SOLUTION BRIEF

Step Up Your Security on Microsoft Azure with Fortinet

Executive summary

Security today requires consistent tools and policies across data centers, branch offices, and clouds. The goal is to attain uniform policy enforcement, visibility, and orchestration wherever the compute occurs. The average security stack, which includes multiple, disparate tools, can lead to operational silos and security gaps that prevent organizations from achieving this goal.

Organizations must realize the importance of converging and uniting security, network, and computing practices. An integrated suite of security products that provides protection, no matter where their applications and data live, is the answer.

The organizations that power the world run on Microsoft Azure and protect their clouds and data centers with Fortinet's enterprise-class security solutions. Because of the extensive partnership between Microsoft and Fortinet, Azure customers of any size can leverage jointly engineered solutions to migrate to– and grow in–the cloud with confidence.

Understanding the security challenges of cloud adoption

Moving to the cloud has many benefits, from the possibility of creating new revenue streams to a shortened time to market. But cloud migrations also raise particular security considerations. According to the Fortinet 2023 Cloud Security Report[1], ninety-five percent of enterprises reported being "very" to "highly" concerned about cloud security. Several variables contribute to this feeling, including:

- Attack surfaces expand as organizations grow
- Increased complexity from hybrid and multi-cloud deployments
- Lack of visibility due to fragmented security solutions
- Ever-increasing number of networks, devices, and applications with remote work
- Shortage of skilled security professionals to tackle a rapidly evolving threat landscape

Fortinet offers trailblazing protection for Azure

Backed by the continuous research of FortiGuard Labs, the Fortinet Security Fabric is essential to reducing complexity and increasing overall security effectiveness across today's expanding networks. Azure customers can leverage solutions from Fortinet and Microsoft that are designed to work together to achieve comprehensive visibility and multi-layered security.

Why Fortinet

More than 100 integrations between Fortinet and Microsoft.

Recognized as winner of the Microsoft Partner of the Year Award.

A Leader in the 2022 Gartner Magic quadrant for Network Firewalls, SD-WAN, SIEM, and Enterprise Wired and Wireless LAN Infrastructure.

Microsoft has been a Fortinet Fabric Ready Partner since 2017

[1] 2023 Fortinet Cloud Security Report

Managing different Azure security use cases with Fortinet

Use case #1
Safely migrate and build on Azure

Whether you are a Fortinet customer migrating applications to Azure, or an Azure user seeking superior protection for your environment, pairing Fortinet and Microsoft is an effective joint approach for securing your cloud deployments. Fortinet protects Azure-based applications and workloads with solutions for network, cloud platform, and application defense. Fortinet offers a superior set of security solutions that are natively integrated into the Azure infrastructure and available on the Microsoft Commercial Marketplace. Better still, Fortinet's security solutions are all part of a security fabric that extends across clouds and data centers.

The Fortinet Security Fabric is backed by FortiGuard Labs, which gathers and analyzes over 14 billion security events per day. Utilizing artificial intelligence and machine learning, it continuously improves threat intelligence in real-time. The Fortinet Security Fabric uses this data to identify and defend against the latest threats.

- Fortinet solutions integrate with numerous Azure services, including Azure Sentinel, Azure Active Directory, Azure Security Center, Microsoft Defender for Cloud, Azure Cloud Functions, Azure Application Gateway, and more.
- FortiGate Next-Generation Firewall (NGFW) for Azure secures native, hybrid, and multi-cloud environments. FortiGate NGFW can recognize and understand unique applications and make relevant security decisions around proprietary traffic, detect botnets, and segment traffic.
- FortiWeb web application firewall (WAF) protects business-critical web applications and their APIs from attacks. Advanced ML-powered features improve security and reduce administrative overhead.
- Integration with Azure Virtual Machine facilitates scale-up and scale-out security.

Use case #2
Defend web applications and their APIs built on Azure

According to Verizon's 2022 Data Breach Investigation Report, web applications are the top action vector in security incidents, and in 42 percent of breaches.[2] FortiWeb Cloud can protect all of an organization's web applications and APIs in one solution that is simple to deploy and easy to manage. With FortiWeb Cloud, organizations benefit from enterprise-level features while saving time and budget. FortiWeb Cloud delivers advanced visual analytics and machine learning capabilities to defend against such threats as the OWASP Top 10 and zero-day attacks. It goes beyond traditional WAFs to offer advanced features, including:

- API discovery and protection to enable B2B communications and support your mobile applications.
- Bot management to take action on malicious bots, while welcoming good bots, with automated identification and mitigation.
- Threat analytics to reduce alert fatigue and ensure analysts can quickly focus on the most important threats.
- The latest threat intelligence with signature updates and analytics from FortiGuard Labs.

[2] 2022 Data Breach Investigations Report | Verizon

Use case #3

Build a global SD-WAN with Azure Virtual WAN integration

Azure Virtual WAN is a networking service that allows customers to leverage the Azure network backbone so they can build high-speed global transit network architectures. Fortinet FortiGate Secure SD-WAN for Microsoft Azure vWAN can be deployed directly into the Microsoft WAN hub, securing both north/south and east/west traffic and allowing organizations to utilize Microsoft Azure as a global backbone for their secure SD-WAN deployments.

This solution deploys a set of FortiGate NGFWs as a managed application in Azure vWAN to support a secure SD-WAN with layer 4-7 inspection. Fortinet Secure SD-WAN delivers enterprise-class security and branch networking between Azure VNETs, the internet, and corporate branches or datacenters. Organizations can easily integrate SD-WAN and NGFW into all traffic flows, and enforce layer 4-7 inspection and control powered by FortiGuard Labs. Cost-effective and offering fast connectivity, FortiGate for Azure vWAN delivers operational efficiencies through automation, deep analytics, and self-healing.

- Deploy the FortiGate NGFW within vWAN to secure intra-cloud connectivity, as well as-site-to site, remote user and private connectivity.
- Centralize control with FortiManager, which offers a single pane of glass view that reduces vulnerabilities from configuration errors.
- Remain compliant with FortiAnalyzer, which simplifies compliance management and reporting with customizable regulatory templates, audit logging, and role-based access control, eliminating the need for many manual processes related to auditing.

Use case #4

Improve protections for Microsoft Windows on Azure Virtual Desktops

A complete desktop and app virtualization solution, Windows Virtual Desktop (WVD) runs in the cloud. In order to facilitate remote work, more companies are turning to WVD. However, these installations need sophisticated routing and security in order to connect to data centers, branches, and client-to-site access to Azure services. By offering network inspection across all of these footprints with virtual private network (VPN) linkages from the endpoint into the cloud, FortiGate includes the ability to enforce advanced security policies such as zero trust and data leak prevention.

- FortiGate NGFW adds to the core capabilities of Azure by providing network inspection across data centers, branches, and client-to-site access to Azure resources via virtual private network (VPN). It interconnects from the endpoint, through the premise, and into the cloud.
- FortiGate's deep packet inspection capabilities, along with SSLi for inspecting encrypted traffic, ensure network security.
- FortiGate's support for secure SD-WAN allows for secure connectivity among branches and virtual desktops.
- FortiGate is ideal for enforcing zero trust policies, promoting rigorous validation before remote users and devices access their Microsoft environment.

Use case #5
Protect SAP S/4HANA migrations

As organizations upgrade their existing SAP system or convert to S/4HANA, many leverage Microsoft Azure, which is optimized for SAP workloads. Fortinet utilizes a holistic approach to secure the entire SAP landscape, including Azure:

- Fortinet's SAP connectors may communicate with a variety of SAP components to automatically safeguard newly launched instances, share data with SAP Enterprise Threat Detector, or automatically detect and secure SAP traffic even when unexpectedly new ports are utilized.
- Fortinet solutions for SAP can secure SAP landscapes whether they are on-premises or in the cloud, allowing organizations to have a single, consistent set of security policies and tools wherever the compute occurs.
- Fortinet's close relationship with Microsoft and SAP, including participating on Microsoft's SAP Advisory board, has enabled Fortinet to engineer security solutions for SAP on Azure that provide best of breed security.

In collaboration with Microsoft, Fortinet has developed several solutions for SAP including:

- Network Security for SAP Enterprise Landscapes
- Application Security to secure SAP Solutions
- Enhance SAP Identity Management with Zero Trust Access
- Equip SAP Security Operations Centers
- Secure RISE with SAP

Seek a security partner, not a product

Making a decision in cloud security should focus on seeking the best global security partner, not on tactical decisions about products.

Fortinet, a leading security provider and the worldwide leader of unified threat management solutions, keeps your workloads and applications safe on Microsoft Azure. Powered by comprehensive threat intelligence and more than 20 years of cybersecurity innovation and experience, the broad suite of Fortinet solutions protects any application on Azure.

To learn how to gain the most advanced protection on Azure, visit:
www.fortinet.com/azure

FORTINET®

www.fortinet.com