Security Without Compromise

Response to Request for Information on Current and Future States of Cybersecurity in the Digital Economy

Prepared for:

The Commission on Enhancing National Cybersecurity

c/o the National Institute of Standards and Technology

100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899

In Response to:

Federal Register Notice Number 81 FR 52827

Published August 10, 2016

Submitted by:

FORTINET®

899 Kifer Road, Sunnyvale, CA 94086

September 9, 2016

Table of Contents

1. Purpose

The Commission on Enhancing National Cybersecurity has requested information about current and future states of cybersecurity in the digital economy. It intends to analyze and use the information it collects to formulate recommendations for the President on ways to strengthen cybersecurity in both the public and private sectors. One of the topics it has asked respondents to address is challenges and approaches to critical infrastructure cybersecurity.

This document discusses the challenges inherent in protecting critical infrastructure and describes a promising new approach that Fortinet, Inc. is employing to meet these challenges.

2. About Fortinet, Inc.

Fortinet, Inc. (NASDAQ:FTNT) is a 16-year-old cybersecurity company based in Silicon Valley. We specialize in cyber threat research; cybersecurity product research and development; and the design, implementation, and support of cybersecurity platforms based on Fortinet-brand physical and virtual security appliances and FortiGuard software subscription services. We are the world's largest network security appliance supplier (measured in units sold) and provide goods and services to more than 270,000 private and public sector customers worldwide. Our products protect critical infrastructure in multiple industries as well as mission-critical systems used by national, state, and local government agencies.

3. Challenges to Critical Infrastructure Cybersecurity

Presidential Policy Directive 21 (PPD-21), issued in February 2013, articulates the importance of ensuring the that networks and systems in industries that provide vital services to American society are secure, can withstand potential attacks including cyber attacks, and can quickly recover from such attacks. The critical infrastructure that resides within these industries is diverse and complex. In encompasses distributed and non-distributed systems, both custom and commercial hardware and software, and, in some cases, systems that cross national boundaries. Nevertheless, the owners of these systems face several common challenges. One common challenge lies in the sheer volume of the threats that organizations now face on a daily basis. For example, an executive from Symantec was recently quoted as saying that the company has seen a 300% increase in ransomware attacks between 2015 and 2016. These attacks, which are more prevalent in the U.S. than in other countries, have been especially common in the country's manufacturing and health care sectors. Verizon's 2016 Data Breach Investigations Report, which draws on data from leading cybersecurity companies and public agencies charged with combatting cyber threats, confirms that financially-motivated cyber attacks are on the rise, as are espionage-related attacks. A second common challenge that has received a great deal of attention is the steady, dramatic increase in the number of smart devices that connect to the internet – i.e., the Internet of Things (IoT). Cisco has estimated that by 2020, the number of smart devices connected to the internet will reach 50 billion – which is double the number connected today. In a survey conducted by BlackHat in 2016, hundreds of IT professionals were asked what concerned them most looking two years out. The number one answer given in both the 2016 survey and in a similar survey conducted by BlackHat in 2015 was the potential for IoT-related attacks. The follow-up question in the survey asked if they had the security staff necessary to defend against current threats - 84% of the responses ranged from "what staff?" to admitting the need for help.

Critical Infrastructure Sectors*

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy (electricity, oil, natural gas)
- Financial services
- Food and agriculture
- Government facilities
- Healthcare and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation
- Water and wastewater systems

* Source: Department of Homeland Security

Which brings us to the third common challenge facing critical industries: organizational constraints. One known constraint is that there are simply not enough experienced information security professionals to keep pace with the cybersecurity challenges facing government and critical industries. This challenge reveals itself in a myriad of ways, including in the amount of time it typically takes to discover a breach (on, average, more than 6 months according to a recent study by the Ponemon Institute – which also notes that 83% of breaches are discovered by someone outside of an organization). A second constraint has to do with the fact that in many organizations, network operations centers (NOCs) and security operations centers (SOCs) operate in siloed environments, and lack the tools necessary to obtain a holistic view of the organization's threat landscape in real time. As the U.S. Army Cyber Command noted in a recent request for white papers, better technology for security information and event management (SIEM) could help address this need because actions/events can happen so quickly in cyberspace that automated means of monitoring the threat landscape are often more useful than their manual counterparts.

3. The Security Fabric: A New Approach to Protecting Critical Infrastructure

Fortinet believes that the challenges discussed above must be addressed in two ways. The first is obvious: the USA needs to make (and is making) a concerted effort to expand the cybersecurity labor pool. Fortinet is doing its part to address this need by working to bring more veterans into the cybersecurity industry. We are doing this through our FortiVets Program, which strives to help veterans with backgrounds in cybersecurity find jobs in our industry and by improving veterans' access to high-quality cybersecurity training courses.

The second way to address the challenges described above is to provide cybersecurity professionals with technology tools that increase their productivity. At Fortinet, we are addressing this through our Security Fabric, which is designed to simplify network monitoring and management through a unique and integrated philosophy and approach across the Fortinet family of network-security-related products.

The concept for the Security Fabric arose from the observation that as networks become larger and more complicated, organizations tend to make their network security platform larger and more complicated as well. This is often counterproductive at worst and marginally useful at best because complexity reduces the productivity of cybersecurity professionals who are already spread thin. What is needed more often than not is a simple approach that addresses three things:

- **Segmentation** – Networks need to be intelligently segmented into functional security zones. End-to-end segmentation, from IoT to the cloud, and across physical and virtual environments, provides deep visibility into traffic that moves laterally across the distributed network, limits the spread of malware, and allows for the identification and quarantining of infected devices.
- **Collaborative intelligence** – Local and global threat intelligence needs to be shared between security devices, and a coordinated response between devices needs to be orchestrated centrally.
- **Universal policy** – A centralized security policy engine that determines trust levels between network segments, collects real time threat information, establishes a unified security policy, and distributes appropriate orchestrated policy enforcement. Fortinet's Security Fabric integrates technologies for the endpoint, access layer, network, applications, data center, content, and cloud into a single collaborative security solution that can be orchestrated through a single management interface.

The Security Fabric accomplishes the above within the context of a solution with these five attributes:

- **Scalable:** A comprehensive security strategy needs both depth (performance and deep inspection) and breadth (end to end.) Security not only needs to scale to meet volume and performance demands, it needs to scale laterally, seamlessly tracking and securing data from IoT and endpoints, across the distributed network and data center, and into the cloud. The Fortinet Security Fabric provides seamless,

ubiquitous protection across the distributed Enterprise, from IoT to the cloud, as well as inspection of packet data, application protocols, and deep analysis of unstructured content – all at wire speeds.

- **Aware:** The Fabric behaves as a single entity from a policy and logging perspective, enabling end-to-end segmentation in order to reduce the risk from advanced threats. Security professionals not only need to see data that flows into and out of their networks, but how that data traverses the network once it is inside the perimeter. The Fortinet Security Fabric enables end-to-end network segmentation for deep visibility and inspection of traffic travelling the network, and control of who and what gets to go where, thereby reducing the risk from advanced threats.

- **Secure:** It must be possible to share global and local threat intelligence and mitigation information in a ways that decreases time-to-protect and ensures that the all component of the network security platform work together seamlessly. Fortinet's Security Fabric behaves as a single collaborative entity from a policy and logging perspective, allowing individual product elements to share global and local threat intelligence and threat mitigation information.

- **Actionable:** Big data cloud systems correlate threat information and network data to deliver actionable threat intelligence in real time. It is not enough to detect bad traffic or block malware using discrete security devices. What is needed is a common set of threat intelligence and centralized orchestration tools that allow security to dynamically adapt as threats are discovered anywhere, not just in your network, but anywhere in the world. Fortinet's big data cloud systems centralize and correlate threat information and network data to deliver actionable threat intelligence to every security device in your network's security fabric in real time.

- **Open:** Well-defined, open APIs allow leading technology partners to become part of the fabric. Of course, a true security fabric will let you maximize your existing investment in security technologies, which is why Fortinet has developed a series of well-defined, open APIs that allow technology partners to become part of the Fortinet Security Fabric.

SIEM technology, which we discussed briefly above, plays an important role in the Security Fabric. By leveraging our SIEM product, FortiSIEM, Fortinet can provide broader visibility into the threat landscape by collecting contextual information from hundreds (or thousands) of Fortinet devices and third-party devices, from virtual and cloud environments, and from both internal and external threat feed sources. Whereas many current SIEM tools have limited scalability (due to CPU and processing methodology limitations), FortiSIEM can be scaled as the number events per second (EPS) that an organization must process and analyze increases.

6. Additional Information

For more information on how the Security Fabric and FortiSIEM can benefit critical infrastructure in the industries identified on page 1, contact Michael Reinhart, at mreinhart@fortinet.com. For information on how these technologies can be used to protect mission-critical federal IT systems, contact Bryan Skelton at bskelton@fortinet.com.