ForeScout

Continuous Visibility and Control: Building A Solid Foundation for CDM

See

- Gain continuous asset visibility for advanced cybersecurity techniques in later CDM phases.

Control

- Limit access or remove unauthorized devices to help prevent exploitation of internal and external network boundaries.
- Meet network access control requirements for CDM Boundary Protection with a solution that's easily customized to your department's or agency's unique needs and environment.

Orchestrate

- Continuously collect and share information about device behavior with CDM Phase 3 tools.

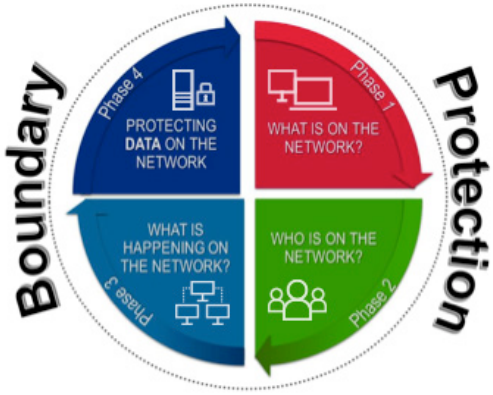

Figure 1: Implementation of the CDM program spans four phases.

The Next Phase of Continuous Diagnostics and Mitigation (CDM)

The federal government's Continuous Diagnostics and Mitigation (CDM) program provides federal departments and agencies with capabilities and tools to secure networks and systems. The program is designed to identify and prioritize cybersecurity risks, enabling cybersecurity personnel to mitigate significant problems first on a continuous basis. Using ForeScout CounterACT®, CDM is laying a foundation to improve the fundamental cyber hygiene of government IT networks, and will soon move to advance the protection of network boundaries.

Federal departments and agencies use commercial off-the-shelf tools to perform automated searches for known cyber flaws, alert network managers of their worst and most critical cyber risks, and efficiently allocate resources to address those risks based on severity. Summary information can feed into an enterprise-level dashboard to provide situational awareness of the cybersecurity risk posture across the federal government.

In 2013, the Department of Homeland Security (DHS), in partnership with the General Services Administration (GSA), established a government-wide acquisition vehicle for CDM. ForeScout is proud to partner with DHS, GSA and other federal departments and agencies, as well as CDM Blanket Purchase Agreement (BPA) participants to transform security through visibility of endpoints, network devices and Internet of Things (IoT) devices by seeing, controlling and orchestrating a system-wide response.

DHS has organized the delivery of CDM tools and services into several phases as shown in Figure 1. Phase 1 and 2 of the CDM program establish the foundational capabilities to protect the federal government's IT systems and data by identifying 'what' and 'who' are on its networks. CDM Phase 1, which is being deployed by many federal agencies, provides capabilities across four tool areas: Hardware Asset Management, Software Asset Management, Configuration Settings Management and Vulnerability Management. Phase 2 focuses on tools and capabilities to identify 'who' is on the network.

Next, under Phase 3, DHS will move to understand 'what' is happening on the network and Boundary Protection, also known as BOUND. Under the BOUND tool area, DHS has grouped multiple tools to secure the network boundaries of federal departments and agencies. BOUND includes tools for Network Access Control, packet and content filtering, data loss/prevention, encryption and key management and certificate authorities.

ForeScout – A Foundational CDM Partner

The CDM program selected CounterACT in Phase 1 as the de facto standard for Hardware Asset Management (HWAM) and visibility. Continuous visibility of 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 later CDM phases. ForeScout's agentless and continuous approach to seeing what is connected to federal networks will enhance the federal government's cybersecurity posture by identifying previously unknown and unauthorized desktop, laptop, network and Internet of Things (IoT) devices on these networks. ForeScout is proud to be providing a baseline cybersecurity capability to a significant number of federal departments and agencies through the CDM program.

ForeScout is flexible, offering numerous configurations in heterogeneous network environments.

- Heterogeneous support of network devices and manufacturers (works with what you have)
- Accomplishes BOUND requirement without network reconfiguration
- Either pre- or post-connect authentication
- Agent and agentless
- Centralized, decentralized and hybrid architecture deployments

ForeScout can enforce a broad range of control actions—from modest to stringent, allowing you to:

- Notify end users, administrators or IT systems about security issues
- Conform with policies, industry mandates and best practices such as network segmentation
- Restrict, block or quarantine non-compliant or compromised devices

To see a complete list of CounterACT control capabilities, visit www.forescout.com/control.

About ForeScout

ForeScout Technologies is transforming security through visibility, providing agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. See devices. Control them. Orchestrate system-wide response.

Learn how at www.forescout.com.

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

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

Protecting the Boundary

The foundational capability ForeScout CounterACT provides in CDM Phase 1 will provide departments and agencies with the information needed to limit access or remove unauthorized devices to prevent exploitation of internal and external network boundaries. BOUND differs from CDM Phase 1 in that CDM moves from a focus on gathering attributes about assets on the network to proactively taking action to restrict or remove access for assets. The CDM boundary controls tool area is focused on managing network access controls by leveraging sensors and tools intended to monitor and manage physical and logical access to networks, data and locations. At ForeScout, we believe the ability to automate the removal of non-compliant devices and limit unauthorized network connections are essential to protect both internal and external boundaries.

As with Phase 1, ForeScout is poised to provide Network Access Control capabilities under BOUND, as these capabilities are already embedded in the CounterACT solution currently being deployed under Phase 1. ForeScout CounterACT will help mitigate risks from inadvertent or malicious connections of unauthorized, rogue and non-compliant devices. CounterACT satisfies the BOUND Network Access Control requirements to help ensure:

- Devices are authenticated to remain connected
- Only authorized and compliant devices are allowed to connect
- Automatic remediation of non-compliant devices
- Devices are located in the appropriate logic segment of the network based on authentication and policy compliance

ForeScout CounterACT also offers flexibility to customize access control solutions to a department's or agency's unique needs and environment. These include high availability configurations for mission-critical networks and the ability to deploy in centralized, decentralized or hybrid network architectures. ForeScout can also be configured to deny access to network services until the devices are authorized to connect (pre-connect) or allow devices limited access to network services while automating updates and security patches to bring devices up to baseline compliance (post-connect). Finally, CounterACT can provide Network Access Control without the need for an agent, but can deploy an agent to the endpoint in circumstances when needed.

Via Phase 1 HWAM deployments, ForeScout offers federal departments and agencies extensive capabilities to determine whether devices are authorized or unauthorized, as well as myriad enforcement options to control device access as required in BOUND and Phase 3.

Phase 3 – What's Happening on the Network

CDM Phase 3 builds on the capabilities in Phases 1, 2 and BOUND to move beyond asset management to a more extensive and dynamic monitoring of security controls. Phase 3 will include preparing for and responding to incidents, ensuring software and system quality is integrated into the network, detecting internal actions and behaviors to determine who is doing what and mitigating security incidents to prevent their spread throughout the network.

CounterACT's ability to see the devices on the network and continuously collect and share information about the behavior of those devices will be a critical source of information for Phase 3 tools. ForeScout Extended Modules orchestrate information sharing and automate workflows among many of the security compliance tools in the federal government that will provide Phase 3 capabilities. ForeScout CounterACT will play a key role in enabling security personnel to rapidly share information between these tools and begin to automate responses to incidents rapidly. For an overview of ForeScout's CDM Phase 3 capabilities, send a note to: CDM@forescout.com.