FORTINET

Best Practices for Securing Your Azure Environment with Fortinet

Table of Contents

Get Multi-layered Security in Microsoft Azure

Executive Overview

As organizations look for ways to increase efficiency, cost-savings, and flexibility, many are deciding to increase utilization of cloud services. According to Gartner, worldwide end-user spending on public cloud services is forecast to grow 40.6% in 2022 to total $362.2 billion, up from $257.5 billion in 2020. For many organizations, a significant portion of their business depends on cloud storage, communications, or infrastructure. Therefore, protecting your systems and assets in the cloud should be a priority.

More and more enterprises are turning to Microsoft Azure to extend internal data centers and take advantage of the agility of the public cloud. While Azure is responsible for securing the infrastructure, the responsibility falls on the organization to protect everything that they put in it. The Fortinet Security Fabric provides Azure and Office 365 users broad protection, native integration, and automated management. This enables customers with consistent enforcement and visibility across their hybrid and multi-cloud infrastructure.

Fortinet provides customers with a broad array of security solutions to protect Azure-based resources and workloads. Fortinet solutions are tightly integrated through the Fortinet Security Fabric and are designed to help customers maintain a consistent security posture across applications, clouds, and data centers. Fortinet protects Azure-based applications with solutions such as FortiGate Next-generation Firewalls (NGFWs).

In this eBook, find out how your business can connect to the cloud, protect cloud applications, and deliver security from the cloud with Fortinet.

Security Challenges in the Cloud

Digital transformation offers tremendous opportunities for businesses to create value and realize efficiencies. However, it also creates new security risks. As cloud migrations accelerate, organizations will need to utilize new techniques to secure this digital transformation.

Expanded Attack Surface

As organizations adopt new technologies to stay competitive and ensure business continuity, their attack surface expands, opening the door for cybercriminals to exploit network environments. With a range of modern management, orchestration, and DevOps environments and tools available, it is easier than ever to adopt a more agile approach to better secure this extended attack surface.

Dealing with Hybrid and Multi-cloud Environments

Many organizations have application and development teams with different needs and priorities, creating a demand to be able to work in different clouds. In fact, according to the Flexera 2022 State of the Cloud Report, "89 percent of enterprises have a multi-cloud strategy" while "80 percent have a hybrid cloud strategy." While different teams may be using different clouds, the security team needs to have one consistent approach to security.

Added Complexity

Along with the expanded attack surface and the challenges of hybrid and multi-cloud, one of the factors behind complexity is a proliferation of isolated "point" security products. With multiple disparate security products and solutions, it can be challenging to maintain visibility and meet compliance requirements.

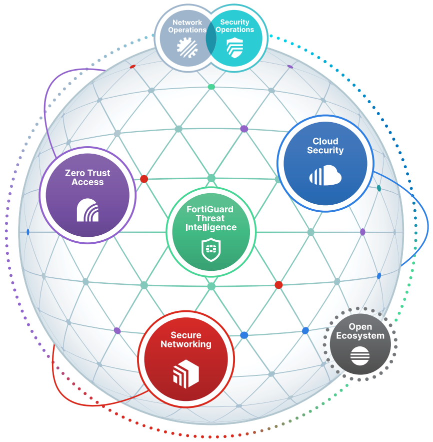
As organizations seek ways to reduce this operational complexity, they must select and integrate security tools that work across clouds and data centers.

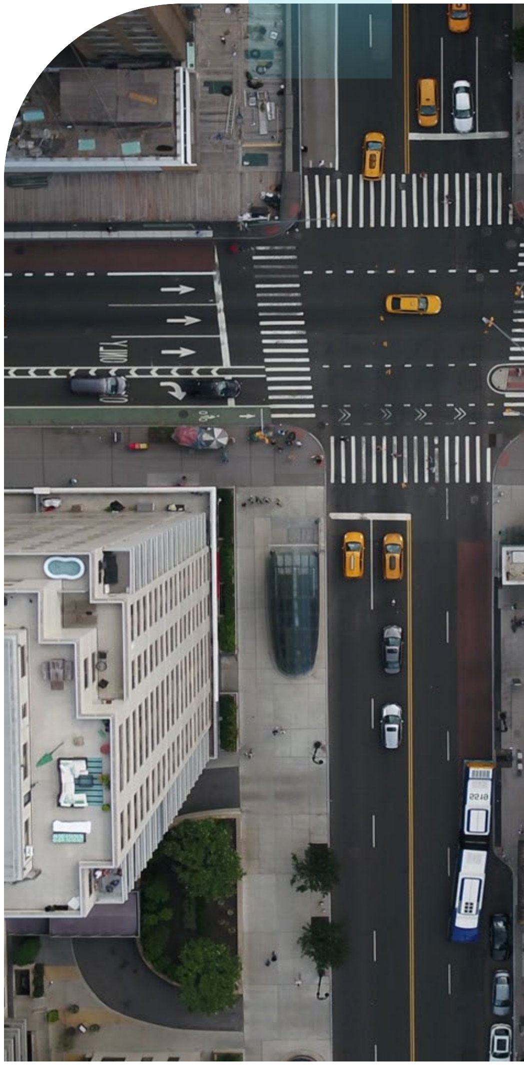
Get Unmatched Security in the Cloud

Making Possible a Digital World You Can Always Trust

As your organization evaluates security solutions for Microsoft Azure, look no further than Fortinet. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface. With more than 20 years of experience in security, Fortinet is one of the world's top cybersecurity brands, delivering broad, integrated, and automated protection to empower organizations to securely accelerate their digital journey.

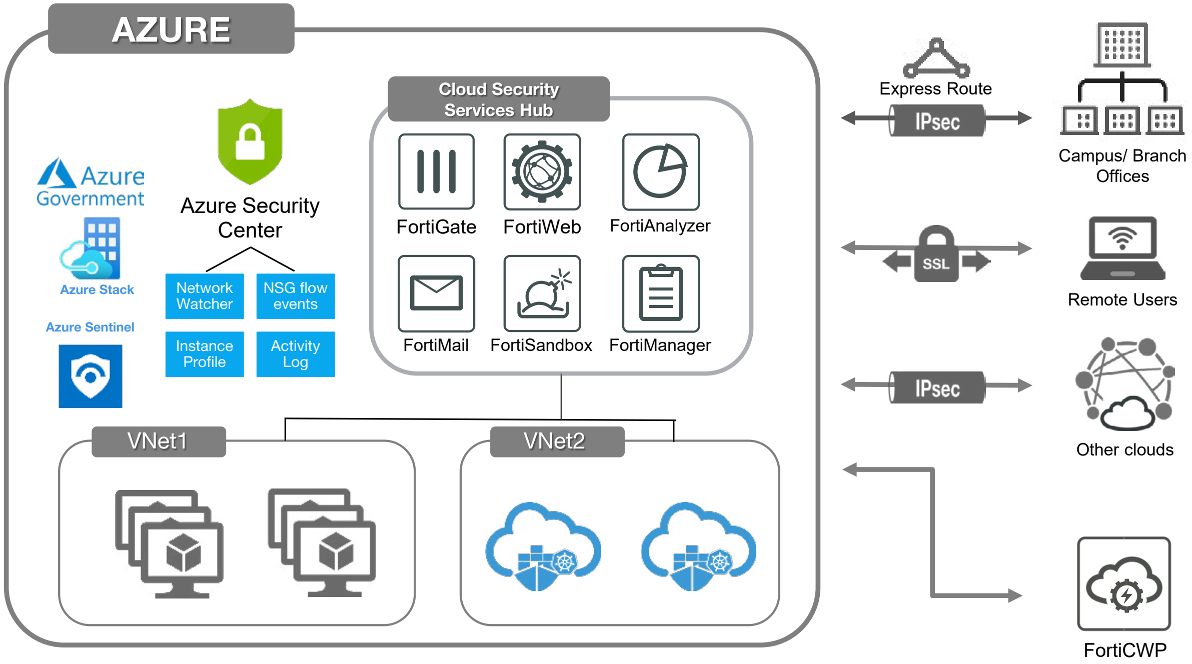
The Fortinet Security Fabric is at the heart of Fortinet's security innovation. It is a platform organically built from the ground up around a common operating system and management framework to enable seamless interoperability, full visibility, and granular control across the entire infrastructure. The platform is augmented with FortiGuard Labs actionable threat intelligence, which facilitates greater efficiencies in threat detection and response, simplifies management, and reduces overall complexity. The Fortinet FortiGuard Labs team collects and processes over 14 billion security events per day using a broad team of cybersecurity researchers and an advanced AI system designed to identify and track down new threats. This actionable threat intelligence is fed to the millions of deployed Fortinet solutions to keep them apprised of, and prepared to detect and defend against the latest threats.





Broad Protection with Fortinet on Azure

Fortinet's broad portfolio of top-rated solutions includes FortiGate NGFW, FortiWeb Web Application and API Protection, FortiAnalyzer for analytics and automation, FortiManager for automation-driven network management, and more–to deliver a simplified, end-to-end security infrastructure.



Achieve Advanced Threat Protection on Azure with FortiGate Next-generation Firewall

Protect against cyber threats with high performance, security efficacy, and deep visibility. FortiGate NGFW on Microsoft Azure provides your business with deep security into the cloud, in the cloud, and across clouds.

As the attack surface expands, FortiGate provides broad, integrated, and automated protection against emerging and sophisticated threats. FortiGate also delivers security for hybrid and multi-cloud environments, including advanced security for Azure Stack and Stack Edge.

Fortinet provides a centralized management solution with a single-pane-of-glass view that improves visibility and reduces complexity across product lines, clouds, and data centers or on-prem. It also streamlines operations for limited or under-resourced administrators and security staff.

Leveraging one security solution that works across your cloud and on-prem deployments, reduces your training needs, and ensures that IT compliance is deployed consistently across environments.

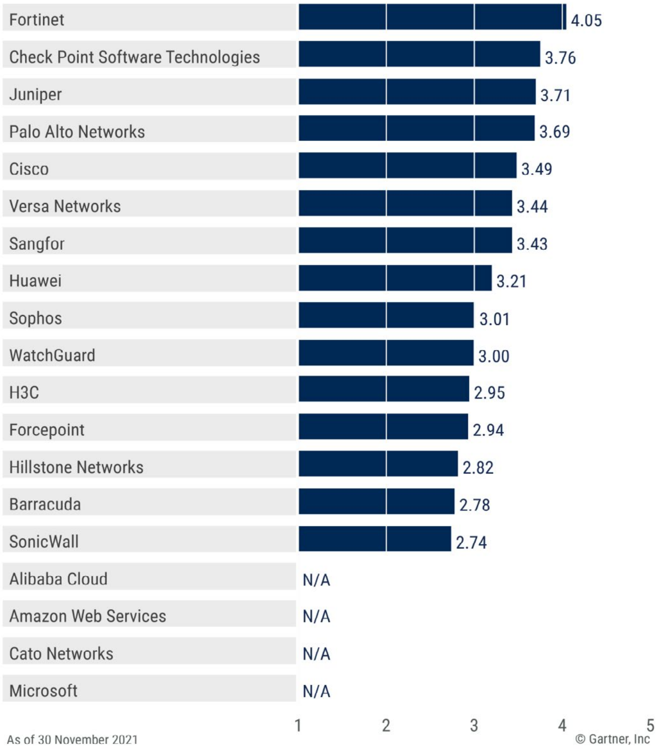
Into the Cloud
Accelerate cloud on-ramps with high-speed secure connections, protect your geographically dispersed assets, and deliver business-critical services.

In the Cloud
Gain complete content and network protection in Azure by combining stateful inspection with powerful security features.

Across Clouds
Simplify multi-cloud security with secure connectivity, network segmentation, and application security for hybrid cloud-based deployments.

2022 Gartner Critical Capabilities for Network Firewalls

Product or Service Scores for Enterprise Data Center



Source: Gartner (January 2022)

“Strong Firewall Solution That Protects Your Business Systems”
– Programmer in the Finance Industry

Gartner
Peer Insights
Customers’
Choice 2022™

Fortinet is proud to be named a Gartner Peer Insights Customers’ Choice in several critical areas:

- Network Firewalls
(Named a 3rd time)
- WAN Edge Infrastructure
(Named a 3rd time)
- Wired and Wireless LAN Access Infrastructure
(Named a 3rd time)

Key FortiGate Use Cases for Azure

FortiGate on Microsoft Azure delivers advanced threat protection capabilities for organizations of all sizes, with the flexibility to be deployed as a next-generation firewall and/or VPN gateway. FortiGate enables a broad set of tried, tested, and carefully engineered solutions for Microsoft Azure.

Azure Virtual WAN integration

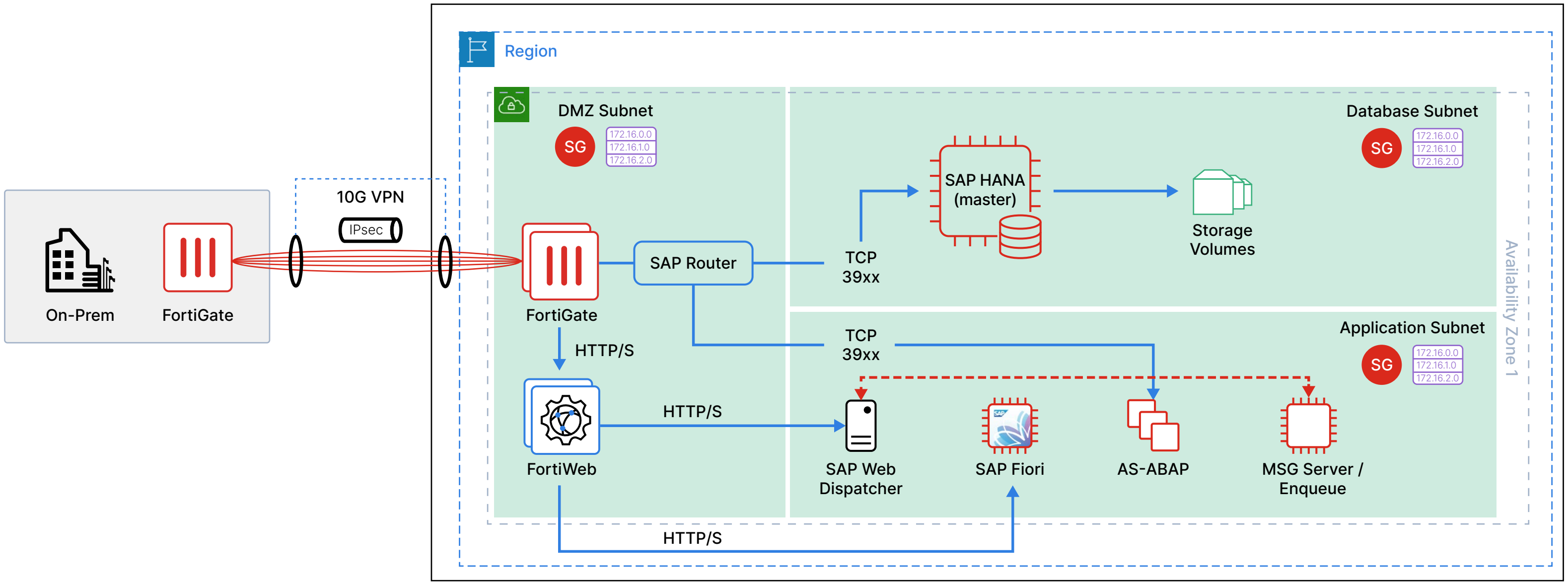
Fortinet Secure SD-WAN for Azure Virtual WAN gives organizations the best combination of automated set-up, ease of use, security, and visibility across their distributed infrastructure. FortiGate NGFW Secure SD-WAN provides an ideal branch and corporate connectivity solution for customers looking to secure and optimize their cloud on-ramp requirements. Fortinet solutions can be used for a direct branch connection to Azure Virtual WAN connectivity, branch to branch connectivity, dynamic path selection, and application-specific path selection.

Windows Virtual Desktop (WVD)

Windows Virtual Desktop is a comprehensive desktop and app virtualization service running in the cloud. Azure customers can deploy WVD within Azure virtual networks (VNets). Typically, these deployments require advanced routing and security for connecting to data centers, branches, and for client-to-site access to Azure resources. FortiGate adds to Azure's core capabilities by providing network inspection across all of these footprints with virtual private network (VPN) interconnections from endpoint into the cloud.

SAP

Used for managing finance, employees, customers, manufacturing and more, SAP systems are the perfect example of the mission-critical applications that must be protected. Fortinet worked with SAP to design reference architectures for securing SAP systems from both internal and external threats. Fortinet solutions for SAP identify vulnerabilities, protect data at rest and secure applications from attack, and provide visibility into organizations' enterprise security posture. Fortinet reference architectures for securing SAP have been carefully tested to provide security you can trust without impacting system performance.



SHIPSERV

Customer Case Study

ShipServ Uses Fortinet Security Tools to Assist Its Move to the Cloud

ShipServ provides the world's largest procurement platform for the marine industry, helping marine buyers easily find suppliers, trade efficiently, and build relationships with those trading partners. Safeguarding customer data is a business-critical imperative for ShipServ.

The ShipServ team launched a project to determine the readiness of the company's infrastructure to support their growth objectives and the roll out of a suite of new innovative products.

After evaluating multiple security solutions, ShipServ decided to augment Microsoft's integrated security measures by implementing a FortiGate NGFW for Azure virtual appliance to deliver heightened intrusion prevention across the entire ShipServ cloud organization. The ShipServ network and edge security devices were also replaced with FortiGate enterprise firewalls. Doing so not only elevated overall threat prevention capabilities, but enabled the creation of secure connections between facilities. The company further enhanced its onsite network security with the addition of Fortinet Wi-Fi Management. The comprehensive capabilities of the FortiGate range–for both physical and virtual appliances–delivered a rich set of choices for ShipServ.

> **"ShipServ is experiencing unprecedented growth and the FortiGates and FortiGate VM give us the agility and flexibility to support wherever the business needs to go."**
> – Dominic Aslan, vice president of IT operations, ShipServ

Summary: Gain Adaptive Cloud Security for Microsoft Azure

As more and more enterprises migrate to Microsoft Azure to take advantage of the many benefits of the cloud, it is more important than ever to ensure that your systems and assets in the cloud are protected.

Fortinet provides customers with a broad array of security solutions to protect Azure based resources and workloads. Fortinet solutions are tightly integrated and designed to help customers maintain a consistent security posture across applications, clouds, and data centers.

To learn more about FortiGate NGFW on Microsoft Azure and start your free 30-day trial, visit fortigate-azure.com.

Fortinet was named a Leader in the 2021 Gartner Magic Quadrant for Network Firewalls for the 12th consecutive time.

April 11, 2022