SELECTING THE RIGHT SOLUTIONS FOR CDM: LEVERAGING THE FORTINET SECURITY FABRIC FOR A MORE CONNECTED GOVERNMENT INFRASTRUCTURE

EXECUTIVE SUMMARY
The U.S. Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program is moving into Capability 3, which focuses on managing the security life cycle and providing tools for rapid response and recovery in the event of a network intrusion or data breach. This capability will require more from IT, infrastructure, and operations than previous capabilities, and a unified security fabric is essential for compliance. This white paper shows federal agencies how they can meet federal certification requirements with the Fortinet Security Fabric, a broad, integrated, and automated framework for network security.

BUILDING A SELF-HEALING CDM INFRASTRUCTURE
The DHS CDM program provides federal agencies with a means of updating and procuring software, hardware, and services to better manage and secure their information systems. CDM data feeds into agency-level dashboards and then is aggregated into a federal-level dashboard to assist in monitoring and reporting. Dashboards provide risk scoring to allow agencies to identify and prioritize the most critical issues.

CDM is divided into four capabilities and is currently moving into Capability 3: Managing the Security Life Cycle. Capability 3 seeks to answer the question, “What is happening on the network?”, making boundary protection and incident response paramount. To achieve the appropriate monitoring of security controls, agencies must improve integration between network security and infrastructure components and automate risk reporting.

Meeting compliance requirements for Capability 3 of CDM requires a network that can evolve and guard itself against a changing threat landscape. Solutions must comply with federal certification requirements including National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 and National Information Assurance Partnership (NIAP) Common Criteria certification. It’s also valuable (although not required) for solutions to be listed on the Commercial Solutions for Classified (CSfC) Program’s approved components list. All products must be on the CDM Approved Products List (APL). The Office of Management and Budget has issued an updated guidance that outlines new Continuous Diagnostics and Mitigation program requirements for agencies to comply with the Federal Information Security Modernization Act (FISMA) of 2014. Agencies are now directed to submit justification if they choose to buy continuous monitoring tools and capabilities outside of the General Services Administration’s IT Schedule 70 CDM tools special item number, CDM Dynamic and Evolving Federal Enterprise Network Defense, and other contract vehicles.
The future for federal agencies’ IT infrastructure lies in intent-based networking, which involves building a network with the intelligence to trigger automated responses to proactively defend against new and evolving threats. An intent-based network provides the broad visibility, integrated detection of advanced threats, and automated response that CDM requires. This white paper describes how federal agencies can build a tightly integrated ecosystem of solutions—from next-generation firewalls to endpoint protection to behavioral intelligence—using the Fortinet Security Fabric, which leverages Fortinet and Fortinet Fabric-Ready Partner products.

FORTINET ADDRESSES IT AND OPERATIONAL REQUIREMENTS FOR CDM

Fortinet has mapped our portfolio of products and solutions to the requirements outlined for CDM Capability 3, with many DHS-approved CDM products on the CDM APL under the CDM DEFEND (Dynamic and Evolving Federal Enterprise Network Defense) government-wide acquisition contract. The Fortinet Security Fabric is an architectural approach that is a perfect fit for CDM, integrating physical and virtual network security appliances, endpoint protection software, and security information and event management (SIEM) software. It enables network security solutions to work cooperatively with one another to achieve the following objectives for CDM Capability 3:

MANAGE BOUNDARIES AND EVENTS

In order to keep boundaries defined and secure and proactively manage security events, agencies need toolsets that will enable ongoing assessments, fast incident response, and contingency planning while meeting data privacy requirements through network segmentation. Traditional network borders are disappearing as agencies move to public cloud and increase mobile adoption, requiring security solutions that can adapt. Fortinet solutions address the requirements of the borderless network today and into the future.

DESIGN AND BUILD-IN SECURITY

Adding a patchwork of security products after the fact to fill gaps is becoming less and less effective; protecting agency networks in today’s threat environment requires forethought and careful integration. Creating security policies, planning for future needs, and ensuring effective security requires solutions that work together across a security fabric. Design and Build-In Security (DBS) is an objective of CDM Capability 3 that focuses on developing trustworthy systems from the ground up. By identifying deficiencies in their own code and automating security lockdowns of vulnerable code, agencies can address security weaknesses. DBS includes static and dynamic assessments, runtime instrumentation and analysis, and ongoing residual risk assessments, as well as supply chain risk management.

The Fortinet web application firewall, FortiWeb, is an advanced threat protection solution that helps agencies fill security gaps during their software development life cycles, due to its integration with some of the industry’s most frequently used vulnerability scanners. FortiWeb protects against attacks that target vulnerabilities in the web application code. Due to Fortinet’s Security Fabric Alliance partnerships with companies such as Qualys, HP, IBM, and WhiteHat, FortiWeb supports native integration into these vulnerability scanning platforms to support real-time sharing of detected vulnerabilities in software development environments. These joint solutions provide for automated mechanisms that will dynamically protect networks from being compromised by detected vulnerabilities and provide the additional benefit of automatically patching these same vulnerabilities.

OPERATE, MONITOR, AND IMPROVE

With continuous monitoring and improvement of security being a major focus of CDM Capability 3, solutions are required that can provide full audit trails and accountability while maintaining the integrity of systems and information. Ongoing risk and security assessments are essential. Fortinet offers a Security Audit Update Service, which helps agencies identify critical vulnerabilities and configuration weaknesses and take appropriate action.

BRINGING IT ALL TOGETHER FOR CDM

The Fortinet Security Fabric connects critical security and networking technologies—from firewalls to content and application security to secure access points—for seamless security across the distributed network. Regardless of whether an agency’s security is managed in an on-premises.gov domain as a physical appliance or virtual machine, across wired and wireless networks, or managed as a single enterprise via hybrid cloud designs that bridge physical data centers with multiple cloud providers, security must be easy to administer, yet powerful in its scope of security and traffic visibility. The Fortinet Security Fabric can dynamically adapt to evolving CDM infrastructure requirements by segmenting the entire network, helping agencies prevent the lateral movement of threats. Visibility is not lost with segmentation. Once segmentation is configured in FortiGate next-generation firewalls (NGFWs), segmented traffic can be easily viewed within the FortiView interface.
The Fortinet Security Fabric includes incident response capabilities that allow agencies to automate response methods such as quarantine, notifications, configuration adjustments, and custom reports in real time. Automated attack surface analysis provides recommendations and trending data on security compliance and best practices adoption.

Fortinet offers a comprehensive security solution with components that map to specific areas of CDM, as shown in the chart below:

**CDM Area Mapping**

<table>
<thead>
<tr>
<th>Product Family</th>
<th>Manage Boundaries</th>
<th>Manage Events</th>
<th>Operate, Monitor and Improve</th>
<th>Design and Build in Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Appliance</td>
<td>Virtual Appliance</td>
<td>Client Software</td>
<td>Bound</td>
<td>Ongoing Assessment</td>
</tr>
<tr>
<td>FortiAnalyzer</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>FortiAuthenticator</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>FortiClient</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>FortiGate</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>FortiMail</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>FortiSandbox</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>FortiSIEM</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>FortiWeb</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

* Extends a framework of malware detection across the infrastructure

**FABRIC-READY PARTNERS**

Fortinet supports our fabric with a formalized program that includes participation from other leading manufacturers listed on the CDM APL. These companies work with Fortinet to provide advanced integration between the feature sets of the individual products so that when they are deployed together, much of the integration and application programming interface (API) development work is already complete. Agencies benefit from a simplified solution that’s faster to deploy and yields predictable results that have already been tested.

The Fortinet Fabric-Ready Partner Program enables Fortinet and partner products to cooperatively integrate via open APIs, providing a rich and flexible ecosystem for CDM. By integrating existing network security infrastructure into the Fortinet Security Fabric, agencies can minimize costs while still enjoying the benefits of a unified fabric described in this white paper. Fortinet also offers technical deployment guides for many partner solutions to accelerate deployment. The Fabric-Ready Partner program is growing rapidly, with new partners added every month.

Some Fabric-Ready Fortinet Alliance Partners in the CDM space include:

For more information and a complete listing of Alliance Partners, see Fortinet Technology Alliances.
MODERNIZING THE FEDERAL ARCHITECTURE TO ADDRESS TODAY’S THREAT LANDSCAPE

A complete solution for CDM could start by deploying FortiGate NGFWs to secure the evolving agency border and perimeter. Additional components relating to advanced threat protection, access management, endpoint protection, and forensics are then added until all requirements are met. Only proven Fabric products are selected to ensure interoperability and automation while reducing development costs.

MEETING CDM OBJECTIVES TODAY AND TOMORROW

The U.S. Department of Homeland Security’s CDM program is a logical progression toward realizing a more secure stance against the vast number of cyber threats fighting to breach our national infrastructure on a daily basis. Fortinet Federal is working closely with government customers and CDM prime contractors to ensure that the CDM solutions they offer can incorporate our newest, most innovative technology. By leveraging Fortinet technologies and solutions from Fabric-Ready Partners, federal agencies can successfully meet CDM’s objectives today without compromising on the needs of tomorrow.

To learn more about how Fortinet Federal can help your government agency achieve its CDM initiatives, visit our U.S. Federal Government webpage at www.FortinetFederal.com.