FORTINET FEDERAL

SOLUTION BRIEF

# Modernize Networks, Cut Costs, and Strengthen Cybersecurity with Fortinet Federal

## Executive Summary

United States federal agencies continue to struggle with effectively mitigating today's increasingly sophisticated cyberthreats with a strained budget and insufficient staffing. Multiple mandates, including executive orders and memorandums ranging from adopting zero-trust architecture[1] to returning to in-person work,[2] drive how federal IT and security professionals must ensure cybersecurity. In the case of returning to the office, cybersecurity focus will need to shift from remote office security to modernizing networking and security at government offices of all sizes. Federal agency security infrastructure may have to be upgraded or replaced to keep up with ever-evolving and AI-driven threats, achieve modernization initiatives, and comply with mandates.

Federal agencies need an innovative security platform that strengthens their cybersecurity posture while meeting complex demands within tight budget constraints. Fortinet offers a unique, proven approach that consolidates technologies and converges networking and security, enabling agencies to modernize network and security infrastructure while lowering costs. Fortinet Federal has extensive experience and expertise working with federal agencies to deliver solutions that exceed unique agency requirements for procurement, security efficacy, support, and cost.

Fortinet has been recognized as a Leader in the inaugural 2025 Gartner® Magic Quadrant™ for Hybrid Mesh Firewall, with the highest placement for Ability to Execute.[3]

## Solutions That Deliver Comprehensive Security While Lowering Costs

Fortinet adopts a holistic approach to cybersecurity with an integrated platform, the Fortinet Security Fabric, enabling seamless, efficient operations with consistent and consolidated AI-powered protection across the entire infrastructure. As the core of Fortinet Security Fabric, FortiGate Next-Generation Firewalls (NGFWs), also known as hybrid mesh firewalls, coordinate with other security devices. This enables collection and analysis of security data across the entire network to help agencies reduce complexity, eliminate security silos, and optimize user experience.

Built on patented Fortinet security processors, FortiGate NGFWs accelerate security and networking and mitigate security risks with consistent, real-time protection and responses against even the newest and most sophisticated AI-enabled threats. By converging security and networking in a single operating system (FortiOS), management is simplified, visibility is improved, and costs are reduced. FortiGate NGFWs offer a multitude of features and benefits, including:

- **Unified management** reduces complexity and automates security posture across all edges.
- **Lower TCO** is achieved with built-in SD-WAN, routing, LAN/WLAN/WWAN controller, and zero-trust capabilities.
- **Secure direct internet access** aids compliance with TIC 3.0 requirements.[4]
- **Microsegmentation** isolates secure zones in a data center or cloud environment.
- **Custom ASICs** enable inline SSL inspection with little to no impact on performance.
- **Comprehensive, integrated AI-driven security services** deliver real-time threat protection.

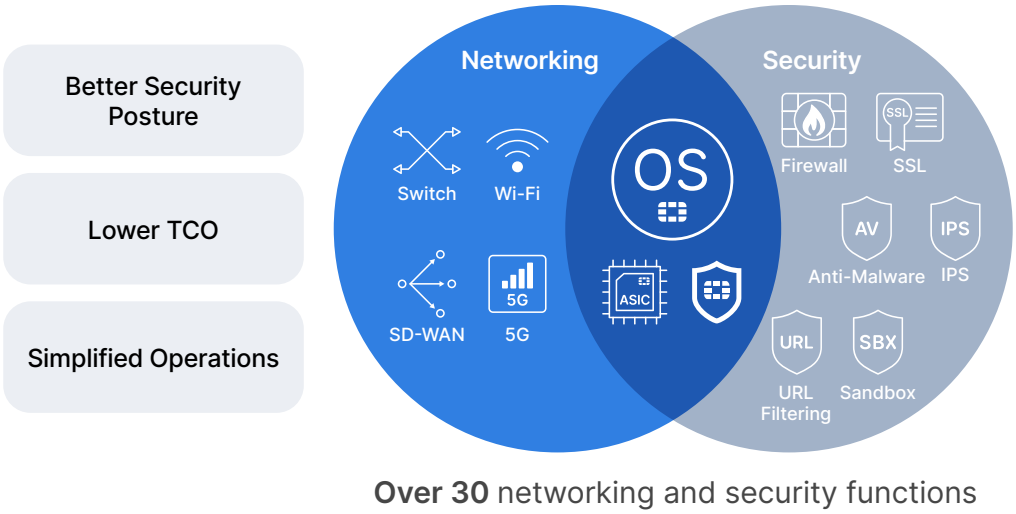


Figure 1: Networking and security convergence delivers better protection, simpler management, and faster performance.

## Key Federal Solution Components

**FortiGate NGFWs:** Options for every environment from the small remote office to hyperscale and AI data centers (flexible form factors include hardware appliances, virtual machines, as-a-service, ruggedized, and cloud-native firewall)

**Routing, SD-WAN, LAN/WLAN/WWAN controller features:** No additional license and no additional cost

**FortiGuard AI-Powered Security Services and FortiCare:** Full Layer 7 security inspection and 24×7 support

**FortiSwitch secure Ethernet switches:** Offer many features, including NAC, without additional licensing.

**FortiAP access points:** Centrally managed by the integrated WLAN controller of any FortiGate

**Professional services:** Optional service for transition and steady state operation

## Secure Solutions Tailored to U.S. Federal Government Agencies

With a sole focus on supporting U.S. civilian, intelligence, and defense organizations, Fortinet Federal offers technical and contracting advantages to agencies including:

- **Exceptional supply-chain security** with products that are secure by design and FIPS certified: Fortinet Federal has one of the most robust and independently validated Security of Supply programs, developed in partnership with the Department of Defense. Fortinet Federal standard operations include voluntary additional testing and certification of hardware and software that exceeds those required by current Federal Acquisition Regulations (FAR and DFAR). Fortinet Federal also maintains independent warehousing, shipping, and technical support organizations that are 100% dedicated to U.S federal agencies to track security during the packaging and delivery process.
- **Risk-mitigated transitions:** Fortinet Federal engineers and implementation staff have the expertise and experience to plan, coordinate, and implement a transition program that minimizes risk, ensures no disruptions to critical operations, and quickly ramps up agency staff to handle ongoing operations. Fortinet Federal's professional services team is composed of vetted U.S. citizens who understand on-site agency project implementation requirements.
- **Simplified licensing, predictable costs:** Fortinet Federal uses simplified SKUs and part numbers that make contract administration easier to understand and manage. Most U.S. federal customers choose to purchase support and licensing through a single, bundled SKU. This simplifies the contracting process and eliminates hidden costs, resulting in predictable pricing for licenses and annual maintenance renewals.

## Vetting Fortinet Solutions

For agencies pursuing network modernization, Fortinet Federal offers resources designed to support informed planning and procurement. These resources include market research, product evaluations, and contract compliance. Agency staff can make informed decisions with:

- Technical deep dives with Fortinet Federal SMEs
- Product demonstrations and performance comparisons at a customer site, at the Fortinet Federal lab (in Reston, Virginia), or by virtual meeting
- Architectural and design analysis and recommendations
- Preliminary Bill of Materials with Rough Order of Magnitude pricing

FortiGate is the most widely deployed network firewall, with over 50% market share worldwide.[5]

## Procuring Fortinet Technology: Government Contracts and Partnerships

- Fortinet technology is available to U.S. Government customers through multiple contracts, including SEWP V, EIS, GSA-70, CIO-SP, and other GWAC and agency-specific contracts.
- Fortinet Federal partners with resellers, including small and small disadvantaged businesses, telecom carriers, and federal systems integrators that serve as prime contractors for specific agency requirements.

## Unrivaled Security and Federal Agency Expertise

Fortinet is an industry leader in secure networking. Fortinet is the first vendor to organically develop and integrate SD-WAN, NGFW, advanced routing, and ZTNA application gateway capabilities on a single platform. Fortinet is also the only vendor with purpose-built ASICs to accelerate and offload network and security functions. Fortinet's portfolio of over 50 enterprise-grade products is the largest integrated offering available, delivering proven cybersecurity everywhere you need it. More than 900,000 customers trust Fortinet solutions, which are among the most deployed, most patented, and most validated in the industry.

The Fortinet Federal team is dedicated to trusted cybersecurity for government. For additional information and support designing and implementing the most cost-effective and future-proof solution for your organization, please contact Fortinet Federal at info@fortinetfederal.com or at 1-833-386-8333.

[1] Shalanda D. Young, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, Executive Office of the President, January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[2] Charles Ezell, Guidance on Presidential Memorandum Return to In-Person Work, U.S. Office of Personnel Management, January 22, 2025. https://www.opm.gov/media/q0tbu2eq/guidance-on-presidential-memorandum-return-to-in-person-work.pdf

[3] Gartner, Magic Quadrant for Hybrid Mesh Firewall, By Rajpreet Kaur, Adam Hils, Charanpal Bhogal, Esraa ElTahawy, Feng Gao, Tiffany Taylor, 25 August 2025 https://www.fortinet.com/resources/analyst-reports/gartner-magic-quadrant-hmf

[4] U.S. General Services Administration, Trusted internet connections, U.S. General Services Administration, accessed May 28, 2026. https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/telecommunications-and-network-services/trusted-internet-connections

[5] 650 Group, Next Generation Firewall, 650 Group, accessed June 1, 2026. https://650group.com/reports/next-generation-firewall-ngfw

FORTINET FEDERAL®

www.fortinetfederal.com

Copyright © 2026 Fortinet Federal, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet Inc. or Fortinet Federal, Inc. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet or Fortinet Federal, and Fortinet and Fortinet Federal disclaim all warranties, whether express or implied, except to the extent Fortinet Federal or Fortinet enters a binding written contract, signed by authorized officials of Fortinet or Fortinet Federal (as the case may be), with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written.

**Fortinet Federal, Inc.**
12005 Sunrise Valley Drive, Suite 201
Reston, VA 20191

Phone: 1-833-386-8333
Email: info@fortinetfederal.com

July 3, 2026 10:24 AM / MKTG-2891-0-0-EN