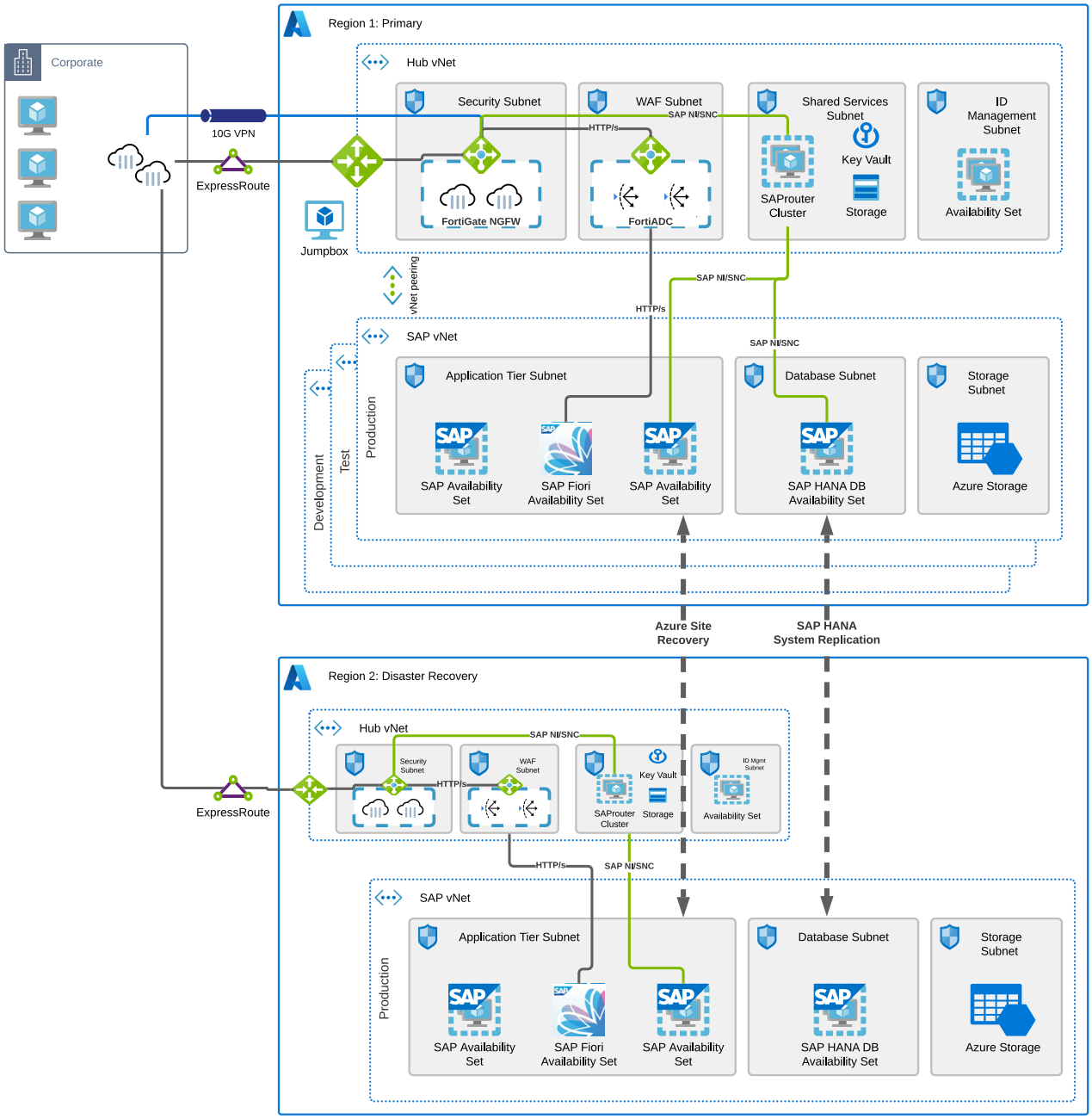

Figure 2: Fortinet reference architecture for SAP S/4HANA on Microsoft Azure.

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

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

Physical **FortiGate next-generation firewalls (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

The **FortiWeb web application firewall (WAF)** is a dedicated HTTP(s) protection platform that not only protects against Open Web Application Security Project (OWASP) threats but also provides virtual patching and auto tuning, and uses AI and ML to detect threats faster.

Evaluate SAP compliance

FortiCWP assesses cloud configuration security posture, detects potential threats originating from misconfiguration of cloud resources, monitors user behaviors and cloud network traffic, and provides comprehensive compliance reports and alerts.

Protects web applications

FortiWeb Cloud WAFaaS natively integrates into Azure to protect your hosted web applications without deploying and managing infrastructure.

Conclusion

Protecting SAP's business-critical infrastructure and systems becomes especially difficult for migrations from traditional data centers to S/4HANA running on Microsoft Azure, creating the opportunity for blind spots in the security posture. SAP systems are protected with Fortinet's holistic coverage that ensures 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.

[1] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime magazine, November 13, 2020.

[2] "The Bi-Directional Cloud Highway: Critical Insights into Today's Cloud Infrastructures," Fortinet Industry Trends, August 13, 2019.

December 14, 2021 1:06 PM
1014914-0-0-EN