MAKING CDM WORK: CONTINUOUS DIAGNOSTICS AND MITIGATION REQUIRES A UNIFIED ECOSYSTEM

EXECUTIVE SUMMARY

As more and more federal agencies progress through the phases of the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program, integration between security solutions must become the "new best of breed," allowing agencies to build a unified ecosystem that automatically shares threat intelligence to enhance security and reduce costs.

SUCCEEDING WITH CDM

CDM is a federally funded program intended to fortify the cybersecurity of government networks and systems. It provides federal agencies with dashboards and tools to identify and prioritize cybersecurity risks, enabling cybersecurity personnel to mitigate the most significant problems first. CDM is essential to strengthening federal networks against attack, but if agencies are using disparate point products and lack automated risk reporting, significant time and resource requirements can make CDM expensive and complex to manage. Agencies can avoid falling into this trap by planning their CDM architecture as a unified whole, leveraging best-of-breed tools already deployed, and ensuring that gap-fill solutions are implemented to facilitate automation.

Extensive solution research is key to spending wisely using the CDM DEFEND (Dynamic and Evolving Federal Enterprise Network Defense) government-wide acquisition contract. Agencies should make sure to select security components that can work together and with the organization's existing solutions. Most agencies are nearing completion of CDM Phases 1 and 2, identifying what users and which devices are on their network. Moving into CDM Phases 3 and 4, which focus on continuous network monitoring and data protection, respectively, agencies will need to substantially improve the integration between their network security and infrastructure components.

Ultimately, success with CDM requires:

- A unified, integrated CDM ecosystem
- Regular auditing, leveraging CDM to automate Federal Information Security Management Act (FISMA) reporting
- A commitment to refreshing legacy systems and outdated technology

Agencies that follow these recommendations stand to gain the most value from CDM while avoiding the financial impact and reputation damage of a data breach.

A UNIFIED, INTEGRATED CDM ECOSYSTEM

Above all else, CDM solution components need to be able to talk to one another and exchange information. An integrated CDM platform supports automated and orchestrated processes, taking the manual effort and time lag out of diagnostics and mitigation. To build a truly integrated CDM ecosystem, agencies need to:

ADOPT INTENT-BASED NETWORKING.

To respond quickly to attacks, security devices need to share threat intelligence in real time. Intent-based networking is the third generation of network security, taking software-defined networking to the next level by adding a layer of intelligence that enables networks to be self-healing, proactive, and integrated to respond to new types of attacks. The eventual goal is full automation: a completely self-sufficient network that can predict future attacks and synchronize network security actions without human intervention.

To varying degrees, most federal agencies are undergoing digital transformations, making it even more important to increase network agility. Knowing who and what is on the network (including Internet of Things [IoT] devices and cloud) and what's happening everywhere on the network becomes all the more critical.

Intent-based networking requires using open application programming interfaces (APIs) and plugins to integrate with an agency's existing network security infrastructure and tie discrete solutions into an integrated whole. Look for CDM solutions that deliver universal and centralized control over networking components and advanced threat protections beyond what traditional security platforms or point solutions can offer. Ask vendors how they are laying the groundwork for intent-based networking capabilities in their current solutions, and how they fit into their product roadmaps.

ENSURE THAT STRONG VENDOR PARTNERSHIPS ARE IN PLACE.

To succeed for the long run, federal agencies need a unified security fabric combined with a rich partner ecosystem of technologies and services. Ideally, partners will integrate with the chosen security fabric via open APIs, allowing agencies to use a mixture of best-of-breed technologies for CDM. Some agencies will want to look for partnerships that include operational technology (OT) security outside the scope of traditional IT, such as industrial control systems. Increasingly, digital transformations are driving convergence.

USE A FABRIC ARCHITECTURE.

A security fabric is an intelligent framework that connects security devices from various technology partners together across multiple areas, allowing agencies to achieve CDM goals using solutions they have already paid for and deployed. A fabric architecture is a perfect fit for CDM because, when implemented correctly, it covers the entire attack surface and provides shared intelligence for fast, automated threat response. Beginning in Phase 3, CDM must fit into the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF), a holistic approach to categorizing information and information systems that is difficult to implement without an intelligent security fabric.

A truly unified fabric should map to eight essential areas:

1. **Network Security.** As network boundaries disappear and OT, cloud and mobile networks, and IoT converge, segmentation has become the fundamental defense strategy for borderless networks. To be effective, it must be accomplished with significant agility and granularity. Even as increasingly sophisticated cyberattacks pound the agency network perimeter, Fortinet high-performance firewalls provide consolidated advanced security and deep visibility that protects the network from known and unknown threats.

   The Fortinet Security Fabric can dynamically adapt to evolving CDM infrastructure requirements by segmenting the entire network, helping agencies prevent the movement of threats. Fortinet solutions support microsegmentation of VMware virtual server environments down to the hypervisor level with VMware NSX integration, enabling automated security deployments across an agency network. Macrosegmentation addresses the gap in security deployments for east-west traffic in hybrid cloud deployments. With so many agencies focusing on cloud migrations, many are forgetting that a hybrid cloud model should be the focus to maintain security visibility across the on-premises to public cloud pathway. In addition, hybrid cloud models help preserve network performance by reducing the latency of traffic processing that is frequently experienced by conducting all of one's traffic and security inspection processing purely in the public cloud.

   Macrosegmentation works hand in hand with microsegmentation to secure the traffic streams that define agencies' hybrid cloud networks. In recognition of the value that macrosegmentation provides in an enterprise network architecture, Fortinet addresses macrosegmentation with its Fabric Partnership with Arista by leveraging the programmability of Arista's extensible operating system (EOS) and combining CloudVision Macro-Segmentation Services (MSS) with the Fortinet Security Fabric.

2. **Multi-cloud Security.** Many agencies have multiple cloud deployments, which makes consolidated security prevention and detection difficult. Fortinet's integrated virtual and physical cloud solutions protect all your dynamic cloud environments and Software-as-a-Service (SaaS) applications.

   In the U.S. General Services Administration's 2017 Hybrid Cloud Almanac, the convergence of digital services was highlighted as evidence that federal agencies are now focusing on the overall computing experience and not on the solution itself.[1] Thus, it's critical for agencies to deliver a multi-cloud security model that unifies the security administration experience for network and security administrators as much as it delivers an effective security model that is transparent to federal network users.

3. **Web Application Security.** Unprotected web applications are easy entry points for hackers to exploit. The FortiWeb web application firewall uses the latest threat intelligence to protect web applications from sophisticated attacks. Artificial intelligence (AI) capabilities will become more and more critical, allowing agencies to detect malicious files that have never been seen before. Recognizing this need, Fortinet makes the FortiGuard AI self-evolving detection system a part of every Fortinet solution.
4. **Email Security.** The majority of malware still enters networks via email attachments. The FortiMail secure email gateway inspects incoming and outgoing email, blocks malicious messages, and prevents sensitive information from being leaked. Federal agencies can also use FortiMail to comply with the DHS's Binding Operational Directive 18-01 (BOD-18-01), which requires agencies to revamp their email security protocol by deploying STARTTLS, Secure Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). For more information, see the Fortinet blog "How Federal Agencies Can Use FortiMail to Comply with BOD-18-01."[2]
5. **Advanced Threat Protection.** Agencies combating security threats on all fronts need world-class threat intelligence updates automatically delivered to their security solutions. FortiGuard Threat Intelligence shares information about newly discovered exploits. Fortinet sandboxing solutions isolate and inspect any suspicious files detected by security tools.
6. **Secure Unified Access.** Securing business communications, personally identifiable information (PII), and mobile devices requires much more than access control, because typical Wi-Fi solutions only address connectivity and access security. Fortinet's secure access solutions integrate tightly to enable a common security policy across the network, addressing network, application, and device management requirements as well as providing secure Wi-Fi.
7. **Endpoint Security.** Endpoint devices connected to the network are common entry points for threats. But endpoint solutions often don't share threat intelligence with the rest of the network, which slows down threat response. By integrating into the Fortinet Security Fabric, FortiClient adds another layer of automated security for better overall network protection.
8. **Management and Analytics.** Seeing and understanding threats and events throughout the network is a big challenge for enterprises with disparate security products. Fortinet solutions for logging, reporting, and centralized security management pull data from Fortinet and Fabric-Ready security products, providing the visibility to efficiently manage security processes and automate responses. Management and analytics are critical, and the Fortinet Security Fabric allows data to be consolidated in a variety of security information and event management (SIEM) tools to improve visibility.

REGULAR AUDITING

Another benefit of a unified CDM architecture is that with unified visibility, that provides reporting and logging all in one place, it's easier to audit the entire fabric. Vendors that offer truly integrated solutions may include automated security fabric audits as part of their next-generation firewall functionality, regardless of whether the firewall is deployed at the perimeter, data center, or in the cloud. This helps agencies tune their network configurations and gain more visibility and control. By providing a score based on how many checks the network passes or fails during each audit, agencies can build confidence that their network is getting more secure over time.

REFRESH LEGACY SYSTEMS

Although the cost of new systems can be high, the cost avoidance can be higher. U.S. federal agencies spend approximately 80% of their IT budgets on operating and maintaining outdated legacy systems—more than $60 billion a year.[3] Legacy systems can also be more difficult to secure, with outdated or unpatched software and hard-coded passwords. Integration and automation can reduce costs while significantly reducing the time it takes for agencies to mitigate detected threats in real time, without needing direct human intervention to do so.

CDM DEFEND is the perfect contract opportunity for agencies to upgrade and eliminate the security silos that have made it challenging for them to keep up with CDM deployment and adoption timelines. Agencies that choose Fortinet solutions benefit from the same forward-looking security architectures that protect global enterprises from ransomware outbreaks months before the threats appear in the public media's front-page stories.

A MORE SECURE FUTURE

When it comes to building a self-evolving network on a government budget, DEFEND may be the perfect opportunity for many federal agencies to catch up and build a resilient infrastructure that will protect them from tomorrow's threats. CDM can help agencies improve their security posture and transition from a culture centered around annual security audits to one that continually measures the success of network security in real time. Further, a solution that natively integrates components across the CDM phases adds tremendous efficiencies and greatly increased security.

Learn more about security challenges federal agencies face and solutions on our federal agency resource hub: http://hub.fortinet.com/federal.

1 U.S. General Services Administration Cloud Computing Services, "2017 Hybrid Cloud Almanac."
2 Felipe Fernandez, "How Federal Agencies Can Use FortiMail to Comply with BOD-18-01," Fortinet blog, October 30, 2017.
3 Frank Konkel, "Some Agencies Spend More Than 90% of IT Budgets on Legacy Systems," Nextgov, October 25, 2016.

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

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

July 20, 2018 2:07 PM