FORTINET

Five Advantages of Fortinet Data Center Firewalls

Table of Contents

Executive Overview

Digital transformation has profoundly impacted business operations, 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 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), enables organizations to build the dynamic, hybrid environments they need without compromising 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: FortiGate firewalls can identify and block potential threats in real time by processing and analyzing data more quickly. 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 unmatched performance among firewall vendors, 5X the industry average for firewall throughput, 8X the industry average for SSL inspection throughput, and 3X the industry average for firewall throughput.[1]

The unique convergence of networking and security in Fortinet's patented ASIC enables FortiGate NGFWs to deliver higher throughput and lower latency while reducing power consumption, leading to better security performance and lower operating costs for your data centers.

- **Faster inspection and decryption:** By offloading the intensive tasks of decrypting SSL traffic from the CPU, Fortinet's ASIC helps reduce the time for data to pass through.
- **Accelerated DDoS protection:** Fortinet ASICs handle higher volumes of packets more efficiently than leading CPUs, allowing FortiGate devices to quickly identify and block abnormal traffic patterns.
- **Better fragmentation reassembly:** ASIC-enhanced FortiGates dramatically reduce latency and improve overall network performance, especially during peak traffic.
- **Boosted elephant flows:** Our patented ASICs can process large, long-lived flows more effectively than traditional CPUs to reduce the burden of network bandwidth in data centers.

Advanced Threat Protection

FortiGuard AI-Powered Security Services 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 they occur in your network.

- **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 them before they can cause significant damage.
- **Improved accuracy:** AI and ML improve threat detection accuracy, 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 Security Platform

FortiOS is the unified operating system (OS) that runs the broad portfolio of technologies that comprise the Fortinet Security Fabric. This enables the delivery of a single security platform for deploying consistent management and analytics across your entire distributed network. This unified 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 to 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:** FortiOS supports the broadest functionalities, allowing businesses to extend capacity without having to manage multiple operating systems, reducing complexity and enabling faster growth.
- **Better performance:** FortiOS optimizes CPU, memory, and other resources to minimize performance impact, providing the industry's fastest and most reliable security across all Fortinet devices.

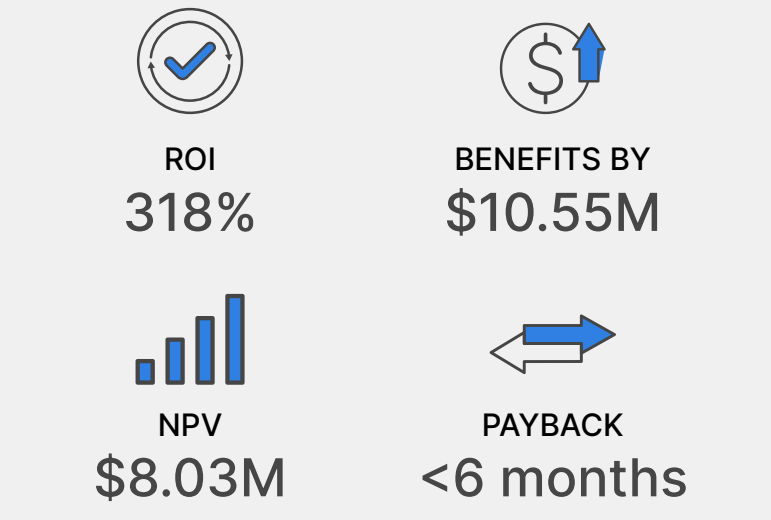
Fortinet holds the No. 1 position for units shipped, with over 50% of the global market share.[2]

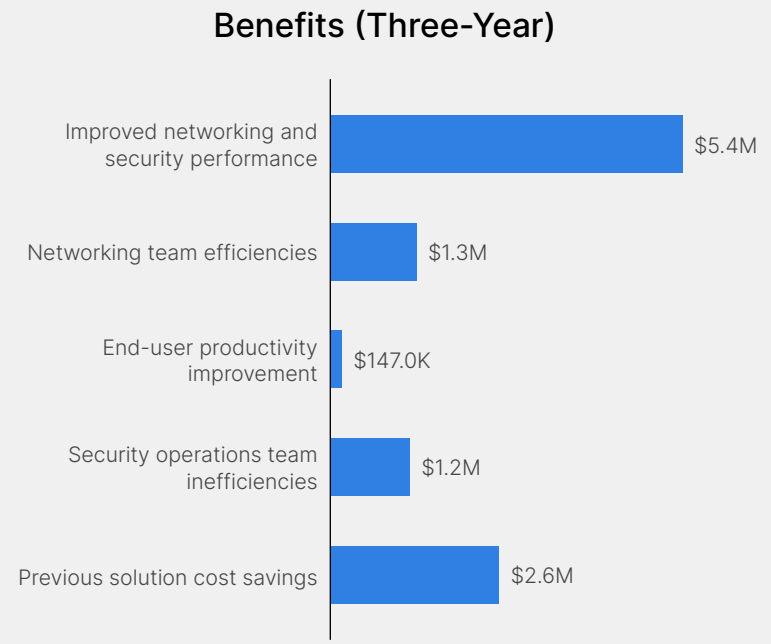
Enhanced Sustainability

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 84% fewer watts per Gbps of throughput and are 6.7X more energy-efficient (BTU/h per Gbps) than competitive solutions.[3]

Aggressive ROI

Forrester's Total Economic Impact (TEI) study shows FortiGate firewalls for data centers deliver 318% ROI over three years with a payback of less than six months. Key results include improved networking and security performance, increased networking and security team efficiencies, end-user productivity gains, legacy solution cost savings, and eco-friendliness for better sustainability.





FortiGate data center firewalls, combined with our AI/ML security services, provide the best price performance in the industry. They help USI Insurance improve network reliability, reduce operational costs, and achieve a better user experience.

USI Insurance: Convergence of Networking and Security

NGFW to secure the data center and edge

Customer Challenges

- **Data Center Migration** - move geographic locations and add a second DC
- **Simplification** - needed support for hybrid IT architecture
- **Network Complexity** - complexity of managing disjointed products

Why Fortinet

- **Fabric** - extend the secure fabric with FortiGates in both the data center and branch locations
- **Consolidation** - delivered consolidation and best ROI among all vendors
- **Visibility** - better visibility and management with FortiManager

Fortinet Solution

- FortiGate high-end securing the internet edge
- Intrusion prevention, virus outbreak protection service, anti-malware, and FortiSandbox Cloud

200+ locations

10,000 employees

$2.5B in revenue

Key Customer Benefits

10x faster application performance

50% fewer outages

40% lower connectivity costs

Summary

Fortinet data center firewalls offer several critical advantages, including better performance, advanced threat protection, a unified platform, 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 IPv4 firewall throughput, SSL Inspection throughput, and threat protection throughput for all Fortinet data center firewall models versus an aggregate average of published IPv4 firewall throughput, SSL Inspection throughput, and threat protection data of similar competitive models.

[2] 650 Group, Worldwide Network Firewall Vendor Shares, Q1 24. June 2024.

[3] The comparison is based on the published data from the FortiGate 1000F series and select firewalls in a similar price range.

FORTINET

www.fortinet.com

March 17, 2025 1:42 PM / MKTG-1109-0-0-EN