FORTINET FEDERAL

ISSUE BRIEF

Meet New Cybersecurity Mandates With a Platform-based Approach

In May 2021, the Biden administration established two broad goals in the Executive Order on Improving the Nation's Cybersecurity (EO): adopt zero trust architecture and accelerate movement toward secure cloud services. The EO also set ambitious deadlines associated with these goals.

The Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA) followed up in September with further guidance to help agencies meet the goals set out in the EO.

OMB's draft Federal Zero Trust Strategy sets forth five major goals for agencies to reach by the end of fiscal year 2024 regarding identity, devices, networks, applications, and data. CISA's draft Cloud Security Technical Reference Architecture (TRA) guides agencies' secure migration to the cloud by explaining considerations for shared services, cloud migration, and cloud-security-posture management. Additionally, the agency's draft Zero Trust Maturity Model aims to assist agencies with zero trust strategy and implementation.

Substantial work is required to meet the mandates laid out in the EO. OMB, for example, said it expects that "moving to a zero trust architecture will be a multi-year journey for agencies, and the federal government will learn and adjust as new technologies and practices emerge." The good news is that many agencies are well on their way to meeting both goals. They've begun implementing technologies that contribute to zero trust architecture, such as endpoint detection and multi-factor authentication (MFA), and they're in the cloud. The EO directs agencies to accelerate what they are already doing and to do it in a way that implements zero trust.

To meet the requirements of the EO without the benefit of additional staff or funding, agencies will need to find economies of scale, such as:

- Incorporating existing technologies, such as endpoint detection and MFA, into an enterprisewide cybersecurity platform, thus avoiding the need to rip and replace point solutions.
- Considering technologies that combine the functions of multiple legacy devices before refreshing existing devices. For example, a next-generation firewall may perform the functions of a half-dozen legacy devices. Multi-function technologies can conserve budget and staff time.
- Operating technologies in multiple environments, for systemwide visibility.

Zero Trust

Zero trust is a network security philosophy that assumes there is no implicit trust granted to IT assets or users based solely on their physical or network location. Authentication and authorization of both user and device are discrete functions performed before allowing access to an enterprise computing resource. User or device identity verification is conducted when a connection is established, and a new check can be triggered by events such as accessing a different application or an unexpected change in user behavior.

Ensuring Security Across the Enterprise

Ensuring security becomes increasingly complex as agencies move more functions to the cloud. That's because native levels and types of security vary from cloud to cloud. These differences can create gaps in security, which can create security vulnerabilities. Multi-cloud environments also obscure visibility across the enterprise, because agencies must use multiple consoles for configuration, management, and other tasks.

To ensure consistent security, improve visibility, and streamline management across the enterprise, agencies need cybersecurity solutions that are designed to operate in multiple environments, from public clouds to on-premises data centers, and that are connected via a common platform. Technology teams benefit from the ability to provision the same security rules across environments and monitor enterprisewide operations via a centralized dashboard. End-users benefit from seamless access to their data and applications.

Turning a Security Liability Into an Asset

As agencies continue to expand their network footprints, the potential attack surface for malicious actors also expands. Branch offices, remote work, field operations, and proliferating end-user devices all create potential points of entry and exploit.

However, a platform approach to cybersecurity can turn this challenge—the size, complexity, and sheer volume of endpoints and connections—into a net advantage, by making it the equivalent of a smart sensor network. The cybersecurity platform enables agencies to instrument key parts of their network and leverage the artificial intelligence and machine learning (AI and ML) that powers their security devices to understand what normal and abnormal network activity looks like in real time, and to determine what abnormal behaviors are malicious or potentially harmful.

Malicious actors typically try to breach a system multiple times before succeeding; AI and ML capabilities allow agencies the opportunity to detect attackers trying and failing so they can prepare for future attacks. AI and ML also help agencies sort through false alarms and alert technology teams to actual threats. Security devices can then react to the threat automatically and in real time, or they can be programmed to alert a human to the potential problem—or both.

All in Action

Fortinet network detection and response identifies cybersecurity incidents in progress based on anomalous network activity to reduce risk and impact of cyber threats. FortiNDR includes a virtual security analyst capability that can operate in an unsupervised mode, helping lean SecOps teams fully analyze and investigate new threats in the shortest period of time. This portable and powerful "security-analyst-in-a-box" comes pretrained with more than 6 million malware features and the ability to examine 100,000 files per hour. With 99% initial accuracy, it can identify and classify threats and pinpoint entry and lateral spread of a piece of malware and its variants. And, accuracy improves over time as FortiNDR learns an agency's environment. Each platform can expand the analytics capability of the SOC team, improving response time and freeing key resources to investigate more complex events.

Elevating Agency Cybersecurity With a Comprehensive Platform

In recent years, cybersecurity solution developers have embraced a platform approach that enables devices and solutions across the computing environment to exchange data in an automated fashion, even across vendors. This approach essentially offers free synergy and greater capability to organizations that embrace it. It enables agencies to:

- Implement best-of-breed solutions from multiple vendors
- Take an incremental approach to technology upgrades, because they don't need to rip and replace existing technologies
- Manage cybersecurity solutions via a centralized dashboard that provides enterprisewide visibility
- Reallocate security operations staff from routine to high-level activities
- Create a virtuous circle by adding more solutions to a common platform, which closes gaps in cybersecurity coverage and enables the platform provider to correlate more data, thus improving the platform's ability to identify cyber threats

Fortinet pioneered the platform-based approach to cybersecurity with the Fortinet Security Fabric. It's an open ecosystem that incorporates Fortinet security technologies protecting more than 50 aspects of networking, computing, and connectivity and interoperates with more than 480 products from other vendors. Across the cybersecurity landscape, Fortinet's platform is the most mature and offers the broadest coverage of the potential attack surface—from edge, to core, to cloud.

Agencies choose Fortinet Federal for its:

Open ecosystem. Because the Fortinet Security Fabric integrates with more than 480 products from other vendors, agencies can continue to use their existing security technologies, both on-premises and in the cloud. When they're evaluating new technologies, agencies can choose from a full slate of best-of-breed solutions.

Flexible and consistent configurations. Because agencies have varied missions and may face unique threats, Fortinet Federal allows them to control their solution configurations, in a process that is as easy as setting a radio dial. For example, a law enforcement agency may need to access the dark web to conduct investigations, but it wants to leverage zero trust to ensure such activity does not compromise the agency's core network or set off alarms for other agencies. In addition, the Fortinet Security Fabric facilitates consistent configuration and policy management across the security infrastructure, which reduces security risks resulting from configuration errors and manual data compilation.

Global threat intelligence. The Fortinet Security Fabric is informed by anonymized telemetry reported by over 6 million devices deployed in more than 500,000 customer organizations worldwide. These devices protect customer networks worldwide using actionable information generated from 100 billion security events these devices detect each day. This data and Fortinet's sophisticated AI and ML capabilities have allowed it to identify more than 900 previously unknown (zero-day) types of attack. In addition, Fortinet participates in more than 200 information-sharing partnerships with other companies, governments, and organizations around the world, including the Cyber Threat Alliance that it helped to found in 2014.

AI- and ML-powered threat detection. Integrated AI and ML capabilities help agencies quickly identify known and new adversaries and malware, reduce the number of false alarms, detect insider threats, and enable either an automated or human cybersecurity response.

Spending Smarter With SD-WAN

The cybersecurity EO creates requirements but not additional funding, which means agencies need to spend smarter. One way to do that is by embracing the power of software-defined wide-area networking (SD-WAN), which uses software-based controllers, application programming interfaces and/or policy-based configuration to communicate with hardware/virtual infrastructure and direct traffic across a wide-area network.

SD-WAN enables agencies to evolve their networking from a hub-and-spoke architecture—in which devices must be physically connected to one another in remote locations, and where local traffic is often forwarded to a central location for security inspection before delivery to its final destination—to a software-defined wide-area networking architecture that determines the optimal path for traffic and facilitates peer-to-peer data flows in the field. With SD-WAN, traffic could be sent over multiprotocol label switching (MPLS), 3G/4G/5G, or broadband at any moment, based on the real-time availability and performance of each, the priority the agency has assigned to the specific application, and desired user performance requirements. For example, agencies can dedicate bandwidth to mission-critical collaboration platforms but not social networking tools.

For agencies with branch offices or field operations, SD-WAN enables approved traffic to connect directly to the internet and pushes security out to the edge or branch office. As a result, users in the field environment have faster, more secure, more reliable, and less costly access to core agency IT functions and web services. One organization with 1,200 field offices reduced its costs by $100 million annually and increased its network capacity by as much as 50 times after moving from dedicated Tier 1 lines to SD-WAN.

Meeting Mandates With the Fortinet Security Fabric

The Fortinet Security Fabric can help agencies meet the mandates laid out in the recent cybersecurity EO (No. 14028) efficiently and cost effectively, while leveraging best-of-breed technologies and AI capabilities that speed threat detection and response.

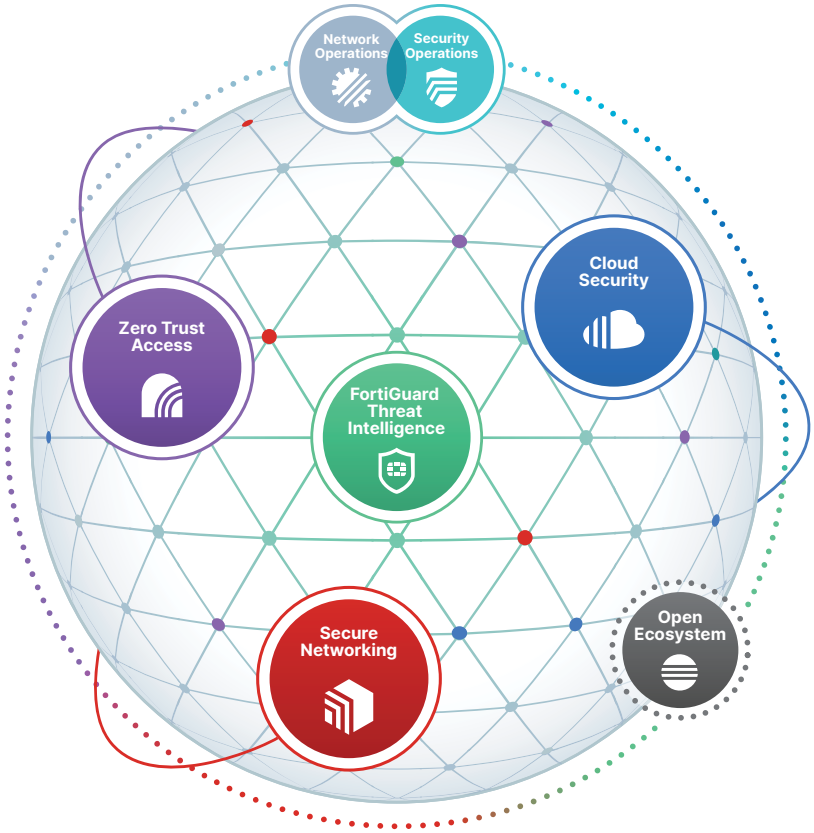

Figure 1: The Fortinet Security Fabric enables multiple security technologies to work seamlessly together, across all environments and supported by a single source of threat intelligence, under a single console. This eliminates security gaps in the network and hastens responses to attacks and breaches.

FORTINET FEDERAL®

www.fortinet.com/federal

May 26, 2022 10:52 AM
1603200-0-0-EN