



Data Center Firewall Toolkit

Table of Contents

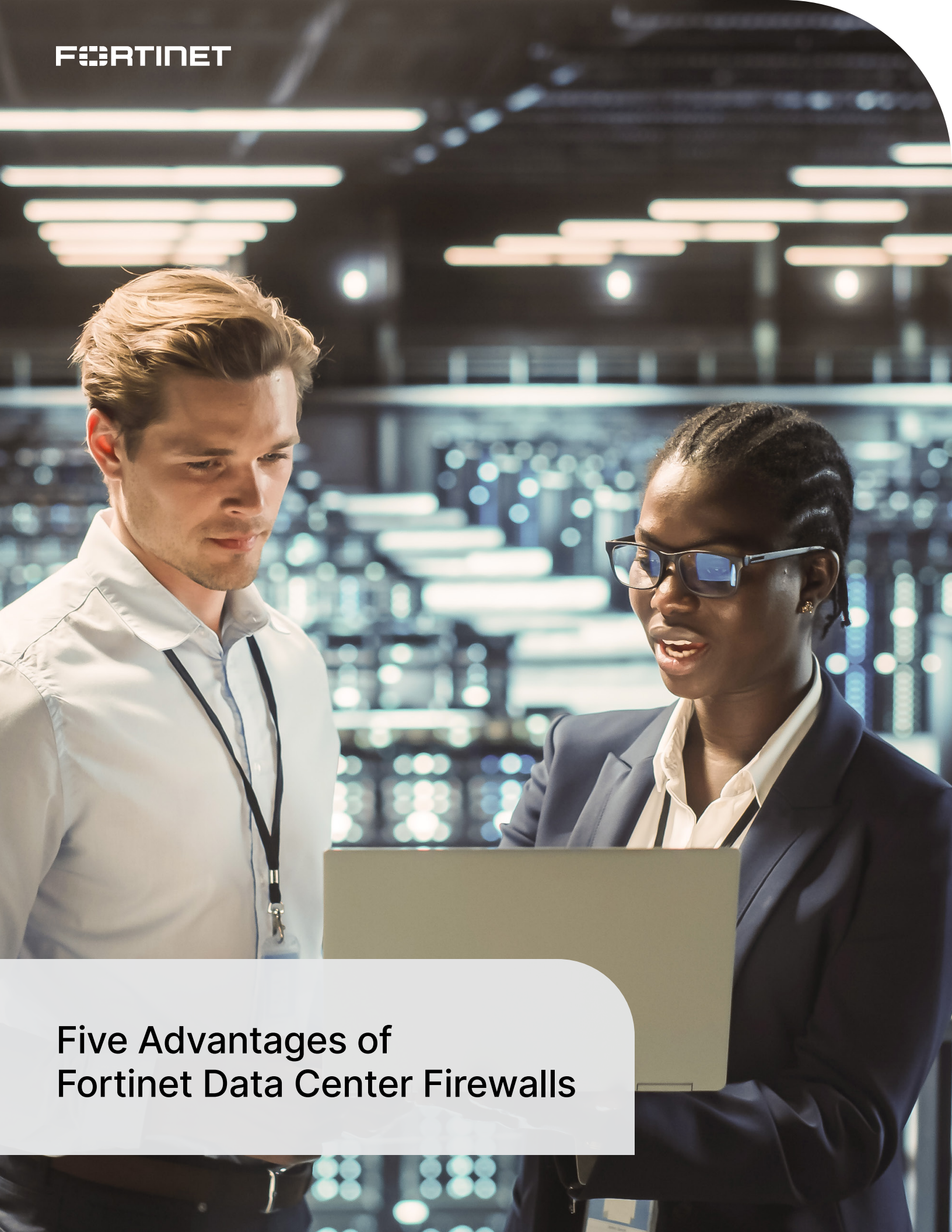
Five Advantages of Fortinet Data Center Firewalls 3

Industry Insights: Boost Your Data Center’s Performance
and Security with FortiGate 7000F Series 8

Checklist: Top Six Recommendations to Improve
User Productivity With a Hybrid Architecture11

Case Study: USI Insurance 13



The background of the entire page is a photograph of two IT professionals in a data center. On the left, a man with light brown hair, wearing a white button-down shirt and a lanyard, is looking down at a laptop. On the right, a woman with dark hair and glasses, wearing a dark blue blazer over a white shirt, is also looking at the laptop and appears to be speaking. The data center background is filled with rows of server racks and glowing blue lights, creating a high-tech atmosphere.

Five Advantages of Fortinet Data Center Firewalls

Executive Overview

Digital transformation has profoundly impacted how businesses operate, enabling companies to leverage advanced technologies to improve efficiency, productivity, and innovation. This shift from traditional, manual processes to more automated, data-driven approaches has led to better customer experiences and increased profitability. It has also had an intense impact on IT networks.

With the vast amount of data now traversing the network through physical, virtual, and cloud IT infrastructures, the central importance of the data center in today's distributed networks cannot be ignored. And because of this, securing today's complex data center environments must be a top priority.

Fortinet's comprehensive portfolio of data center cybersecurity solutions, including FortiGate Next-Generation Firewalls (NGFWs), enable organizations to build the dynamic, hybrid environments organizations need without compromising on security or performance.

Here are the top five reasons to choose Fortinet for your next data center firewall solution.



Highest Performance

Fortinet is the only vendor to leverage custom ASIC technology to support the high-performance and resource-intensive requirements of today's data centers. We are also the only vendor to offer scalable 400G I/O ports with integrated routing for ultra-low, single-digit microsecond latency. This emphasis on performance delivers critical advantages: By processing and analyzing data more quickly, FortiGate firewalls identify and block potential threats in real time. Encrypted data and streaming video can be inspected without impacting network performance. And faster network speeds ensure that applications can be optimized for better productivity and a consistent user experience.

Fortinet's data center firewalls deliver five times the performance of the industry average, eight times the industry average for SSL inspection throughput,¹ and three times the industry average for firewall throughput.^{2,3}

Advanced Threat Protection

The FortiGuard AI-Powered Security Suite leverages artificial intelligence (AI) and machine learning (ML) to provide advanced threat protection across its comprehensive security portfolio. It continuously assesses risks and automatically responds to and counters known and unknown threats across all threat vectors, including network, endpoint, cloud, and application security. And because FortiGate data center firewalls are also natively part of the Fortinet Security Fabric, they are fully integrated into the extended fabric, ensuring coordinated detection and enforcement across your entire attack surface. This unique framework approach can rapidly adjust its security posture to detect and respond to newly discovered attacks, regardless of where in your network they occur.

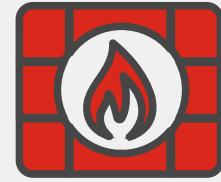
- **Enhanced threat detection:** ML algorithms detect advanced threats that traditional security solutions may miss to identify and respond to threats more quickly and effectively.
- **Proactive threat response:** AI-powered automation responds to threats in real time to contain and remediate threats before they can cause significant damage.
- **Improved accuracy:** AI and ML improve the accuracy of threat detection, reducing false positives and providing more accurate threat intelligence.

- **Reduced security management overhead:** Consolidating security functions reduces complexity while lowering costs and improving efficiency.
- **Scalability:** High scalability allows businesses to add new security functions and increase capacity without additional management overhead.
- **Comprehensive coverage:** Comprehensive security covers all threat vectors, including data center, campus, branch endpoint, cloud, and application security.
- **Advanced functionality:** The only vendor to include SD-WAN, ZTNA, inline sandboxing, and SOC-as-a-Service in their firewall platform.

Unified FortiOS

FortiOS is the unified operating system (OS) that runs the broad portfolio of technologies that are part of the Fortinet Security Fabric. This includes our [hybrid mesh firewall](#) (HMF), a unified security platform for deploying consistent management and analytics across your entire distributed network. This unified OS approach delivers comprehensive visibility and protection against security threats, simplifies operations, ensures compliance, and reduces complexity to increase operational efficiency. It also authenticates and grants explicit access to applications and data center resources, allowing organizations to consolidate crucial security and networking capabilities.

- **Enhanced security:** Consistently enforces policies across all security devices to protect against advanced threats, including ransomware malware, viruses, and other cyberattacks.
- **Simplified management:** Its unified management console reduces the time and resources required to manage security, allowing IT teams can focus on other priorities.
- **Improved visibility:** Broad deployment delivers deep visibility into network activity and security events so administrators can identify and respond to security threats quickly and effectively.
- **Increased scalability:** High scalability allows businesses to extend capacity without having to manage multiple operating systems to reduce complexity and enable faster growth.
- **Better performance:** FortiOS is optimized for performance, providing the industry's fastest and most reliable security across all devices.



Fortinet's unique converged approach also enables our firewalls to be seamlessly incorporated into a hybrid mesh firewall architecture that "enables security policy controls to be defined and workloads connected on any network in on-premises-first organizations."⁴

According to IDC, Fortinet holds the No. 1 position for units shipped at more than 8.4 million for a market share of 48%.⁵

Enhanced Sustainability

Fortinet data center firewalls are the most energy-efficient in the industry, helping organizations save on energy consumption and reduce their carbon footprints. Our FortiGate data center firewalls are also designed to operate with high efficiency and low power consumption, reducing the total cost of ownership. They consume 66% less power than rival solutions,⁶ use 83% fewer watts per Gbps of throughput,⁷ and are 6.5X more energy-efficient (BTU/h per Gbps) than competitive solutions.⁸ As a result, Fortinet data center firewalls have earned the 2021 ENERGY STAR® certification, certifying that they meet the strict energy-efficiency guidelines set by the U.S. Environmental Protection Agency (EPA).⁹

Aggressive ROI

Fortinet data center firewalls, combined with our AI/ML security services, provide the best price-performance ratio in the industry, delivering an aggressive ROI. Current FortiGate customers have experienced the following:

- 50% lower cost for a global technology service provider¹⁰
 - 500 hours saved by the IT team at a top U.S. school district¹¹
 - \$5M saved through IT cybersecurity consolidation by a leading U.S. university¹²
 - \$800K saved by a North American bottler¹³
-
- Recognized as a Leader in the Gartner® Magic Quadrant™ for Network Firewalls 13 times¹⁴
 - Positioned highest for Ability to Execute in the 2022 Gartner® Magic Quadrant™ for Firewalls¹⁵
 - Received the highest scores for the Enterprise Data Center Use Case in the Gartner® Critical Capabilities for Network Firewalls four times in a row¹⁶
 - Recognized as a leader in the Forrester Wave™: Enterprise Firewalls, Q4 2022 report¹⁷ (Oct 2022)



Summary

Fortinet data center firewalls offer several critical advantages, including better performance, advanced threat protection, unified FortiOS, broad security coverage, energy efficiency, and a strong ROI. These advantages make Fortinet data center firewalls an excellent choice for organizations seeking high-performance network protection with an impressive ROI.



¹ The average of SSL Inspection throughput for all Fortinet firewall models for the data center versus an aggregate average of published SSL Inspection throughput data of similar competitive models.

² The average of IPv4 firewall throughput for all Fortinet firewall models for the data center versus an aggregate average of published IPv4 firewall throughput of similar competitive models.

³ Fortinet, [“A comprehensive data center cybersecurity solution,”](#) March, 2023.

⁴ Gartner, [Magic Quadrant for Network Firewalls](#), Rajpreet Kaur, Adam Hills, Tom Lintemuth, 19 December 2022.

⁵ Nancy Liu, [Fortinet Continues to Invest in Custom Chips to Power Security Offerings](#), SDX Central, 9 February 2023.

⁶ Based on new models of the 2022 FortiGate F series (compared to equivalent models from the previous generation).

⁷ FG-1000F versus competitors.

⁸ Fortinet Press Release, [“Fortinet’s Latest Next-Gen Firewall Helps Customers Achieve Sustainability Goals by Consuming 80% Less Power Than Rivals,”](#) 2 November, 2022.

⁹ Fortinet, [Sustainability Report 2022](#), February, 2023.

¹⁰ [Synacor case study.](#)

¹¹ [School District of Philadelphia case study.](#)

¹² [University of South Carolina case study.](#)

¹³ Available upon request with a signed NDA.

¹⁴ Gartner, [Magic Quadrant for Network Firewalls](#), Rajpreet Kaur, Adam Hills, Tom Lintemuth, 19 December 2022.

¹⁵ Ibid.

¹⁶ Gartner, Critical Capabilities for Network Firewalls, Adam Hills, Rajpreet Kaur, Thomas Lintemuth, 17 May 2023.

¹⁷ Forrester, [Forrester Wave™: Enterprise Firewalls, Q4 2022 report](#), Oct 2022.

Boost Your Data Center's Performance and Security with FortiGate 7000F Series

The Most Comprehensive Data Center Security Solution

What Is a Hybrid Mesh Firewall?

Data centers are in the midst of an evolution. Physical, virtual, and cloud infrastructures are converging and changing the nature of on-premises data centers. Some believe this trend toward hybrid networks spells the end of the data center as well as traditional data center security—but they are far from dead.

A data center will always be an important element of any architecture. Therefore, fortifying data centers remains as vital as ever. To secure the modern evolving data center, Fortinet has the industry's most comprehensive data center cybersecurity solution. It's called FortiGate 7000F Series Next-Generation Firewall (NGFW) and it offers increased threat protection, performance, and energy efficiency.

Significantly Better Than the Industry Standard

The FortiGate 7000F Series sets the standard for comprehensive data center security that protects mission-critical data across hybrid IT infrastructure. Performance and security are the two pillars of any NGFW, and, compared to the industry standard, the FortiGate 7000F Series delivers a security compute rating of:

- 5x NGFW performance
- 2x better threat protection
- 2x IPSec VPN throughput

Also, FortiGate 7000F Series is 73% more energy efficient per Gbps of firewall throughput compared to the industry standard. (To learn more about how our FortiGates compare to competing products, read the blog titled: Benchmarking Security Performance with Fortinet's Security Compute Ratings.)



FG-7000F Series NGFW

Fortinet Security Compute Rating Table

Specification	FortiGate 7080F	Secure Compute Rating	Industry Average	Palo Alto Networks PA-5450	Check Point QLS 800	Cisco Firepower 9300	Juniper Networks SRX 5800
Firewall (Gbps)	1190	2.9x	410	200	205	235	1000
NGFW (Gbps)	330	5.3x	62.5	-	96	29	-
IPSec VPN (Gbps)	370	3.4x	110	87	49	74	230
Threat protection (Gbps)	312	4.1x	76.8	123.6	30	-	-
SSL Inspection (Gbps)	320	11.4x	28	-	-	28	-
Concurrent sessions	600 million	3.6x	~166 million	100 million	32 million	195 million	338 million
Watts per Gbps Threat Protection	23.4	2.5x	58.5	23	93.9	-	-

Eliminate Point Products and Reduce Complexity

Like all FortiGate NGFWs, the FortiGate 7000F Series eliminates point products, reduces complexity, and enables the industry's best performance and return on investment (ROI).

Since our beginning, Fortinet has designed and built security devices so that they never become a performance bottleneck. The FortiGate 7000F Series continues to follow that founding principle, delivering 1.2 Tbps of firewall throughput coupled with 312 Gbps of threat protection—using 60% fewer watts of Gbps threat protection compared to the industry average.

Scaling without disrupting operations is a concern for many organizations, which is why the FortiGate 7000F Series was built to reduce the need for point products and simplify operations. It includes a high-power, energy-efficient eight-slot chassis that can house up to six Fortinet Processor Modules (FPMs) and includes 400GE ports that empower businesses to meet their evolving needs. (Fortinet remains the only firewall vendor to offer 400GE ports.)

The ASIC Advantage

Like all FortiGate solutions, the cornerstone of the FortiGate 7000F Series's performance and power savings is proprietary ASIC security processing units (SPU) specifically engineered for security and networking purposes.

Our NP7 network processor delivers trail-blazing VXLAN hardware acceleration and IPsec Elephant flows. The NP7 is designed to accelerate essential network functions such as IPv4, IPv6, Multicast, GRE, and IPsec decryption, among others. And the FortiGate 7000F Series supports 4.5 million connections per second session setup speeds for firewall and NAT sessions, supplying hyperscale security for hyperscale data centers.

Accelerating Security Functions

The FortiGate 7000F Series also addresses the need to find and mitigate risk as quickly as possible. Our CP9 content processor acts as a co-processor to the main CPU to offload resource-intensive processing and drive content inspection to accelerate security functions. Additionally, the CP9 performs fast inspection of real-time traffic for application identification, all without compromising user experience. It enables full network visibility, thus eliminating blind spots.

The parallel path processing architecture embodied with our latest NP7 and CP9 security processors offers unmatched L4-L7 performance. These all-new capabilities build on the industry-leading security and threat detection included in all of the Fortinet NGFW offerings:

- The FortiOS operating system is the foundation of the Fortinet Security Fabric—the industry's highest-performing cybersecurity mesh platform that delivers coordinated detection and enforcement across the entire attack surface. FortiOS is a single operating system that provides centralized and unified management and visibility across the network.
- FortiGuard AI-Powered Security Services, developed by FortiGuard Labs (the Fortinet elite cybersecurity research organization), counter threats in real time with machine-learning-powered, coordinated protection.
- Intrusion prevention provides the most up-to-date defenses against stealthy network-level threats to protect organizations from thousands of IPS signatures covering known vulnerabilities and exploits.
- Application control service quickly creates policies to allow, deny, or restrict access to applications or entire categories of applications to keep malicious, risky, and unwanted applications out of your network through control points like the data center.



Hybrid Mesh Firewall Ready

As businesses increasingly turn to hybrid environments to address the rise in cloud-based applications and remote workforces, it's critical for NGFWs, including solutions like the FortiGate 7000F Series, to work in conjunction with firewalls deployed across the network—including in the cloud.

Hybrid mesh firewall (HMF) is an emerging term for a unified security platform that provides coordinated protection to multiple areas of enterprise IT, including corporate sites such as branches, campuses, and data centers; public and private clouds; and remote workers.

Because FortiGate and all other Fortinet firewall solutions were and continue to be built on FortiOS, we have delivered on the HMF concept for years. Using Fortinet solutions empowers IT teams with centralized and unified management and an open ecosystem that enables consistent security policies across all firewall deployments.

To learn more about the FortiGate 7000F Series and our associated services for the data center, visit the Fortinet NGFW web page.



CHECKLIST

Top Six Recommendations to Improve User Productivity With a Hybrid Architecture

The speed of business is accelerating the data center's journey toward digital transformation, requiring new hybrid network architectures that combine on-premise data centers with hybrid clouds. However, to meet the needs of organizations expanding their digital transformation, the underlying enabling technologies must be more reliable, energy-efficient, and secure than ever.

On-premises and virtual data centers are vital pieces in today's ever-evolving networking puzzle. In this new model, security is essential—not just to protect resources and assets but to enable the network to accelerate and adapt without introducing unknown risks that can jeopardize the enterprise.

Here are six things organizations need to do to position themselves for success.

- ☒ **1. Invest in a Flexible Next-Generation Firewall**

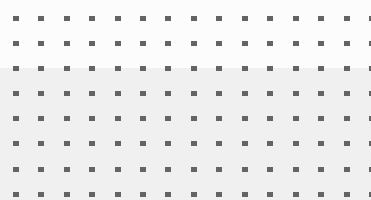
Organizations need to invest in a next-generation firewall that includes technologies like SD-WAN, universal ZTNA, in-line sandbox, and SOC-as-a-Service. These technologies improve WAN connectivity by providing better user experience with direct internet access, while LAN and WLAN provide faster access to local devices and users. In addition, organizations should consider investing in network firewalls that utilize Application-Specific Integrated Circuits (ASICs). They are designed for a specific application or purpose, such as accelerating network security functions beyond general-purpose CPUs.
- ☒ **2. Deploy Unified Networking and Security**

Security can't be an afterthought. When security solutions are not well-integrated with each other or the underlying network, security risks and gaps arise as the attack surface expands and adapts. These blind spots are vulnerable to sophisticated multi-step attacks and are partly responsible for the dramatic rise in successful ransomware attacks. Hence, it is important to look for a unified security framework to deliver automated and reactive security that spans the entire attack surface. Organizations also need to converge their security with networking to protect digital acceleration efforts.
- ☒ **3. Combining Zero Trust Edge Strategy With Consistent Security and Networking**

With new network edges being created on-premises and in the cloud, it is critical that the unified convergence of networking and security be available everywhere, combined with ZTNA to enable explicit access for applications and continuous verification of users and devices. This convergence is the heart of a Zero Trust Edge strategy. Also, flexibility in providing this convergence is key in securing digital acceleration for hybrid deployments.
- ☒ **4. Speed Operations With Centralized and Automated Management**

The exponential growth of network edges, cloud platforms, and tools can significantly increase operational complexity. Furthermore, poor visibility of and analytics gaps in the network along with tasks performed manually degrade the end-to-end digital experience.

These issues increase the time to configure, manage, and troubleshoot. They also add to operation costs and errors that can cause network outages and reduce flexibility. With centralized and automated management and a dashboard able to span the whole network and security stack, the delivery of network services across their entire life cycle is expedited. Removing manual configuration eliminates a major cause of downtime and security breaches.





5. Increase Visibility With End-to-End Digital Experience Monitoring

Traditional network performance monitoring, IT infrastructure monitoring, and application performance monitoring provide NOC teams with limited visibility. These types of monitoring don't provide the performance insights into critical business applications that customers need. They also severely hinder the visibility that frontline NOC and help desk teams need to resolve issues.

A modern digital experience monitoring platform is required to give your NOC team superior visibility. It allows for the observation of any application, starting from the end-user, across any network, and to the infrastructure the application is hosted on. It can enrich incident management and supply holistic remediation of performance issues.



6. Consolidate and Simplify Operations To Provide Instant ROI

Organizations adopting modern networking technologies with integrated security achieve better ROI than point products with limited security. Furthermore, it improves employee productivity with better user experience and simplified operations.

Conclusion

Many organizations still use a traditional architecture to connect offices to the data center for application access. However, with users working from anywhere and applications distributed across multi-cloud/SaaS environments, this legacy network design is an obstacle for digital acceleration and creates user experience challenges. Organizations that want to have better user productivity and secure network edges need to invest in a modern hybrid network architecture.

Fortinet is the only vendor in the industry to offer an NGFW that includes SD-WAN, universal ZTNA, in-line sandbox, and SOC-as-a-Service that can protect any edge at any scale. Offering the best convergence of networking and security, Fortinet empowers organizations to adopt modern networking technologies essential for digital acceleration. Forrester's [Zero Trust Edge Model](#) validates Fortinet's convergence approach.



CASE STUDY

Insurance Broker USI Ensures WAN Security Plus Higher Performance, Less Downtime, and Streamlined Management

As one of the world's largest insurance brokerage and consulting firms, USI Insurance Services works with a wide array of businesses and individuals, specializing in the delivery of property and casualty insurance, employee benefits, personal risk, and program and retirement solutions.

USI has been on a dramatic growth trajectory ever since its founding in 1994. In less than 30 years, it has ballooned from 40 employees generating \$6.5 million in annual revenue to more than 9,000 associates and more than \$2 billion in revenue. "We have experienced hypergrowth," explains Senior Network Engineer Joe Mogelinski. "I have been with USI for about six years, and the company has doubled in size since I started."

This hypergrowth has resulted in a corporate wide-area network (WAN) that spans the United States. Mogelinski's team of three network engineers is responsible for network and security management, with assistance from about 25 regional IT operations professionals. A group of analysts set security policy and monitor security events, "but they are not the ones deploying the technology," Mogelinski says. "For the three of us to manage networking and security in 182 offices from coast to coast, it is imperative that we minimize complexity."

Eye-Opening Deployment of Data Center Firewalls

As an insurance brokerage and consulting firm, USI handles highly sensitive information, most of which resides in the company's two data centers. And until recently, all communication to and from the 182 offices was backhauled to the data centers. Thus, the top cybersecurity priority for Mogelinski and his team has long been securing the network edge.

That is why, when the headend firewalls in the data centers needed a refresh a couple of years ago, the team evaluated multiple options to be sure they were using the best possible technology. USI's security analysts had relied on the FortiSIEM security information and event management solution for several years. Still, most of the company's networking and security infrastructure—including the data center firewalls—was standardized on another industry leader. USI considered FortiGate Next-Generation Firewalls (NGFWs), the legacy edgeseurity solution, and another competitor.



"We had a bake-off among the three heavy hitters from the Network Firewall Analyst Report. We weighed all the pros and cons. We ended up replacing our legacy firewalls with FortiGates, and once we deployed the Fortinet solutions, we fell in love."

Joe Mogelinski
Senior Network Engineer,
USI Insurance Services

Details

Customer:
USI Insurance Services

Industry: Insurance

Headquarters:
Valhalla, New York

**Number of Secure SD-WAN
Locations:** 182

"We had a bake-off among the three heavy hitters from the Network Firewall Analyst Report," Mogelinski says. "We weighed all the pros and cons. A huge negative for the legacy firewalls was that they were very difficult to manage and maintain. As a result of our analysis, we ended up replacing our legacy firewalls with FortiGates, and we introduced FortiManager and FortiAnalyzer to manage them. Once we deployed the Fortinet solutions, we fell in love." USI engaged FortiCare Professional Services to help with the implementation and to bring Mogelinski and his team up to speed. "We quickly got good at managing them," he says. "Right away, we were very happy with the firewalls' ease of management and performance." They also liked the Fortinet licensing model.

"Fortinet offers the hardware as it is," Mogelinski says. "You can plug into any of the interfaces and expect to get whatever throughput the datasheet says. Unlike some of Fortinet's competitors, which require you to buy additional licensing for the firewalls to reach their full capability, you do not have to have a second tier of licensing to reach the FortiGates' published speeds."

All in all, this first experience with FortiGates "opened our eyes," Mogelinski adds. "We said, 'If we are getting this much out of these devices, in this segment of the network, what happens if we add Fortinet solutions in other places?'"

Nationwide Rip and Replace

A couple of years later, Mogelinski had the chance to answer that question, as the firewalls and software-defined WAN (SD-WAN) throughout USI's many offices needed a refresh. The complexity of the legacy infrastructure put a perpetual strain on the network engineering group. They liked the idea of consolidating SDWAN networking and security in a single device at each location.

Plus, Mogelinski asserts: "We already knew how well the FortiGates were securing the headends. We implicitly trusted that technology to protect our offices as well. We were somewhat invested in the legacy product, but we decided to switch to Fortinet and start fresh. We did a proof of concept for Fortinet Secure SD-WAN, and everybody at USI agreed that transitioning the entire WAN infrastructure to FortiGates was a no-brainer."

The rollout itself proved the wisdom of that decision. USI standardized on a single firewall model with a cable modem and multiprotocol label switching (MPLS) connectivity. Mogelinski and his team built a tool to customize the firewalls' configuration. "Once we finished our proof of concept, we had a 'golden template,'" he says. "We used the configuration generator tool to plug in variables that differed from site to site, like IP address. Then the tool would generate a configuration for the firewall in the form of two files that we saved to a USB drive."

USI engaged a Fortinet technical account manager (TAM) for a year to support the rollout. "He hopped in right away and reviewed our SD-WAN design and configurations," Mogelinski says. "Within an hour, he was rattling off best practices that we had not included in the plan. He quickly became like part of our team. In fact, he was so helpful that we just renewed the TAM agreement for five more years."

Business Impact

- WAN downtime cut in half: From around 40 outages per year to fewer than 20.
- Internet connectivity up to 10x faster from office locations
- Network engineering team can focus on more value-added activities due to networking and security solutions' ease of management
- Less than five minutes of office downtime to roll out a new firewall
- \$1 million a year in savings on WAN hardware and support

Products and Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiSIEM

Services

- FortiCare Professional Services
- FortiCare Technical Account Manager

FortiGuard Security Services

- Antivirus
- Virus Outbreak Protection Service
- Intrusion Prevention System
- Anti-malware



Once deployment got underway, the SD-WAN project proceeded very quickly. When a firewall arrived at a USI office, an operations staff member would fly or drive there with the appropriate USB stick. “They would plug the USB stick into the new firewall, power it on, and in less than 10 minutes, the FortiGate was functional,” Mogelinski says. “The on-site folks would log off. The operations team member would literally move three cables from the old firewall to the FortiGate, and that was it. The process was seamless, and the downtime was well under five minutes per site.”

Within two months, all the company’s sites had been converted to FortiGate. “It is incredible, when you pick the right technology, how quickly and easily you can make it work,” Mogelinski adds.

“It is incredible when you pick the right technology how quickly and easily you can make it work”

Joe Mogelinski
Senior Network Engineer,
USI Insurance Services