Toolkit: Network Security in the Cloud

Introduction

Your choice of a next-generation firewall (NGFW) is an important one. There is more to making this choice than just looking at features and prices. You need to look at your organization's broader security infrastructure and consider the functionality you will need today, tomorrow, and even years from now. Just as important, you need to ensure that your security vendor is a partner who can support your organization today and far into the future.

This document will help you understand what is driving cloud security, the challenges the cloud brings, and it provides some guidelines on selecting a network security solution for the cloud.

Table of Contents

POINT OF VIEW

Why Digital Acceleration Needs a Hybrid Mesh Firewall Approach

Executive Summary

Organizations large and small have adopted digital transformation initiatives to enable them to deliver business growth and meet organizational objectives. The pace of this transformation has accelerated as organizations have sought to address challenges caused by the global pandemic. IT teams were forced to move many applications to the cloud faster than originally planned. These rapid changes increased cybersecurity risks and imposed a heavy burden on infrastructure teams, often due to the plethora of new, platform-specific security tools.

With moving to public clouds and modernizing data centers at the heart of this transformation, care and attention must be given to ensuring that your networks and data are secure and that security can be easily managed across clouds and data centers.

> *"The ability to view the entire infrastructure on a single pane of glass is a huge benefit to our architecture, network, and security teams."*
>
> **Jessie Hawkins**
> Systems Architect
> University of South Carolina

Digital Acceleration: The Journey to Cloud Starts with a Hybrid Mesh Firewall

Organizations pursuing digital acceleration have various strategies and are at different stages with their cloud adoption and application journey. In many cases, organizations are lifting and shifting virtualized application workloads from their virtual data centers into the cloud, while some are refactoring applications to integrate with cloud provider services, and a few are actually architecting applications to be cloud native. Regardless of where they are in their journey, all of them have major concerns about their applications and data security.

For most organizations, securing this application journey to the cloud begins with securing the network that connects their users, branches, and data centers to the cloud. As a next step, they focus on securing the cloud network that connects to cloud provider services and workloads in the public cloud and hybrid cloud. Organizations at an advanced level of cloud maturity then move on to securing the networks that connect their application infrastructure in a multi-cloud deployment. Getting the cloud network ready for deploying applications causes plenty of challenges, including setting up a robust cloud perimeter for every network setup by various types of users, implementing advanced security for compliance, and streamlining their network and security operations without being run over by runaway cloud costs.

A hybrid mesh firewall (HMF) is a network of next-generation firewalls (NGFWs) able to run locally and in the cloud that can be centrally managed and can automate security updates and responses across the entire network. By utilizing an HMF, organizations can reduce management overhead, consolidate security analytics, and reduce the strain on staff that comes from having to manage disparate firewalls on each cloud and in each data center.

Cloud Network Security Challenges and Trends

Because cloud transformation plans and application journeys vary across organizations, network security challenges differ. There are, however, some fundamental challenges that are the same across organizations. Here are some key challenges faced by organizations deploying applications into public and private clouds:

- **Uncontrolled outbound communications**

  This type of communication from a cloud deployment happens when outbound web traffic attempts to connect to low-reputation sources (based on the domain or hostname). These connections could be established by malicious spyware or malware trying to exfiltrate sensitive data or connect to an external command-and-control server. On the other hand, the traffic could originate from developer workloads contacting developer tools like GitHub or application workloads contacting external servers for software updates.

- **Lateral movement of threats**

  In the cloud and virtualized data centers, there is typically no control or protection put in place to inspect the traffic flowing between different VNETS or between workloads in the same virtual network. This leaves room for malicious or compromised internal actors to introduce threats that can quickly propagate through the virtual data center or in the cloud. Another important threat vector to consider is the software supply chain and open-source software, which may have been compromised. Developers inadvertently use these resources, introducing external threats that can propagate laterally and launch catastrophic attacks.

- **Limited bandwidth for secure connectivity into the cloud**

  As organizations use more and more cloud services, they onboard traffic at many locations, including HQ, on-premises data centers, branches, and remote locations. In many of these cases, they may use virtual private network (VPN) technology to connect to the cloud. Organizations have an option to use cloud-provider VPN gateways. Still, most of these gateways do not offer the bandwidth performance needed to deliver the best application experiences to users across different locations.

- **Fragmented management and policy infrastructure**

  When organizations start using more than one cloud provider, often alongside their physical, virtual data centers, their operations teams are too frequently burdened with managing multiple, often incompatible, platform-specific security tools. They must manage different consoles and set up different policies across these diverse platforms. This leads to a higher cost of training and may leave security gaps among the various environments.

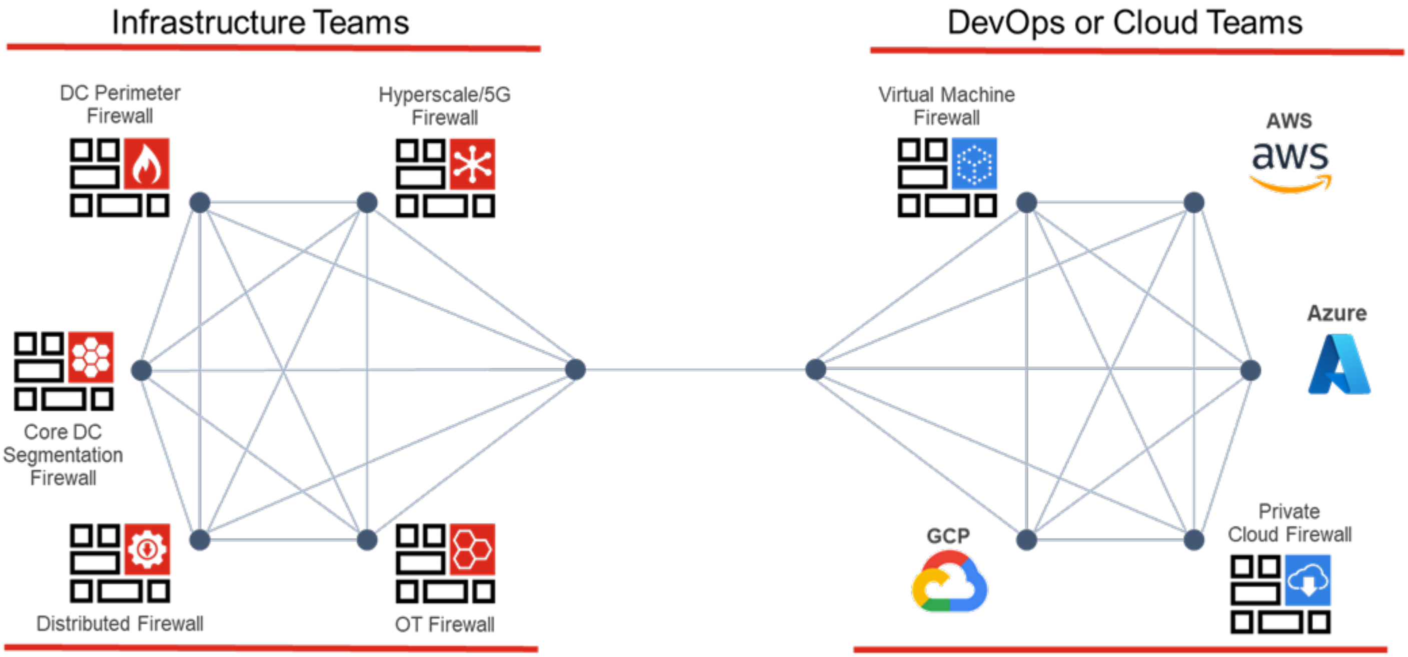
An Effective Roadmap to Protect the Cloud Network

The application journey for any organization essentially lays out the evolution of their cloud transformation, which in turn drives the roadmap for rolling out their cloud network security. It starts with the application journey's lift-and-shift phase, essentially the organization's cloud migration phase. In this phase, they are focused on providing secure connectivity from various locations to the application workloads in the cloud.

Once the organization gets accustomed to cloud usage, it evolves to refactor and rearchitect a select set of applications or even create cloud-born applications. In this cloud expansion phase, it may expand its footprint to tens or hundreds of cloud networks. At this stage, organizations are primarily deploying robust, high-scale routing to interconnect the organization's virtual networks on any cloud provider. But it will also need to ensure that it can effectively manage security on-premises and in the cloud. This requires eliminating siloed security solutions for ones that work together in a security mesh. In most cases, this means weaving the network firewalls, both cloud-based and physical, into an HMF infrastructure.

Next, the organization builds and deploys cloud-native architectures or runs complex IT infrastructures spanning multiple clouds. Organizations in this cloud-native or multi-cloud phase typically implement efficient networks to get users from tens or hundreds of locations to access their workloads in multiple clouds. The organization may even connect application infrastructures across cloud providers by routing the traffic at their data centers or leveraging cloud-provider, or service-provider managed network services. In any case, the organization will need to secure the network connecting to these multiple clouds and also **secure the networks connecting across the clouds.**

Organizations need AI- and ML-powered intrusion prevention systems (IPS), aggressive patch management strategies, and the threat intelligence all coupled into a hybrid mesh firewall to secure modern, multi-site environments.



On-Premises Data Center, Campus, and Data Firewall

Cloud and Cloud-Native Firewall

Conclusion

The answer to safely moving to the cloud for digital acceleration is reducing complexity and increasing security effectiveness with an HMF approach. An HMF benefits organizations with centralized visibility, management, and automation across all solution points, allowing them to leverage intelligence sharing for faster response times. Ultimately, this reduces complexities, solves cloud cybersecurity skills and resource gaps, and increases overall security effectiveness. As such, organizations should look for solutions that integrate and support a broad, integrated, and automated cybersecurity fabric.

SOLUTION BRIEF

The Top Challenges of Cloud Network Security

Cloud security is a broad topic, encompassing network security, application security, data security, identity and access management, workload protection, and much more. In this document, we will focus on network security fundamentals. However, it is important to note that network security tools should not be considered in isolation. Security solutions should be designed to work together to form a security fabric that can extend from data centers to branch locations then to the cloud or multiple clouds.

What is cloud network security?

Cloud network security refers to the technology, policies, controls, and processes used to protect data and workloads in public and private clouds. It focuses on protecting cloud networks from unauthorized access, modification, misuse, or exposure.

Cloud network security forms one of the foundational layers of cloud security. It enables companies to embed security monitoring, threat prevention, and network security controls into their cloud infrastructure to help manage the risks of the dissolving network perimeter.

$4.45 M

According to a recent report, the average cost of a data breach was $4.45 million in 2022.[1]

Cloud network security challenges

Cloud computing can be just as secure as traditional, on-premises computing. However, cloud deployments do present some challenges unique to cloud environments, such as:

1. **Lack of skilled cloud security experts**
   According to the Fortinet 2023 Cloud Security Report,[2] 43% of companies reported that the shortage of qualified staff is their biggest “day-to-day headache” in protecting cloud workloads. Cloud security requires high technical skills and knowledge to implement and maintain it effectively. However, many organizations face a shortage of qualified and experienced cloud security professionals who can handle the complexity and diversity of cloud security challenges. The cloud security skills gap can result in inadequate or ineffective cloud security practices, policies, and solutions and increased vulnerability and risk for organizations using cloud computing.

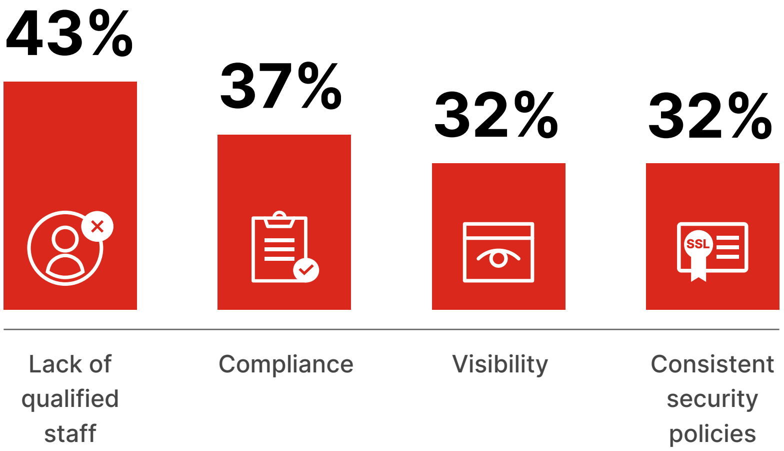


Figure 1: Reported biggest operational, day-to-day headaches trying to protect cloud workloads

2. **Legal and regulatory compliance**

   Compliance requires ensuring that cloud-based applications and data meet different industries' and regions' standards and regulations. However, cloud environments are often complex, dynamic, and heterogeneous, which makes it difficult to monitor and enforce compliance policies consistently.

   Cloud providers and the organizations that rely on them must comply with various laws and regulations that govern data protection, privacy, and security in different regions and industries. These include the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and others. Compliance requires in-depth visibility into an organization's systems and data across clouds and data centers.

3. **Lack of visibility**

   Modern IT environments are highly distributed, with applications deployed across private data centers, multiple public clouds, and edge locations. This means that most enterprises have potentially hundreds of applications spreading across a combination of SaaS-based, IaaS-based, private DC-based, or edge locations. Adding even more complexity is that shadow IT groups can spin up applications without full knowledge of the IT team.

   As organizations build out their hybrid IT infrastructure, they must have end-to-end visibility of the IT environment and eliminate any blind spots, as it is impossible to manage something that you cannot "see." Visibility must be **broad** to identify and scan resources, activities, and potential vulnerabilities across the entire compute surface. Visibility must also be **deep** to pierce the veil of encryption to identify malicious or inappropriate traffic. And it must be application aware to quickly identify known and unknown applications and apply appropriate security and routing policies, including zero trust policies.

4. **Consistent security policies**

   The Fortinet 2023 Cloud Security Report also found that 69% of organizations surveyed were using two or more cloud providers,[3] with each provider promoting its own network security tools and services. Unsurprisingly, companies that have relied on their cloud vendors for security are finding it a challenge to offer and enforce consistent security policies across clouds and data centers.

   With multiple cloud providers in use, it can be difficult to keep track of everything and ensure that each component is configured correctly. Every cloud service provider has a different approach to security, models, responsibilities and compliance obligations, best-practice recommendations, and names for the same services. Worse, these security products may have different features and different detection rates. Given the above, it comes as little surprise that many organizations struggle to offer consistent security policies when relying on varied security tools.

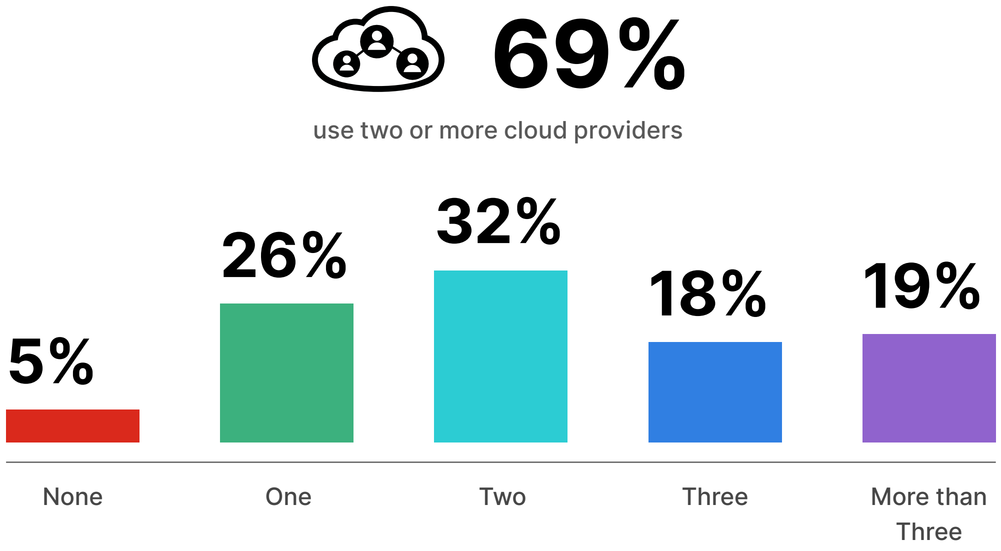


Figure 2: Most organizations struggle to apply consistent security policies across clouds.

5. **Expanded attack surface**

   The attack surface is the sum of all possible entry points, or attack vectors, where an unauthorized user can access a system with nefarious intent. These include applications, code, APIs, ports, servers, websites, and even orchestration and automation systems. The attack surface also includes shadow IT, in which users bypass IT to use unauthorized applications or devices.

   By definition, cloud services are accessed over the internet, making them more exposed to potential attackers. In this way, cloud computing is similar to DMZs in traditional networks, making them more vulnerable to attacks. Further, cloud-specific technologies and interfaces introduce new attack vectors that might not exist in traditional IT environments. These include attacks targeting cloud APIs, orchestration platforms, containerization systems, and serverless architectures.

6. **Complexity**

   Complexity is the enemy of security. In fact, Gartner famously stated that by 2025, human failure, largely due to complexity, will be responsible for over half of significant cybersecurity incidents.[4] Complexity is not new; it's been creeping up on us for years. Multi-cloud and other complicated, heterogenous platform deployments have recently accelerated overly complex deployments. At the same time, security budgets, approaches, and tools have remained static. As complexity rises, the risk of breach accelerates at approximately the same rate.

7. **Human error**

   Human error, the inevitable result of the six factors above, is ultimately at the root of most data breaches. Cloud computing, especially when multiple clouds are in play, increases the likelihood of mistakes and misconfigurations that can lead the best defenses to fail. For example, 59% of cybersecurity professionals surveyed said that misconfiguration remains the biggest cloud security risk.[5] These mistakes are all the more likely when organizations rely on cloud-specific security tools. One of the priorities of any digital transformation effort should be to reduce human errors by reducing complexity, reducing the number of tools staff need to learn and manage, reducing the attack surface, and increasing visibility into cloud systems, traffic, and users.

CHECKLIST

How to Select a Virtual NGFW

Executive Summary

The shift to a hybrid workforce and the rapid adoption of cloud services have allowed today's users to connect to any resource from any location using any device. While this flexibility is necessary, it also expands the attack surface, opening the door to new threats. Organizations need to be sure their network security enables complete visibility across the entire distributed infrastructure. Otherwise, it will be impossible to effectively deliver and coordinate security protection with fast enough threat detection and remediation.

However, broader economic and social trends are leading many organizations to rethink their approaches to network security as part of new digital transformation projects. The Internet of Things (IoT), the rise of hybrid-cloud computing, the vast increase in remote work demands, the distribution of data center and application resources, the convergence of IT and operational technology (OT), and the continued shortage of skilled security professionals are just a few of the realities driving organizations to reassess their security strategies.

One outcome of these changes is the realization that network security tools, especially firewalls, can't work in isolation. Instead, they must work together, forming a hybrid mesh firewall (HMF). This unified security platform provides coordinated protection to multiple areas of enterprise IT, including corporate sites, such as branches, campuses, data centers, public and private clouds, and remote workers.

Requirements for Evaluating NGFWs

Ten key criteria should guide the evaluation and selection of NGFWs for enterprise edges or data centers.

☑ Use the same firewall wherever your compute occurs

Complexity is the enemy of security. The solution to this is to reduce the number of security solutions by using the same firewall on all platforms and in all locations. Simply put, the important criteria in selecting a virtual NGFW is that it has the same interface, features, and functionality as the firewalls used elsewhere in your organization, so long as they all can be managed through a common management plane. This will reduce the strain on your security team, reduce the likelihood of misconfigurations and mistakes, and help ensure you have holistic visibility into your security posture.

One of the most essential components of an HMF is its ability to traverse today's multi-cloud and hybrid data center environments. HMFs can coordinate protection across every IT domain (corporate sites, public and private clouds, and remote workers) using a unified management console. This allows enterprise IT to automate its protection capabilities, such as collecting and correlating data, performing AI-assisted deep analysis, and coordinating a unified response across the network without duplicating efforts, re-creating policies, or investing needless manual hours when a cybersecurity skills gap already constrains resources.

☑ Effectiveness

A security system is only as good as its ability to detect threats. However, the effectiveness of NGFW solutions is difficult to determine on your own. In this scenario, third-party testing is invaluable. One excellent source for efficacy data is CyberRatings.org, a nonprofit member organization dedicated to providing visibility and transparency on the effectiveness of cybersecurity products and services. While not all firewall vendors have agreed to be tested, those that did, like Fortinet, often offer the report on their website. See the latest report here.[6]

☑ Threat protection performance

Threat protection performance is a measurement of how an NGFW performs while running full threat protection, including firewalling, intrusion prevention, antivirus, and application control. It is critical for the NGFW to sustain high performance when full threat protection is turned on.

Many NGFW providers are ambiguous about how they represent their threat protection performance claims. Documented performance claims should be examined carefully to ensure they reflect testing under load, with threat protection fully engaged.

☑ Built with Sustainability in Mind

The management interface is where many security architects are stymied in their selection process. Careful attention may have been paid to the management system's user interface and functionality, but if it is limited to the NGFW, security teams will have to toggle between multiple dashboards to assess vulnerabilities and respond to threats. End-to-end visibility and control are possible only if the NGFW is part of a broad, integrated security architecture, across which it can share threat information with other network devices and receive threat intelligence automatically.

Single-pane-of-glass management is more effective from a security standpoint and is operationally more efficient, reducing administrative time and training costs.

☑ Future proof your purchase

Some cloud vendors promote their own relatively basic firewalls for use on their clouds. These products should be avoided because they lead to further fragmentation of your security toolset and because they generally lack the functionality considered standard with modern advanced NGFWs. You should purchase the product you need today with an eye on what you might need tomorrow. Ensure that your firewalls support advanced features, such as:

- **Anchoring an SD-WAN**
- **Zero-trust enforcement**
- **Intent-based segmentation**
- **Botnet detection**
- **Data loss prevention**
- **Sandboxing**
- **SSL (TCS) inspection for ingress and egress**

☑ Automation

Network automation is essential to keep up with the speed and sophistication of today's threats. But it is impossible to implement when your various point security tools, including your NGFW deployments, operate in a silo. Automation must combine software and processes to provision, configure, manage, and optimize all physical and virtual devices within your network. With everyday functions automated and repetitive processes streamlined and controlled, network service availability and overall user experience improve.

Network automation can reduce human error, improve efficiency, and ultimately lower costs. Employees can be dynamically authenticated and connected to the network to improve an organization's overall productivity levels. And with zero-touch provisioning, new devices can be configured and made ready for use by employees right out of the box, enabling them to start work faster without downtime. But network automation isn't enough. Your security fabric must also automate security functions. Security automation enables coordinating activities among different firewall mesh components to accelerate detection and decrease response times to security events. Events occurring anywhere across the firewall mesh should be monitored, and action responses should be able to defend any destination.

☑ Artificial intelligence, machine learning, and threat intelligence

Complex networks and an expanding threat landscape require coordinated protection. It’s not enough that firewalls span different areas of the network. They must also utilize artificial intelligence and machine learning (AI/ ML) capabilities to effectively detect and protect against known and unknown threats. AI/ML-powered security enables HMFs to identify and classify applications, web URLs, users, devices, malware, and more—all while automating policy enforcement across domains. Artificial intelligence and machine learning are at the heart of HMF automation and can significantly reduce the amount of manual work involved in protecting enterprise IT and OT.

☑ Flexible firewall pricing options

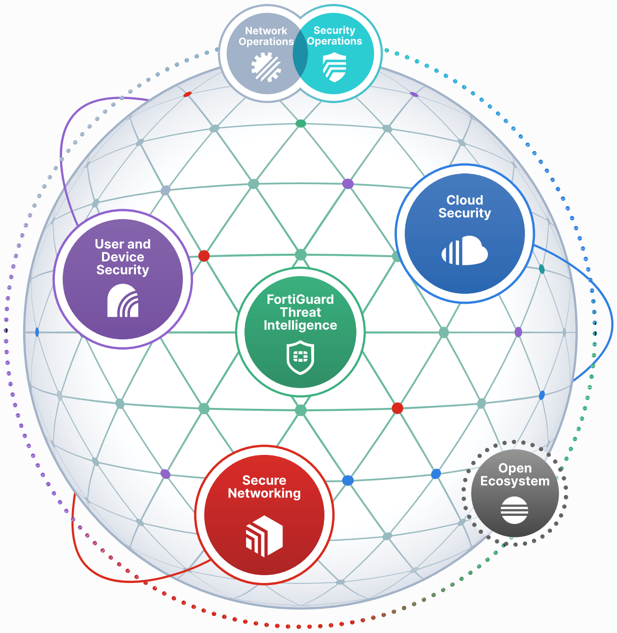
As business needs change, organizations require the flexibility to deploy a broad range of firewall types without being locked into a single form factor. And they need to be able to move assets from place to place as the network continues to evolve. Flexible pricing models enable organizations to adapt to changing network requirements, pay for what they use, customize their security services, and manage their budgets effectively. These pricing models offer greater flexibility and cost control, which is crucial given network security’s dynamic and evolving landscape.

☑ Security fabric

A hybrid mesh firewall, however robust, is only part of your broader security infrastructure. Today’s security also requires a comprehensive and integrated cybersecurity architecture that provides advanced protection and visibility across the entire network infrastructure. This approach must combine a full range of security solutions, including firewalls, endpoint protection, secure access, and cloud security, into a unified framework and tools that enable and support a modern security operations center (SOC). A well-designed security fabric enables organizations to detect and respond to threats in real time, automate security policies, centralize configurations, and share threat intelligence across different security components, creating a cohesive and effective defense against cyberattacks.

A Partner You Can Trust

Security purchasing decisions are about more than just technology. They are about building a partnership that may continue long after the product’s end of life. It is vital to work with a vendor with a long history of innovation and investment in technology, service, support, and, above all else, security research so you can remain ahead of your cyber adversaries. Metrics worth considering include the partner’s R&D budget, global presence, analyst validations, number of patents filed, breadth of an integrated portfolio, and a history of uncovering zero-day threats.



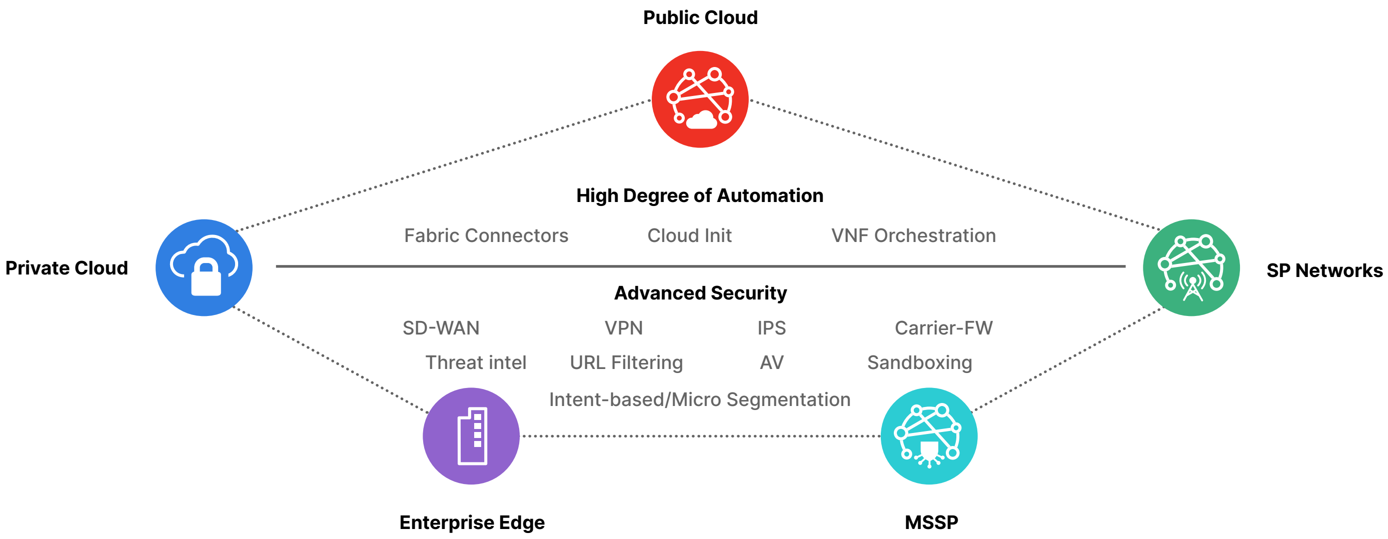
FERTINET

FortiGate Virtual Next-Generation Firewall

The FortiGate VM delivers NGFW capabilities for organizations of all sizes, with the flexibility to be deployed as an NGFW or VPN gateway. It protects against cyberthreats with high performance, security efficacy, and deep visibility.

FortiGate VM delivers protection from a broad array of network security threats. It offers the same security and networking services included in the FortiOS operating system and is available for public, private, and Telco Cloud (VNFs). A consistent operational model across hybrid cloud, multi-cloud, and service provider environments reduces the training burden on security teams.

FortiGate is available for all major hypervisors and supports all major clouds. See the FortiGate Virtual Appliance data sheet for details.



Network Perimeter Security

Protect networks from unauthorized access and external threats. Control traffic based on protocols, ports, applications, and user identities.

Application Control

Enforce application-specific security and traffic policies with application control.

Threat Detection

Utilize AI/ML-driven threat intelligence to detect ingress and egress traffic threats without impacting performance.

Segmentation

Isolate threats and prevent breach transversal with advanced network segmentation.

Secure Remote Access

Allow remote workers and branches to securely access resources with IPsec VPN and SD-WAN technology.

Secure Cloud Connectivity

Enable secure networking to, from, and between clouds with FortiGate VM.

FORTINET

CASE STUDY

Water Treatment Company Improves Customer Service and Performance With Private Cloud

Tower Water provides water treatment, cooling tower, and heating, ventilation, and air conditioning (HVAC) cleaning services for high-rise buildings in New York City, northern New Jersey, and Philadelphia. The family-owned business was founded in 1992 by Russell and Noah Baskin, and its client list includes famous high rises, premier A-class buildings, among others.

Matthew Marlowe had been an IT consultant for the firm since 2012, and was brought on as the company's full-time IT director in 2018. His charter was to bring the growing company's IT infrastructure to current standards, boost its performance, and implement process improvements.

Modernizing a Legacy Cloud Architecture

At the time, Tower Water's IT infrastructure was largely public cloud-based. "Of course, such a setup brings the benefit of full disaster recovery capabilities and the ability to log in from anywhere," Marlowe observes. "However, our employees were seeing more and more issues with latency and performance, and this was starting to impact customer service. Fixing that was going to require us to buy more RAM, which would have doubled our subscription costs. We were also having more problems getting adequate support from our cloud provider and from third parties."

From a security perspective, Tower Water had minimal protection. "We did have an open source-based physical firewall, but other than that we relied on the built-in tools from our cloud provider," Marlowe recalls. "They did not offer web filtering or sandbox analysis, and only offered antivirus filtering at the network level."

Broadening Access to SCADA Architecture

This arrangement was satisfactory for Tower Water's business for a time, but it eventually became inadequate for several reasons. First, the growth of the company required a more mature infrastructure to avoid downtime and latency issues. Second, worker expectations were changing, with Tower Water employees requesting access to corporate resources from their personal devices to make them more productive in the field.

But a third factor really hit home with Tower Water's leadership: evolving customer expectations. Specifically, Tower Water maintains supervisory control and data acquisition (SCADA) devices on cooling towers atop high-rise buildings, which control the chemicals added to the water that circulates through the HVAC system. "These devices are called 'digis' in the industry—digital routers embedded with SIM cards," Marlowe explains. "They have static public IP addresses, and we were able to modify our legacy firewall's rules to allow only traffic from us. Although the traffic was not encrypted, it was secure enough for the way we operated."

TOWER WATER

> *"Moving to the virtual private cloud infrastructure will cost half as much as staying in the public cloud—and the infrastructure is more robust and secure."*

Matthew Marlowe
Director of IT, Tower Water

Details

Customer: Tower Water

Industry: Water Treatment Consulting

Location: Somerset, New Jersey

Business Impact

- Staff time savings up to 72 hours due to speedy deployment
- 50% savings in monthly private cloud costs compared with public cloud-based infrastructure
- 80% cost avoidance in monthly telco subscription by rerouting traffic using Fortinet SD-WAN

Now the owners of the high-rise buildings are requesting their own access to the digis on their properties. Tower Water realized that providing such access would require a new, more strategic approach to both networking and security.

Securing a New Virtual Environment

After researching available options, Tower Water decided to bring most of the company's services in-house with a new, virtualized infrastructure. Marlowe selected Nutanix AHV as the company's hypervisor. "Once that decision was made, I turned to finding a new threat management solution to protect this infrastructure," he explains.

An early question was whether to purchase a physical next-generation firewall (NGFW) or go with a virtual one. "Going virtual made the most sense since almost the rest of our infrastructure would be virtual," Marlowe states. "This simplifies maintenance and allows for full backups of the router rather than just configuration backups."

As Marlowe researched virtual firewall providers, he learned that Nutanix is a Fortinet Fabric-Ready Partner. This means that Fortinet and Nutanix leveraged the collaborative power of the Fortinet Security Fabric to develop and validate joint solutions. For Marlowe, that meant the FortiGate VM virtual NGFW was prevalidated and ready for deployment on Nutanix AHV. The Fabric-Ready solution resulted in greater controls, deeper visibility, enhanced security, and seamless policy enforcements in the virtual network. What is more, Marlowe had worked extensively with Fortinet technology at two other companies in the past, developing significant expertise with—and respect for—the technology. As a result, the decision to select FortiGate VM was an easy one.

Tower Water elected to add the unified threat management subscription bundle to the FortiGate purchase. This gives the company access to a number of Fortinet services, including advanced malware protection, sandbox analysis with FortiSandbox Cloud, application control, and intrusion protection. "FortiGate VM met our needs for everything," Marlowe asserts. "We now have a stable core firewall router, web filtering, virus protection, and secure VPN. And the fact that sandbox analysis is included in the subscription means that we can protect our network traffic from zero-day threats without adding another line item of cost."

Business Impact (contd.)

- Unscheduled downtime reduced from 4% to none
- Customers can access their own SCADA devices—securely and easily
- Peace of mind from being able to afford 24×7 support because of choosing a virtual NGFW

Solutions

- FortiGate Secure SD-WAN
- FortiGate VM
- FortiSandbox Cloud
- FortiGuard Security Services
- FortiCare 24×7 Service

> *"FortiGate met our needs for everything. We now have a stable core firewall router, web filtering, virus protection, VPN, and secure SD-WAN."*
>
> **Matthew Marlowe**
> Director of IT, Tower Water

Saving Time and Money With Deployment

Some aspects of the deployment are still in progress, but Tower Water is already realizing tangible value from its Fortinet deployment. One quick win was with the speed of the initial deployment. "Even with my relatively high level of expertise, such a project typically takes a week or two of uninterrupted work," he says. "With FortiGate VM, I was able to go from an open box to fresh configurations in a single day. Of course, I made tweaks after that, but the basic system was up and running." This represents a savings of 32 to 72 hours of staff time compared with a typical deployment.

The company has also realized cost savings from the software-defined wide-area network (SD-WAN) capabilities in the FortiGate VM. "The building we are in uses Bigleaf Networks for network routing," Marlowe explains. "We are on a minimal, 50-megabyte-per-second plan with them. This means that we have potential latency problems when traffic is high. Rather than buying more capacity from Bigleaf, we are using FortiGate Secure SD-WAN to route some traffic directly to the Verizon cellular network when needed, bypassing Bigleaf altogether. This helps us avoid an 80% increase in our monthly subscription fees to scale their service."

Realizing Many Additional Benefits

Tower Water is also realizing cost savings in its move from a public cloud to a virtualized, private cloud environment with Nutanix and Fortinet. “Long term, we found that this was clearly the right solution for us,” Marlowe contends. “Looking at monthly expenditures over five years, moving to the private cloud, virtual infrastructure with Nutanix and Fortinet will cost half as much as staying in the public cloud—and the infrastructure is more robust and secure.”

Avoidance of downtime is another benefit. “We were down 4% of the time with our public cloud infrastructure, and we continually struggled to convince our cloud providers that it was their problem and not ours,” Marlowe recalls. “Since we have deployed our virtual, private cloud infrastructure nine months ago, we have not had any unscheduled downtime. This means our employees in the field can service customers whenever they need to.”

Another customer service benefit is the ability for building owners to access their own digis—which will be rolled out in the near future. “Our digis now connect with the FortiGate VM VPN, and the traffic is encrypted,” Marlowe describes. “And we will soon provide VPN accounts to our customers to enable them to access the devices on their buildings.” Using intent-based segmentation capabilities in the FortiGate VM, Marlowe will create firewall rules that provide each external user with access to the devices he or she owns—but block their access to all other devices and the rest of the network.

Fabric-Ready Partner

- Nutanix

“Everything just works—the products, the integration, the support. I expect this Fabric-Ready partnership to meet our needs for a long time to come.”

Matthew Marlowe
Director of IT, Tower Water

Operationally, the seamless Integration between FortiGate VM, FortiSandbox Cloud, and Nutanix is a huge timesaver. “This was probably the biggest factor that led us to choose Fortinet,” Marlowe says. “The ability to spin up FortiGate VM instances instantaneously in Nutanix—and make ongoing modifications on the fly—will save countless hours of my time over the years.”

Benefiting From a Strong Leadership

Marlowe subscribed to FortiCare 24×7 support for the virtual NGFWs. “The fact that we went with FortiGate VM means that 24×7 service was financially feasible for our small company, as it is less expensive than with an appliance,” he explains.

Around-the-clock availability of support brings significant peace of mind despite the fact that Marlowe has not needed to use it much. “I actually did not need to call them at all during deployment,” he recalls. “I did call them about one issue after deployment, and they diagnosed and fixed it within an hour. My experience at other companies is that FortiCare support is bar none.” Marlowe is also a big fan of the Fortinet Cookbook, which is full of tips and best practices. “I used several of its recipes to deploy FortiGate VM for our specific environment.”

For Marlowe, Tower Water’s relationship with Nutanix and Fortinet is strong. “Everything just works—the products, the integration, the support,” he concludes. “I expect this Fabric-Ready partnership to meet our needs for a long time to come.”

FORTINET

Related Products

NGFWs are powerful tools with a seemingly endless array of features, but they don't stand alone. Your firewall should be part of a firewall mesh that extends across platforms and part of a broader security fabric, one that encompasses support tools (central management, sandboxing, analytics) and additional security solutions (WAF, EDR, XDR, NDR, MDR, endpoint security, SOAR, identity management). Some important related products include:

FortiManager

FortiManager delivers unified management for consistent security across complex hybrid environments for protection against security threats. Key benefits include accelerated zero-touch provisioning with best-practice templates for deployment at scale of SD-WAN and streamlined workflows between the Fortinet Security Fabric and integrations with 300+ ecosystem partners.

FortiManager provides granular device and role-based administration and zero-trust multi-tenancy deployments for large enterprises and a hierarchical objects database for re-use of common configurations to serve multiple customers for clear visibility of every device and user on the network.

Highlights:

- Single-pane management and provisioning
- Fabric automation
- Monitoring and visibility
- Security policy and objects management

FortiAnalyzer

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

Integrated with the Fortinet Security Fabric, FortiAnalyzer enables network and security operations teams with real-time detection capabilities, centralized security analytics, and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.

Highlights:

- Centralized network monitoring and visibility
- Advanced threat and vulnerability detection with event and log data correlation
- Augmented NOC/SOC operations for real-time response, analytics, and reporting
- Automation to save time, reduce errors, and improve efficiency
- Multi-tenancy solution with quota management
- Administrative domains for operational effectiveness and compliance
- 70+ reports and 2,000+ ready-to-use datasets, charts, and macros

FortiSandbox

FortiSandbox detects and analyzes zero-day malware and other advanced file-based threats. The combination of service and product provides a comprehensive, coordinated, integrated, and scalable approach to advanced detection and protection from file-based zero-day threats. Inline sandboxing offers the industry's first inline blocking on an NGFW. Flexible deployment options include Platform-as-a-Service, SaaS, virtual machine, and hardware appliances to suit any use case and type of organization.

FortiGate CNF Cloud-Native Firewall

FortiGate Cloud-Native Firewall is a managed firewall service that removes complexity while improving security efficacy and supporting consistent security policies across different AWS environments. Organizations with no infrastructure to manage can focus on their business operations in the cloud, easily deploying effective security policies to protect their business-critical applications and data. FortiGate CNF is based on FortiOS and offers the same level of security managed by the same tools as FortiGate VM.

FortiGate CNF is designed for three critical use cases:

- Outbound traffic inspection: Content inspection of outgoing traffic from AWS workloads to the internet
- Inbound traffic protection: Deep visibility into incoming traffic and advanced security measures to protect AWS workloads
- East-west traffic filtering: Inspection and control of traffic between AWS VPCs and preventing the lateral spread of threats

Additional Resources

Data Sheets

- FortiGate Virtual Appliances Data Sheet
- FortiGate VM ESXi Data Sheet
- FortiOS Data Sheet

Fortinet Document Library

Ordering Guide for Cloud and Virtual NGFWs

Free Product Demo

[1] “Cost of Data Breach Report,” IBM, 2023.

[2] Fortinet 2023 Cloud Security Report.

[3] Ibid.

[4] “Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025,” Gartner, Feb. 20, 2023.

[5] “2023 CyberRatings.org Enterprise Firewall Report,” CyberRatings.org, accessed Sept. 5, 2023.

[6] Ibid.

www.fortinet.com

September 26, 2023 9:26 PM

2343766-0-0-EN