WHITE PAPER

Fortinet Federal Government Cybersecurity Solutions

Efficiently Protecting U.S. Government Data and Critical Infrastructure Against Advanced Nation-state Threats

Executive Summary

U.S. federal agencies operate some of the world's largest and most complex digital networks, but many of them rely on older, legacy technology for critical operations. Add to this the fact that the federal government is highly targeted by nation-state adversaries and traditional criminals alike, and the need for comprehensive cybersecurity protection is readily apparent. Fortinet provides a platform that enables end-to-end integration of an agency's security architecture, and a broad suite of security and networking tools that addresses multiple use cases. An integrated security infrastructure allows for true automation of security processes, from detection to remediation.

"What will the OPM data breach cost the United States? ... [T]he total figure might eventually reach $1 billion."[1]

The U.S. federal government is massive, with more than 2 million full-time employees and hundreds of thousands of contractors who access electronic resources.[2] Some agencies within the federal government maintain some of the world's largest IT networks. Achieving an adequate level of cybersecurity protection at this scale would be a challenge at any organization. But the federal government owns some of the world's most sensitive—and coveted—data. And compromised systems could lead to disastrous consequences—for national security, the economy, and technological innovation.

Adversaries seeking to infiltrate federal government systems have a variety of motivations. Nation-state actors actively conduct cyber warfare, and they have been stepping up their game in recent years.[3] These adversaries attempt to steal national security secrets, take critical infrastructure offline, interfere in elections, and conduct industrial espionage.

In addition, federal government data is attractive to more common types of criminals, who seek personal and financial information that is valuable on the dark web. Targets range from the employment records of current and former federal employees to the tax returns of all Americans. The 2015 breach at the Office of Personnel Management (OPM), the government's civilian HR team, compromised very sensitive data on millions of current and former employees.[4]

The Department of Homeland Security is charged with helping federal agencies step up their cybersecurity efforts through new laws like the Cybersecurity and Infrastructure Security Agency Act of 2018.[5] Although this requirement comes with financial resources, many agencies have a long way to go,[6] and a fragmented cybersecurity strategy is not going to work—from either a policy or a technology perspective.

Key Federal Government Cybersecurity Challenges

Nation-state Threat Landscape

Many U.S. adversaries have been developing increasingly sophisticated cyber-warfare capabilities for years or even decades and are now stepping up those efforts. Many experts say that the U.S. is not well-prepared to defend itself against this growing threat.[7] The federal government is constantly targeted by nation-state actors who seek to conduct espionage, steal classified information, disrupt government operations, cripple critical infrastructure, interfere in elections, and erode citizens' trust in government. Combating all such threats is critical to national security and a well-functioning civil society.

Mission Continuity

Each federal government agency has a critical purpose, and business continuity must be a consideration for every decision. The consequences of operational disruption for almost any federal entity could impact the lives of thousands or even millions of people, and downtime can result from fast-moving malicious attacks that are difficult to catch by manually executed security processes. Operational stability can also be jeopardized by latency and the inability to fully coordinate action across the range of affected IT assets.

Resource Allocation

The Budget Control Act of 2011 reduced budgets across the board for most agencies. Moreover, Congress has frequently funded the government through stop-gap continuing resolutions lasting from months to the entire fiscal year. For most agencies, the result has been flat budgets that effectively shrink their spending power every year because of inflation. In addition, agencies' ability to execute "new starts" or programmatic initiatives is impeded when a continuing resolution is in force. The overall uncertainty curtails agencies' ability to plan for the future when it comes to cybersecurity. Lean budgets have resulted in heavy emphasis on cost reduction and careful analysis of return on investment (ROI) for new projects. Resource constraints also put the government at a disadvantage in dealing with the cybersecurity skills shortage,[8] as private companies are able to pay more for scarce talent.

> **"Given the sustained vulnerabilities identified by numerous Inspectors General, the Subcommittee finds that the federal government has not fully achieved its legislative mandate under [the Federal Information Security Management Act] and is failing to implement basic cybersecurity standards necessary to protect America's sensitive data."[9]**

Integration of Infrastructure

In response to a growing attack surface and an increasingly advanced threat landscape, agencies tend to deploy point security products to cover new gaps in protection. These solutions usually do not integrate or communicate with each other, resulting in security silos that obscure visibility and shared situational awareness. This ratchets up risk by potentially allowing threats to slip through a fragmented protection infrastructure. A disaggregated security architecture also reduces operational efficiency, as manual security workflows are required to bring a semblance of visibility and coordinated response to threats. Architectural silos also increase operational costs by creating redundancies in licensing, staff skills requirements, and product support needs.

Cloud Readiness

Many federal agencies continue to maintain their entire IT infrastructure in-house, with systems containing especially sensitive information sometimes air gapped from the internet. However, a growing number of agencies are now looking at cloud services as a way to stretch limited resources and increase efficiency.[10] Protecting a growing cloud infrastructure is a more recent business need for federal agencies than for most other industries, and security solutions must be ready to provide government-scale protection for cloud resources.

Compliance Reporting

All federal agencies are now required to adhere to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Many of them must comply with NIST guidance for multiple types of information—and demonstrate this compliance to auditors. Diverting staff from cyber operations to preparing audit reports is both time-consuming and an inefficient use of talent. The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program provides funding to help agencies upgrade their systems, and requires that cybersecurity systems be integrated to enable automated visibility and reporting.

Use Cases

Fortinet solutions for federal government customers address a variety of use cases, including the following:

On-premises Perimeter Security

Many federal agencies keep all their data in-house, and do not use technologies like Wi-Fi, software-defined wide-area networking (SD-WAN), or Software-as-a-Service (SaaS). Security concerns are certainly a part of the motivation behind this stance. In many cases, however, the bigger reason is reliance on older technology—which brings its own challenges as an aging infrastructure can have vulnerabilities not found in newer systems.[11]

This means that advanced firewall protection is especially critical for legacy systems. To prevent intrusions and breaches, agencies must be able to detect and deflect today's advanced and ever-evolving threats—including malware within encrypted network traffic—without slowing operations or impeding the agency's mission.

FortiGate next-generation firewalls (NGFWs) provide scalable, comprehensive protection for both older and newer infrastructure without slowing network traffic. Purpose-built application-specific integrated circuit (ASIC) chip processing results in the industry's best performance—even when large amounts of traffic encrypted with secure sockets layer (SSL) or transport layer security (TLS) encryption is inspected.[12] Built-in capability for **intent-based segmentation** ensures that network resources are adequately divided for appropriate access control, and built-in capability for SD-WAN ensures that agencies can offer secure and efficient services to their remote users and branch office locations. And **FortiGuard service bundles for FortiGate** help ensure protection against zero-day and polymorphic threats.

Multi-domain Networks

Federal agencies operate some of the nation's largest and most complex networks. Many exist across multiple IP domains, sometimes with each domain housing data at a different level of sensitivity and accessible to different groups of employees and contractors. This sprawling infrastructure creates challenges around visibility and centralized control, threatening both security and operational efficiency.

To provide the best protection and make the most efficient use of taxpayer resources, these massive networks need a coordinated and integrated approach to cybersecurity that extends across domains. End-to-end integration is the only way to unlock full visibility and automation of threat detection, response, and compliance reporting. As a result, projects funded by the Department of Homeland Security's CDM program require integration.[14]

The **Fortinet Security Fabric** provides a comprehensive, cross-domain security architecture that delivers single-pane-of-glass visibility and automation of security processes. **Intent-based segmentation** ensures that all resources in a network are accessible to those who need them and blocked from those who do not. **FortiNAC** network access control ensures that only authorized devices connect to the network, and **FortiManager, FortiAnalyzer,** and **FortiSIEM** provide visibility, control, and reporting capabilities that help leaders view their agencies' security posture at a glance.

Advanced Threat Protection

As discussed, nation-state adversaries mount growing numbers of attacks against the federal government, and common criminals continually seek information that is valuable on the black market. Threat actors are using increasingly sophisticated technology to make their attacks more effective. They use automation, artificial intelligence (AI), and machine learning (ML) to create more zero-day malware, make phishing emails more realistic, and develop attacks that can get through traditional security solutions. And they are starting to use things like swarm technology to accelerate their attacks and make them more effective.[16]

> "The high proportion of IT funding that goes toward keeping older government systems alive has frustrated lawmakers in oversight and appropriations hearings who say they want to see more money dedicated to modernization efforts."[13]

> "As the world becomes increasingly interconnected, we expect these actors to rely more and more on cyber capabilities when seeking to gain political, economic and military advantages over the United States and its allies and partners."[15]

To fight back, federal agencies must have robust, real-time threat intelligence and the insight to enable effective response. As new malware variants proliferate, it is also critical that effective detection of unknown or zero-day threats be a part of the mix. Integration of the security architecture is key, as it enables real-time sharing of threat intelligence across the infrastructure.

FortGuard Labs maintains one of the world's largest intelligence networks and has been using AI to detect unknown threats for nearly eight years. AI and ML capabilities are also integrated into the **FortiSandbox** sandbox analysis tool, the **FortiWeb** web application firewall (WAF), **FortiClient** and **FortiEDR** advanced endpoint security technology, and **FortiInsight** user and entity behavior analytics (UEBA). This coordinated and layered approach helps agencies discover zero-day attacks in real time while minimizing false positives and other productivity-draining threat-intelligence outcomes. It also improves cybersecurity staff productivity and decreases risk.

Zero-trust Access

Gone are the days when requiring a username and password to gain access to a network resource was adequate for cybersecurity, as the concept of trust is no longer static. Devices change IP addresses as they move around, stolen credentials are bought and sold on the dark web, and legitimate insiders can create threats of their own—accidentally or deliberately.

The resulting risk means that many federal agencies should operate under a zero-trust model, which replaces the concept of a trusted network with an approach in which all users and endpoints must be verified on a case-by-case basis, and access to data is set by policy or handled on a "need-to-know" basis. The zero-trust approach must be managed strategically, with logical network segmentation to keep unauthorized users away from specific resources and multiple layers of verification and compliance.

Robust **intent-based segmentation** features in **FortiGate NGFWs** provide the foundation for effective enforcement of zero-trust access by segmenting the network according to evolving business needs. **FortiAuthenticator** and **FortiToken** provide identity and access management to verify users, while **FortiNAC** network access control keeps tabs on devices. **FortiClient** and **FortiEDR** provide advanced endpoint security to help detect and remediate attacks on devices before they can spread on the network. **FortiInsight** UEBA technology watches for anomalies in behavior, while **FortiDeceptor** helps lure attackers into revealing themselves and generate useful threat intelligence on their tactics, techniques, procedures, and intent.

"[T]he [federal] government will likely spend $9.1 billion in fiscal year 2024 on cloud computing, an increase from $5.3 billion in FY2019."[17]

Common Operational and Security Awareness

Big federal agencies struggle to achieve full visibility into the entirety of their vast networks, whether their infrastructure is entirely on-premises or includes hybrid cloud deployments. And the larger federal government continues to lack integrated situational awareness of threats and vulnerabilities across agencies. This lack of visibility hampers the effort to respond to threats that move at machine speed. As a result, a coordinated attack on multiple agencies is often difficult to contain.

The Department of Homeland Security is keenly aware of this issue and is working a coordinated approach that includes providing resources to agencies to help them address this problem.[18] At the end of the day, the key lies in building a security architecture that is integrated across an entire agency, enabling centralized visibility and control and maximum automation of security processes and reporting.

The **Fortinet Security Fabric** provides this end-to-end integration, from the data center to multiple clouds to the network edge. This enables a more proactive, consistent approach to security across an agency. **FortiManager, FortiAnalyzer,** and **FortiSIEM** provide centralized visibility, control, and reporting with maximum automation. **FortiCWP** cloud workload protection tools extend this integration to a hybrid cloud network, and feature native integration with each major public cloud provider and a coordinated approach to securing all of them.

Third-party and Insider Threat Protection

Insider risk is a major threat at federal agencies—sometimes by employees acting with nefarious intent, but often by users who cause problems by accident. In addition to federal employees, tens of thousands of contract and third-party employees access federal networks and data, many off-site and under conditions over which the government exercises little control. With everything from critical infrastructure to military secrets to protect, agencies must diligently guard against third-party threats.

Assigning usernames and passwords is no longer adequate for federal agencies to protect against insider threats. Authorized people can access or share data inappropriately, and criminals can steal authorized users' credentials without their knowledge, sometimes moving laterally in the network for months before being detected. As a result, agencies must take a multipronged approach to insider threat protection, monitoring the behavior of users, inspecting devices when they request access, and proactively working to bring adversaries into the open.

Fortinet enables this kind of layered approach to threat protection in a fully integrated platform. **FortiAuthenticator** and **FortiToken** identity and access management solutions verify users, while **FortiNAC** network access control keeps tabs on devices. The **FortiClient** and **FortiEDR** advanced endpoint security tools help detect and remediate attacks on devices before they can spread on the network. **FortiInsight** UEBA technology watches for anomalies in behavior, while **FortiDeceptor** helps lure attackers into revealing themselves. In many ways, **intent-based segmentation** features in **FortiGate NGFWs** provide the foundation for insider threat prevention by segmenting the network according to specific operational and access requirements.

Fortinet Differentiators

These factors make Fortinet the best choice for federal government cybersecurity:

Performance at Scale

Fortinet provides NGFWs with purpose-built ASIC chip processing for high performance and low latency. The result is the industry's best performance.[19] And unlike many competing solutions, this performance is not impacted by SSL/TLS encryption inspection. This performance is maintained even at the massive scale of a federal agency.

Integration

The **Fortinet Security Fabric** delivers a flexible platform for building an end-to-end, integrated security architecture across multiple domains, highly classified systems, and cloud-based resources. An **open application programming interface (API)** and **Fabric Connectors** help federal agencies to integrate third-party tools for niche coverage and to maximize prior investments.

"As the world becomes increasingly interconnected, we expect these actors to rely more and more on cyber capabilities when seeking to gain political, economic and military advantages over the United States and its allies and partners."[20]

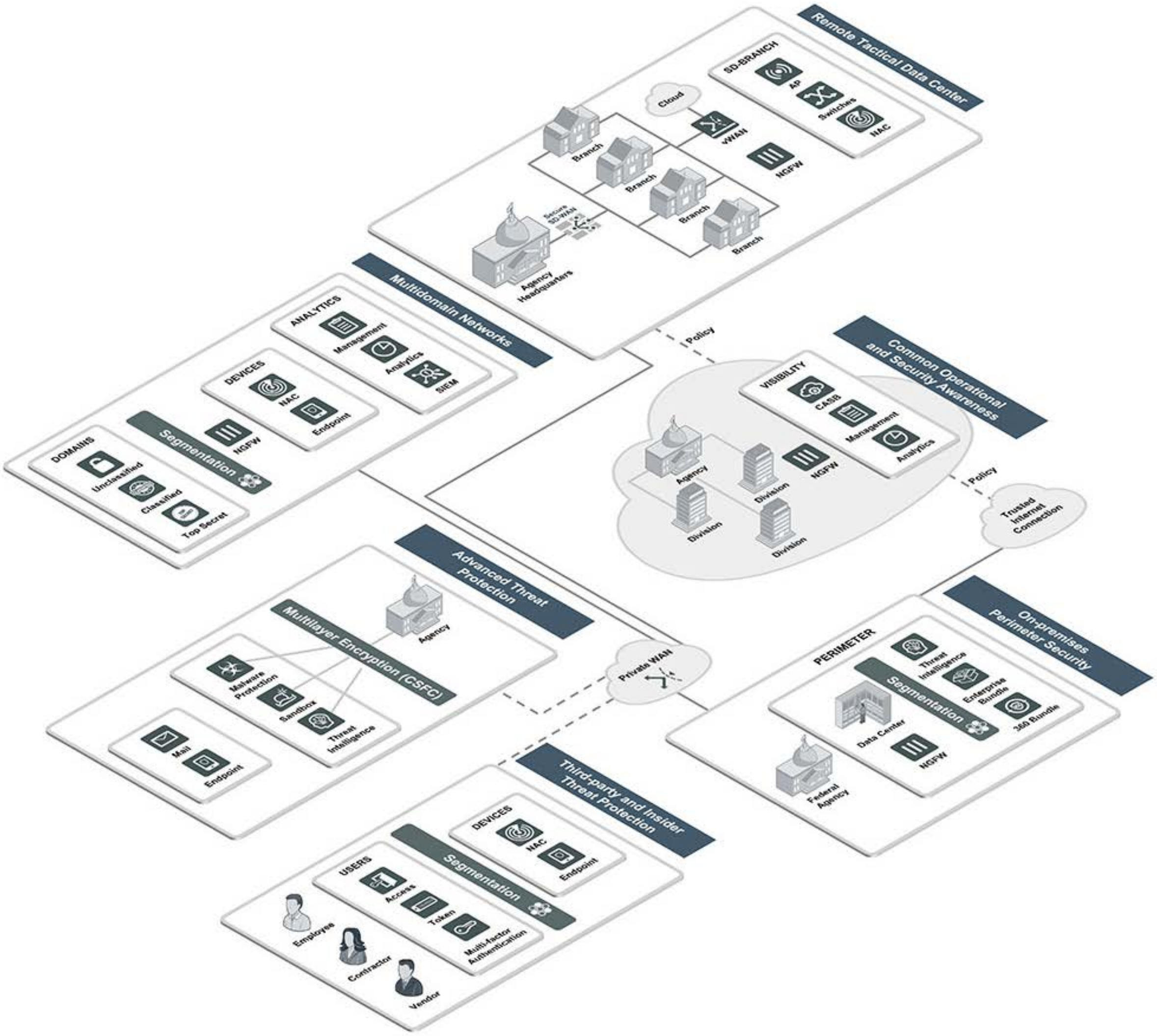

Figure 1: Federal cybersecurity solutions from Fortinet address many use cases to help agencies fight back against cyber warfare and fulfill their missions.

Consolidation

Fortinet's broad, scalable solution enables large, cabinet-level agencies to build their entire security core architecture on a single platform and adapt to future requirements. This eliminates the need to "rip and replace" the entire security infrastructure every few years.

Compliance

Fortinet simplifies the process of achieving compliance and documenting performance to auditors. With an integrated architecture visible through a single pane of glass, reporting and remediation of problems is automated. This is in contrast with disaggregated security approaches, which require significant manual work to correlate reports from different tools.

Cloud Ready

The Fortinet Security Fabric is built for distributed hybrid cloud environments, with cloud-native security tools that integrate with each other and with in-house infrastructure. As federal entities move more resources to the cloud, they can be assured of integrated, comprehensive protection.

Cost-effective

Fortinet delivers the lowest total cost of ownership (TCO) in the industry due to high-performance throughput and low latency powered by purpose-built ASIC security processors.[21] As a result, Fortinet NGFWs achieved top scores in NSS Labs' Security Value Maps for Next-generation Firewalls and Breach Prevention Systems.[22]

Conclusion

The U.S. federal government is targeted by foreign and domestic adversaries and has struggled to secure its networks and data. Fortinet is a U.S.-owned company offering a range of best-in-class cybersecurity products and services that can enhance security and productivity across government. The Fortinet Security Fabric enables a holistic, proactive approach to protecting the nation's critical infrastructure and information assets.

[1] Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," CSO, November 6, 2018.

[2] "Federal Employees By State," Governing, January 25, 2019.

[3] Joseph Marks, "The Cybersecurity 202: U.S. adversaries are raising their cyber game, intel officials warn," The Washington Post, January 30, 2019.

[4] Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," CSO, November 6, 2018.

[5] "Cybersecurity," U.S. Department of Homeland Security, accessed January 16, 2020.

[6] Derek B. Johnson, "Senate turns up a decade of federal cybersecurity failure," FCW, June 26, 2019.

[7] Craig Ford, "Cyber warfare is here and we are not prepared," CSO, February 1, 2019.

[8] Phil Muncaster, "Cybersecurity Skills Shortage Tops Four Million," Infosecurity, November 7, 2019.

[9] "Federal Cybersecurity: America's Data at Risk," Permanent Subcommittee on Investigations, U.S. Senate Committee on Homeland Security and Governmental Affairs, accessed January 16, 2020.

[10] Andrew Eversden, "What the federal cloud market could look like in 5 years," Federal Times, September 2, 2019.

[11] Derek B. Johnson, "Senate turns up a decade of federal cybersecurity failure," FCW, June 26, 2019.

[12] "Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests," Fortinet, January 2019.

[13] Derek B. Johnson, "Senate turns up a decade of federal cybersecurity failure," FCW, June 26, 2019.

[14] "Making CDM Work: Continuous Diagnostics and Mitigation Requires a Unified Ecosystem," Fortinet, July 20, 2018.

[15] Quotation from Dan Coats, director of National Intelligence, in "The Cybersecurity 202: U.S. adversaries are raising their cyber game, intel officials warn," Washington Post, January 30, 2019.

[16] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[17] Andrew Eversden, "What the federal cloud market could look like in 5 years," Federal Times, September 2, 2019.

[18] "Situational Awareness and Incident Response," U.S. Department of Homeland Security, accessed January 16, 2020.

[19] "Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests," Fortinet, January 2019.

[20] Quotation from Dan Coats, director of National Intelligence, in "The Cybersecurity 202: U.S. adversaries are raising their cyber game, intel officials warn," The Washington Post, January 30, 2019.

[21] "Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests," Fortinet, January 2019.

[22] "Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests," Fortinet, January 2019.

FORTINET®

www.fortinet.com

February 6, 2020 8:21 AM

D:\Fortinet\White Paper\Vertical Marketing - Federal Gov\wp-fortinet-federal-government-cybersecurity-solutions-V2.1-262020-820AM