SOLUTION BRIEF

Protect Your Hybrid Network's Expanding Attack Surfaces with FortiGate Next-Generation Firewalls

Executive Summary

The network attack surface has dramatically expanded with the rapid proliferation of the mobile workforce, multi-cloud adoption, and Internet-of-Things (IoT) devices. Enterprise IT teams must defend corporate sites that have direct internet access, such as branches and campuses, on-premises data centers, public clouds, and remote workers. However, effectively and efficiently securing all of your attack surfaces can be very complicated and difficult. In fact, a recent report found that 84% of organizations have suffered a breach caused by a failure in controls in the past 12 months. It also showed that cybersecurity teams are overwhelmed with data, and on average use 61 different tools and 58 reports or dashboards.[1]

FortiGate Next-Generation Firewalls (NGFWs) offer a game-changing solution to stop today's sophisticated, evasive threats and zero-day attacks. By leveraging over 15 years of FortiGuard Labs security and AI/ML expertise, FortiGates deliver the highest level of threat protection. Add to that seamless scalability, unparalleled performance, and simplified policy management across appliances, cloud, and hybrid deployments, and you have the ideal hybrid mesh firewall solution to secure even the most complex distributed networks.

If cybercrime were a nation in 2026, it would be the world's third-largest economy, behind the U.S. and China, costing businesses an estimated $20 trillion.[2]

Distributed Networks Are a Larger Target

New technologies help organizations become more efficient and expand geographically, but this also changes the network infrastructure. These hybrid and distributed environments come with more attack surfaces and inconsistent controls across locations. To address these and future challenges, FortiGate NGFWs:

- Reduce complexity and costs by consolidating products and services
- Stop even the latest and most sophisticated threats with integrated, real-time security services
- Deliver transparency and control by inspecting all types of traffic—from clear text to encrypted (SSL/TLS)—with no performance slowdown
- Enable visibility and automation with access to network and security events for contextual visibility, while simplifying operations with automated processes
- Include quantum-safe defenses for protection now and in the future

FortiGate NGFWs and the Fortinet Security Fabric: Consolidation and Integration

FortiGate NGFWs simplify security complexity with consolidation and help deliver end-to-end security with integration into the Fortinet Security Fabric. The firewalls uniquely include secure SD-WAN and ZTNA capabilities without additional licenses, providing support for distributed branches and remote users at no extra cost, easily and simply.

As a key component of the Fortinet Security Fabric platform, FortiGate NGFWs work seamlessly with Fortinet products and solutions to secure organizations with coordinated, automated, policy-based responses to accelerate time to resolution. When a FortiGate NGFW detects an event, it communicates with the Security Fabric, which determines what information will be shared across the enterprise. For example, when malware is detected in one part of the organization, the Security Fabric shares threat intelligence with the rest of the IT infrastructure. In addition, when a policy is created for one security solution, the Security Fabric can contextually apply that same policy across other security solutions in the architecture for consistent control.

All deployed FortiGate devices across the network infrastructure are interconnected via the single, integrated Security Fabric platform. This integration provides comprehensive, real-time protection while simplifying deployment and reducing the need for multiple touchpoints and policies across the enterprise.

Top Performance: Custom-Built ASICs

FortiGate NGFWs also deliver protection that keeps pace with the accelerating demands of high-performance enterprise networking. Every FortiGate NGFW appliance is powered by a patented security processor with the industry's only converged security and networking chip. This unique innovation enables FortiGate NGFWs to provide extremely high throughput and exceptionally low latency while delivering proven security effectiveness.

Regardless of where the firewall is deployed, with FortiGate, there is no need to choose between security and performance. The FortiGate NGFW family includes flexible form factors with a variety of price-performance points that can be deployed at the enterprise edge, data center edge, or branch offices to provide secure access to multiple clouds. FortiGate NGFWs can also be deployed in the data center as part of an intent-based segmentation solution.

Fortinet is recognized in 11 Gartner® Magic Quadrants™ and is named a Leader in the Hybrid Mesh Firewall, Wired and Wireless LAN Infrastructure, and SASE Magic Quadrant reports.

Industry-Leading Security Effectiveness: FortiGuard Labs

Extensive knowledge of the threat landscape and the ability to respond quickly at multiple levels are the foundations for effective network security. FortiGate NGFWs leverage AI-powered threat intelligence services from FortiGuard Labs to deliver top-rated security and immediate protection against known, AI-driven, and zero-day threats.

The FortiGuard Labs global threat research team collaborates with Fortinet product developers to ensure dynamic security intelligence services. Security updates are delivered automatically across the Security Fabric for real-time protection.

Fortinet receives consistently high marks in real-world security effectiveness tests including Cyber Ratings.org,[3] NetSecOpen,[4] and Virus Bulletin,[5] due to our combination of in-house research, information from industry sources, and advanced machine-learning capabilities. Third-party verification shows that our threat intelligence is highly accurate and effective.

Optimized Operational Efficiency with GenAI-Driven Management: FortiManager

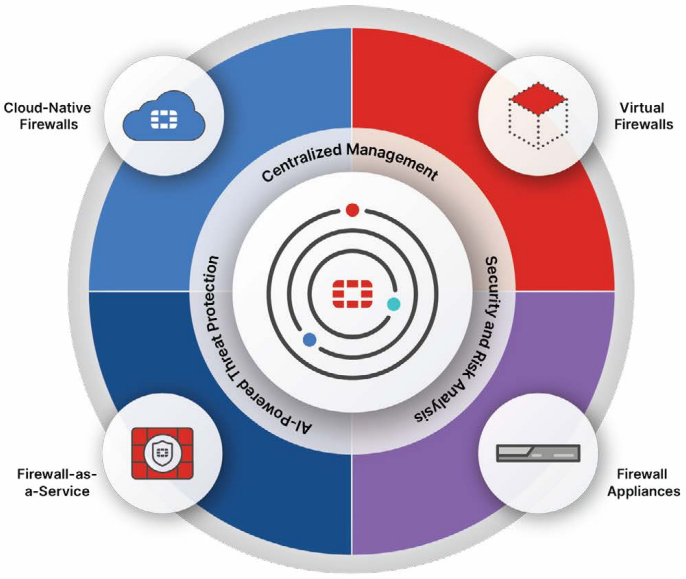

Figure 1: FortiGate helps distributed enterprises unify network security and simplify management.

Centralized security management and visibility consolidate multiple management consoles into a single pane of glass and enable automation-driven management. Specifically, a highly intuitive view of applications, users, devices, threats, cloud service usage, and deep inspection gives network engineering and operations leaders a better sense of what is happening on their networks. This strategic view allows them to easily create and manage more granular policies to optimize security and network resources.

FortiManager provides unified management and visibility across the entire network and connected devices. Network leaders can transparently observe traffic and set consolidated policies with granular security controls. With FortiAI-Assist, network management is automation-driven and analytics-powered, delivering actionable insights and streamlined operations through a unified single-pane-of-glass console.

Enabling Future-Proof Defense: Quantum-Safe Security

The rapid evolution of quantum computing makes quantum-safe security a business imperative. Organizations can leverage the built-in quantum-safe features in FortiOS to defend against emerging threats, including harvest-now, decrypt-later attacks. Additional support for Quantum Key Distribution (QKD) integrations enables interoperability with leading QKD vendors via standardized interfaces. This capability underscores Fortinet's proactive approach to quantum-resilient network security by integrating quantum-safe key exchange mechanisms into our NGFW architecture.

Security without Compromise: FortiGate NGFWs

FortiGate NGFWs incorporate robust, forward-looking security to protect all attack surfaces in hybrid and distributed enterprises with one easy-to-manage solution. Our hybrid mesh firewall approach simplifies deployment, ensures consistent controls, and offers flexible form factors. With Fortinet, you can deliver proven, high-performance security across your entire infrastructure.

[1] The Security Leaders Peer Report 2026, Panaseer, November 2025. https://resources.panaseer.com/reports/2026-security-leaders-peer-report/

[2] Bernard Marr, The 7 Cyber Security Trends Of 2026 That Everyone Must Be Ready For, Forbes, September 26, 2025. https://www.forbes.com/sites/bernardmarr/2025/09/26/the-7-biggest-cyber-security-trends-of-2026-that-everyone-must-be-ready-for/

[3] Morningstar, CyberRatings.org and NSS Labs Announce Follow-On Enterprise Firewall Results, November 25, 2025. https://www.morningstar.com/news/pr-newswire/20251125da32764/cyberratingsorg-and-nss-labs-announce-follow-on-enterprise-firewall-results

[4] Fortinet, NetSecOpen Certifies FortiGate Next-Generation Firewall with 99.98% Security Effectiveness, accessed December 15, 2025. https://www.fortinet.com/corporate/about-us/product-certifications/netsecopen

[5] Fortinet, Virus Bulletin, accessed December 15, 2025. https://www.fortinet.com/corporate/about-us/product-certifications/virus-bulletin

Gartner, Magic Quadrant for Email Security, By Max Taggett, Nikul Patel, 1 December 2025.

Gartner, Magic Quadrant for Security Information and Event Management, By Andrew Davies, Eric Ahlm, Angel Berrios, Darren Livingstone, 8 October 2025

Gartner, Magic Quadrant for Hybrid Mesh Firewall, By Rajpreet Kaur, Adam Hils, Charanpal Bhogal, Esraa ElTahawy, Feng Gao, Tiffany Taylor, 25 August 2025

Gartner, Magic Quadrant for Endpoint Protection Platforms (EPP), Evgeny Mirolyubov, Franz Hinner, Deepak Mishra, 14 July 2025

Gartner, Magic Quadrant for SASE Platforms, By Jonathan Forest, Neil MacDonald, Dale Koeppen, 9 July 2025

Gartner, Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure, By Mike Leibovitz, Christian Canales, Nauman Raja, Tim Zimmerman, 25 June 2025

Gartner, Magic Quadrant for Security Service Edge, By Charlie Winckless, Thomas Lintemuth, Dale Koeppen, Charanpal Bhogal, 20 May 2025

Gartner, Magic Quadrant for Data Center Switching, By Andrew Lerner, Simon Richard, Nauman Raja, Jorge Aragon, Jonathan Forest, 31 March 2025

Gartner, Magic Quadrant for Cyber-Physical Systems Protection Platforms, By Katell Thielmann, Wam Voster, Ruggero Contu, 12 February 2025

Gartner, Magic Quadrant for Access Management, By Brian Guthrie, Nathan Harris, Yemi Davies, Steve Wessels, 11 November 2025

Gartner, Magic Quadrant for Privileged Access Management, By Abhyuday Data, Paul Mezzera, Shubham Gera, Tarun Rohilla, Michael Kelley, 13 October 2025

December 20, 2025 10:10 PM / MKTG-2641-0-0-EN