FORTINET FEDERAL

ISSUE BRIEF

# Modernize Networks, Cut Costs, and Strengthen Cybersecurity with Converged Technology

## Fortinet Federal Delivers Trusted Solutions and Savings to the U.S. Government

In 2025, U.S. Federal agencies continue to face a significant dual challenge – confront and mitigate dynamic cybersecurity threats with increasingly strained budget and staff resources. Several current mandates drive how Federal IT and security professionals must act, including:

- Executive Order on Improving the Nation's Cybersecurity EO 14028
- The Federal Zero Trust Strategy M-22-09
- OMB Memorandum on Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents M-21-31

Moreover, the new Executive Memorandum requiring a Return to In-Person Work may well require agencies to reassess networking and security infrastructure at offices that have insufficient capacity, or aging equipment. Some infrastructure may need to be upgraded, refreshed, or replaced to deal with the high bandwidth demands and expanding security needs of a resurging on-premise staff.

To meet the complex and competing demands to improve cybersecurity postures, agencies are looking to new technologies and innovative capabilities that will best support their operational requirements. Given the goals to simultaneously strengthen cybersecurity initiatives and modernize networking infrastructure, government personnel are required to consider vendor diversity, defense in depth, micro-segmentation, and zero trust strategies.

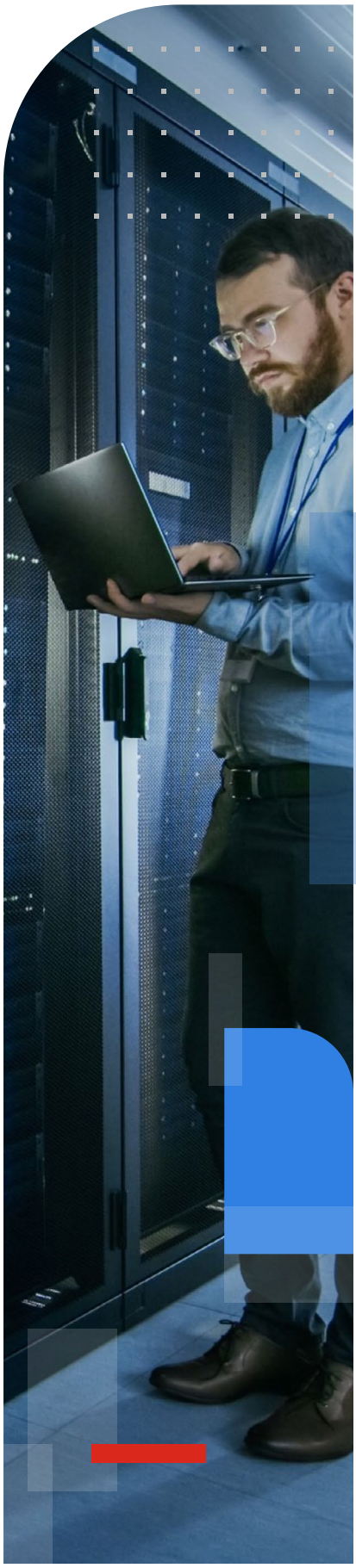
To address limited funding for new IT investment, one area of particular focus is reducing the significant annual investment in ongoing support and maintenance of legacy IT infrastructure. Traditional IT support and licensing arrangements, including Enterprise License Agreements (ELAs), can consume more than half of agency IT spending.

### Leverage New Technology to Secure the Enterprise and Drive Savings

New technologies that drive convergence of networking and security requirements provide agencies a compelling option for modernizing and upgrading their network and security infrastructure while driving down costs.

Fortinet offers this capability uniquely through its Next Generation Firewall (NGFW), which delivers a trifecta of benefits, including:

- First, the advanced cybersecurity protections of the NGFW provide for trusted direct Internet access and compliance with TIC 3.0 requirements.
- Second, the NGFW is a cost-effective, modernized router replacement.
- Third, it enables Software-Defined Wide Area Network (SD-WAN) capabilities at no additional cost or licensing.



With an agile, AI-enabled approach to network modernization, the Fortinet NGFW enables agencies to implement their priority cyber initiatives, tailored to their missions, including:

- A **Zero Trust Strategy** that leverages multiple security measures to protect enterprise IT assets from cyberthreats.
- **Micro segmentation** to isolate secure zones in a data center or cloud environment that enables IT administrators to gain more granular control over applications and workloads.
- **In-line SSL** inspection with minimal impact to performance.
- A full range of **security inspection and prevention capabilities** that focus on defeating sophisticated malware and ransomware.

Importantly, and unlike other offerings, the Fortinet NGFW combines routing and SD-WAN in the same platform, allowing for true convergence of networking and security technologies – consequently reducing CAPEX and OPEX.

Fortinet's NGWF also provides agencies flexibility to deploy technologies that meet their agency's operational demands today and as their networking requirements evolve:

- as hardware – on premise
- as virtual machines in private or public clouds, and
- in a hybrid cloud model

With Fortinet integrated technology, all of these capabilities are delivered in a single platform, operating system, and management interface – the combined savings of which can exceed 40% over traditional, multi-product, MPLS-based network architectures. Savings come from:

### Building Blocks of a Fortinet Federal Converged Solution

- **FortiGate Next Generation Firewall (NGFW)***
  - From FG-40F-USG for remote and home offices…to FG-4401F-TAA-FGDUS or greater for Data Centers and 400G connectivity
- **FortiManager and FortiAnalyzer:** For management, logging, and reporting
- **FortiGuard support & licensing bundle:** Full Layer 7 security inspection and 24×7 support
- **Professional Services:** Optional service for transition and steady state operation
- **Routing Features**: No additional license and no additional cost
- **SD-WAN Features:** No additional license and no additional cost

- Migration from expensive MPLS circuits to less expensive WAN technology
- Combining technologies in a single platform or product
- Lower product costs
- Operational efficiencies and lower ongoing support and licensing

## Drive Lower Costs with Industry-Leading Cybersecurity Technology

Fortinet's technology recently was named Gartner 2024 Peer Insights Customers' Choice for Network Firewalls and is a recognized leader in the Gartner Magic Quadrant for Network Firewalls in Ability to Execute.

That is one reason why the 650 Group states that "Fortinet is the #1 vendor for firewall shipments globally with more than a 50% (market) share," far exceeding any alternate technology provider. Further, Fortinet has an exceptional "catch rate" among cybersecurity vendors, with a 99.88% Security Effectiveness Score according to independent evaluator CyberRatings.org. Moreover, as the price-to-value leader, the Return-on-Investment with a Fortinet NGFW deployment, is significantly better than traditional approaches which do not leverage converged networking and security capabilities.

*Fortinet has a wide variety of FortiGate models tailored to specific customer requirements. These include devices with built in WiFi and 3G/4G and 5G connectivity, as well as ruggedized versions. All Fortinet NGFWs support routing and SD-WAN, and have built in switch and Access Point controllers at no additional cost.

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

With a sole focus on supporting U.S. Civilian, Intel, and Defense organizations, Fortinet Federal offers the following technical and contracting advantages to its agency customers:

- **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 comprises vetted U.S. citizens familiar with 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, which not only simplifies the contracting process, but also eliminates hidden costs and provides for predictable pricing for licenses and annual maintenance renewals.

**Deciding to Buy Means Deciding to Trust.**

Forbes recently ranked Fortinet in the Top Ten of the 2025 Most Trusted Companies in America.

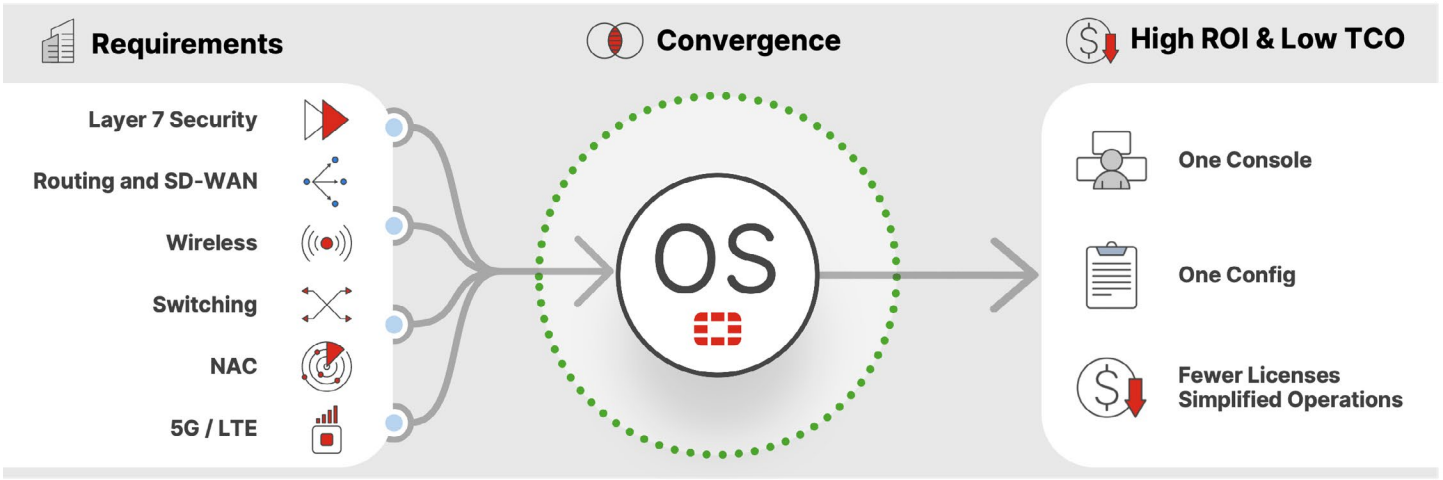
**No. 7: FORTINET**

Source: Forbes, Most Trusted Companies in America list. Edited By Alan Schwarz November 21, 2024

## Vetting Fortinet Solutions for your Agency

For agencies considering a network modernization initiative, Fortinet Federal provides a variety of resources to help cyber and network modernization contracting officials make data-driven decisions to support market research, product evaluation, and contract compliance. Agency staff can avail themselves of:

- 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
- Rough Order of Magnitude Bill of Materials and pricing



## Unrivaled Security, Unprecedented Performance.

FortiGate Next-Generation Firewalls (NGFWs) protect data, assets, and users across today's hybrid environments. Built on patented Fortinet security processors, FortiGate NGFWs accelerate security and networking performance to effectively secure the growing volume of data-rich traffic and cloud-based applications. FortiGate NGFWs, backed by FortiGuard AI-Powered Security Services, help you prevent cyberattacks and mitigate security risks with consistent, real-time protection and responses against even the newest and most sophisticated threats.

**17x**

Faster firewall performance than competition with leading standard CPUs

**62%**

Average reduction in product energy consumption

**99.98%**

Security effectiveness with perfect scores in 3 test scenarios

## 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.

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.**

FORTINET FEDERAL®

www.fortinetfederal.com



January 2025