Continuous Diagnostics and Mitigation

CounterACT Security Platform

The ForeScout CounterACT Security Platform provides real-time monitoring, control and policy-based remediation of managed, unmanaged and non-traditional devices to serve as a cornerstone for CDM. Here's how:

See

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor managed devices, BYOD and IoT endpoints

Control

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints
- Improve compliance with industry mandates and regulations

Orchestrate

- Share contextual insight with IT security and management systems
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

To ensure an acceptable and consistent level of confidentiality, integrity and availability of information assets, government IT organizations must comply with a growing number of regulations, directives and standards. The main objective is to eliminate intrusions (confidentiality), protect sensitive information (integrity) and mitigate exposure to denial of service cyberattacks (availability).

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based and cost-effective cybersecurity and more efficiently allocate cybersecurity resources.

The "continuous" requirement in CDM doesn't necessarily mean 24x7; instead, it means recurring assessments at an interval commensurate with the value of the information and the estimated level of risk. Federal publications provide guidelines for determining the frequency of assessment, based on criteria such as security control volatility, system impact levels in terms of function protected and any identified weaknesses. These guidelines define Detection Interval Latency (DIL) as the metric used in measuring and auditing the acceptable level of response in a CDM security program.

CDM Adherence Challenges

Rather than a passive reaction and documentation approach, CDM demands proactive, data-centric, risk-based action. This typically requires a significant shift in security infrastructure, as process and data integrations must cross organizational, data and system boundaries. In the CDM framework, data collection, asset management and risk management processes happen continually, not periodically, across the environment. The biggest technical challenges for IT organizations are associated with the integration and correlation of the continuously streaming data.

As new data about the IT environment becomes available, the CDM system is required to ingest the data and respond by elevating thresholds and adapting network policies and control actions in a perpetual feedback loop. CDM also requires the streamlining of costly security operations to help senior federal officials gain greater visibility into their organization's security health and risk management information. An effective implementation should collect data from ongoing processes, correlate against multiple contextual factors, take action automatically where appropriate and present the remaining issues in priority order.

Highlights

Real-time visibility. Gain automated, real-time visibility of endpoints as they connect to your network. Even detect stealthy sniffer devices that do not utilize an IP address.

Active Asset Management. Generate a real-time inventory of your network: devices, hardware, operating systems, applications, patch levels, processes, open ports, peripheral devices, users and more.

Policy-based Access Control. Limit network access to authorized users and devices with or without 802.1X for switch port security.

Continuous Monitoring. Assess the security and compliance posture of endpoints in real-time before and after they connect to your network. Detect endpoint configuration violations, malicious behavior and tailor the response based on the severity of the violation.

Automated Remediation. Automate the remediation of noncompliant endpoints by auto-updating the endpoint configuration and protection systems, patches and updates, and installing, activating or disabling applications or peripherals.

HBSS Integration. Increase situational awareness and incident response by automatically detecting and remediating endpoints with missing or broken Host Based Security System (HBSS) agents. Grant, deny or limit network access based on compliance standards assessed by HBSS.

Compliance Reporting. Produce real-time reports reflecting your level of policy compliance. Shorten Detection Interval Latency (DIL) by initiating compliance scans as hosts connect to the network, rather than waiting for time-based scans.

Implementation Requirements

To embrace CDM, organizations must invest in real-time asset discovery and vulnerability management; automated, intelligence-driven response mechanisms; and continuous feedback of data into an enterprise management system. Furthermore, the system needs to be easily deployed within your existing IT framework.

A real-time asset discovery and vulnerability management system should use a combination of passive and active discovery and monitoring techniques to detect and profile systems on the network, independent of operating system or form factor. Passive discovery techniques monitor traffic to see which devices are alive. Active discovery techniques probe the network to track down idle devices. Together, full and constant visibility of IT assets can be achieved. As soon as someone installs or reconfigures a device on the network, the change can be detected and the device can be assessed. Finally, the asset management system should include the ability to assess the security postures and vulnerabilities of endpoints on the network.

The automated response mechanism should be able to take inputs from the asset discovery and vulnerability management system and, based on this information plus an awareness of endpoint behavior, generate a set of intelligent responses designed to reduce enterprise risk. The responses should be appropriate based on the severity of the policy compliance violation and/or the behavior of the endpoint. For example, the response system should be able to respond with actions such as:

- Send an alert to the individual or the appropriate IT management team
- Automatically remediate the endpoint or trigger a third-party system to remediate the endpoint
- Limit network access
- Block network access

Asset data and automated control actions should be fed back into other aspects of the CDM system in order to optimize the efficiency and effectiveness of the overall system (see Figure 1). For example, linkages between the CDM system and the organization's security information and event management (SIEM) systems helps ensure that compliance reports generated by the SIEM system are accurate.

The CDM system should also feed information into agent-based systems such as antivirus, patch management and mobile device management (MDM) systems in order to ensure that these systems are aware of unmanaged endpoints that are on the network.

Finally, the CDM system should be quick and easy to deploy. For example, the system should:

- Deploy within the existing network infrastructure without the need to re-architect the network
- Integrate with existing network infrastructure
- Not rely on in-line deployment or any other single points of failure
- Not require the installation of additional endpoint agents

Highlights (continued)

Mobile and Wireless Controls. Detect and enforce security controls on mobile devices such as smartphones and tablets. Enforce wireless compliance through integration with wireless network infrastructure.

Non-disruptive Deployment. CounterACT can be deployed in a phased approach to minimize disruption and accelerate results.

IT Interoperability. Leverage integration with existing IT infrastructure such as directory services, patch management, endpoint protection, vulnerability assessment, SIEM and MDM systems.

ForeScout CounterACT® as a Cornerstone for CDM

ForeScout CounterACT® addresses the requirements for CDM and can serve as the centerpiece of your CDM solution. CounterACT provides real-time visibility and control for endpoints on your network including smartphones, tablets, netbooks and other corporate and personal mobile devices connected to your network.

CounterACT uses a combination of discovery techniques to accurately classify endpoints through passive and active interrogation techniques. CounterACT's agentless solution enables it to work with various types of endpoints—managed and unmanaged, known and unknown.

CounterACT can assess the security posture of endpoints on your LAN/WAN environment. This is especially important for unmanaged bring your own device (BYOD) endpoints because your existing endpoint management systems are typically blind to these devices. CounterACT can assess the security posture of managed devices (domain-connected computers) without the need to deploy an additional agent to those devices; this is a critically important factor that aids in the rapid deployment and ease of operation of the CounterACT system. CounterACT can assess the security posture for unmanaged BYOD devices via the installation of a lightweight dissolvable agent. This agent supports Windows®, MacOS and Linux. It can be automatically deployed when the user connects to the network and registers their identity on the system. Regardless of whether or not an agent is used, CounterACT can perform a wide range of compliance checks including monitoring for required software, software versions and patch versions, device configuration and endpoint vulnerabilities, just to name a few. It integrates with leading network, security, host-based security system and identity platforms to provide real-time endpoint intelligence and security posture awareness.

ForeScout CounterACT includes a wide range of endpoint remediation actions based on the endpoint's security posture. CounterACT can direct the antivirus server to automatically update a non-compliant host, or it can prompt the patch management system to update the device's operating system, or it can disable unauthorized software. In addition, CounterACT supports the leading SIEM systems to provide endpoint configuration details, correlate access and compliance violations and expedite incident response. CounterACT includes built-in reports to help you monitor policy compliance, support regulatory audit requirements and produce real-time inventory reports.

ForeScout CounterACT is sold as either a virtual or physical appliance that deploys seamlessly within your existing network, typically requiring no infrastructure changes, and adding no latency to your network operations. The CounterACT appliance installs out-of-band, avoiding latency or potential for network failure, and can be centrally administered to dynamically manage tens or hundreds of thousands of endpoints from one console.

ForeScout CounterACT employs a proven approach for IT risk management. Devices that access your network are identified, controlled, remediated (if you wish), and continuously monitored to ensure compliance and protection. Its compliance engine will detect when devices or users are out of compliance with your security policy and track down users who are engaging in risky behavior such as using Peer-to-Peer (P2P) applications, USB drives, smart phones, and other unauthorized activities. Non-compliant computers and/or users will be displayed in the main console, including the reason for non-compliance and details such as location of the device.

Lastly, CounterACT helps IT managers achieve acceptable Detection Interval Latency (DIL) metrics by integrating with compliance scanners to add event-based scanning functionality. Through this integration, CounterACT triggers the compliance scanner when a host connects to the network. The addition of event-based scanning will significantly improve your DIL metric. ForeScout CounterACT integrates with a number of leading vulnerability assessment (VA) scanners such as Tennable® Nessus, BeyondTrust® Retina, and Qualys®, and other integrations are under development.

Reduce Complexity and Increase Efficiency

In the past, IT security managers tended to address each risk with a specific technical solution. Regulatory mandates were addressed with specialized controls. This provided an acceptable level of short-term security and compliance. Today we know that security solutions that are independent of each other increase complexity, and complexity increases risk as well as the manpower cost of administration. The lack of interconnectivity among IT controls is a primary challenge that makes it difficult for IT departments to manage risk efficiently. It also results in poor situational awareness and limited actionable information for rapid threat detection and risk mitigation.

ForeScout CounterACT helps solve this problem. CounterACT integrates with existing systems to create a responsive and accurate continuous monitoring system that cuts through complexity to give you much greater efficiency by design. As a result, the system enables real-time visibility, deep endpoint inspection, continuous monitoring, and automated remediation, system integration with other security management systems, rapid deployment and low total cost of ownership.

Figure 1: Desired State — ForeScout CounterACT provides real-time visibility of your network and shares information bi-directionally with existing operational and security infrastructure.

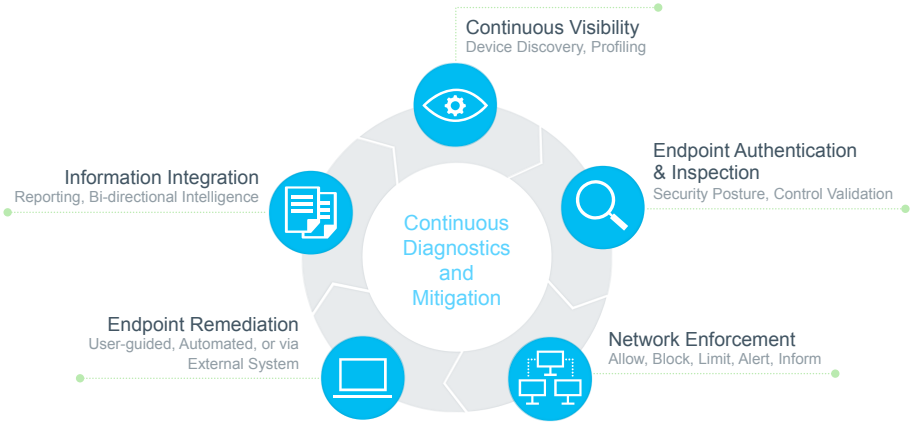

Figure 2: ForeScout's intelligent security automation platform provides real-time visibility and automated control.

Continuous Diagnostics & Mitigation Criteria[1]		ForeScout CounterACT
Asset Discovery & Classification	Discover unauthorized or unmanaged hardware on a network, discover unauthorized or unmanaged software configuration in IT assets on a network.	CounterACT discovers network devices in real-time and maintains a comprehensive database of hardware and software assets. The inventory can be searched and organized by various hardware and software attributes. Inventory reports can be generated.
Assessment	Assess the security posture of endpoints resulting in an accurate and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings.	CounterACT can assess the security posture of endpoints on your LAN/WAN environment. This is especially important for unmanaged devices (BYOD) because existing management systems are typically blind to these devices. CounterACT can perform a wide range of compliance checks including monitoring for required software, software versions and patch versions, device configuration and endpoint vulnerabilities. It integrates with other host-based agents/tools and vulnerability scanners to obtain additional compliance information.
Authentication & Access Control	Prevent, remove and limit unauthorized network connections/access to prevent attackers from exploiting internal and external network boundaries and then pivoting to gain deeper network access and/or capture network resident data in motion or at rest. Manage account access, security-related behavior, credentials and authentication.	CounterACT can block or restrict access to unauthorized devices as well as devices which become non-compliant while connected to the network. CounterACT is event driven and will re-assess an endpoint when a configuration changes in its operating system.
Automated Mitigation & Remediation	Prevent exploitation of the system by consciously designing the system to minimize weaknesses and building the system to meet that standard in order to reduce the attack surface and increase the effort required to reach the parts of the system that remain vulnerable.	When compliance violations are detected, CounterACT can respond based on the severity of the violation by simply alerting or notifying the IT staff, or auto-remediating, quarantining or blocking non-compliant endpoints. It can also interface with a third-party system such as patch management.
Situational Awareness	An accurate and timely endpoint status is essential to support awareness, effective control, and reporting of any organizational security issues in the network.	CounterACT provides comprehensive situational awareness by identifying endpoints on the network and integrating with other security management systems such as endpoint lifecycle management products, asset management systems, databases, SIEM, VA, and antivirus products, resulting in real-time endpoint intelligence and security posture awareness. In addition, it supports SIEM systems to provide endpoint configuration details, correlate access and compliance violations.

[1]Reference "Continuous Diagnostics & Mitigation Criteria"
https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f154da08471898c2e7a9ab05595c3df6

ForeScout ControlFabric® Architecture

The integration between ForeScout CounterACT and your CDM solution is just one of many IT system integrations that leverage ForeScout ControlFabric Architecture. ControlFabric is an open technology enabling ForeScout CounterACT and other solutions to exchange information and more efficiently mitigate a wide variety of security issues. Learn more at www.forescout.com/controlfabric.

Take the ForeScout Challenge

Let us know which ForeScout solution is right for you, and we'll arrange a free on-site evaluation.

About ForeScout

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. More than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions.*

Learn more at www.forescout.com.

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

* As of October 2015