Fortinet + Azure Secure Cloud Migrations

Table of Contents

Executive Overview

The COVID-19 pandemic brought hard lessons for many businesses trying to empower their employees to continue working safely and productively under new conditions. One key initiative has been migrating their business-critical data and applications from on-premises servers to the cloud. The cloud's ability to instantly scale and be accessible everywhere has helped drive new productivity in uncertain times. However, these changes have also accelerated the need for cloud-based innovations in how we do business and secure critical data.

All innovation comes with risks, and migrating to the cloud is no different. No matter the cloud service provider (CSP), securing data during migration to the cloud is important, especially in today's world where cyber threats grow exponentially and data ecosystems are gaining more complexity. The need to ensure and maintain regulatory compliance and audited records for sensitive data creates even more risk of potential exposure.

Fortinet's mission is to deliver the most innovative, highest-performing network security fabric to secure and simplify your IT infrastructure. We are a leading global provider of network security and SD-WAN, switching and wireless access, network access control, authentication, public and private cloud security, endpoint security, and AI-driven advanced threat protection solutions for carriers, data centers, enterprises, and distributed offices.

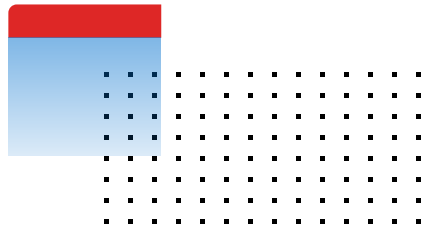
Cloud Migration Challenges

As cloud migrations accelerate, those securing this digital transformation will need to utilize new techniques and efficiencies to meet the needs of the business at speed. The attack surface grows once a business begins migrating its data and applications to the cloud, which in turn increases the need for comprehensive security that protects sensitive data during migration. Some common pain points for businesses during migration include:

- Reduced visibility and control during migrations
- Protecting vulnerable internet accessible management APIs
- Unnecessary complexity driven by cloud vendor lock-in and multi-cloud setups
- Staff strain

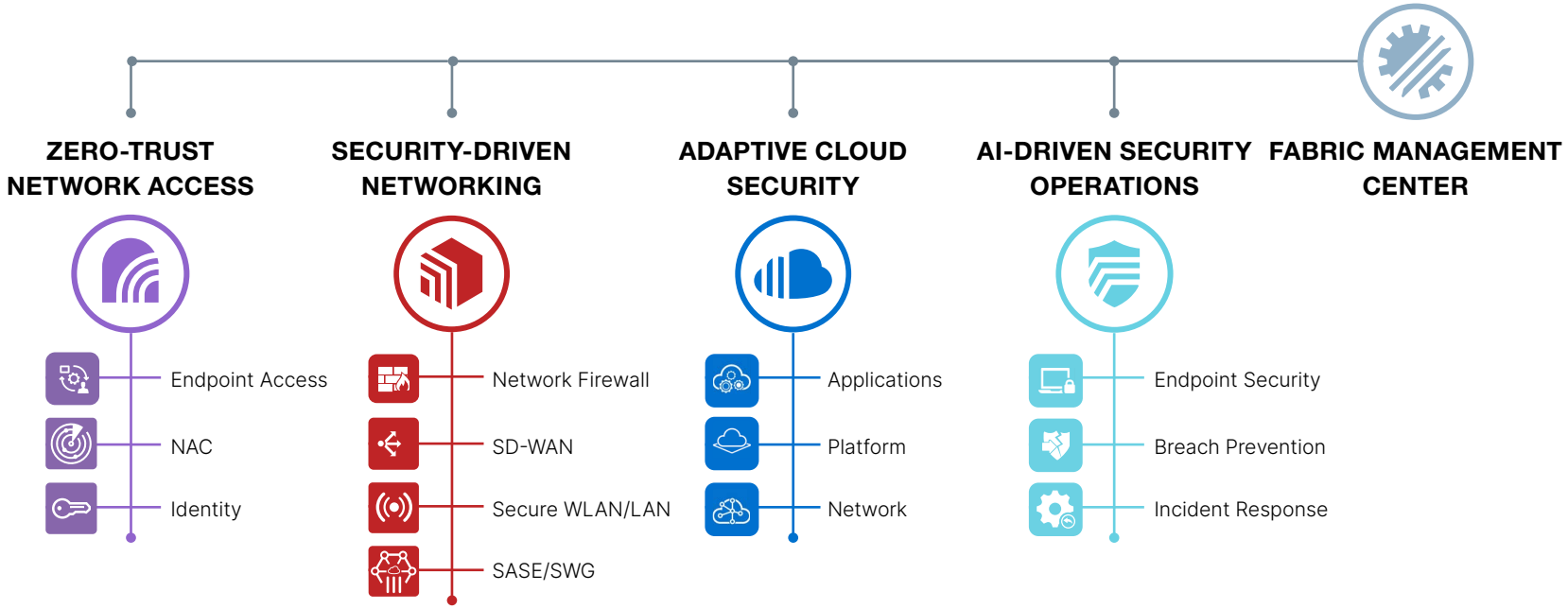
These threats are not insurmountable, but they do represent a significant risk to a successful migration.

While some of these pain points are addressed by modern security best practices, having a focused and specific solution ensures not only visibility but control over your data during migrations, while protecting the full surface of attack. This, combined with CSP-provisioned AI, can help ensure that applications and data migrated to the cloud are safe and secure. Fortinet can help businesses unblock and automate secure data management and cloud migration.



The Security Fabric

Securing data effectively in the modern world requires multiple layers of security to cover a wide attack area with a security fabric. This **security fabric** approach serves to ensure that data is protected and that all sensitive data meets regulatory compliance and includes each of the following components:



Cloud Migration Challenges

Creating a Zero Trust Network

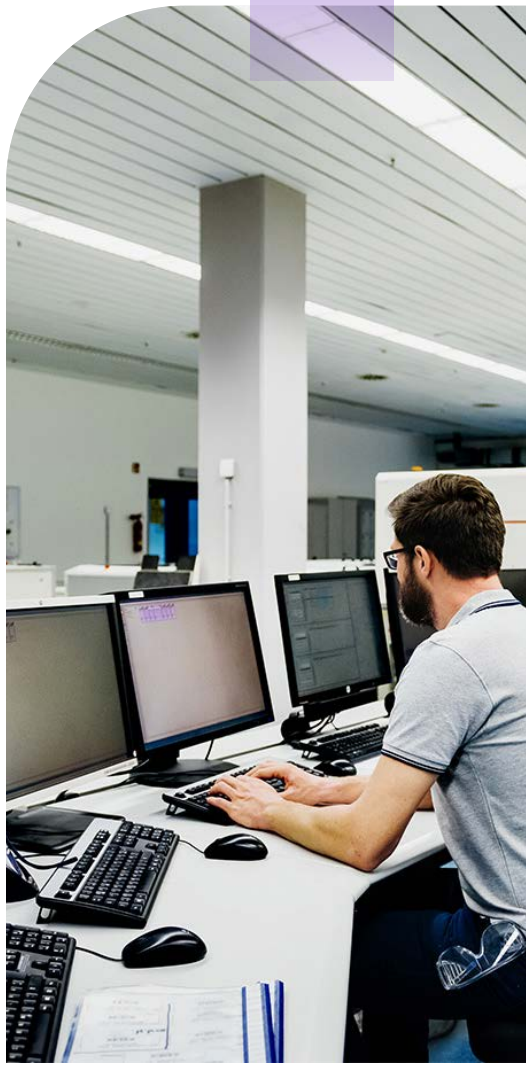
Since networks now have numerous edges, it is no longer feasible to create a single defensible boundary rendering perimeter-based access control strategies ineffective. In a zero-trust network, all communications are encrypted, and user identities and context are used to establish trust. Multi-factor authentication (MFA) reduces risks from external bad actors, while mandating least-privilege restricts access to the minimum that a user needs based on their role or relationship with the organization.

- Assume compromise
- All communication encrypted
- Use user identity and context to establish trust
- Monitor everything and apply concept of least privileged access

Security-driven Networking

Security-driven networking is an essential strategy for securing today's dynamic and evolving digital infrastructures. Powered by a uniform fabric of connected platforms deployed in every possible environment, security-driven networks provide consistent visibility across the entire perimeter as it adapts and changes, optimizing and securing traffic.

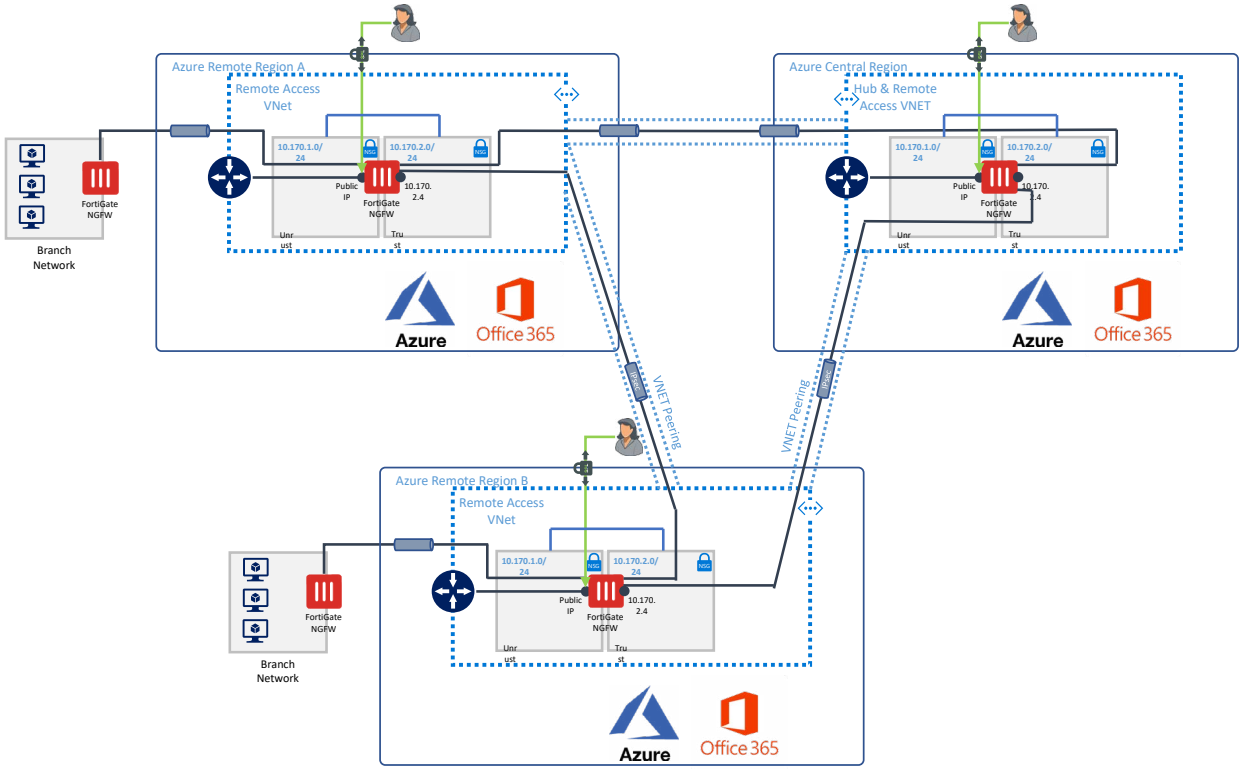
- Built around a security fabric
- Apply access control and segmentation
- Consistent protection for workflow and applications
- Optimize and secure traffic with Secure SD-WAN
- Utilize next-generation firewall (NGFW) to secure traffic with IPS, sandboxing reputation and more



Security-driven Networking

Global Secure SD-WAN through Azure

Fortinet has reference architectures to help you deliver Security-driven Networking. Here is an example of a global, secure SD-WAN through Microsoft Azure.

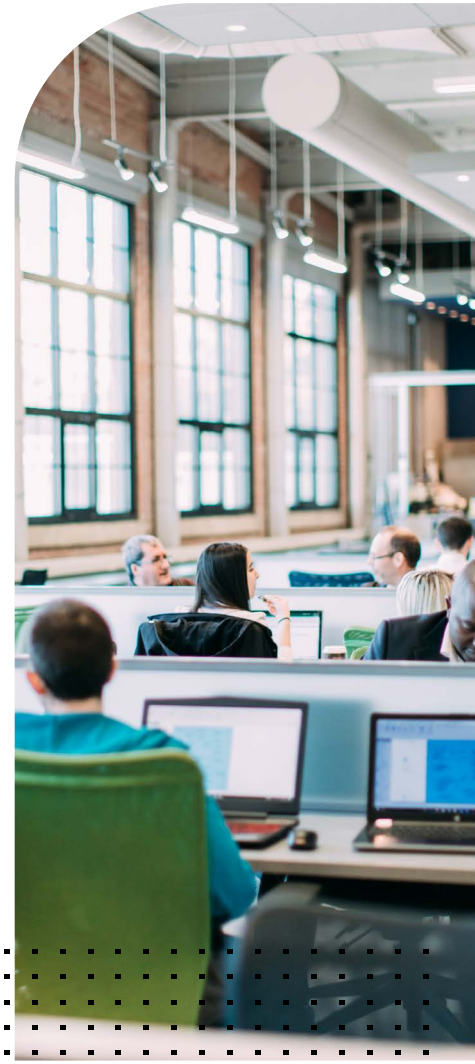


Adaptive Cloud Security

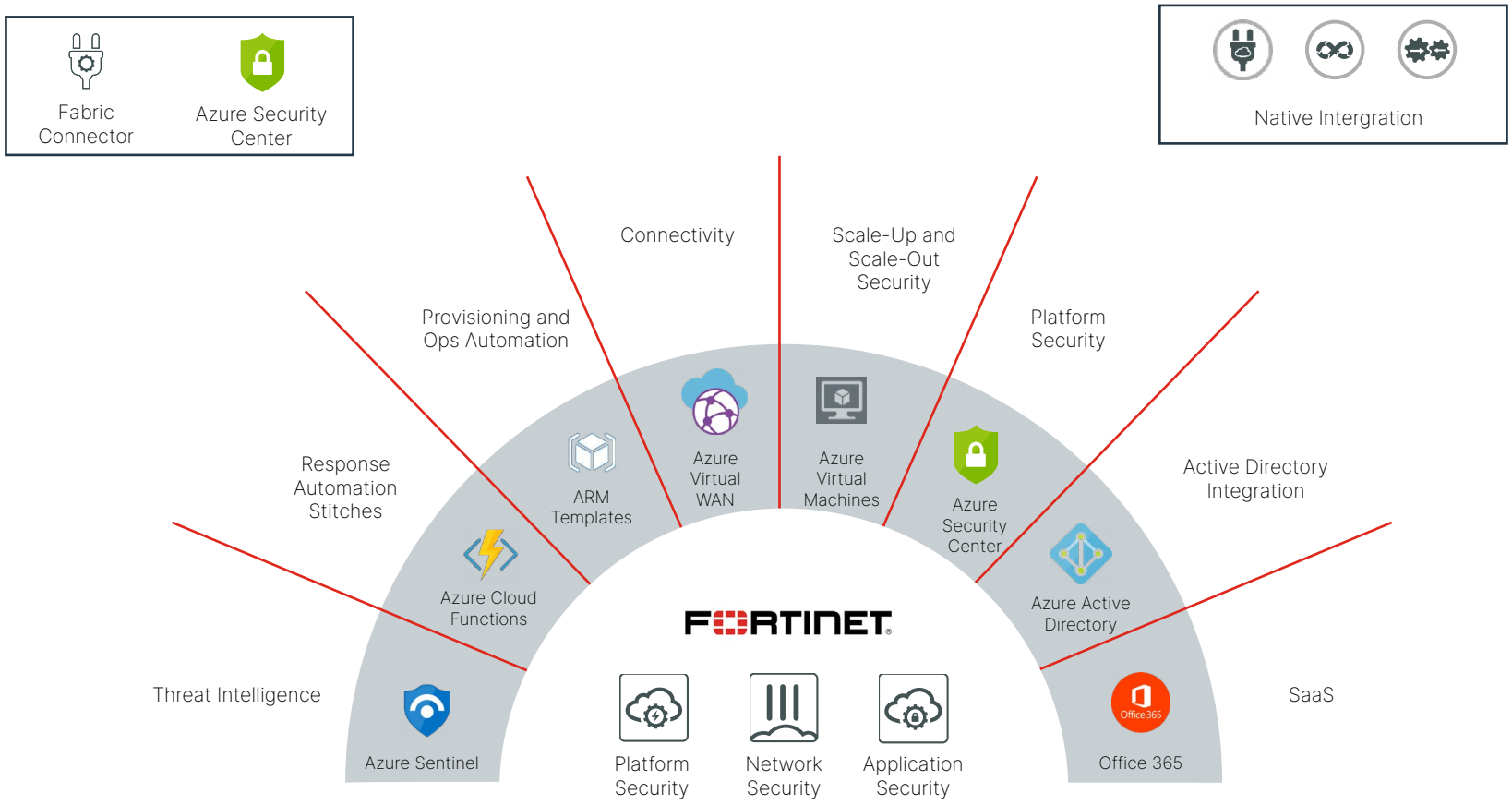
Adaptive cloud security allows you to both benefit from the flexibility and scalability of the cloud and still maintain the level of security that your data requires. While new cloud use cases are created and existing use cases evolve every day, data security requirements still must be met adequately, no matter where the data may reside. True adaptive cloud security provides a single-pane-of-glass view across all cloud platforms, providing visibility no matter where your data lives while applying security-driven networking concepts to all cloud workloads.

The Fortinet Security Fabric extends to the cloud – providing single-pane-of-glass management and automation across clouds and data centers. With Fortinet you can benefit from enterprise-class security – wherever your compute occurs.

- Apply security driven networking to cloud workloads
- Application Security with artificial intelligence (AI) driven web-application firewall (WAF) driven WAF
- Cloud workload protection
- Automation templates for programmatic configuration and deployment



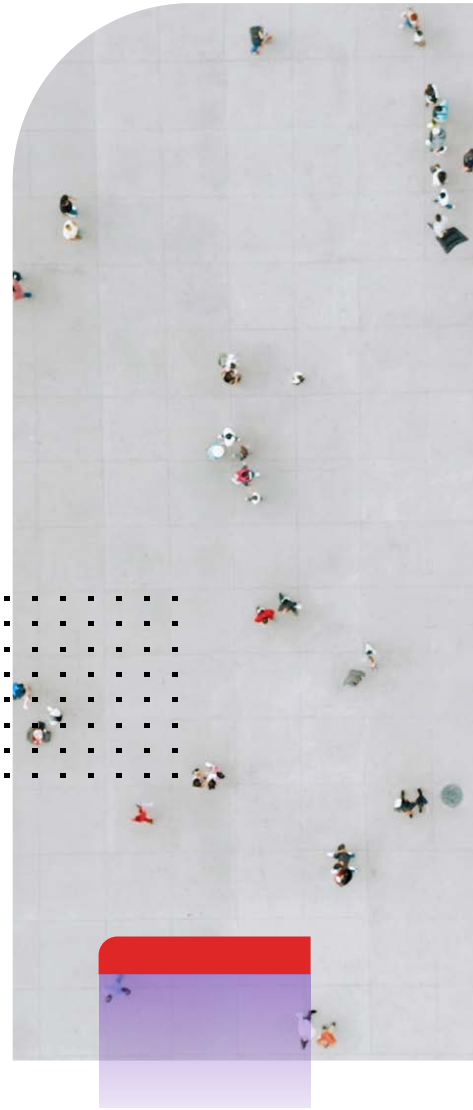
Fortinet and Azure Integration



AI-driven Security Operations

With machine learning (ML), AI and neural network capabilities, cloud service providers can help augment the speed of your cybersecurity response to new threats and with collected data. AI-driven security operations can help identify threats before they happen, freeing up your team of cybersecurity experts. This augmentation can be the difference between an overwhelmed and overworked cybersecurity team and a focused and efficient one.

- Hundreds of threat researchers
- More than 700 security patents
- Processing 100 billion security events
- Utilizing next generation AI and machine learning
- Discovered over 870 zero-day vulnerabilities
- Sending out more than 1 billion updates a day



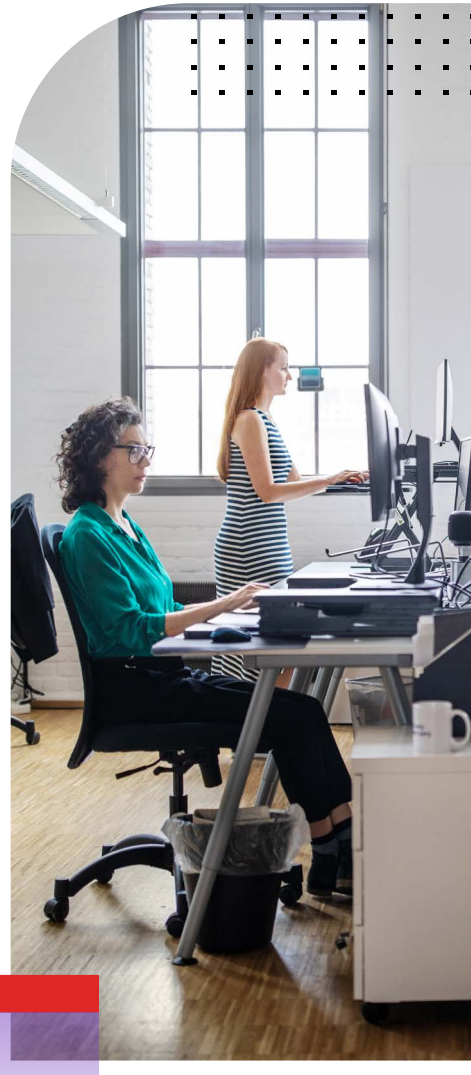
Fabric Management Center

All of this must be tied together through a security fabric that is both powerful and easy to use and to automate. The security fabric must include shared analytics, shared threat information and the ability to automate across security platforms so you can automate deployments, workflows, policy management, and responses.

To address the need for network, application and platform security, Fortinet provides:

- Powerful central management and automation
- The broadest set of cloud security solutions on the market
- And deep, native integration into Microsoft Azure

The Fortinet Security Fabric does more than just provide visibility into your overall security posture, it can actually enhance security through automation so that if one Fortinet solution identifies an elevated threat condition, other Fortinet products can be automatically employed to mitigate the risk. Fortinet also provides templates and tools for automating configuration and deployment of Fortinet's solutions.



Secure Cloud Migration with Fortinet and Azure

Fortinet, a global leader in security, offers a single platform for cloud security migration that can help mitigate additional risk by simplifying management and centralizing it into one single platform.

Foritgate Next Generation Firewall (NGFW) are network firewalls powered by purpose-built security processing units (SPUs) including the latest NP7 (Network Processor 7). They enable security-driven networking, and are ideal network firewalls for hybrid and hyperscale data centers.

FortiWeb is a web application firewall (WAF) that protects hosted web applications and API from attacks that target known and unknown exploits. Using machine learning to model each application, FortiWeb defends applications from known vulnerabilities and from zero-day threats.

FortiManager VM runs and manages Fortinet next-generation firewalls (NGFWs) on most hypervisors (for private clouds) and software-defined network (SDN) platforms. It provides single-pane-of-glass management for unified, end-to-end protection across the extended enterprise. It also delivers insight into network traffic and offers enterprise-class features for threat containment.

FortiAnalyzer VM gives critical insights into threats but also accurately scopes risk across the attack surface. This enables organizations to pinpoint where immediate responses are required. It also offers automated responses to threats for near real-time mitigation.

Securing SAP S/4HANA

Secure your SAP S/4HANA Migration with Fortinet

Fortinet offers unprecedented security and visibility for organizations seeking to secure SAP applications in the cloud. Fortinet's solutions for SAP include network security, application security, and workload protection, and can be extended with end-point security and well as with central management and analytics. Fortinet also offers two-factor authentication tools, device and access control to help ensure that only approved users and devices are allowed to connect, and endpoint security and remediation. All Fabric components receive actionable threat intelligence updates driven by artificial intelligence via FortiGuard Labs.

Business leaders embrace SAP HANA to stay on top of emerging trends and evolving business requirements. But while SAP transforms business processes with intelligent automation, it is also a leading cybersecurity target. New implementations of SAP systems, SAP upgrades, conversions to S/4HANA are now in the cloud rather than on-premises. These cloud-based SAP deployments add agility and scalability but they also expand the attack surface. Fortinet takes a holistic approach to secure SAP systems by protecting all SAP data generated by edge devices, endpoint systems, users, applications, databases, third party systems in on-premises, hybrid, and multi-cloud environments. Fortinet solutions for SAP include:

- FortiGate Next Generation Firewall
- FortiWeb Web Application Firewall
- FortiSandbox Cloud
- FortiADC / FortiGSLB

A Global Security Leader

Fortinet has years as a proven enabler and unblocker for secure data management and cloud migration. Fortinet solutions provide the most rigorously tested security available, natively and via open API across your security infrastructure. Fortinet has received more industry validation for performance and security effectiveness than any other vendor. Fortinet believes that this recognition validates their technology innovation and leadership.

Fortinet was named a Leader in the 2020 Gartner Magic Quadrant for Network Firewalls for the 11th time.

Beyond Gartner, Fortinet has been independently tested and validated by many of the world's most reputable third-party organizations. Fortinet is the only company to receive 9 NSS Labs recommendations across all 9 key NSS Labs tests, nearly 2X the nearest competitor. Fortinet is certified in 8 technology areas by ICSA and passed the last 19 consecutive ATD test cycles. We are the only vendor with all three Virus Bulletin VB100, VBSpam, and VB Web certifications. Fortinet was also validated by AV-Comparatives and more.

FIGURE 1. MAGIC QUADRANT FOR NETWORK FIREWALLS

Source: Gartner (November 2020)

See how Gartner has also recognized Fortinet in WAN Edge Infrastructure, Web Application Firewalls, and Wired and Wireless LAN Access Infrastructure.

A Gartner Peer Insights Customers' Choice™

Recognized by 3,600+ Customers in Multiple Categories and Markets

Customers' Choice

- Enterprise Firewall
- WAN Edge/SD-WAN
- Wired and Wireless LAN Access Infrastructure

Top 5
Vendor in 8 markets

3,600
Reviews

14
Markets

Unparalleled 3rd Party Validation

Certification	Fortinet	Check Point	Cisco	Palo Alto Networks	Juniper	FireEye
NSS Next-Gen Firewall	•	•	o	•	o	x
NSS DC Security Gateway	•	x	•	•	•	x
NSS Next-Gen IPS	•	x	o	•	o	x
NSS DC IPS	• •	x	•	x	x	x
NSS Breach Detection	•	x	•	x	x	•
NSS Breach Prevention	•	•	•	•	•	x
NSS WAF	•	x	x	x	x	x
NSS Advanced Endpoint*	•	•	x	•	x	x
NSS SD-WAN	•	x	x	x	x	x
ICSA ATD – Sandbox	•	x	x	x	•	x
ICSA ATD – Email	•	x	x	x	x	x
ICSA Network Firewall	•	•	x	x	•	x
ICSA Network IPS	•	x	x	x	x	x
ICSA Anti-malware Network	•	x	x	x	x	x
ICSA WAF	•	x	x	x	x	x
Virus Bulletin 100	•	x	x	x	x	•
Virus Bulletin Spam	•	x	x	x	x	x
Virus Bulletin Web	•	x	x	x	x	x
Common Criteria	•	•	•	•	•	•
FIPS	•	•	•	•	•	•
UNH USGv6/IPv6	•	•	•	•	•	x

• Recommened/Certified o undisclosed x did not participate

NSS Labs AEP Test: Vendor products now receive a letter rating. Green here denotes a favorable “A” rating or better

Ways to Consume

Fortinet breaks down the walls that inhibit security visibility and management between and across on-premises and cloud environments. Their security solutions have flexible deployment solutions. Licenses purchased from a Fortinet channel partner for different products are transferrable across platforms. Fortinet solutions, like FortiGate NGFW and FortiWEB WAFaaS can be consumed using a pay-as-you-go (PAYG) on-demand usage model with Microsoft Azure.

To learn more visit Adaptive Cloud Security for Microsoft Azure or contact us at azure@fortinet.com.

www.fortinet.com

May 19, 2021 1:28 PM

FRTN3639_Azure-Secure-Cloud-Migrations_EBK_2021

123456-0-0-EN