



Don't Compromise

Why You Need to Go Beyond
Azure's Native Cloud Security



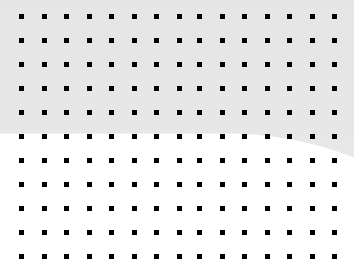
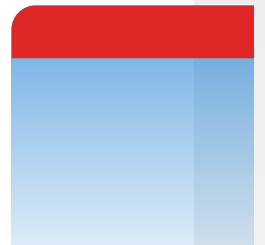


Table of Contents

Executive Overview	3
Security Challenges in the Cloud	4
Get Unmatched Security in the Cloud	5
Achieve Advanced Threat Protection on Azure with FortiGate Next-generation Firewall	7
The Need to Go Beyond Native Cloud Security	8
Key FortiGate Use Cases for Azure	11
Summary: Gain Adaptive Cloud Security for Microsoft Azure	12
Customer Case Study: ShipServ	13



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 2020 State of the Cloud Report](#), “93 percent of enterprises have a multi-cloud strategy” while “87 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.

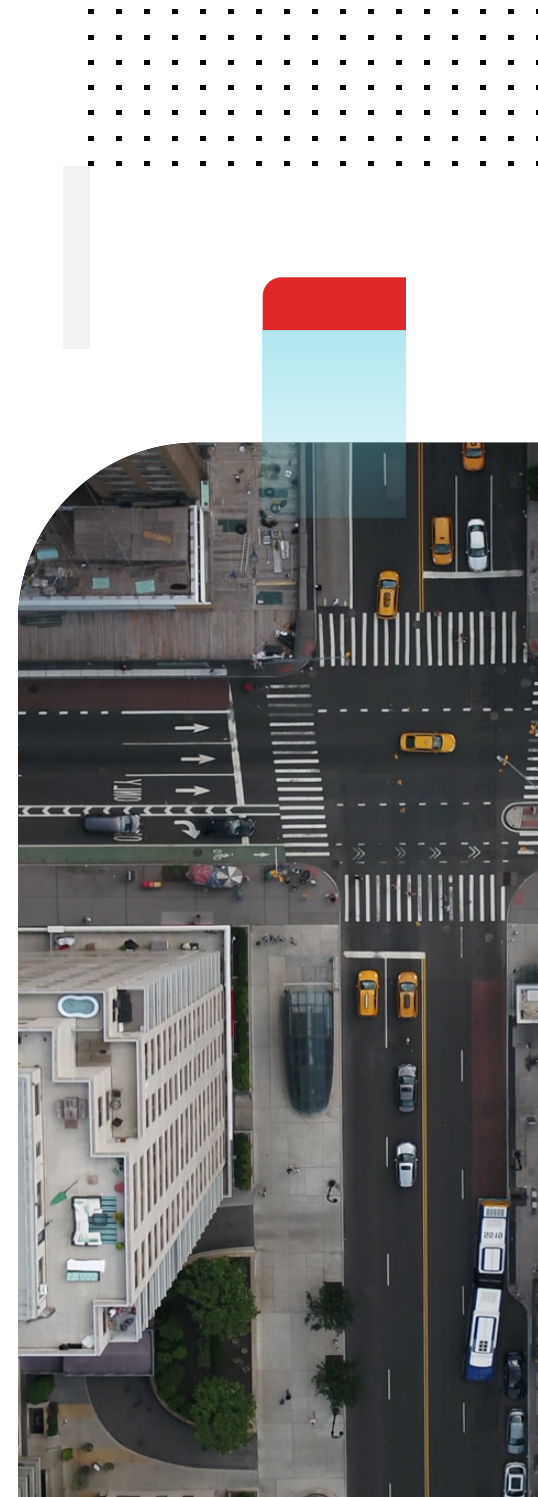
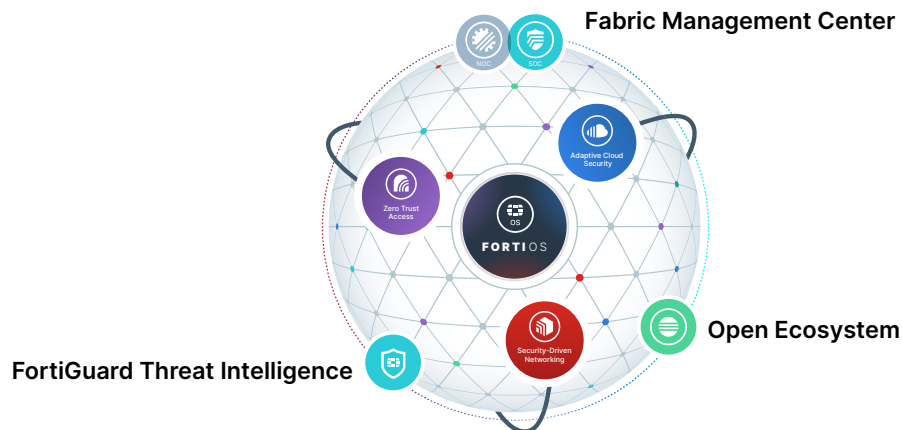


Get Unmatched Security in the Cloud

Making Possible a Digital World You Can Always Trust

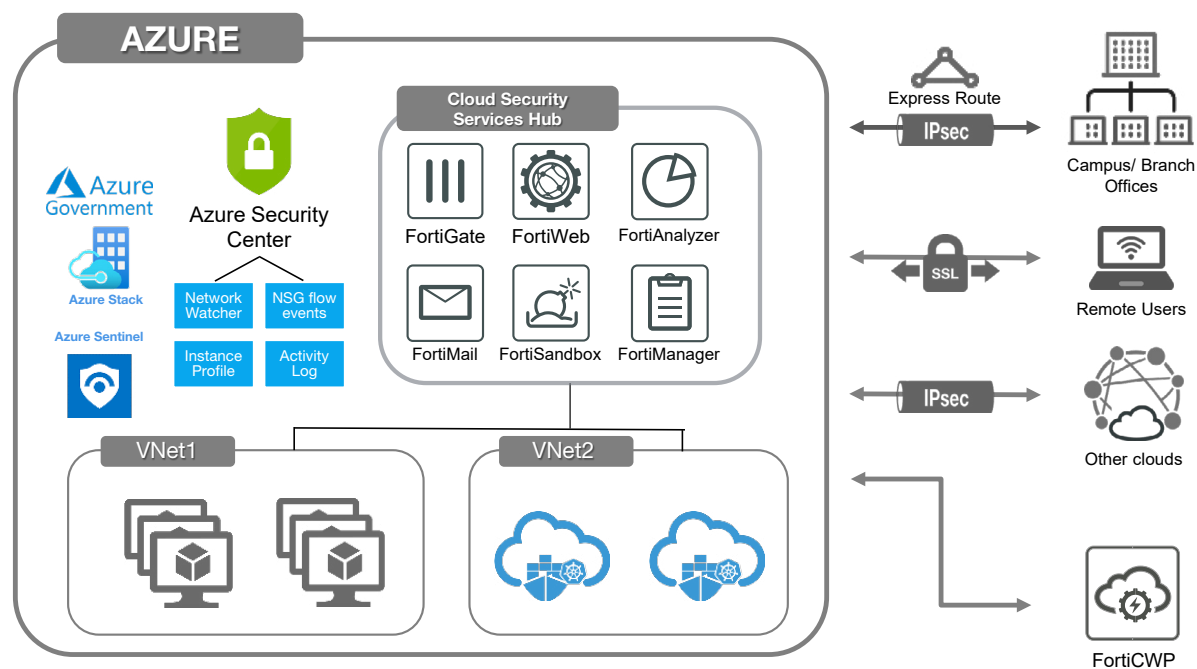
As your organization evaluates security solutions on Microsoft Azure, look no further than Fortinet. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface. With more than 20 years of experience in security, Fortinet is one of the world's top cybersecurity 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.



The Need to Go Beyond Native Cloud Security

While network security services provided by cloud vendors like Microsoft's Azure Firewall service may be sufficient for customers with basic security requirements, organizations with mission-critical workloads or who utilize a mix of clouds and on-prem computing should consider a solution like FortiGate. FortiGate NGFWs offer proven efficacy through consistent security policies and management across clouds and data centers.

Microsoft's Azure Premium Firewall service, an extension of Microsoft's Azure Standard Firewall, may be a convenient option for existing Azure-only customers due to the integrated nature with the Azure ecosystem. However, this service lacks the capabilities that a security-centric solution like FortiGate NGFW can provide.

Fortinet was named a Leader in the 2020 Gartner Magic Quadrant for Network Firewalls for the 11th consecutive time. Additionally, Fortinet FortiGate NGFWs scored the highest in the Enterprise Data Center (3.71/5) and SMB (3.52/5) Use Cases in the [“2020 Gartner Critical Capabilities for Network Firewalls”](#) report.



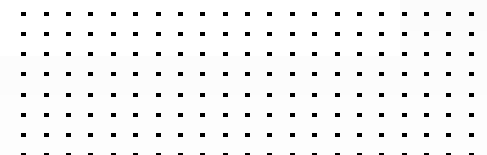
FortiGate Capability Comparison with Azure Premium Firewall

FortiGate NGFW goes beyond native cloud security to provide enterprises with the advanced security features that they need to protect against threats in the cloud.

	Fortinet FortiGate	Azure Premium Firewall
Gartner Network Security Leader	✓	✗
NSS Labs Tested and Validated	✓	✗
Bot Protection	✓	✗
Data Loss Prevention	✓	✗
Security Fabric Integration*	✓	✗
Automation Stitches**	✓	✗
Consistent Security Across Hybrid and Multi-cloud Environments	✓	✗
Application-aware firewall	✓	✗
SD-WAN	✓	✗

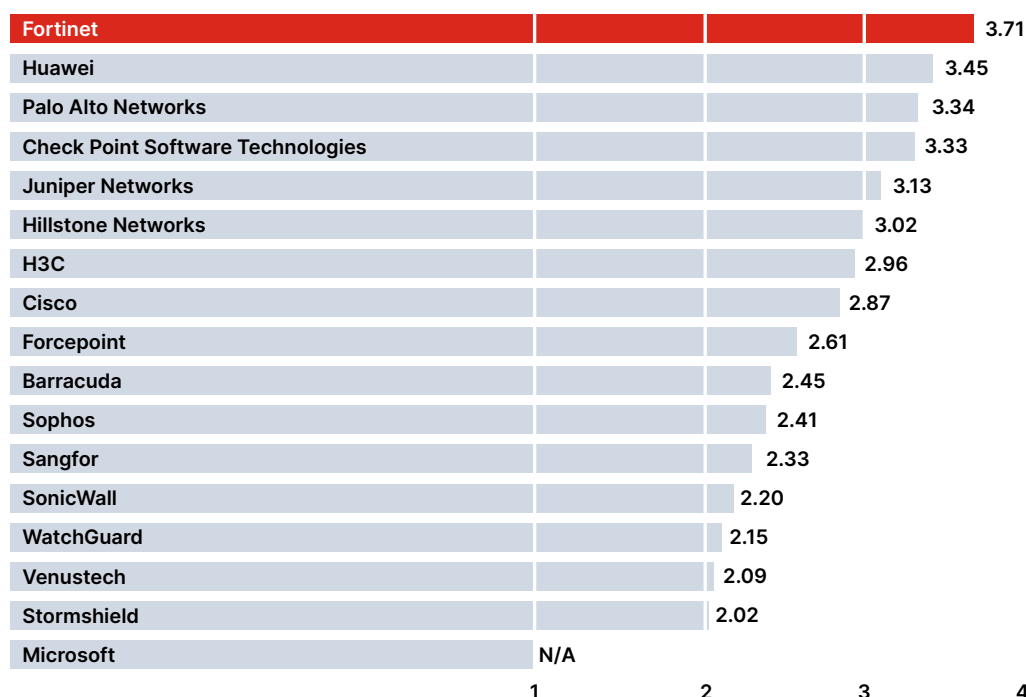
*The Fortinet Security Fabric offers integrated and unified security, operations, and performance, not only between Fortinet products, but across the entire broader Fortinet ecosystem. This enables advanced security features such as threat intelligence sharing and automated policy enforcement.

**Fortinet offers automated integrations across Fortinet products such as automation stitches between FortiADC and FortiGate.



2020 Gartner Critical Capabilities for Network Firewalls

Product or Service Scores for Enterprise Data Center



Source: Gartner (November 2020)

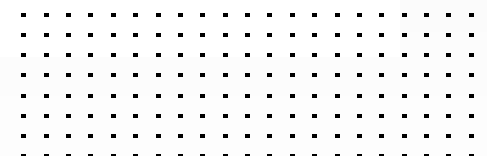
“Strong Firewall Solution That Protects Your Business Systems”

Programmer in the Finance Industry



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

- Network Firewalls
(Named a 2nd time)
- WAN Edge Infrastructure
(Named a 2nd 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.

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.

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.





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. Microsoft Azure supports a variety of security solutions and technologies to protect applications and data in the cloud. But Azure does not provide complete, enterprise-class security. Organizations need deep visibility and granular control security policies—not only within Azure but across other clouds and data centers.

Gain multi-layered security in the cloud with FortiGate NGFW on Microsoft Azure. FortiGate NGFW goes beyond the basic security features of Azure firewall, providing your business with next-generation firewall capabilities.

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.





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





Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.