# ForeScout CounterACT CONTINUOUS DIAGNOSTICS & MITIGATION (CDM)

ForeScout

# CONTENT

## Introduction

This document has been created to explain the mechanisms used by ForeScout CounterACT™ that adhere to the requirements for the Federal Continuous Diagnostics & Mitigation (CDM) Program, or what private sector organizations are calling Continuous Monitoring.

## Overview of Continuous Diagnostics & Mitigation (CDM)

In 2010, the U.S. government began shifting its security approach from periodic assessments to continuous monitoring. This program is called Continuous Diagnostics and Mitigation (CDM). The CDM program provides continuous monitoring, diagnosis, and mitigation activities designed to strengthen the security posture of federal networks. "Continuous" in this sense 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 prioritized risk. The most common recurring assessment plans call for a reassessment of each device within 72 hours. CDM calls for detecting new equipment within seconds of connecting the equipment to the network.

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. To ensure an acceptable and consistent level of information asset confidentiality, integrity, and availability, government IT organizations must comply with a large number of additional regulations, directives, and standards. The main objective of government IT security programs, including CDM, are to eliminate intrusions (confidentiality), protect sensitive information (integrity), and mitigate exposure to cyber-attacks (availability).

The CDM program is tasked with providing federal agencies and state and local governments with the ability to enhance and automate their existing network monitoring capabilities, correlate and analyze critical security-related information, and strengthen risk-based decision making at the enterprise level to meet these operational standards and regulations for federal data. The CDM program will allow for the correlation and analysis of security-related information across the federal enterprise. Using input from the sensors and agency-level dashboards, officials at each agency will be able to quickly identify which problems to fix first, and empower technical managers to prioritize and mitigate risks. Eventually the administration expects that civilian agencies must and will enhance their cyber security posture and improve their Federal Information Security Management Act (FISMA) score by implementing CDM and offering Continuous Monitoring as a Service (CMAAS).

## CDM Requirements

A Request for Information (RFI) was released by the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program in 2012. The DHS is tasked with leading the CDM initiative in the Federal sector in an effort to change security requirements from a passive reaction and documentation approach to a proactive, data-centric, risk-based action approach. This new approach 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 must happen continually, not periodically, across the environment. The biggest technical challenges for IT organizations are 1) obtaining real-time awareness of every device that is connected to the network, and 2) integrating and correlating the continuously stream of information that comes from time-based periodic scanners.

The 2012 DHS RFI identifies specific areas of information management that are required by CDM as a basis to identify, prioritize, and utilize Federal data:

1. **Hardware Asset Management**
   Prevent attackers from exploiting unauthorized and unmanaged hardware by maintaining an inventory of all hardware assets, so IT organizations can either remove unmanaged hardware from the network, or assign it to be remediated.

2. **Software Asset Management**
   Prevent attackers from exploiting unauthorized software by ensuring that software inventories reflect any variance from the organization's approved software inventory, and to control software versions and patch levels so that integrity can be maintained.

3. **Configuration Management**
   Prevent the exploitation of weak configuration settings (including port, protocols and services) by defining an appropriate desired operational state for these settings and maintaining it in operation. This capability addresses the modification of parameters that affect the underlying behavior of the software or hardware.

4. **Vulnerability Management**
   Prevent attackers from exploiting vulnerabilities by using the National Vulnerability Database [NVD] and other tools to find and remove such vulnerabilities. This capability ensures that vulnerabilities are identified and removed or remediated from operational systems faster than they can be exploited.

5. **Manage Network and Physical Access Controls**
   Prevent, remove and limit unauthorized network (or physical) connections/access to prevent attackers from exploiting internal and external network boundaries and then pivoting to gain deeper network access and/or capture network endpoint data in motion or at rest.

6. **Manage Trust in People Granted Access**
   Prevent insider attacks by carefully screening new and existing persons granted access for evidence that access might be abused.

7. **Manage Security-Related Behavior**
   Prevent general users from taking unnecessary risks to prevent attackers from exploiting network and application users via social engineering scams. Prevent users with elevated privileges and special security roles from taking unnecessary risks to prevent attackers from exploiting poor engineering and/or remediation.

8. **Manage Credentials and Authentication**
   The Manage Credentials and Authentication capability ensures that account credentials are assigned to, and used by, authorized people. This covers credentials for physical and logical access.

9. **Manage Account Access**
   Prevent access beyond what is needed to meet business mission by limiting account access and eliminating unneeded accounts to prevent attackers from gaining unauthorized access to sensitive data.

10. **Manage Response to Incidents**
    Prevent repeat of previous attacks and limit the impact of ongoing attacks by using forensic analysis, audit information, etc to; a) appropriately respond to end ongoing attacks; and, b) identify ways to prevent recurrence to prevent attackers from maintaining ongoing attacks and exploiting weaknesses already targeted by others.

11. **Manage Preparation for Contingencies**
    Prevent loss of confidentiality, integrity and/or availability by being prepared for unanticipated events and/or attacks that might require recovery and/or special responses, preventing attacker's compromises from being effective by adequate recovery.

12. **Design and Build Security into the System**
    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.

13. **Manage Assessments to Find and Fix Weaknesses**
    Prevent attackers from exploiting weaknesses by finding and prioritizing weaknesses, and fixing the most important weaknesses first. This capability addresses software before it is installed and operational.

14. **Manage Audit Information and Accountability**
    Prevent persistent attacks and weaknesses by using audit information to identify them and initiate an appropriate response.

15. **Manage Overall Operational Control Limits**
    Prevent attackers from exploiting weaknesses by using functional and operational control limits to help senior managers determine when to authorize operation of systems, and when to devote extra attention to reducing risks by identifying and resolving system weaknesses.

In September 2010, the DHS Federal Network Security Branch issued a document called Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture Report that addresses these areas of management. At its core, CAESARS is a decision support system that is modeled on implementations in Federal agencies that have proven to be effective in visualizing endpoint security posture details in order to derive actionable information that is prioritized. CAESARS framework summarizes continuous monitoring in four steps: 1) Find everything on the network. 2) Check it for vulnerabilities. 3) Remediate or remove vulnerable devices. 4) Report everything up.

## CDM Challenges

To embrace CDM, organizations must invest in real-time hardware and software asset discovery; configuration and vulnerability management systems; automated, intelligence-driven response network access control mechanisms; and systems that continuously feed data back into an enterprise management system for complete situational awareness. Typical "real-time" network security or asset management systems demand a great deal of processing power and a large volume of bandwidth on your network. Gaining an accurate "real-time" situational awareness with an enterprise management system depends on the endpoint data that it is receiving from your network. The correlation of endpoint data in addition to the bandwidth and processing power that is required to initially gather it provides a significant challenge to IT organizations.

The raw processing and bandwidth issues aside, there are also significant demands on the type of information that is processed, where and how that information is captured from your network, and then the data collation necessary to make action decisions on a risk-based approach.  What actions are appropriate for each situation on your network? Can these actions be automated? What devices will provide blocking actions or redirect a user's device to the appropriate resources? Furthermore, the system needs to be easily deployed within an existing IT framework.

A large part of meeting this challenge is to reduce data processing by only collecting and processing the required data in the first place. For example, instead of periodically assessing all characteristics of all endpoints, only assess system configuration settings on systems that have changed, and only assess systems that have not been assessed recently.

Basically, this security platform should measure risk, prioritize it and take action; detect changes to endpoints that deviate from an organization's compliance standard for that type of endpoint; detect threats on the network; collate the endpoint data to provide an accurate response to reduce risk; and enable action to be instituted either manually or automatically.

So, if there is a platform that could automate most or all of these tasks, what attributes would this real-time platform have to meet this challenge?

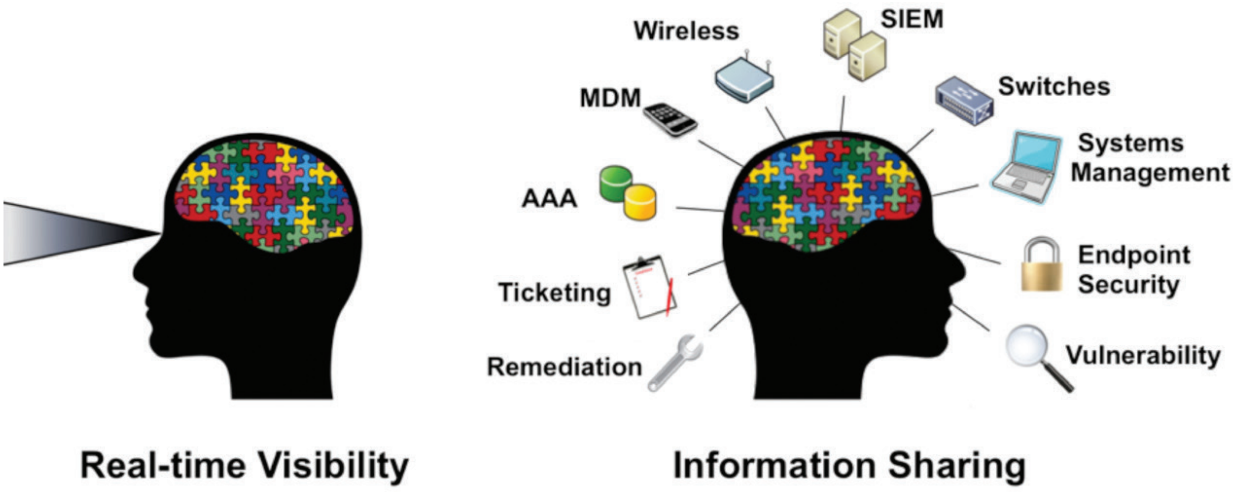


***Figure 1:*** *CDM should enable the desired state of real-time visibility and information sharing with other third party systems for a coordinated response to security requirements.*

## ForeScout CounterACT as a foundation for CDM

ForeScout CounterACT is an intelligent security automation and control platform that enables an organization to meet CDM requirements. CounterACT does this with real-time visibility of hardware and software for all endpoints, automating actions to address asset issues and access control, and an integration interface that allows the bi-directional sharing of information with other security management systems on your network.  CounterACT integrates with network infrastructure equipment, vulnerability and configuration management systems, endpoint remediation systems, SIEMs, and MDM systems. One key attribute of CounterACT is that all of the endpoints on your network are monitored. CounterACT discovers 100% of the endpoints attached to your enterprise.

To do this, CounterACT utilizes a combination of discovery techniques to provide real-time visibility, including both passive and active endpoint discovery, inspection, and monitoring that replaces the time and processing constraints of relying on a mega scan. Then CounterACT automatically assesses the endpoint security posture of all endpoints on your LAN/WAN environment. CounterACT also integrates with network, security, host-based security system (HBSS) and identity platforms to provide continuous real-time endpoint intelligence and security posture awareness yielding a CDM solution that has redundancy and scalability.

CounterACT's agentless solution enables it to work with managed and unmanaged endpoints. This is especially important for unmanaged devices, because your existing endpoint management systems are typically blind to these devices. CounterACT then has the ability to assess the security posture of all endpoints without the need to deploy an additional agent to those devices, including the security posture for unmanaged devices (e.g. BYOD). Regardless of whether or not an agent is used, CounterACT can perform a wide range of compliance checks on all endpoints including monitoring for required software, software versions and patch versions, device configuration and endpoint vulnerabilities.

Once an endpoint posture is accessed, ForeScout CounterACT offers 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 prompt the patch management system to update the device's operating system, or disable unauthorized software. In addition, CounterACT supports Security Information Event Management (SIEM) systems to provide endpoint configuration details, correlate access and compliance violations, and expedite incident response. CounterACT also includes built-in reporting and an executive dashboard to help you monitor policy compliance, support regulatory audit requirements, and produce real-time inventory reports.

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

The diagram below is an overview of how CounterACT continuous monitoring addresses CDM requirements:

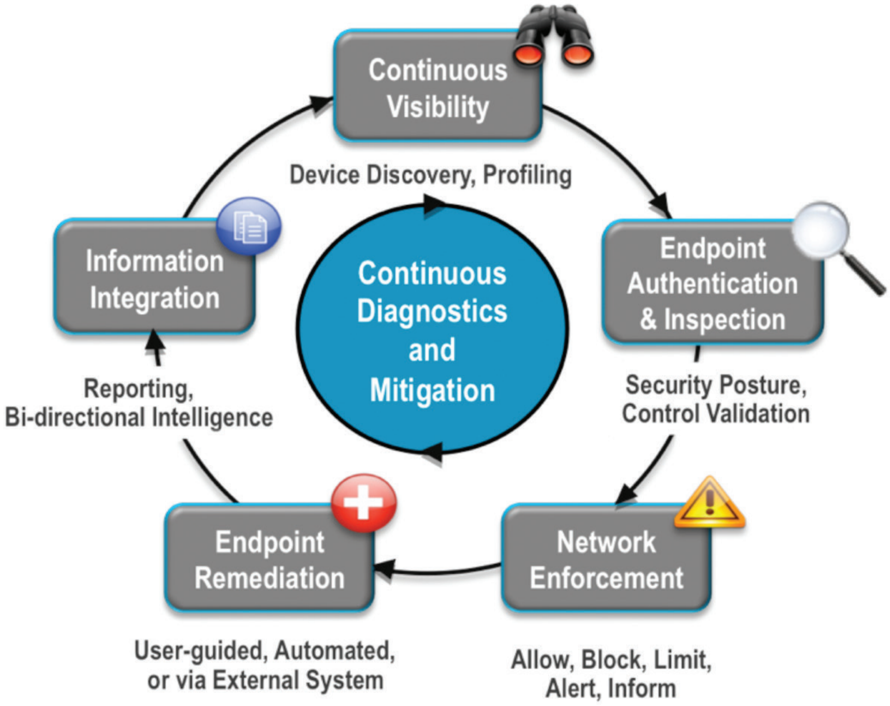

Continuous Visibility
Device Discovery, Profiling
Endpoint Authentication & Inspection
Security Posture, Control Validation
Network Enforcement
Allow, Block, Limit, Alert, Inform
Endpoint Remediation
User-guided, Automated, or via External System
Information Integration
Reporting, Bi-directional Intelligence
Continuous Diagnostics and Mitigation

***Figure 2:** ForeScout CounterACT functionality that meets the continuous monitoring demands of CDM.*

# ForeScout CounterACT addresses CDM

ForeScout CounterACT functionality addresses CDM requirements with the following functions: Asset Discovery & Classification, Security Posture Assessment, Authentication & Access Control, Automated Mitigation & Remediation, and Situational Awareness as shown in the chart below:

| Continuous Diagnostics & Mitigation Requirements | ForeScout CounterACT Functionality | |
|---|---|---|
| Hardware Asset Management (#1)<br>Software Asset Management (#2) | **Asset Discovery & Classification** | CounterACT discovers all network devices in real-time including devices that do not use an IP address and only have a MAC address. CounterACT maintains a comprehensive database of all hardware and software assets. The inventory can be search and organized by various hardware and software attributes. Inventory reports can be generated. |
| Configuration Management (#3)<br>Vulnerability Management (#4) | **Security Posture Assessment** | CounterACT can assess the security posture of all endpoints on your LAN/WAN environment. This is especially important for unmanaged devices (e.g.; 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, just to name a few. It integrates with other host-based agents/tools and vulnerability scanners to obtain additional compliance information on a manual, or event-driven basis. |
| Manage Network & Physical Access Control (#5)<br>Manage Trust in People Granted Access (#6)<br>Manage Security-Related Behavior (#7)<br>Manage Credentials & Authentication (#8)<br>Manage Account Access (#9) | **Authentication & Access Control** | CounterACT can block or restrict access to unauthorized devices, or users, as well as any device which becomes non-compliant at any time while it is connected to the network. CounterACT is event driven and will re-assess an endpoint when a configuration changes in its operating system, or its behavior changes towards other devices on the network. Access Control Lists can be applied to a device based on the user that is logged into that device. |
| Manage Response to Incidents (#10)<br>Manage Assessments to Fix Weaknesses (#13) | **Automated Mitigation & Remediation** | 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 completely blocking non-compliant endpoints. CounterACT can also interface with a third-party system such as patch management. |
| Manage Preparation for Contingencies (#11)<br>Design and Build Security into the System (#12)<br>Manage Audit Information and Accountability (#14)<br>Manage Overall Operational Control Limits (#15) | **Situational Awareness** | CounterACT provides comprehensive situational awareness by identifying all endpoints on the network and integrating with other security management systems such as endpoint lifecycle management products, asset management systems, databases, SIEM, VA, AV resulting in real-time endpoint intelligence and security posture awareness. In addition, CounterACT supports the leading security information event management (SIEM) systems to provide endpoint configuration details, correlate access and compliance violations to expedite incident response providing excellent situational awareness. |

The following examples show how policies can be configured in CounterACT to address each requirement. The CounterACT policy configurations can be categorized into four different "types" of policies: Classification, Clarification, Compliance, and Control.

CounterACT first "classifies" endpoints into easily recognized groups, such as a Windows device or an Apple iOS device, and then "clarifies" these groups further in the second tier of policy flow. The endpoints in the resultant groups are then checked for "compliance" against the organization's security requirements (in this case, CDM requirements). Finally, the complying and non-complying groups have "control" actions that address the remediation needs of each device, or if the endpoint is in compliance, provide access to its authorized resources on the network.

The CounterACT policy types that represent this information and decision flow that address CDM requirements in the policy folders shown below;

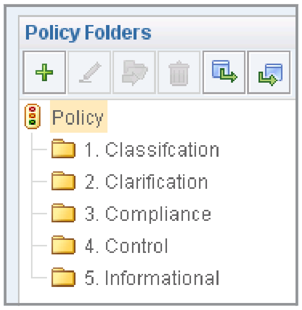
Several CounterACT policies are available "out of the box", for example, the Asset Classification policy.  Custom policies can also be created, tailored to your specific security needs. In the sections below, the CDM requirements are addressed with the appropriate CounterACT functions with examples of the types of policies used and some configurations that satisfy the CDM requirements that match the CounterACT function from the above chart.

## CounterACT Function: Asset Discovery & Classification

| CounterACT Policy Types | CDM Requirements Addressed |
|---|---|
| Classification, Clarification | 1. Hardware Asset Management<br>2. Software Asset Management |

This CounterACT functionality discovers all hardware and software on your network including unauthorized or unmanaged hardware, and unauthorized or unmanaged software configurations in your hardware assets. For example, a policy configuration for Asset Discovery and Classification would look like in Figure 4.

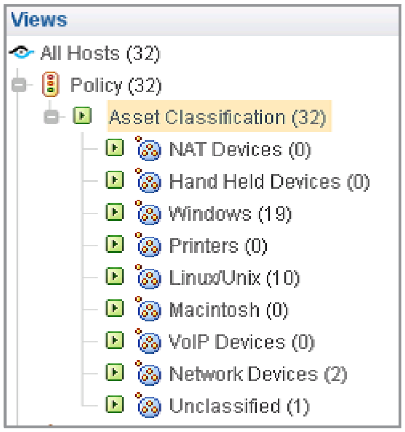
Once CounterACT classifies network endpoints into groups, it lists each device in the appropriate category, as shown in Figure 5.



Policy Folders

- Policy
  - 1. Classifcation
  - 2. Clarification
  - 3. Compliance
  - 4. Control
  - 5. Informational

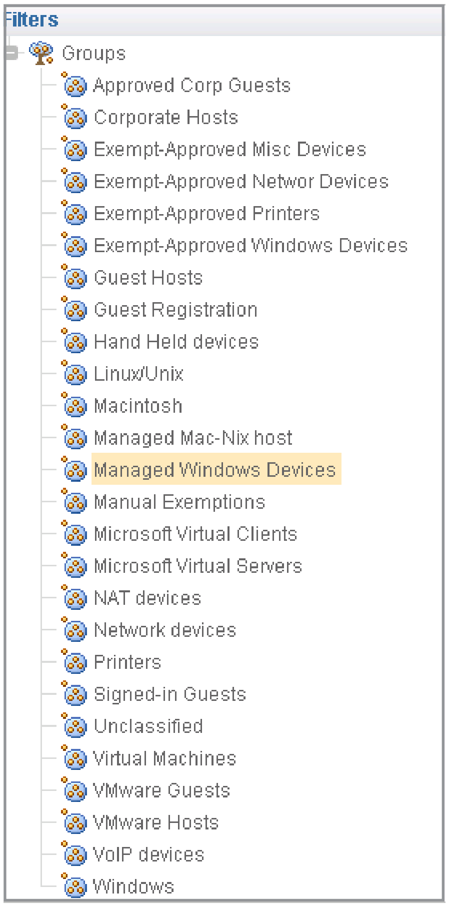
***Figure 3:*** *CounterACT discovers all assets*



Views

- All Hosts (32)
  - Policy (32)
    - Asset Classification (32)
      - NAT Devices (0)
      - Hand Held Devices (0)
      - Windows (19)
      - Printers (0)
      - Linux/Unix (10)
      - Macintosh (0)
      - VoIP Devices (0)
      - Network Devices (2)
      - Unclassified (1)

***Figure 4:*** *CounterACT's policy configuration for Asset Discovery  and Classification*

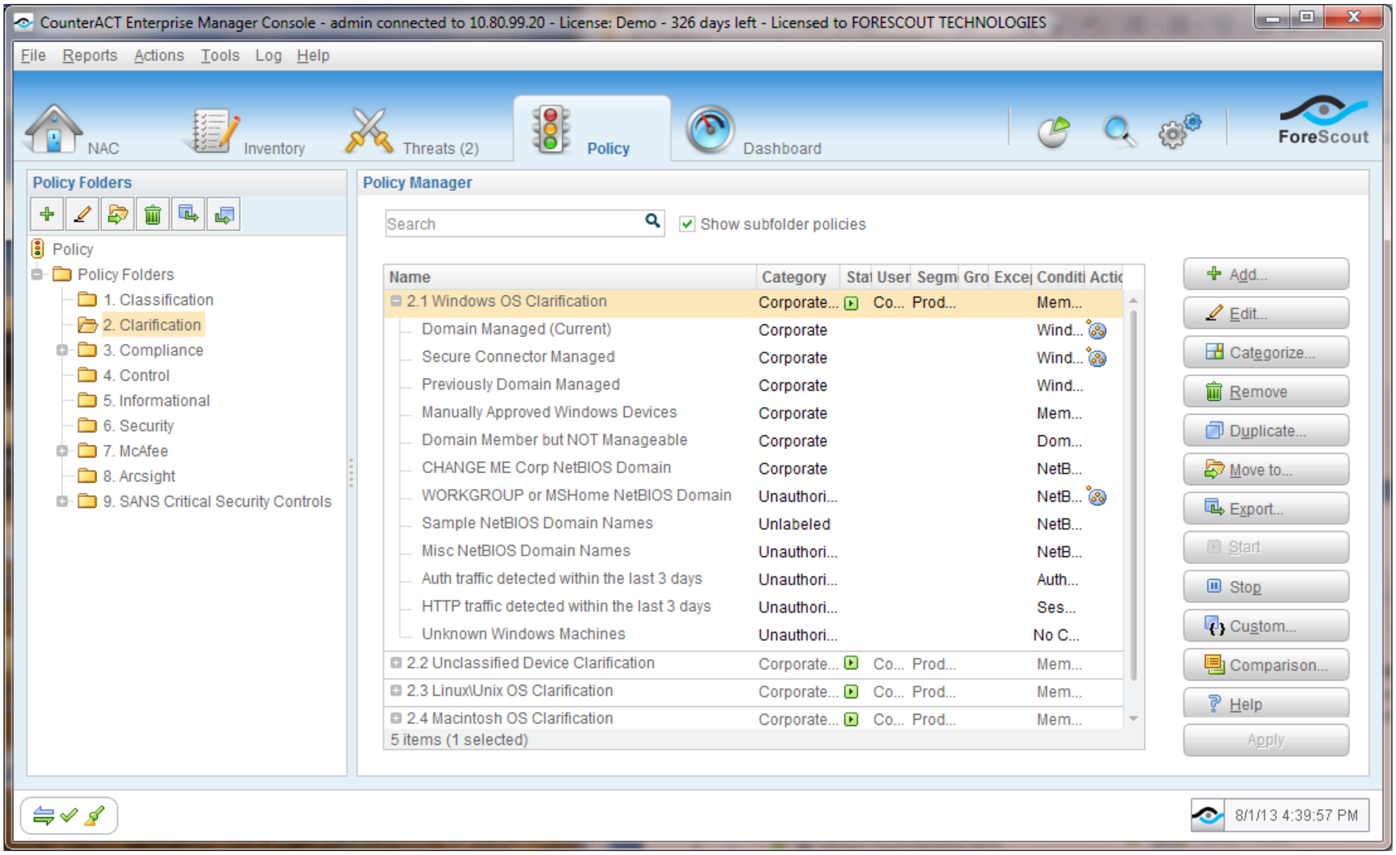


ilters

- Groups
  - Approved Corp Guests
  - Corporate Hosts
  - Exempt-Approved Misc Devices
  - Exempt-Approved Networ Devices
  - Exempt-Approved Printers
  - Exempt-Approved Windows Devices
  - Guest Hosts
  - Guest Registration
  - Hand Held devices
  - Linux/Unix
  - Macintosh
  - Managed Mac-Nix host
  - Managed Windows Devices
  - Manual Exemptions
  - Microsoft Virtual Clients
  - Microsoft Virtual Servers
  - NAT devices
  - Network devices
  - Printers
  - Signed-in Guests
  - Unclassified
  - Virtual Machines
  - VMware Guests
  - VMware Hosts
  - VoIP devices
  - Windows

***Figure 5:*** *CounterACT lists each device in the appropriate category*

CounterACT then gathers additional information about the device. This “clarification” information helps you understand characteristics on a more detailed level, as shown below:



CounterACT Enterprise Manager Console - admin connected to 10.80.99.20 - License: Demo - 326 days left - Licensed to FORESCOUT TECHNOLOGIES

- Policy
  - Policy Folders
    - 1. Classification
    - 2. Clarification
    - 3. Compliance
    - 4. Control
    - 5. Informational
    - 6. Security
    - 7. McAfee
    - 8. Arcsight
    - 9. SANS Critical Security Controls

☑ Show subfolder policies

| Name | Category | Stat | User | Segm | Gro | Exce | Conditi | Actic |
|---|---|---|---|---|---|---|---|---|
| 2.1 Windows OS Clarification | Corporate... | ▶ | Co... | Prod... | | | Mem... | |
| Domain Managed (Current) | Corporate | | | | | | Wind... | |
| Secure Connector Managed | Corporate | | | | | | Wind... | |
| Previously Domain Managed | Corporate | | | | | | Wind... | |
| Manually Approved Windows Devices | Corporate | | | | | | Mem... | |
| Domain Member but NOT Manageable | Corporate | | | | | | Dom... | |
| CHANGE ME Corp NetBIOS Domain | Corporate | | | | | | NetB... | |
| WORKGROUP or MSHome NetBIOS Domain | Unauthori... | | | | | | NetB... | |
| Sample NetBIOS Domain Names | Unlabeled | | | | | | NetB... | |
| Misc NetBIOS Domain Names | Unauthori... | | | | | | NetB... | |
| Auth traffic detected within the last 3 days | Unauthori... | | | | | | Auth... | |
| HTTP traffic detected within the last 3 days | Unauthori... | | | | | | Ses... | |
| Unknown Windows Machines | Unauthori... | | | | | | No C... | |
| 2.2 Unclassified Device Clarification | Corporate... | ▶ | Co... | Prod... | | | Mem... | |
| 2.3 Linux\Unix OS Clarification | Corporate... | ▶ | Co... | Prod... | | | Mem... | |
| 2.4 Macintosh OS Clarification | Corporate... | ▶ | Co... | Prod... | | | Mem... | |

5 items (1 selected)

8/1/13 4:39:57 PM

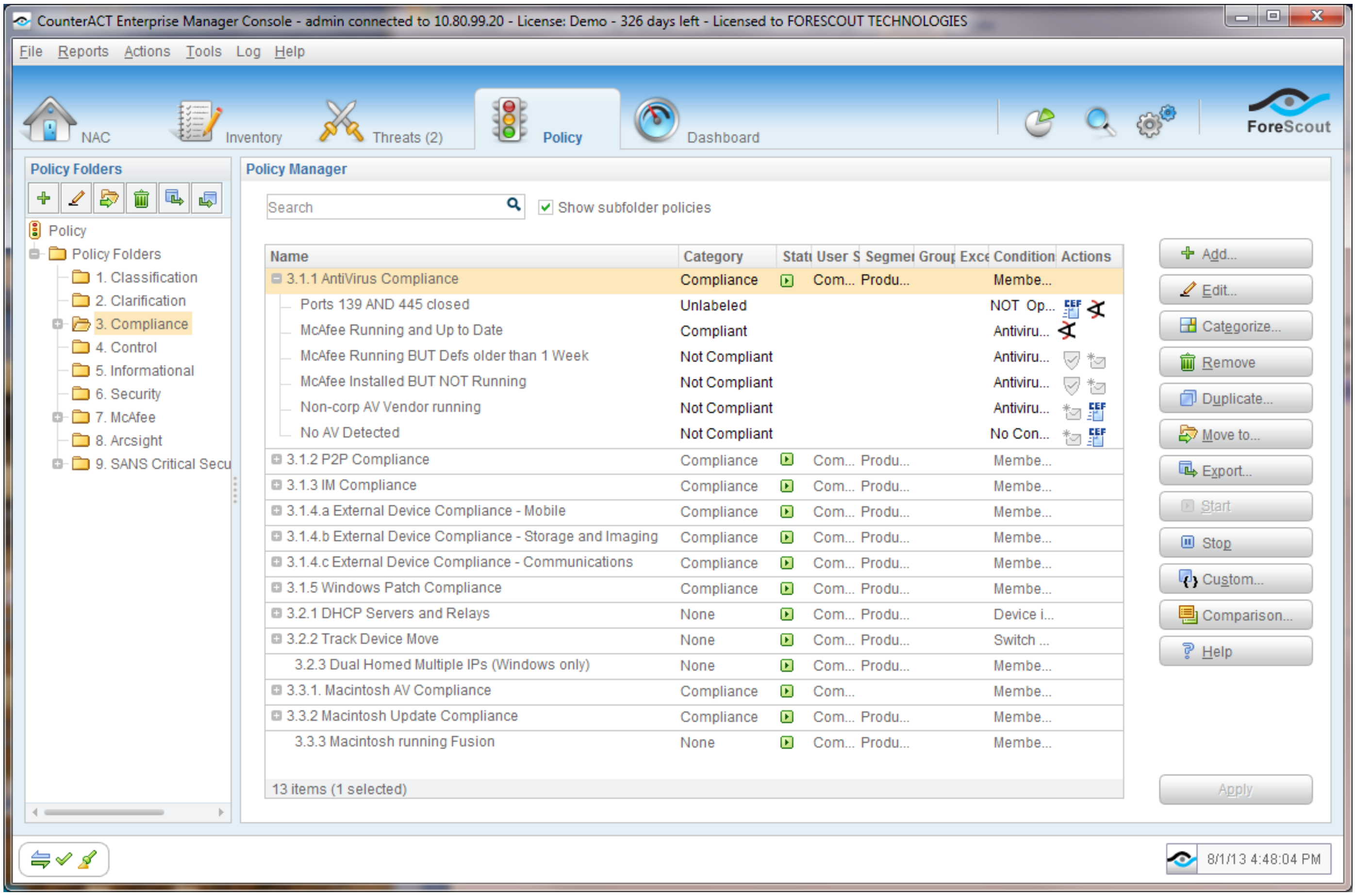
***Figure 6:*** *CounterACT continues to collect information about each device.*

CounterACT can be configured to apply any additional policies to these groups as required. CounterACT has a pre-built asset classification policy, and policies can be customized to specifically address CDM requirements.

## CounterACT Function: Security Posture Assessment

| CounterACT Policy Types | CDM Requirements Addressed |
|---|---|
| Compliance | 3. Configuration Management<br>4. Vulnerability Management |

CounterACT assesses the security posture of all endpoints on your network by performing a range of compliance checks, such as checking for required software, software versions and patch versions, device configuration and endpoint vulnerabilities. CounterACT integrates with other host-based agents/tools and vulnerability scanners to obtain additional compliance information. For example, a Compliance policy configuration for Assessment that can be custom configured, or from a template of compliance policies made available to clients, might look like:



CounterACT Enterprise Manager Console - admin connected to 10.80.99.20 - License: Demo - 326 days left - Licensed to FORESCOUT TECHNOLOGIES

- Policy
  - Policy Folders
    - 1. Classification
    - 2. Clarification
    - 3. Compliance
    - 4. Control
    - 5. Informational
    - 6. Security
    - 7. McAfee
    - 8. Arcsight
    - 9. SANS Critical Secu

Policy Manager

Search ☑ Show subfolder policies

| Name | Category | Stat | User S | Segmen | Group | Exce | Condition | Actions |
|---|---|---|---|---|---|---|---|---|
| ⊟ 3.1.1 AntiVirus Compliance | Compliance | ▶ | Com... | Produ... | | | Membe... | |
| Ports 139 AND 445 closed | Unlabeled | | | | | | NOT Op... | CEF |
| McAfee Running and Up to Date | Compliant | | | | | | Antiviru... | |
| McAfee Running BUT Defs older than 1 Week | Not Compliant | | | | | | Antiviru... | |
| McAfee Installed BUT NOT Running | Not Compliant | | | | | | Antiviru... | |
| Non-corp AV Vendor running | Not Compliant | | | | | | Antiviru... | CEF |
| No AV Detected | Not Compliant | | | | | | No Con... | CEF |
| ⊞ 3.1.2 P2P Compliance | Compliance | ▶ | Com... | Produ... | | | Membe... | |
| ⊞ 3.1.3 IM Compliance | Compliance | ▶ | Com... | Produ... | | | Membe... | |
| ⊞ 3.1.4.a External Device Compliance - Mobile | Compliance | ▶ | Com... | Produ... | | | Membe... | |
| ⊞ 3.1.4.b External Device Compliance - Storage and Imaging | Compliance | ▶ | Com... | Produ... | | | Membe... | |
| ⊞ 3.1.4.c External Device Compliance - Communications | Compliance | ▶ | Com... | Produ... | | | Membe... | |
| ⊞ 3.1.5 Windows Patch Compliance | Compliance | ▶ | Com... | Produ... | | | Membe... | |
| ⊞ 3.2.1 DHCP Servers and Relays | None | ▶ | Com... | Produ... | | | Device i... | |
| ⊞ 3.2.2 Track Device Move | None | ▶ | Com... | Produ... | | | Switch ... | |
| 3.2.3 Dual Homed Multiple IPs (Windows only) | None | ▶ | Com... | Produ... | | | Membe... | |
| ⊞ 3.3.1. Macintosh AV Compliance | Compliance | ▶ | Com... | | | | Membe... | |
| ⊞ 3.3.2 Macintosh Update Compliance | Compliance | ▶ | Com... | Produ... | | | Membe... | |
| 3.3.3 Macintosh running Fusion | None | ▶ | Com... | Produ... | | | Membe... | |

13 items (1 selected)

8/1/13 4:48:04 PM

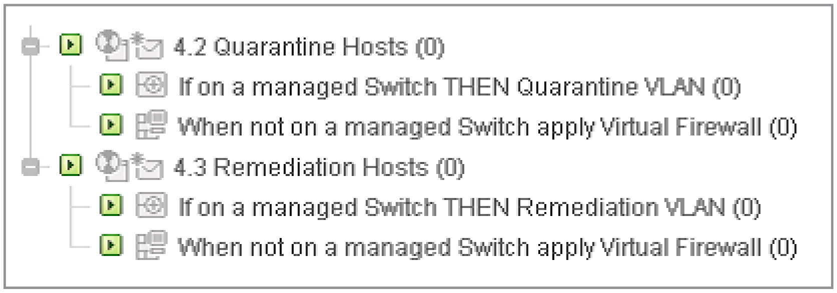
***Figure 7:*** *CounterACT lets you customize configure compliance policies from a template of standard templates.*

# CounterACT Function: Authentication & Access Control

| CounterACT Policy Types | CDM Requirements Addressed |
|---|---|
| Control | 5. Network & Physical Access Control<br>6. Trust in People Granted Access<br>7. Security-Related Behavior<br>8. Credentials & Authentication<br>9. Account Access |

CounterACT can block or restrict access to unauthorized devices as well as any device which becomes non-compliant at any time while connected to the network. CounterACT is event driven and will re-assess an endpoint when a configuration changes on the endpoint. For example, a custom policy configuration has the following "Action" options for Authentication & Access Control:

The resulting CounterACT policies for endpoints that require remediation or quarantine would look like:



4.2 Quarantine Hosts (0)
- If on a managed Switch THEN Quarantine VLAN (0)
- When not on a managed Switch apply Virtual Firewall (0)

4.3 Remediation Hosts (0)
- If on a managed Switch THEN Remediation VLAN (0)
- When not on a managed Switch apply Virtual Firewall (0)

***Figure 9:*** *CounterACT shows policies for endpoints requiring remediation or quarantine.*

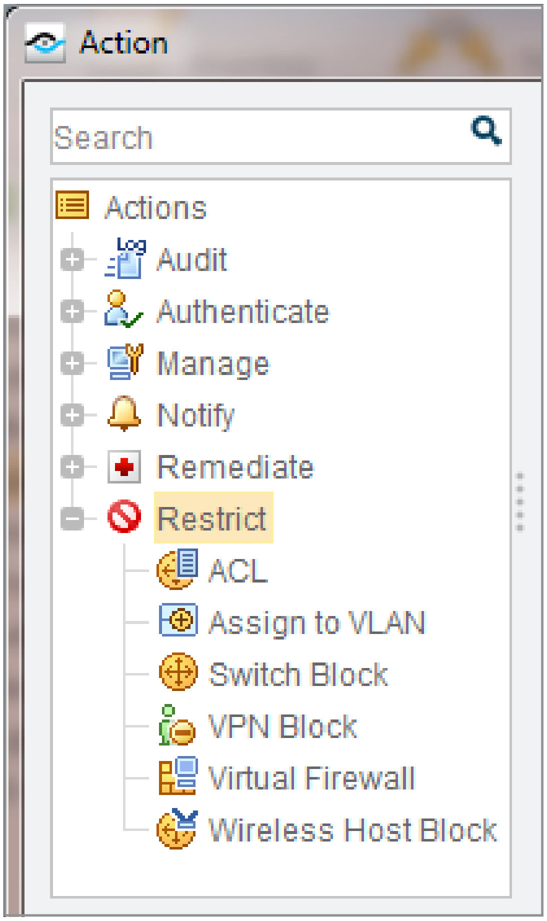
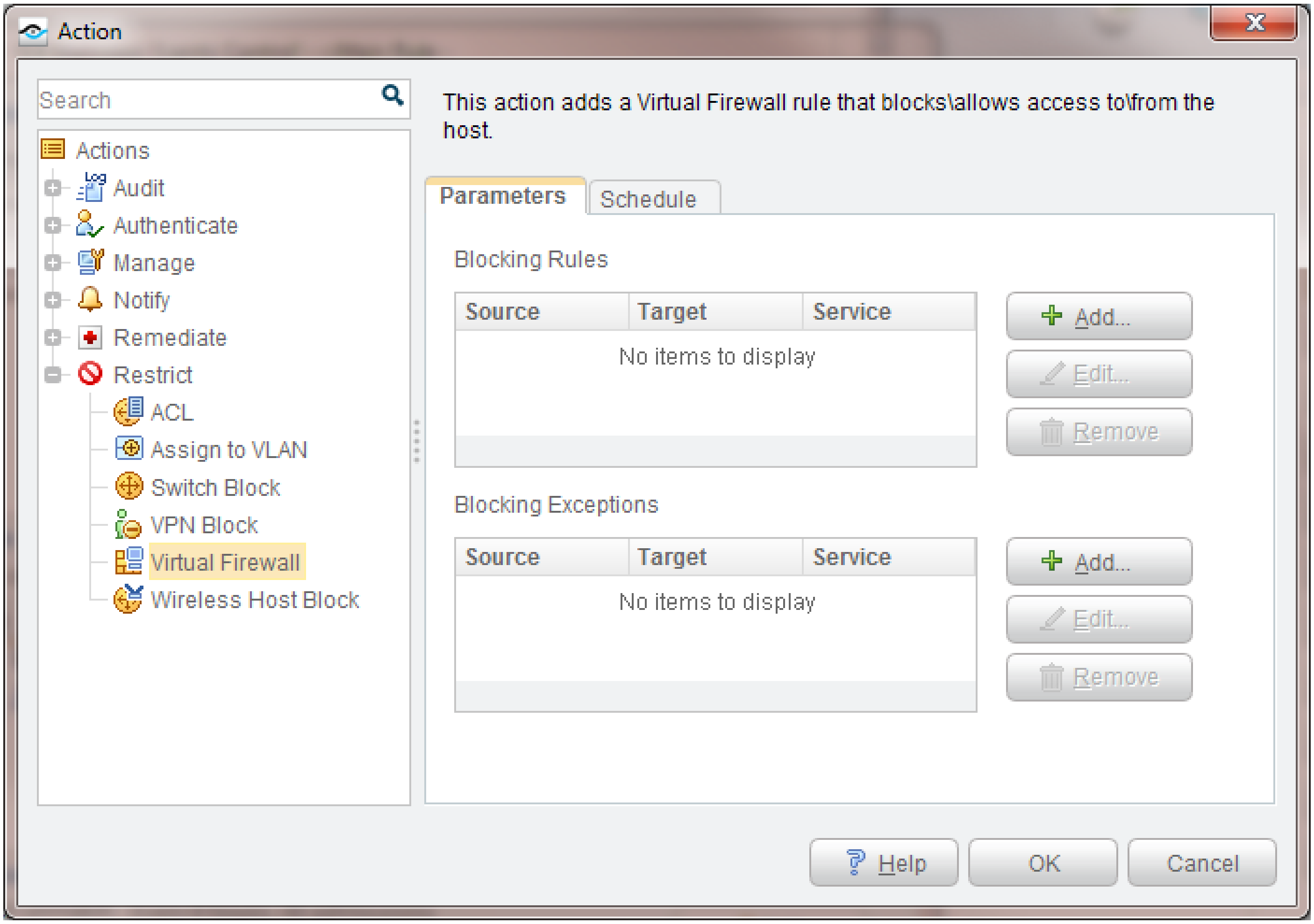


***Figure 8:*** *CounterACT can block or restrict access to unauthorized devices*

Below is an illustration of the Action dialog window that shows some of the options available for building control policies that "Restrict" an endpoint, such as Assign to VLAN, ACL, Blocking, Virtual Firewall, etc.



This action adds a Virtual Firewall rule that blocks\allows access to\from the host.

Blocking Rules

| Source | Target | Service |
|---|---|---|
| | No items to display | |

Blocking Exceptions

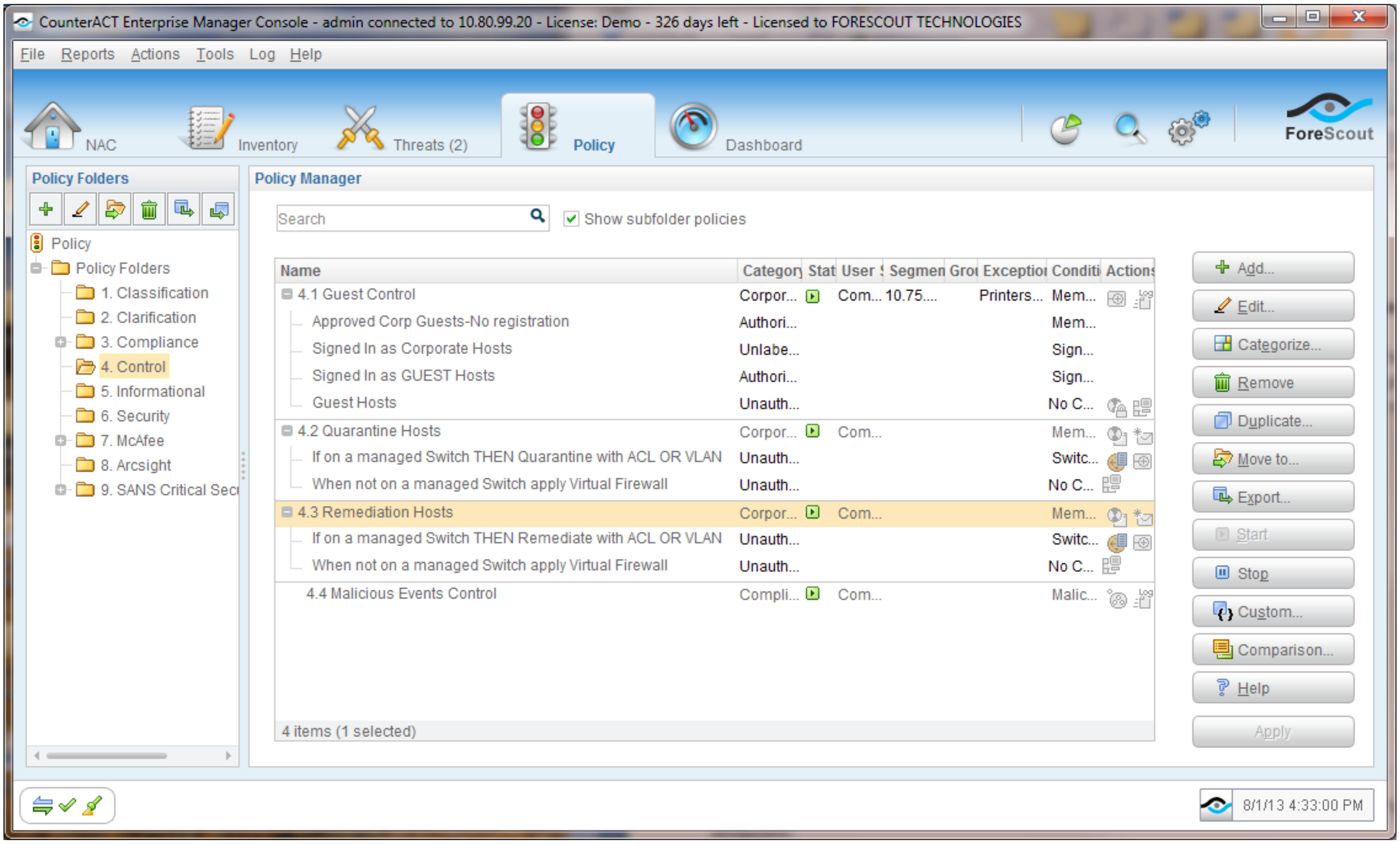
| Source | Target | Service |
|---|---|---|
| | No items to display | |

***Figure 10:*** *The Action dialog window shows several available options building control policies that "Restrict" an endpoint.*

# CounterACT Function: Automated Mitigation & Remediation

| CounterACT Policy Types | CDM Requirements Addressed |
|---|---|
| Control | 10. Response to Incidents<br>13. Manage Assessments to Fix Weaknesses |

When endpoint non-compliance is detected, CounterACT can respond based on the specific type of non-compliance to your security policies by; alerting IT staff, auto-remediating, quarantining, or completely blocking non-compliant endpoints. CounterACT can also integrate with a third-party system such as patch management. For example, a policy configuration for Automated Mitigation & Remediation would look like:

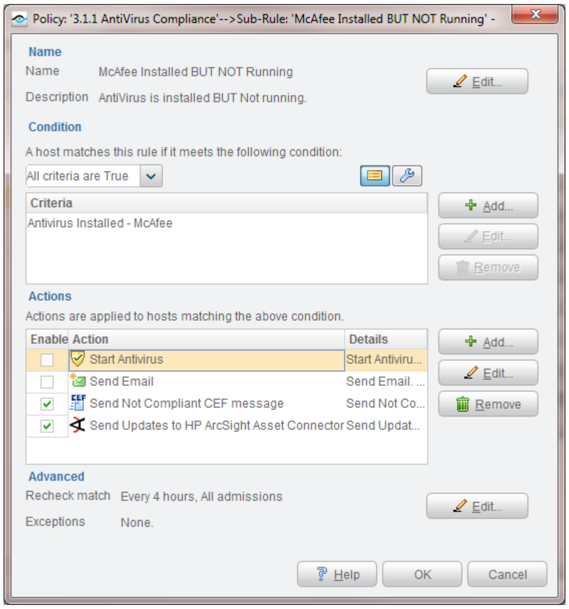

CounterACT Enterprise Manager Console - admin connected to 10.80.99.20 - License: Demo - 326 days left - Licensed to FORESCOUT TECHNOLOGIES

| Name | Categor | Stat | User | Segmen | Grou | Exceptio | Conditi | Actions |
|---|---|---|---|---|---|---|---|---|
| 4.1 Guest Control | Corpor... | ▶ | Com... | 10.75.... | | Printers... | Mem... | |
| Approved Corp Guests-No registration | Authori... | | | | | | Mem... | |
| Signed In as Corporate Hosts | Unlabe... | | | | | | Sign... | |
| Signed In as GUEST Hosts | Authori... | | | | | | Sign... | |
| Guest Hosts | Unauth... | | | | | | No C... | |
| 4.2 Quarantine Hosts | Corpor... | ▶ | Com... | | | | Mem... | |
| If on a managed Switch THEN Quarantine with ACL OR VLAN | Unauth... | | | | | | Switc... | |
| When not on a managed Switch apply Virtual Firewall | Unauth... | | | | | | No C... | |
| 4.3 Remediation Hosts | Corpor... | ▶ | Com... | | | | Mem... | |
| If on a managed Switch THEN Remediate with ACL OR VLAN | Unauth... | | | | | | Switc... | |
| When not on a managed Switch apply Virtual Firewall | Unauth... | | | | | | No C... | |
| 4.4 Malicious Events Control | Compli... | ▶ | Com... | | | | Malic... | |

4 items (1 selected)

***Figure 11:*** *This shows a policy configuration for Automated Mitigation & Remediation*

Another example of a control action would be to restart antivirus software if it is "installed but not running" on an endpoint:



Policy: '3.1.1 AntiVirus Compliance'-->Sub-Rule: 'McAfee Installed BUT NOT Running' -

Name

Name McAfee Installed BUT NOT Running

Description AntiVirus is installed BUT Not running.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

| Criteria |
|---|
| Antivirus Installed - McAfee |

Actions

Actions are applied to hosts matching the above condition.

| Enable | Action | Details |
|---|---|---|
| □ | Start Antivirus | Start Antiviru... |
| □ | Send Email | Send Email. ... |
| ☑ | Send Not Compliant CEF message | Send Not Co... |
| ☑ | Send Updates to HP ArcSight Asset Connector | Send Updat... |

Advanced

Recheck match Every 4 hours, All admissions

Exceptions None.

*Figure 12: This shows how a control action restarts antivirus software "installed but not running" on an endpoint*

CounterACT has the following options for endpoint remediation:

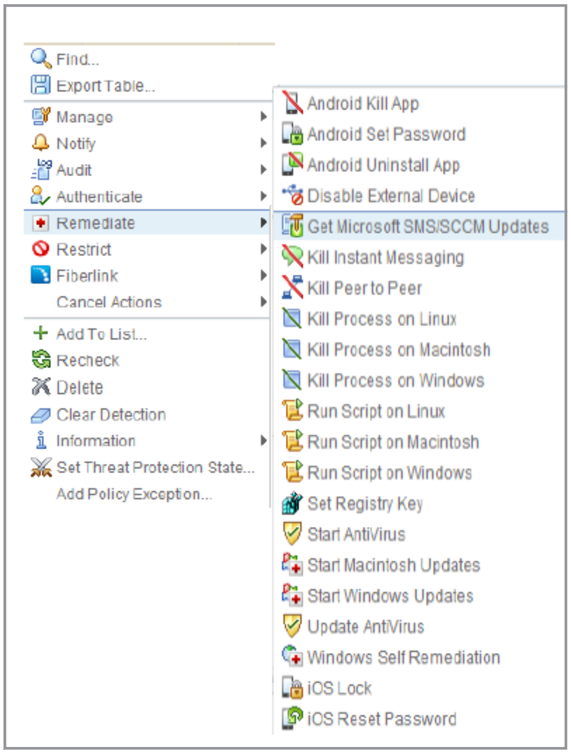
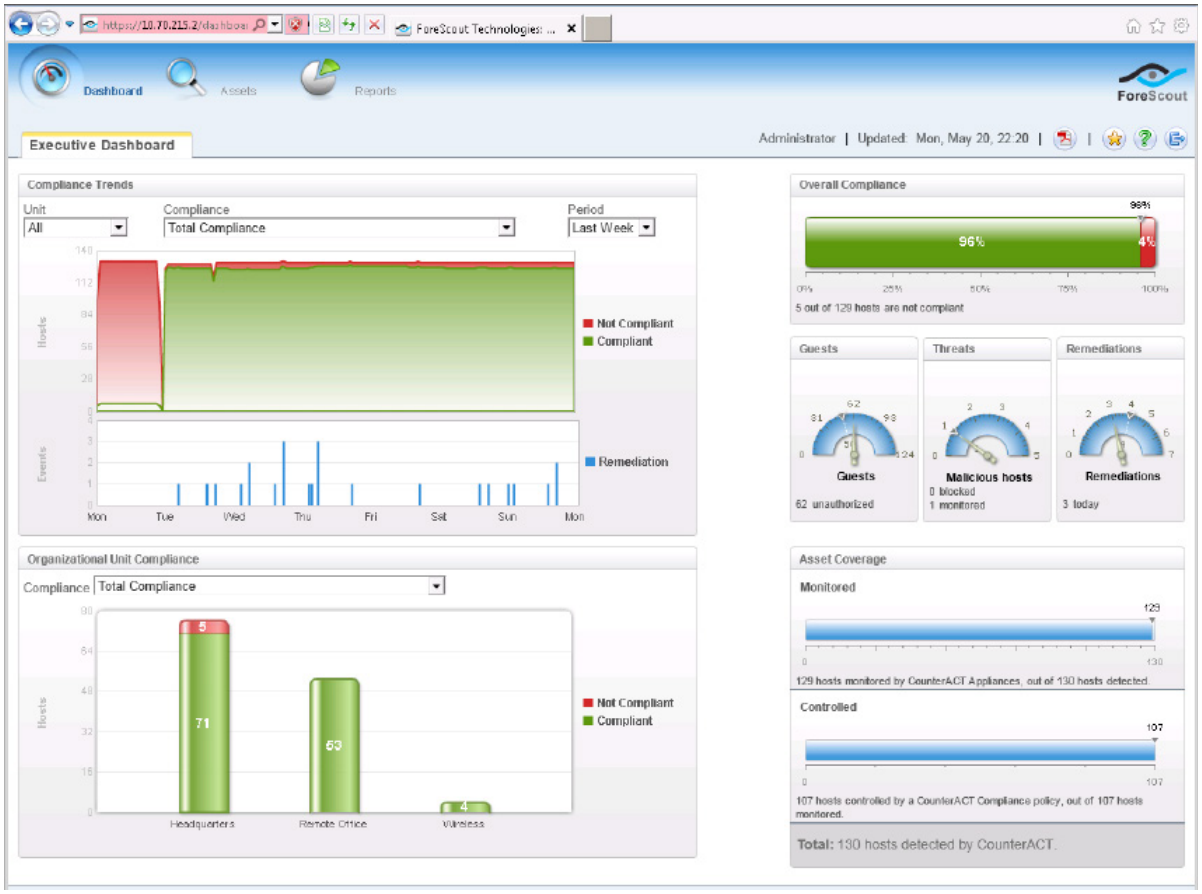


*Figure 13: CounterACT has many options for endpoint remediation*

## CounterACT Function: Situational Awareness

| CounterACT Policy Types | CDM Requirements Addressed |
|---|---|
| Control | 11. Preparation for Contingencies<br>12. Design and Build Security into the System<br>14. Audit Information & Accountability<br>15. Overall Operational Control Limits |

CounterACT provides comprehensive situational awareness by identifying all endpoints on the network and integrating with other security management systems resulting in real-time endpoint intelligence and security posture awareness. CounterACT can integrate with third party security management systems such as; endpoint lifecycle management products, asset management systems, databases, Vulnerability Assessment, and AntiVirus. In addition, CounterACT supports the leading security information event management (SIEM) systems to provide endpoint configuration details, correlate access and compliance violations to expedite incident response while providing excellent situational awareness. This situational awareness and reporting flow is either internally set up within CounterACT's Executive Dashboard, or it is a bi-directional integration with a 3rd party system. Here is a snapshot of CounterACT's Executive Dashboard:



Administrator | Updated: Mon, May 20, 22:20 |

Unit: All
Compliance: Total Compliance
Period: Last Week

5 out of 129 hosts are not compliant

62 unauthorized

0 blocked
1 monitored

3 today

Compliance: Total Compliance

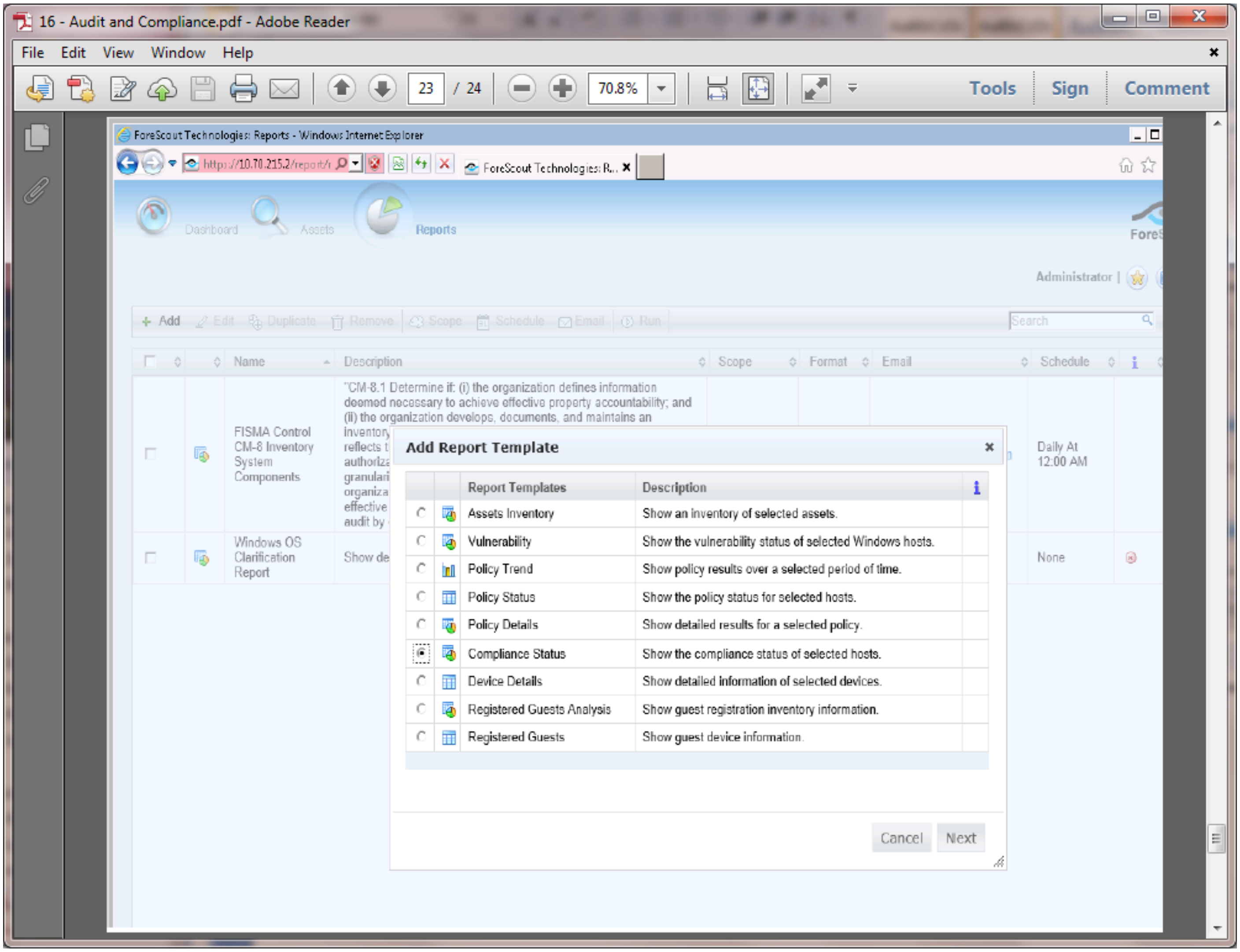
129 hosts monitored by CounterACT Appliances, out of 130 hosts detected.

107 hosts controlled by a CounterACT Compliance policy, out of 107 hosts monitored.

**Total:** 130 hosts detected by CounterACT.

***Figure 14:*** *CounterACT's Executive Dashboard*

CounterACT's Executive Dashboard has a selection of report templates to work from:


16 - Audit and Compliance.pdf - Adobe Reader
File Edit View Window Help
23 / 24
70.8%
Tools Sign Comment
ForeScout Technologies: Reports - Windows Internet Explorer
http://10.70.215.2/report/
ForeScout Technologies: R...
Dashboard
Assets
Reports
Administrator |
Add Edit Duplicate Remove Scope Schedule Email Run
Search

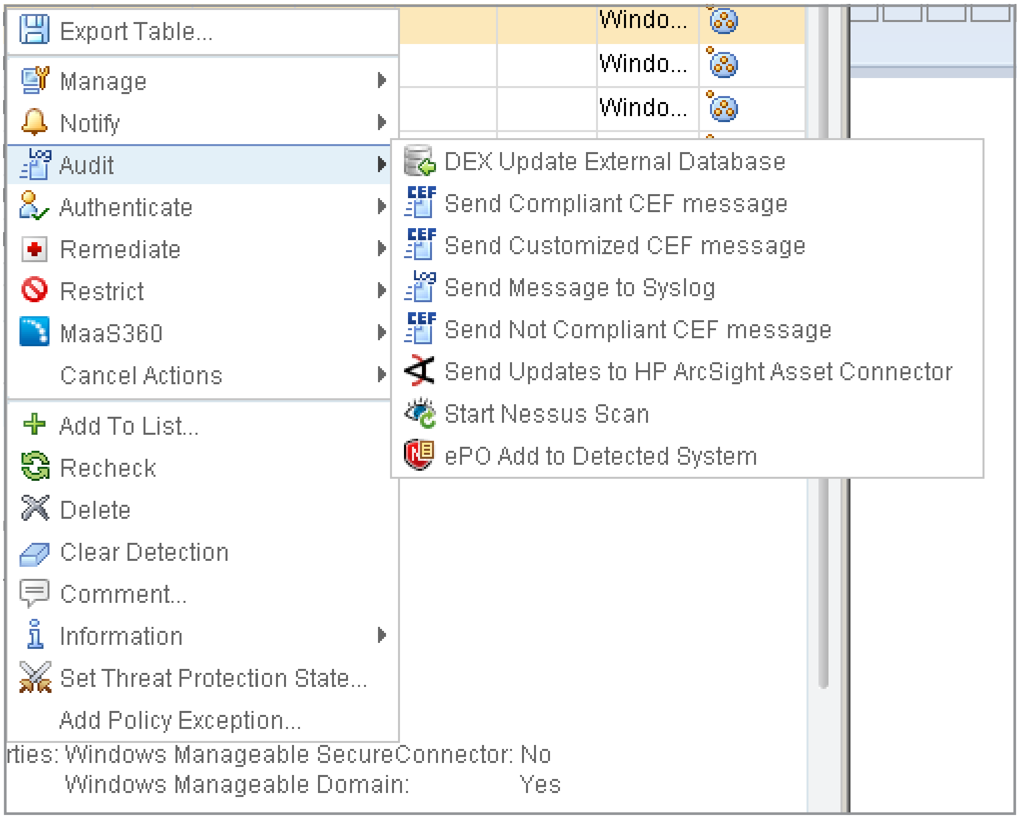
| | | Name | Description | Scope | Format | Email | Schedule |
|---|---|---|---|---|---|---|---|
| □ | | FISMA Control CM-8 Inventory System Components | "CM-8.1 Determine if: (i) the organization defines information deemed necessary to achieve effective property accountability; and (ii) the organization develops, documents, and maintains an inventory reflects t authoriza granulari organiza effective audit by | | | | Daily At 12:00 AM |
| □ | | Windows OS Clarification Report | Show de | | | | None |

**Add Report Template**

| | Report Templates | Description |
|---|---|---|
| ○ | Assets Inventory | Show an inventory of selected assets. |
| ○ | Vulnerability | Show the vulnerability status of selected Windows hosts. |
| ○ | Policy Trend | Show policy results over a selected period of time. |
| ○ | Policy Status | Show the policy status for selected hosts. |
| ○ | Policy Details | Show detailed results for a selected policy. |
| ● | Compliance Status | Show the compliance status of selected hosts. |
| ○ | Device Details | Show detailed information of selected devices. |
| ○ | Registered Guests Analysis | Show guest registration inventory information. |
| ○ | Registered Guests | Show guest device information. |

***Figure 15:*** *Access to report templates from CounterACT's Executive Dashboard*

CounterACT policies can be created to send audit logs in Syslog and/or CEF format to a number of 3rd party security management systems:



rties: Windows Manageable SecureConnector: No
Windows Manageable Domain: Yes

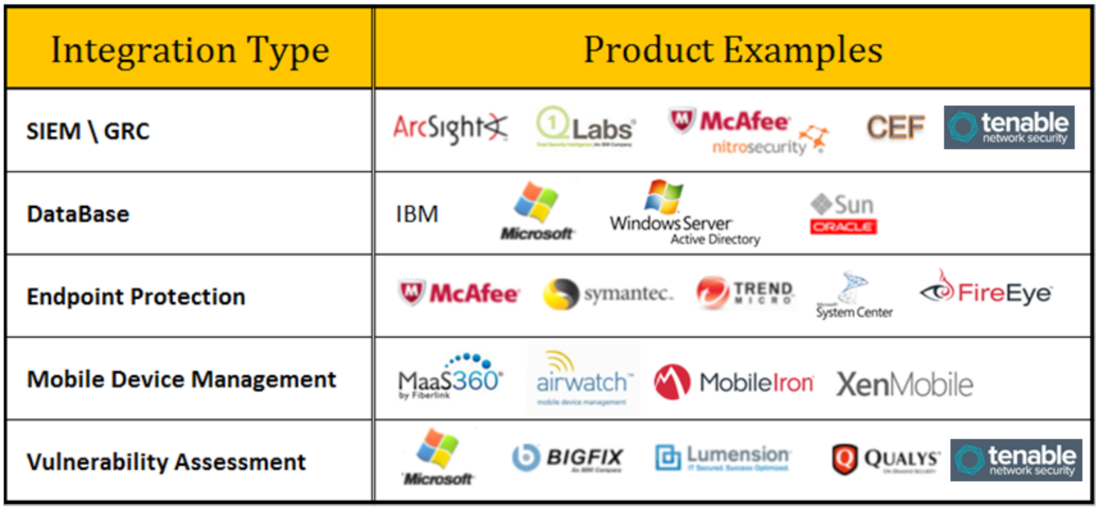
***Figure 16:*** *Setting CounterACT policies for 3rd party security management systems*

## Integrations that Enhance CDM Compliance

By design, CounterACT is an intelligent security automation platform that uses its unique real-time visibility of all network endpoints and its interoperability with existing network security infrastructure to provide a redundant and scalable security solution. CounterACT interoperates with all major vendors and works in any network environment, which minimizes the configuration time required to benefit from the advantages of using its centralized control attributes.

CounterACT collects a broad spectrum of endpoint data logically and directly that is then shared with other network security management systems. With its ability to act as the primary endpoint data collection mechanism, and its security automation tools, CounterACT is a catalyst for an organization to move towards a layered network security infrastructure by providing a multitude of options to discover, assess, and control endpoints. This layered security approach is enabled through CounterACT's ability to integrate with other network security systems on your network. This interoperability allows CounterACT to be configured to meet all CDM compliance requirements either as a single solution or through an integrated solution with your existing network security infrastructure systems.

CounterACT integrates with a number of leading vulnerability assessment scanners, database applications, endpoint protection systems, mobile device management (MDM) systems, and SIEMs, as show below. ForeScout has other integrations under development.



| Integration Type | Product Examples |
|---|---|
| SIEM \ GRC | ArcSight<br>Q1Labs<br>McAfee nitrosecurity<br>CEF<br>tenable network security |
| DataBase | IBM<br>Microsoft<br>Windows Server Active Directory<br>Sun ORACLE |
| Endpoint Protection | McAfee<br>symantec.<br>TREND MICRO<br>System Center<br>FireEye |
| Mobile Device Management | MaaS360 by Fiberlink<br>airwatch mobile device management<br>MobileIron<br>XenMobile |
| Vulnerability Assessment | Microsoft<br>BIGFIX<br>Lumension<br>QUALYS<br>tenable network security |

***Figure 17:*** *CounterACT integrates with numerous 3rd party security systems*

## Summary

ForeScout CounterACT enables the integration of a multiple of endpoint data sources into a security control platform that can be configured to meet CDM requirements now and in the future. Presently, the mandatory CDM requirements include; hardware and software asset management, endpoint configuration and vulnerability management. NAC is a future requirement, Requirement 5, though certain suggestions in requirements 1 through 4 call for NAC like requirements. CounterACT offers the opportunity to manage some or all of these criteria by placing itself at the center of network security management by using its interoperability with existing security management systems on your network, and providing unmatched endpoint visibility with flexible control options.

CounterACT brings real-time visibility of all network devices and network security management system interoperability to you in a centralized control platform that addresses present and future network security requirements for organizations with a few hundred endpoints, or more than 1 million network endpoints.

### About ForeScout

ForeScout enables organizations to accelerate productivity and connectivity by allowing users to access corporate network resources where, how and when needed without compromising security. ForeScout's real-time network security platform for access control, mobile security, endpoint compliance and threat prevention empower IT agility while preempting risks and eliminating remediation costs. Because the ForeScout CounterACT$^{TM}$ solution is easy to deploy, unobtrusive, intelligent and scalable, it has been chosen by more than 1,400 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. Headquartered in Cupertino, California, ForeScout delivers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com.