SOLVING THE CYBERSECURITY CHALLENGES OF FEDERAL AGENCIES

Managing today's network infrastructures can present challenges for federal agency IT leaders—from demands for higher performance, to compliance with new standards and regulations, to integrating emerging technologies as part of digital transformation (DX). While some changes introduce new, dynamic features and IT capabilities, they can also make the network more vulnerable.

Many security strategies that worked in the past are no longer effective. Like their private sector counterparts, federal agencies are now managing borderless networks due to the rise in mobile and Internet of Things (IoT) devices requiring connectivity. In turn, this introduces new opportunities for breach, data loss, and compromised information integrity. Government agencies also typically need high performance. But these performance demands often undermine the effective use of some traditional cybersecurity tools, which cannot keep up with the speed and bandwidth requirements of today's applications. Perhaps the most compelling problem results from security complexity. Today's security infrastructures are typically a patchwork of disparate products and vendors. This creates a security architecture that's hard to manage and one that lacks integrated and automated end-to-end protection.

As a result of these common security gaps, reports of data loss and compromised systems across civilian, defense, and intelligence agencies have become commonplace in the daily news cycle. While threat actors run a wide gamut (from amateur hacktivists to sophisticated nation-state sponsored operations), federal security leaders have a common mandate: manage risk more effectively through better cybersecurity frameworks, tools, and talent.

THE FORTINET SECURITY FABRIC: BROAD, INTEGRATED, AUTOMATED

Fortinet Federal is focused on helping U.S. government agencies address the unique security requirements of their environments. A dedicated team based in the Washington, D.C., area, Fortinet Federal offers an extensive collection of security knowledge—down to the level of agency-specific challenges and priorities.

The Fortinet Security Fabric delivers end-to-end cybersecurity with broad, integrated, and automated defenses for protecting even the most demanding federal agency infrastructures. With the release of our latest operating system (FortiOS 6.0), the Fortinet Security Fabric introduces over 200 critical features and capabilities for securing today's digital attack surface. Some key solution areas include:

- **Network Security:** Integrated secure SD-WAN capabilities within the Security Fabric provide application prioritization for granular control of Software-as-a-Service (SaaS), Voice over Internet Protocol (VoIP), and other business apps. Additional new capabilities include traffic shaping to guarantee bandwidth for critical applications, zero-touch deployment for plug-and-play SD-WAN location management, and one-touch VPN to leverage common cloud VPN access. These capabilities provide federal agencies with the agility to implement zero-trust networks while improving the performance and availability of their networks and implementing zero-trust networks.
- **Multi-Cloud Security:** Expanded cloud connectors within the Security Fabric now include visibility of multiple clouds spanning private, Infrastructure-as-a-Service (IaaS), and native cloud controls, as well as enhanced FortiCASB (cloud access security broker) integration into the Security Fabric for visibility and advanced threat protection of SaaS applications. This enables organizations to have complete visibility of their security posture across all cloud networks to correlate both on- and off-network traffic through a unified security management console.
- **IoT and Endpoint Security:** FortiClient 6.0 includes expanded operating system support for Linux, sharing actionable insight about such systems with the Security Fabric. FortiClient also provides richer intelligence about all types of endpoints, including the application inventory on each device.
- **Unified Access:** Fortinet switches and wireless access points include integrated security features that trigger automated responses to events such as quarantine, when an infected switch or access point is in violation of a configured policy. These types of automated actions offer a responsive speed for containment and mitigation that goes beyond the capabilities of human monitoring and intervention.
- **Email and Web Applications:** FortiMail now supports the new FortiGuard Virus Outbreak and Content Disarm and Reconstruction Services. In addition to existing sandbox integration and analysis to block completely unknown threats, these new services prevent the spread of rapidly emerging attacks and extract active content to thwart attacks using embedded code execution. New widgets provide a comprehensive, centralized view of all email and web applications on a network, with advanced threat protection integrated into the email and web applications within the Security Fabric.
- **Advanced Threat Protection:** Increased regulatory mandates such as the General Data Protection Regulation (GDPR) make automated auditing across networks a critical function. The new FortiGuard Audit and Security Update Service includes expanded audit rules, customized auditing based on network environments, and on-demand regulatory and compliance reports. The new FortiGuard Virus Outbreak Service (VOS) closes the gap between antivirus updates with FortiCloud Sandbox analysis to detect and stop malware threats. The new FortiGuard Content Disarm and Reconstruction (CDR) Service proactively strips potentially malicious content embedded in Microsoft Office and Adobe files before they enter the network.
- **Security Management and Analytics:** New automated workflow capabilities with continuous risk assessment across the Security Fabric allow users to easily set responses based on predefined triggers—such as system events, threat alerts, or user/device status. Response actions, such as quarantine, notification, configuration adjustment, and custom reporting, provide organizations with real-time control of their workflow environments. Automated auditing also provides trending data on a business' security compliance posture. Subscribers to FortiGuard security services receive continuous, real-time updates to protect against the latest attacks.

Federal security spending is expected to grow to **$2.5B (DoD) and $2.2B (civilian agencies)[1]**

Top 5 Cybersecurity Challenges Per Federal CIOs[2]

1. Vulnerabilities from Aging Applications and Technologies
2. Human Error
3. Malware
4. Phishing Campaigns
5. Internet-facing Attacks (e.g., DDoS)

The Fortinet Security Fabric is designed to scale and adapt to the unique and complex requirements of federal agencies and critical infrastructure sectors. Our solutions are on the NSA Commercial Solutions for Classified (CSfC) approved vendors list and are currently deployed to protect classified and unclassified federal systems. Fortinet is certified under relevant federal certification programs focused on information assurance; these include Common Criteria, FIPS, and JITC APL.

In addition to cybersecurity, the Fortinet Security Fabric also enables critical DX initiatives such as data center optimization and cloud migration. Unlike security architectures with point product approaches, our Security Fabric operates across the entire IT domain. And as your infrastructure expands and changes, your security architecture is designed to scale and evolve in lockstep.

For federal CISOs and other security decision-makers, Fortinet's integrated solutions provide consistent, interoperable capabilities that simplify implementation, reduce training costs, and reduce the burden of IT staff for managing tools and products from multiple vendors.

FORTINET FEDERAL: FOCUSED ON AGENCY-SPECIFIC REQUIREMENTS

Our Fortinet Federal team was formed to specifically assist U.S. government customers and address the unique needs of their environments. As a leading provider of cybersecurity solutions in the financial and manufacturing industries, Fortinet brings a wealth of technical know-how and highly rated products to securing U.S. federal agencies. Additionally, our extensive Fabric-Ready Alliance Partners include major networking, cybersecurity, and cloud-services providers.

SECURING THE FUTURE OF FEDERAL CUSTOMERS

As prime targets of the most sophisticated forms of cyberattack, U.S. government agencies require the most comprehensive and iron-clad security available. Fortinet Federal's mission is to ensure that our cybersecurity innovations keep pace with the complex and critical requirements of customers with the most demanding needs.

The Fortinet Security Fabric extends our long-standing commitment to federal customers—delivering proven solutions that leverage best-of-breed investments through integration to address today's most sophisticated threats to U.S. government agencies.

FORTINET GARNERS INDUSTRY RECOGNITION

- NSS Labs "Recommended" ratings across 7 different group tests (more than any other security vendor)
- Gartner MQ "Leader" for Enterprise Network Firewalls and Unified Threat Management
- Fastest growing enterprise network company
- Holds 4x more patents than any other network security vendor
- Shipped more units than any other network security vendor
- Frost & Sullivan MSSP Market Leadership Award recipient

FORTIVET PROGRAM: FORTIFYING THE CYBER WORKFORCE

Fortinet recognizes the valuable skills that veterans of the U.S. military offer the IT workforce. In support of our veterans, we developed the FortiVet program to help guide exceptional men and women from the military into the cybersecurity industry. We provide these candidates with free professional networking, training, and mentoring.

[1] Shawn P. McCarthy, "U.S. Federal Government IT Security Spending Forecast, 2017-2020," IDC Market Forecast, April 2017.

[2] Grant Thornton, "2017 Federal CIO Survey: Transitions: Managing Federal IT in Dynamic Environment," Professional Services Council, September 2017.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

FORTINET FEDERAL HEADQUARTERS
12005 Sunrise Valley Drive, Suite 204
Reston, VA 20191
Tel: +1.408.331.4550
www.fortinetfederal.com

March 23, 2018 12:47 PM

137998-A-0-EN

wp-solving-cybersecurity-challenges-federal-agencies