FORTINET

YOUR CHALLENGES, FORTINET SOLUTIONS: U.S. DEPARTMENT OF HOMELAND SECURITY'S

Continuous Diagnostics and Mitigation Program

The U.S. Department of Homeland Security (DHS) established its Continuous Diagnostics and Mitigation (CDM) program in 2012 to successfully achieve the objectives behind three major goals:

1. **Increase the effectiveness of security at federal, state, and local government agencies.**
2. **Improve the security posture and situational awareness at each of these respective agency levels.**
3. **Transition the federal government from an annual compliance audit-centric culture to one measuring the success of network security based on a continuous measuring of security in real time.**

To date, DHS' CDM program is one of the U.S. government's most important, highly visible efforts to secure our country's critical infrastructure against the continuously evolving cyber threats constantly seeking to "breach the gate." In fact, the importance of the Department of Homeland Security's CDM program is mentioned prominently in the Executive Office of the President's M-16-04 Memorandum.

With so many resources available to help answer the questions of how the CDM program's objectives will benefit federal agencies, Fortinet's Federal team is here to help agencies meet the daunting challenge of selecting a CDM partner with the solutions that are best tailored to their needs. Many of Fortinet's industry-leading, third-party-validated solutions can already be purchased through the CDM program, and we are working closely with CDM prime contractors to ensure that the CDM solutions they offer can incorporate our newest, most innovative technology. The Fortinet security appliances described in the next section represent our core offering for Phase 3. As we explain on the next page, these products are part of the Fortinet Security Fabric – a new, Fortinet-developed intelligent architectural approach that is a perfect fit for CDM's objectives.

FORTINET FEDERAL'S CYBERSECURITY SOLUTIONS FOR CDM

The government has broken CDM into 15 functional areas that span four distinct phases to enable agencies to effectively understand their environment and implement a cohesive security solution. The four phases are as follows:

- Phase 1 – Manage Assets
- Phase 2 – Manage Events
- Phase 3 – Manage the Security Life Cycle
- Phase 4 – Manage Accounts for People and Services

As agencies are now moving into Phase 3, Fortinet has mapped its portfolio of products and solutions to the requirements outlined within this phase. As such, our solutions include:

- Physical and virtual network security appliances
  - Standalone
  - Bundled with FortiGuard security software and FortiCare support services
- Endpoint protection software
- Security and event management software

Specific product families that map to the CDM tool sets for Phase 3 are described below.

				Manage Boundaries	Manage Events				Operate, Monitor and Improve				Design and Build in Security
Product Family	Physical Appliance	Virtual Appliance	Client Software	Bound	Ongoing Assessment	Incident Response	Privacy	Contingency Planning	Audit and Accountability	System Information and Integrity	Risk Assess-ment	Security Assess-ment	
FortiAnalyzer	●	●		●	●	●	●	●	●	●	●	●	●
FortiAuthenticator	●			●		●	●	●	●	●	●	●	●
FortiClient			●	●	●	●	●	●	●	●	●	●	●
FortiGate	●	●		●	●	●	●	●	●	●	●	●	●
FortiMail	●	●		●	●	●	●	●	●	●	●	●	●
FortiManager	●	●		●	●	●	●	●	●	●	●	●	●
FortiSandbox	●	●		●	●	●	●	●	●	●	●	●	●
FortiSIEM		●			●	●	●	●	●	●	●	●	●

FortiAnalyzer: FortiAnalyzer provides agencies with the ability to collect, analyze, and correlate log data from a distributed network of Fortinet security appliances from one central location. The FortiAnalyzer platform uses Fortinet's uniquely effective data collection and services to provide agency personnel with prioritized lists of compromised hosts to quickly identify threats requiring immediate action.

FortiAuthenticator: FortiAuthenticator is Fortinet's purpose-designed user/device authentication appliance that strengthens enterprise security by simplifying and centralizing the management and storage of user identity information. Through integration with existing Active Directory or LDAP authentication systems, FortiAuthenticator enables the transparent identification of network users and
enforces identity-driven policies on enterprise networks.

FortiClient: FortiClient is an independently validated endpoint protection platform that secures a multitude of different operating systems (Windows, Mac OSX, iOS, and Android OS). FortiClient features include the ability for security administrators to configure security compliance checks and
authorized device/user access validation checks. Security administrators are provided with high visibility and control to quickly adapt policies essential for securing the enterprise.

FortiGate: The FortiGate product line is an industry-leading, independently validated, enterprise firewall platform optimized for internal segmentation, perimeter, cloud, data center, and distributed network deployments. FortiGates are well-suited for agency efforts to secure their networks from unauthorized access attempts while providing unmatched performance and superb events visibility.

FortiMail: FortiMail provides agencies with comprehensive coverage for their email infrastructure, which includes anti-spam, anti-phishing, anti-malware, sandboxing, data loss prevention (DLP), encryption, and message archiving. Regardless of whether an agency has a LAN/WAN or cloud-based email infrastructure, FortiMail prevents them from becoming threat delivery systems.

FortiManager: FortiManager provides agencies with a centralized management solution to easily control the deployment of security policies, security updates, firmware revisions, and individual configurations for thousands of FortiOS-enabled devices. In addition, FortiManager facilitates policy/device auditing to prove compliance and track any deviations from the required security policy.

FortiSandbox: FortiSandbox is an independently validated advanced threat protection solution, which offers a combination of proactive detection and mitigation measures that provide an unparalleled level of actionable threat insight. FortiSandbox is easily integrated with Fortinet security appliances for automation of traffic analysis and alerting of detected threats. The unique, dual-level sandbox within the appliance is complemented by Fortinet's award-winning FortiGuard Labs threat intelligence.

FortiSIEM: FortiSIEM provides organizations with a comprehensive, holistic, and scalable solution with patented analytics that manages network security, performance, and compliance standards. FortiSIEM's architecture enables unified and cross-correlated analytics from diverse information sources including logs, performance metrics, SNMP traps, security alerts, and configuration changes. With FortiSIEM as part of its CDM offerings, Fortinet is the only vendor with a distributed event correlation solution that can detect complex event patterns in real time with minimal delay.

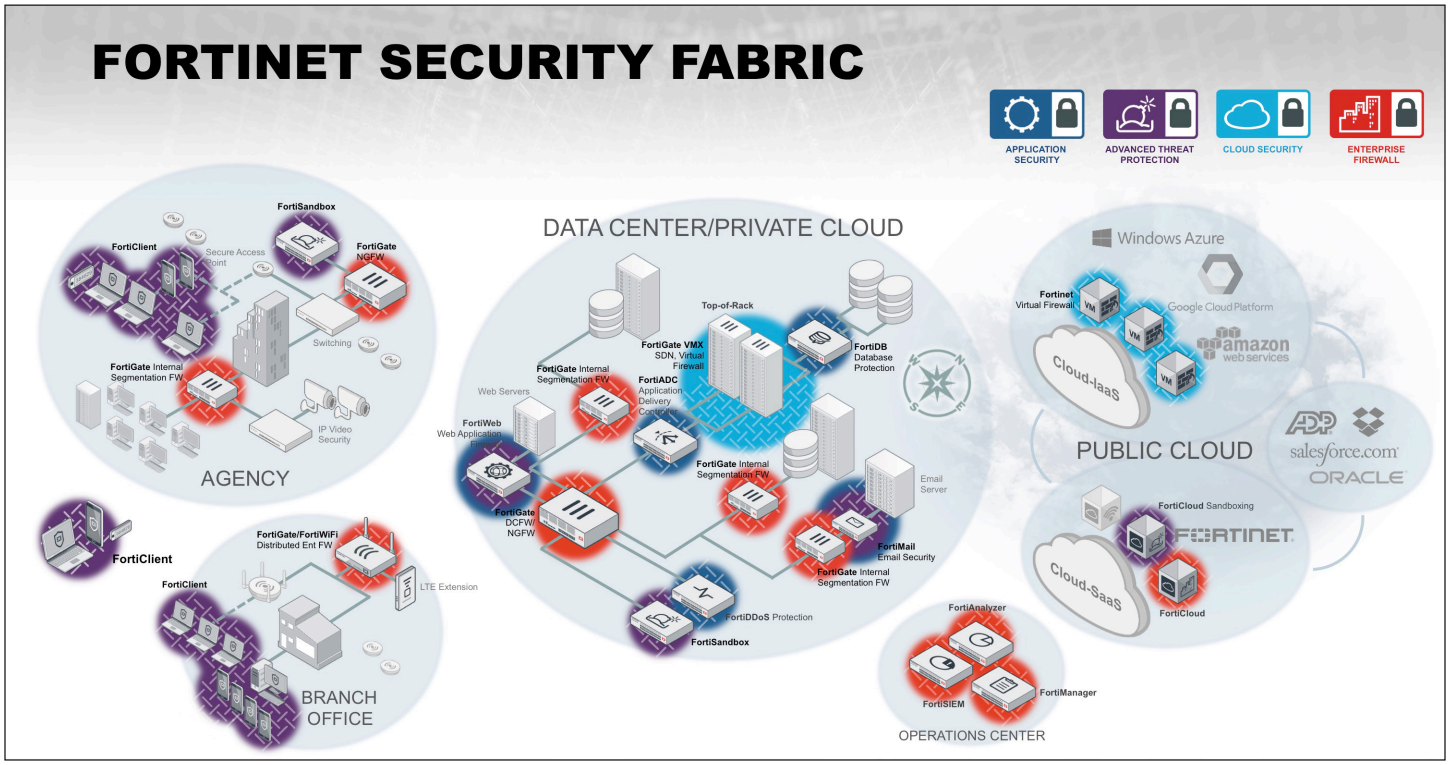
FORTINET SECURITY FABRIC: TYING IT ALL TOGETHER FOR CDM

Since introducing its first security product in 2002, Fortinet has moved beyond protecting the network border to offering a comprehensive security solution that we refer to as the Fortinet Security Fabric. The Security Fabric recognizes the need for a more effective response to cyber threats than simply adding new security devices to an already overburdened collection of security solutions. While keeping pace with the increasing demands of technology remains of critical importance for security solutions, of equal importance is the need to move to a more holistic security architecture that ties discrete security solutions into an integrated whole.

Unlike other disparate point solutions within a security architecture that fail to communicate with one another, all of the Fortinet appliances described in this white paper work cooperatively with each other to realize the vision behind Fortinet's Security Fabric. This Security Fabric works most effectively with Fortinet's solutions at the core, but also has open APIs and
plug-ins to integrate with an agency's existing network security infrastructure.

SUMMARY

The U.S. Department of Homeland Security's CDM program is a logical progression towards realizing a more secure stance against the vast number of cyber threats fighting to breach our national infrastructure on a daily basis. While agencies continue to make the necessary strides towards a successful CDM implementation, Fortinet's Federal team will continue to be a champion of the program and stand ready to assist federal agencies to successfully meet CDM's objectives today without compromising on the needs of tomorrow. To see for yourself how Fortinet's Federal team can be your valued CDM partner, contact our team at federalsales@fortinet.com.



ABOUT FORTINET FEDERAL

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. We empower our customers with intelligent, seamless protection across the expanding attack surface, and with the ability to take on ever-increasing performance requirements of the borderless network - today and into the future. Our federal solutions protect the classified and unclassified systems used by 12 of 15 cabinet-level agencies, and those of numerous independent agencies, utilizing Fortinet's specially configured USG product line. These platforms comply with federal certification requirements including NIST FIPS 140-2, NIAP Common Criteria certification, and are on the Commercial Solutions for Classified Programs (CSfC) approved Components List. Learn more at www.FortinetFederal.com.

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

Fortinet Federal, Inc.
12005 Sunrise Valley Drive
Suite 204
Reston, VA 20191
Tel: 703-815-7197
federalsales@fortinet.com
www.fortinetfederal.com

Jan 10, 2017