FORESCOUT

Solution Brief

CDM Defend

Operationalizing CDM by Moving from Cyber Hygiene to Risk Mitigation

The Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program is in a period of transition. With many core foundational technologies in place, federal civilian departments and agencies must build upon that foundation and operationalize the CDM toolset to mitigate risks in real time.

The CDM program was initiated in 2013 with the goal of identifying risk within federal network environments and then mitigate the most severe risks first. A core goal of the program was to deploy a consistent and complementary set of capabilities across multiple federal civilian environments to gain economies of scale and uniformity of approach. These capabilities include, first and foremost, the ability to continuously identify all assets and users on federal civilian networks. Forescout currently delivers this capability for nearly all federal agencies as the preferred solution for CDM hardware asset management (HWAM). Real-time visibility of all devices connecting to federal networks is a foundational cyber hygiene capability that enables the addition of more advanced cybersecurity techniques that will be implemented in the new Dynamic Evolving Federal Enterprise Network Defense (DEFEND) acquisition phase of the program.

The Challenge

The foundation for CDM is nearly in place for most enterprises with the federal government. Beginning with the essential task of understanding 'What is on the network?' and 'Who is on the network?', DHS has identified on average 75% more devices connected the federal networks than previously reported.[1] With the new DEFEND phase of the program initiated last year, the foundational capabilities previously deployed move into a risk mitigation, operations and maintenance phase. DEFEND's core activities include: the deployment of capabilities to mitigate risk (addressing found vulnerabilities), analytics to generate risk scores (AWARE scores) and data aggregation in the agency and federal dashboard for executive-level decision-making. Pivoting from a 'discovery' to 'mitigation' phase will inevitably be a challenge as those actions have the potential to disrupt the course of business. On the other hand, risk mitigation and data analytics capabilities are likely to have the greatest impact on an agency's ability to defend its information and networks as well as address many agency priorities. For this reason, it is critical that departments and agencies mature their CDM deployments.

The Forescout Solution

Forescout's agentless and continuous approach to asset visibility and management enables complete domain awareness, risk assessment and mitigation and reporting. Forescout shares information bidirectionally with other CDM tools, including agency and federal dashboard solutions, to support and prioritize risk mitigation. The result is an unprecedented ability for departments and agencies to assess and manage cybersecurity risk across the entire Federal civilian enterprise in real time. Moving from point-in-time compliance to continuous compliance assessment, as shown in figure 1, is critical to the success of CDM to move from improving cyber hygiene to automated risk mitigation.

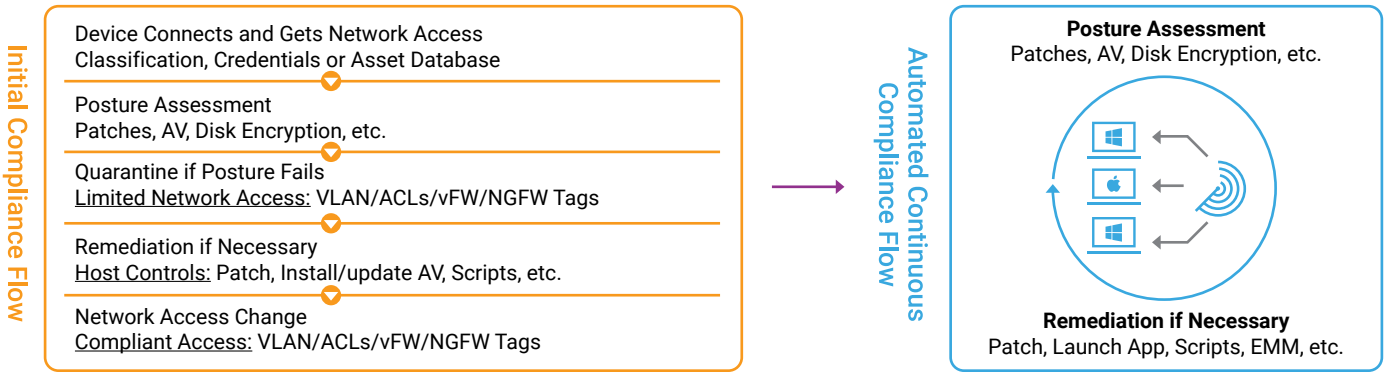

Figure 1 - Continuous Compliance Assessment

The Future

Forescout is committed to the success of the evolving CDM program and to the missions of the federal civilian agencies. CDM's success will be rooted in the achievement of the program's goal to identify and mitigate risk, as well as the extent to which it can also help agencies solve many of their long-standing security challenges.

Forescout is proud to be both a foundational CDM technology through our HWAM capabilities and a leader helping agencies solve some of their emerging challenges in a variety of compute locations that include: legacy data centers, integrated operational technology networks, expanded virtual networks and the federal "Cloud First" initiatives.

Once federal agencies establish their security policies, Forescout's native capabilities to take action and control devices can further help agencies drive down their cyber risk. These capabilities fall into a few broad areas that agencies can pursue as they advance the CDM capabilities in their enterprise:

- **Network Access Control (NAC)** - Control access to enterprise resources based on user profile (guest, employee, contractor), device properties, classification and security posture. Forescout enforces and automates policy-based network and host controls through integrations with heterogeneous physical and virtual network infrastructure. Actions can be automated or administrator-initiated, and gradually increased to minimize disruption while reducing manual effort to enforce network access, improve device compliance, implement network segmentation and accelerate incident response.
- **Network Segmentation** - Apply dynamic network segmentation policies across disparate enforcement technologies in your extended enterprise through a common policy framework.
- **Preparing for Zero Trust Networking** - Discovering and classifying 100% of the IP-connected devices that access the network—not just those with endpoint agents installed and operational—and strictly enforcing least-privilege access policy is the foundational goal of a Zero Trust strategy.
- **Incident Response** – Detecting and assessing a device's compliance upon connection and orchestrating a response in real time with an agency's security and IT management tools increases the productivity of an incident response team and reduces and agency's window of exposure. In addition to accelerating response, the orchestration of response workflows and processes also maximizes the ROI of security tools.

Learn more about Forescout government solutions at **www.forescout.com/industries/government/**

1 https://www.meritalk.com/articles/cdm-the-story-so-far/

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com