Strengthen Your Security Shield with Fortinet and Azure

Table of Contents

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 some particular security issues. One is that an organization's attack surface expands as it increases. 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:

Increased complexity

More than half of businesses currently have hybrid or multi-cloud deployments. This may result in increased security barriers for data transit, compliance initiatives, and inconsistent solutions (native to one cloud provider but not the other, or a solution that is not on-premises friendly).

Shortage of skilled security professionals

Tightened security is hindered by the lack of highly specialized security workers. Globally, there is a need for more than three to four million security professionals, an increase of over 26 percent from 2021. There is a greater need than ever for cybersecurity due to an evolving threat landscape with attacks that are more challenging to identify and defend against.[2] Because of this shortage, only 28 percent of organizations indicated they thought they could defend against a targeted attack in a day or less; 41 percent said they thought they could in a week or less.[1]

Lack of visibility

Early strategies for cloud security often involved deploying an excessive number of different security solutions for various aspects of architecture, resulting in expensive overlap, a fragmented security posture, and security blind spots. Exacerbating the issue, a shortage of qualified security personnel makes it nearly impossible to handle the more than 30 security systems that many organizations ended up with.

App-centric remote and hybrid work

Businesses need to manage and defend an ever-increasing number of networks, devices, and applications. The transition to remote work has increased the demand for more complex solutions that take advantage of scale-enabling technology like AI/ML. Additionally, it necessitates more meticulous control across departments. For instance, configuration management and API calls between engineering and IT must be scrutinized more closely.

Unifying Security Is Key

Security today requires consistent, unified security operations across diverse networks, multiple environments, on-premises data centers, and multiple or hybrid clouds. The goal is to achieve uniform policy enforcement, transparency, and unified orchestration. Multiple, disparate tools can lead to operational silos and security gaps and should be avoided.

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

1. "2023 Fortinet Cloud Security Report"
2. "The cybersecurity talent shortage: The outlook for 2023." Poremba, S. January 5, 2023. Industry Drive.

Fortinet Delivers a Specialized Approach to Cybersecurity on Azure

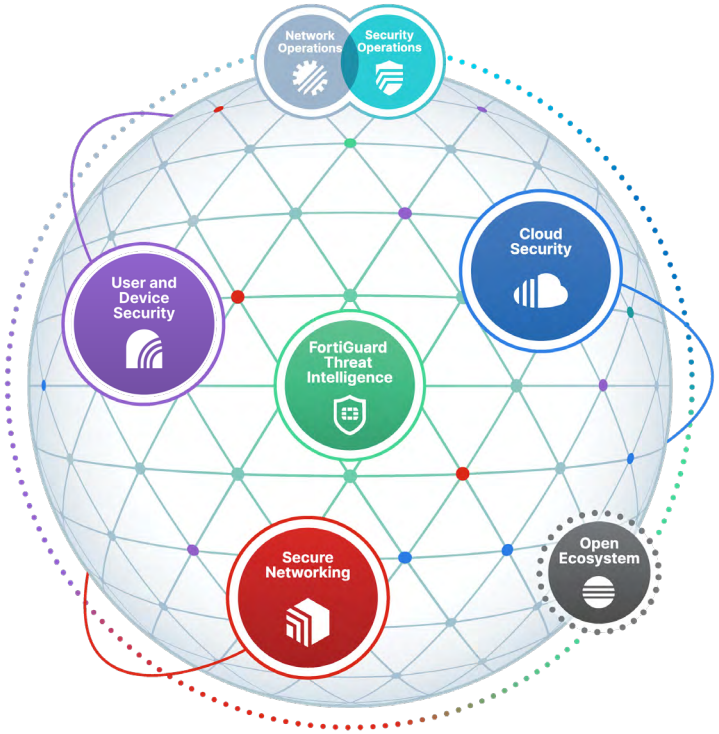
You can protect your organization's cloud workloads and data centers on Microsoft Azure with the Fortinet Security Fabric, which exemplifies Gartner's Cybersecurity Mesh Architecture. Gartner defines a cybersecurity mesh as a collaborative ecosystem of tools and controls to secure a modern, distributed enterprise. Their mesh approach promotes interoperability between distinct security products to achieve a more consolidated security posture and work as a collaborative ecosystem. According to Gartner, businesses that implement cybersecurity mesh architecture by 2024 will see an average of 90 percent reduction in the cost of individual security incidents.[2]

Using joint solutions engineered by Fortinet and Microsoft, and backed by the continuous research of FortiGuard Labs, Azure customers can achieve comprehensive visibility and multi-layered security to stay ahead of emerging threats. The extensive partnership between Microsoft and Fortinet allows businesses of any size to migrate to and grow in the cloud with confidence. Fortinet's robust network, application, and platform security, combined with a commitment to a Zero Trust, provides broad protection, native integration, and automated management.

The Fortinet Security Fabric is essential to reducing complexity and increasing overall security effectiveness across today's expanding networks. New and increasingly complex trends, like work-from-anywhere, are the perfect use cases for a unified security mesh architecture like the Fortinet Security Fabric. Its benefits include deep visibility across all edges, centrally managed distributed solutions, consistent enforcement of policies, and more. It also integrates and interoperates with more than 450 third-party technology partners as part of the Fortinet Security Fabric open ecosystem.

Fortinet also offers consulting services comprised of cloud-agnostic security experts who work with organizations that have hybrid and multi-cloud deployments to get the maximum ROI out of their Azure investments.

Fortinet Security Fabric



2. "The cybersecurity talent shortage: The outlook for 2023." Poremba, S. January 5, 2023. Industry Drive.

Fortinet and Azure Collaborate to Offer Trailblazing Protection

An increasing number of businesses are using Microsoft Azure to supplement their own data centers and benefit from the agility of the public cloud. Organizations turning to Azure want to take advantage of the public cloud benefits without compromising security. While Microsoft secures the Azure infrastructure and isolates the tenants, customers are responsible for ensuring that their workloads and data are secure. Fortinet provides Azure users the confidence to deploy any application in the cloud while maintaining a consistent operational model and managing risks. Fortinet's leadership in network and application security compliments Microsoft identity and endpoint security solutions while helping Azure users connect and protect their cloud workloads.

Fortinet and Microsoft Azure systems communicate with each other; sharing security data and enabling automated updates, bringing superior protection through native integrations, and providing more efficient cloud spending.

More than 100 native integrations between Fortinet and Microsoft provide customers with a strengthened overall security posture. And, Microsoft has been a Fortinet Fabric Ready Partner since 2017.

Users of Microsoft Azure benefit from Fortinet Security Fabric's extensive protection, comprehensive integrations, and automated management. This allows for consistent enforcement and visibility throughout a customer's multi-cloud infrastructure. To secure applications, stop zero-day threats, and manage global security infrastructures from the cloud, the Fortinet Security Fabric offers robust multi-layer security protection. For example, FortiWeb Cloud WAF-as-a-Service (WAFaas) integrates with Azure to protect hosted web applications and APIs without deploying and managing infrastructure.

Finally, deploying Fortinet solutions helps customers meet their Microsoft Azure Consumption Commitment (MACC) for transactable offers that are published on the Azure Marketplace.

Enable Consistent Security and User Experience, Regardless of Location

The Fortinet Security Fabric works with Microsoft security tools, such as Microsoft Sentinel, to provide an intelligent architecture that integrates discrete security solutions into a cybersecurity mesh. This mesh is able to accelerate detecting, monitoring, blocking, and remediating attacks across the entire attack surface. The security fabric delivers more than just visibility into security status of every environment, be it on-prem or cloud-based. Let's take network security as an example.

- The physical topology view shows all connected devices, including access layer devices. The logical topology view shows information about the interfaces that each device is connected to. As a result, organizations do not have to monitor multiple disparate screens and solutions to identify possible issues, and this saves time.
- An application delivery controller or a firewall in one location might detect an attack in layer 7 traffic. It will not only block the attack, but can automatically update security policies on other firewalls, ADCs, and endpoints so they can block traffic from the attacking domain.

Azure services offer the latest autoscaling functionality, load balancing, and traffic management. However, Fortinet extends automation to security, allowing threats detected by one security service to automatically change security policies across your security fabric to limit breaches and remediate vulnerabilities.

Fortinet provides the same level of protection for Azure as it does for on-premises environments. You can secure your Azure workloads with Fortinet using the same tools you use to secure your workloads in other clouds and across branches and data centers. The automated configuration and change management offered by Fortinet lightens the workload of your security team and expedites the handling of security issues.

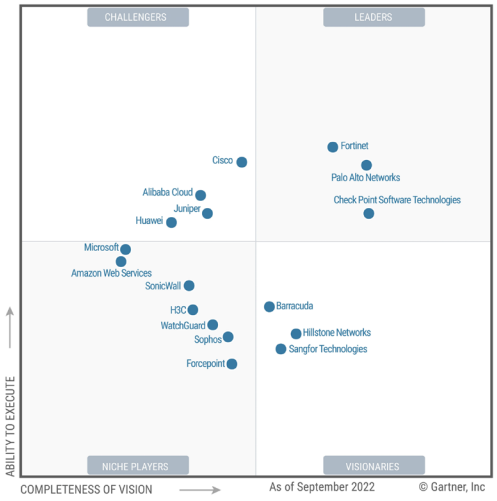
As business demands evolve, Fortinet offers capabilities for automated security solution deployment and scaling. Programmatic delivery of automation enables businesses to incorporate security services with DevOps procedures.

The Fortinet market position and solution effectiveness have been validated by industry analysts, independent testing labs, business organizations and media outlets worldwide. Fortinet counts the majority of Fortune 500 companies among its customers.

Fortinet shines as leader in network firewalls

In the 2022 Gartner® Magic Quadrant™ for Network Firewalls, FortiGate NGFW is recognized as a leader for the 13th time.

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (December 2022)

Managing Different Use Cases with Fortinet

Safely Migrate and Build on Azure

Combining Fortinet security solutions with Microsoft cloud services is an effective strategy for increasing an organization's agility while maximizing security.

Fortinet protects Azure-based applications and data with solutions such as FortiGate-VM NGFW for cloud platform security, and FortiWeb for web application and API protection (available as a VM, a container, and as a SaaS running in Azure). Fortinet is a leading provider in offering customers such a broad array of integrated core cloud security products. Furthermore, Fortinet offers a superior set of security solutions that are natively integrated into the Azure infrastructure and available on the Microsoft Commercial Marketplace. Products are available as pay as you go (PAYG), through Private Offers, and bring your own license (BYOL) procurement.

In addition, FortiGuard Labs gathers and analyzes over 14 billion security events per day, continuously improving threat intelligence in real-time. The Fortinet Security Fabric uses this data to dismantle silos and implement uniform security rules on Azure. Fortinet integrations with Azure Sentinel and Azure Security Center ensure that all security events, whatever cloud or datacenter they occur in, are tracked and analyzed.

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. The Embrace Initiative deepens the Microsoft and SAP strategic partnership to help customers accelerate the migration of SAP workloads to Azure. 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.

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 incidents, and in 42 percent of breaches.[4] 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

4. 2022 Data Breach Investigations Report | Verizon

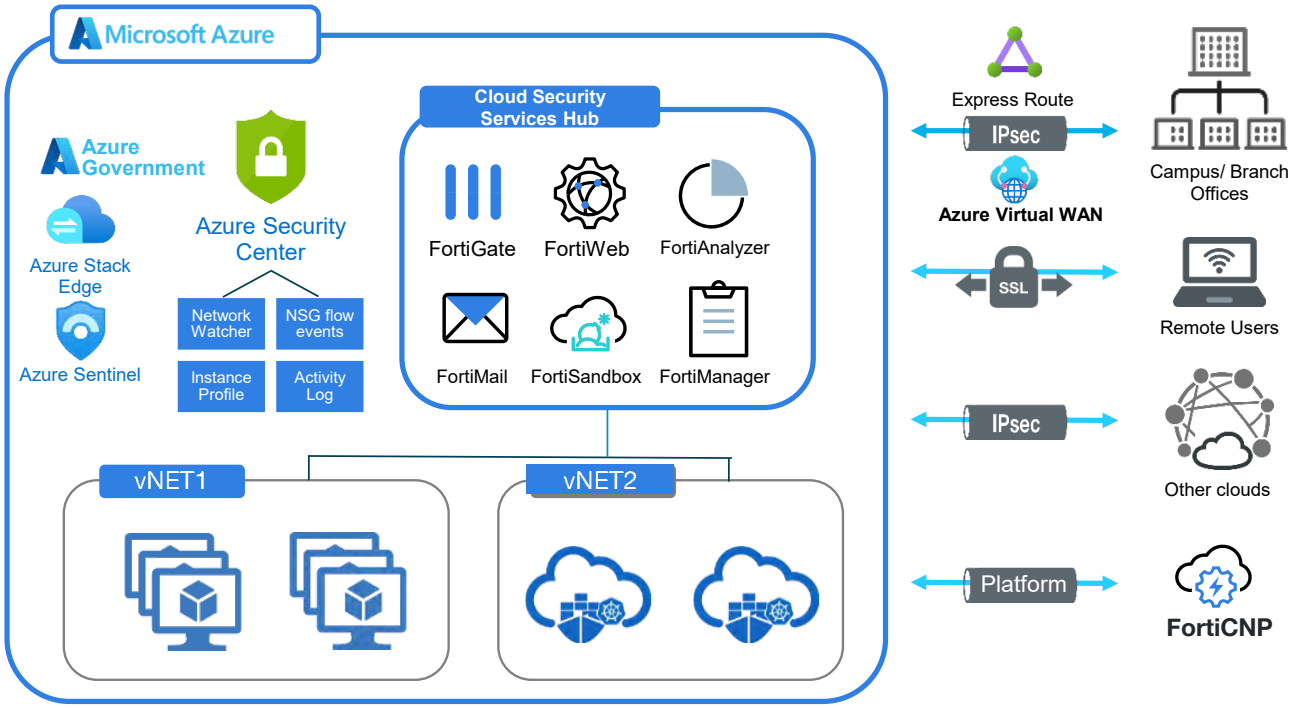
FortiGate Secure SD-WAN with Firewall in Virtual WAN Hub

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 data centers. License requirements, cumulative performance, and Azure pricing depend on scale selection. 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.

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.



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. In fact, Fortinet has been recognized by Microsoft as Partner of the Year for the past four years, including 2023.

Fortinet has also been named a Leader in each of the 2022 Gartner® Magic Quadrant™ for:

- Network Firewalls
- SD-WAN
- Security Information and Event Management (SIEM)
- Enterprise Wired and Wireless LAN Infrastructure

To learn how to gain the most advanced protection on Azure while drawing down your MACC, visit: fortinet.com/azure

April 2023