FORTINET

Top 5 Advantages of the Fortinet Secure AI Data Center Solution

Redefining Firewalls for AI Infrastructure with Speed, Scale, and Sustainability

Table of Contents

Executive Overview

As enterprises increasingly adopt AI-driven automation and integrate large language models (LLMs) into workflows, the volume of traffic, including sensitive of data, moving across networks surges. The increasing amount of AI data traverses the network across physical, virtual, and cloud infrastructure, introducing new performance and security challenges that cannot be ignored. And because of this, securing today's complex data center environments must be a top priority.

The Fortinet Secure AI Data Center solution includes a rich portfolio of FortiGate Next-Generation Firewalls (NGFWs) with integrated FortiAI-enriched protection, management, and analytics in a single platform. This combination enables you to build a dynamic, future-proof, security infrastructure for your AI data center environment without compromising security or performance.

Custom ASIC-Accelerated Performance

FortiGate data center firewalls, powered by patented ASIC technology, deliver hardware-accelerated security with inline inspection at scale without performance slowdowns. This performance advantage means that you'll get real-time threat detection and protection by processing and analyzing data faster than traditional data center firewalls. Encrypted data and streaming video can be inspected without impacting network performance, ensuring better application performance and consistent user experience. As the first vendor to offer high port density, up to 400 GbE, FortiGate supports massive AI workloads with ultra-low latency inspection to meet the most demanding data center requirements.

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 threat protection throughput.[1]

The unique convergence of networking and security in Fortinet's proprietary ASICs enables FortiGate data center firewalls to deliver higher throughput while reducing power consumption, leading to better security performance and lower operating costs for data centers.

- **Faster inspection and decryption:** By offloading the intensive tasks of decrypting SSL traffic from the CPU, Fortinet's ASICs help reduce the time it takes 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 ASICs can process large, long-lived flows more effectively than traditional CPUs to reduce the burden of network bandwidth in data centers.

End-to-End AI-Powered Protection

The Fortinet Secure AI Data Center solution leverages over 15 years of AI and machine learning (ML) innovation to provide advanced threat protection and dedicated LLM defense. It continuously assesses risks and automatically responds to known and unknown threats across all threat vectors, including network, endpoint, cloud, and application security. This unique framework can rapidly adjust its security posture to detect and respond to newly discovered attacks, regardless of where they occur in your network, delivering end-to-end protection.

- **Proactive threat detection and response:** Advanced algorithms identify and respond to emerging threats more quickly and effectively, containing and remediating them before they can cause significant damage.
- **Granular access control:** Advanced authentication and authorization enforce strict, privilege-based access to AI models, protecting sensitive data and reducing risk of internal and external misuse.
- **Zero-trust segmentation:** Isolation of AI workloads from other data center resources, prevents unauthorized east-west traffic and lateral movement. Every interaction is verified, minimizing the blast radius of any compromise.
- **Dedicated LLM defense:** Unique AI runtime security inspects all LLM inputs and outputs to ensure sanitized content in both directions, providing essential security control points throughout the AI workflow.
- **Multilayered security coverage:** Collaboration with FortiPAM, FortiWeb, and FortiDLP delivers one integrated policy framework across networks, users, applications, and data, eliminating the need for a patchwork of point solutions.

Quantum-Safe

Fortinet offers a range of quantum-safe communication methods and tools to empower you to define and adopt a post-quantum security posture. We protect against harvest-now, decrypt-later threats, empowering IT teams to safeguard today's critical data center traffic while staying ahead of tomorrow's quantum threats. Features include:

- **Quantum key distribution (QKD):** This technology allows two parties to exchange cryptographic keys securely and leverages the principles of quantum mechanics to detect any eavesdropping and hacking attempts. QKD offers unconditional security but does have scalability issues, so it's best suited for high-value applications rather than broad usage.
- **Post-Quantum Cryptography (PQC):** We include a robust list of new cryptographic algorithms believed to be difficult for quantum computers to solve. These include methods that rely on the difficulty of lattice-related mathematical problems and decoding error-correcting codes. PQC is readily deployable with few scaling issues, making it better for wide usage than QKD.
- **Enhanced IPsec with PQC:** This allows for secure communication over IP networks, even in the face of quantum computing threats.
- **Hybrid mode:** This mode enables the seamless integration of traditional public-key cryptography and PQC, supporting a gradual transition to PQC while maintaining compatibility with existing systems. By combining the strengths of both approaches, you can achieve a robust and adaptable security posture.
- **Algorithm stacking:** This technique combines multiple cryptographic algorithms to create a more resilient security solution. By layering different algorithms, organizations can significantly enhance the security of their network infrastructure, increasing barriers to potential attacks.

Fortinet is ranked #7, the only cybersecurity company in the top 50, in the Forbes 2025 list of Most Trusted Companies in America.[2]

Operational Efficiency

As part of the Fortinet Security Fabric platform, the Fortinet Secure AI Data Center solution optimizes operational efficiency by streamlining network management, automating security enforcement, and reducing manual intervention. The integration of FortiGate data center firewalls, AI-powered protection, and agentic AI management ensures seamless performance, scalability, and centralized control, enabling faster response times and optimized resource utilization.

- **Consolidated security posture:** Consistently enforces policies across all devices to protect against known and unknown threats, including those targeting high-value data center assets and east-west traffic.
- **Simplified management and visibility:** The single platform enables all Fortinet products and services to work seamlessly, reducing the time and resources required to deploy devices and manage security. Visibility is gained into network activity and security events, so administrators can identify and respond to security threats quickly and effectively.
- **Operational simplicity:** FortiManager provides "one console, one policy" to streamline management for traditional and AI workloads, reducing complexity introduced by AI startups that require separate tools and interfaces.
- **Compliance and audit readiness:** FortiAnalyzer delivers advanced logging, audit trails, and data classification, helping enterprises comply with emerging AI regulations and ensure data governance and transparency.
- **Scalability:** High scalability allows businesses to add new security functions and increase capacity without additional management overhead.

Aggressive ROI with Sustainability

FortiGate NGFWs are the most energy-efficient firewalls in the industry, helping organizations save on energy consumption and reduce their carbon footprints. FortiGate firewalls are 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]

In addition, the Fortinet Secure AI Data Center solution unifies FortiGate NGFWs and FortiAI capabilities into a single, integrated platform, delivering the best price-per-performance in the industry. Fortinet enables organizations across industries to optimize operational efficiency, stay ahead of evolving threats, and achieve the best TCO from their investments.

CUSTOMER SUCCESS STORY

City of Aurora: Performance without Complexity

Fortinet helps the city of Aurora modernize its data center and edge infrastructure with greater visibility into threats and security events, enhanced connectivity, and millions in cost savings on networking and security.

Customer Challenges

- High operational costs from multiple legacy solutions and siloed IT staff
- Lack of security features, segmentation, and robust security measurement, especially for critical infrastructure

Why Fortinet

- Single OS enables seamless interoperability and reduces complexity and costs
- Centralized visibility and real-time reporting and analytics optimize operational efficiency
- AI-enriched security intelligence proactively detects and blocks malicious threat and events
- Segmentation provides added level of protection to critical infrastructure
- Secure SD-WAN balances network traffic and optimizes secure connectivity

Key Customer Benefits

$5M+
in savings on devices and services over five years

$150K
reduction in annual electricity expenses

66%
faster for switch configurations

92%
in time savings on VPN configurations

2x
the bandwidth and boosted network performance

Summary

The Fortinet Secure AI Data Center solution offers several critical advantages, including better performance, advanced threat protection, a unified platform, broad security coverage, energy efficiency, and quantum-safe features. These advantages make Fortinet an excellent choice for organizations seeking high-performance data center protection with 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] 2025 Most Trusted Companies in America, Forbes, November 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

December 4, 2025 4:48 PM / MKTG-2404-0-0-EN