An Independent Assessment of ForeScout CounterACT®

DR160408F

June 2016

Miercom
www.miercom.com

Contents

1 – Executive Summary

Miercom was engaged by ForeScout Technologies, Inc. to independently verify the capabilities and effectiveness of its novel CounterACT appliance. CounterACT provides an agentless solution for network visibility of the endpoints – corporate, BYOD, guest and IoT – connected to networks. In addition, CounterACT enforces policy-based network and host-based controls that support corporate policy compliance and use cases such as network access control, BYOD/mobile security, threat response and guest management. The completeness of CounterACT's visibility includes discovering and classifying corporate and personal devices, rogue devices and IoT components such as IP security cameras, network infrastructure equipment (switches, routers, firewalls, VPN controllers and so on).

The testing focused on CounterACT's agentless ability to quickly discover, classify and assess endpoints, including those that IT managers are unaware of, and its ability to apply network and host-based controls to enforce security policy. CounterACT also supports an optional agent for use cases where organizations want to deploy a permanent or dissolvable agent.

ForeScout and Miercom engineers collaborated on a rigorous test methodology. A variety of real-world network environments were created in Miercom's lab. In one scenario, for example, we measured the time it took CounterACT to discover and classify 500 concurrently connecting endpoints – a combination of Android and Apple smartphones and tablets, desktops, laptops, infrastructure equipment and simulated Windows and Linux endpoints.

Key Findings and Observations

- **100 percent endpoints discovered and classified**. CounterACT promptly discovered and provided full visibility of 100 percent of the endpoints in all the network environments tested. In one case 500 endpoints were detected and fully classified in less than 5 seconds.
- **Posture assessment and compliance monitoring**. CounterACT's compliance assessment policies provided real-time information about endpoint security posture and state changes.
- **Real-time visibility and controls**. CounterACT provided real-time visibility into corporate, BYOD and guest endpoints on the network. Visibility, endpoint compliance and host/network controls were completed without the installation of endpoint agents.
- **Policy configuration and management**. A rich array of built-in policies for visibility and controls can readily be applied, imposing varying degrees of limitation on unauthorized/non-compliant devices. The console is easy to navigate and software upgrades and module installation are straightforward.

Based on test results validating the efficacy of discovery, classification, assessment and control capabilities, and the ease of management and customization, we proudly award the *Miercom Performance Verified Certification* to ForeScout CounterACT.

Robert Smithers
CEO
Miercom

2 – About the Product Tested

ForeScout CounterACT is a physical or virtual security appliance that can be deployed out-of-band, providing IT administrators with network-wide visibility of devices the instant they connect to the network. CounterACT also provided host and network controls.

Device coverage includes:

- Corporate wired and Wi-Fi desktops, laptops, servers, virtual machines, etc.
- BYOD smartphones, tablets and laptops
- Visitors' wireless and wired devices
- Network infrastructure devices – switches, routers, VPNs, firewalls, Wi-Fi controllers and access points, etc.
- IoT– IP-networked devices, such as security cameras, climate-control sensors, manufacturing equipment, medical devices, etc.

CounterACT is offered as an appliance via six low- to high-capacity models, and as a virtualized-server version. We tested a model CT-10000 appliance, running version 7.0 service pack 2.0.0 software.

ForeScout CounterACT
Model CT-10000
Version 7.0 SP2.0.0

Key characteristics of the CounterACT appliance tested include:

- Link bandwidth and speed: 1 Gbits/s; with 2 – 4 port cards for 8 ports
- Recommended maximum number of managed switches: 200
- DB-9 serial port, three USB 2.0 ports
- DB-15 VGA port
- One CD-ROM drive, three RAID hard disk drives
- 744W power consumption; 2900 BTU/hr cooling
- 2U, 19-inch rack-mounted; 57 pounds.

CounterACT provides the IT department with:

- Visibility of devices connected to their network
- Assessment of endpoint compliance (to the company's security policy)
- Mitigation of risks and threats from non-compliant or infected endpoints
- Ability to provide appropriate network access based on user, device and host security posture

CounterACT does not require software agents running on endpoints or previous knowledge of connecting devices.

In addition, CounterACT orchestrates information sharing and operations among disparate network infrastructure and security tools to accelerate incident response. In our test bed, we implemented CounterACT network and endpoint control operations. The testbed consisted of switch, router, firewall and wireless infrastructure equipment from various vendors including Cisco, Check Point and D-Link.

How does CounterACT discover and classify endpoints on the network without any agents? Based on our testing, the system uses just about every protocol, process, tool and trick available, including passive and active techniques such as:

- Polling of switches, wireless controllers, firewalls and other network devices
- Monitoring DHCP requests
- NMAP scans
- SNMP traps from switches and wireless controllers
- NetFlow from switches, wireless controllers and routers
- Watching all network traffic on a SPAN (traffic-copied) switch port
- Monitoring of 802.1x requests to the RADIUS server
- Monitoring HTTP user agents

CounterACT collects a wide range of endpoint properties such as device type, ownership (corporate, BYOD, guest), operating system, network connection details and endpoint posture such as applications installed, vulnerabilities, etc. CounterACT policies create device groups which are endpoints with common endpoint properties. These defined groups are used to provide information about what is on the network and corporate compliance standards. IT personnel can further create CounterACT policies using these defined groups to determine actual endpoint network access or initiate remediation actions for non-compliant endpoints.

CounterACT reacts in real-time to display each new endpoint entering the network, classifies the endpoint by device type and places it in the appropriate defined group.

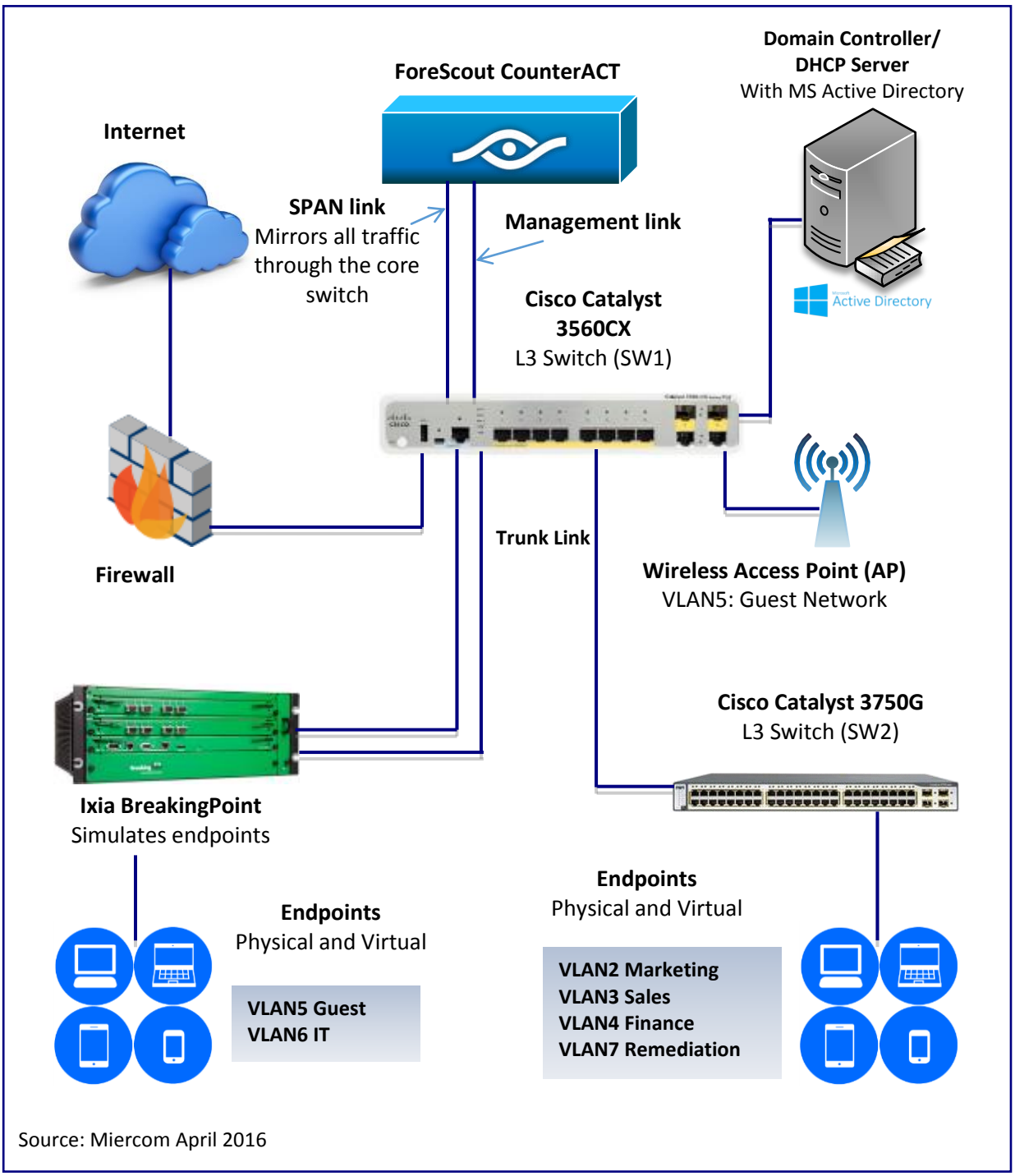
IT staff can define CounterACT polices that have network or host controls applied to an endpoint based on the evaluation of that endpoint's type and posture. Controls vary from mild to strong in terms of the limitations imposed on the endpoint. The controls can be host-based, such as limiting the use of a plug-in disk drive, or network-based, such as assigning the device to the limited-access Guest VLAN. CounterACT offers a full complement of security enforcement controls, from mild to strong, allowing IT staff to grant the correct level of network access to people, applications and devices.

The following section describes the test bed and the set-up of the network environment used to test the CounterACT system.

3 – How We Did It

A typical customer network was simulated in our lab. The network consisted of a Cisco access switch, Cisco core switch, Cisco wireless controller and access point, Check Point firewall, Microsoft Active Directory (AD), a DHCP Server and a Domain Controller. Ixia BreakingPoint was used to simulate certain types of endpoints, along with other physical endpoints.

Test Bed Setup



Source: Miercom April 2016

For this test, we used the following methods: SNMP traps on switches and wireless controllers (WLC), DHCP classification, SNMPv2 RW on switches and WLC, polling switches/WLC/firewall, NMAP, integration with AD, domain credentials on endpoints for deep inspection, HTTP user agents, HTTP hijack (intercept HTTP traffic and redirect) and SPAN (monitor network traffic). Not all these methods were required, but it allowed us to use multiple techniques to potentially capture large numbers of endpoint properties.

SPAN was configured on the Cisco 3560 to forward a copy of all network traffic to ForeScout CounterACT. We note that CounterACT can also be deployed without mirroring all network traffic via SPAN, but our testing utilized this configuration for advanced use cases like NAT/Rogue wireless device detection, vFW and HTTP hijack.

Mirroring traffic has no effect on network performance. We also observed that network performance was unaffected by CounterACT in our test-bed environment.

Endpoints. Both physical and virtual devices were used as endpoints in the network test bed. We deployed 30 physical devices and five virtual devices, consisting of: servers, laptops, smartphones, tablets, switches, desktops and a firewall. These employed a spectrum of different operating systems including Windows, Mac OS, Linux, Android and Apple iOS.

In our test bed, virtual endpoints were running on VMware ESXi server and Ixia BreakingPoint. Virtual devices were simulated by servers running VMware and by Ixia's BreakingPoint system.

BreakingPoint is a security test solution capable of simulating thousands of endpoints, real-world traffic, attacks, and fuzzing to ensure the highest quality of security and performance in a network. In our test bed, BreakingPoint simulated as many as 500 mainly Windows-based endpoints.

Corporate devices. Endpoints that are owned by an organization and have access to the relevant network to get the services they need to be productive. CounterACT can inspect and remediate these corporate devices without requiring endpoint agents.

BYOD/Guest devices. Endpoints that are not owned by an organization. These are typically guest devices or employees' personal devices attempting to access the corporate network. If required, CounterACT can inspect and remediate the BYOD/Guest devices by auto-installing a lightweight dissolvable agent that disappears upon reboot.

Corporate network. Several VLANs were set up, which collectively represented the organization's internal network (see the test-bed diagram). Corporate endpoints with Active Directory credentials that comply with corporate policies were provided access to these network segments.

Guest VLAN. This network had Internet access only. BYOD endpoints were assigned to this network until they successfully authenticated using corporate credentials (optional check for endpoint compliance) and guest endpoints were provided Internet access upon completing guest registration.

Test cases. The following sections summarize the tests conducted and the results obtained in these areas:

- **Discovery and Classification**
- **Posture/Compliance Assessment**
- **Control**
- **Deployment and Management**

Some of the test cases used quantifiable metrics to measure how well CounterACT performed its key tasks, while others yielded a more qualitative assessment on issues such as console navigation, effectiveness, and integration with other vendors' devices and systems.

Network Equipment CounterACT Works With

Upon request, ForeScout provided the following list of network equipment and endpoint protection technologies with which CounterACT currently integrates. In addition, ForeScout noted this list is continually being expanded. We only tested with a few of these (see test-bed diagram) and found that interworking was straightforward.

ForeScout also offers integration with leading network and endpoint security platforms like ATD systems, NGFW, SIEM, EMM, VA systems, Endpoint Protection Platform and Threat Intelligence systems using ForeScout Extended Modules.

Type of equipment	Supported vendors	
Endpoint Management Systems	Microsoft SMS/SCCM	
Firewalls and VPNs	Check Point Cisco Forcepoint Stonesoft Fortinet	Juniper Nortel Palo Alto Networks
Wireless / Access Points	Aerohive Aruba Cisco Meru	Motorola Ruckus Xirrus
Switches / Routers	Alcatel Apresia Arista Brocade/Foundry Cisco Comtec D-Link DASAN Enterasys Extreme	Force10 H3C Hirschmann HP Huawei Juniper Linksys NEC Nortel
Endpoint protection	360 Safe Active Virus Shield AhnLab Avas AVG Avira BitDefender CA eTrust ClamAV Comodo eScan ESET NOD32 EstSoft F-Secure Gdata Hauri K7 Kaspersky	LANDesk Lightspeed McAfee Microsoft ForeFront/System Center Endpoint Protection Microsoft Security Essentials New Technology Wave Panda PC Ziggy Rising Sophos Symantec Trend Micro Vipre

4 – Discovery and Classification

The tests in this section measured the effectiveness and speed with which CounterACT discovered and classified different types of endpoints, as well as the accuracy of the device classifications.

With the increasing number of unmanaged devices such as BYOD, Guest and IoT, it is critical to discover, classify and assess the different types of endpoints on any network. Without knowledge of the devices on the network, it is impossible to determine the attack surface and identify potential threat vectors.

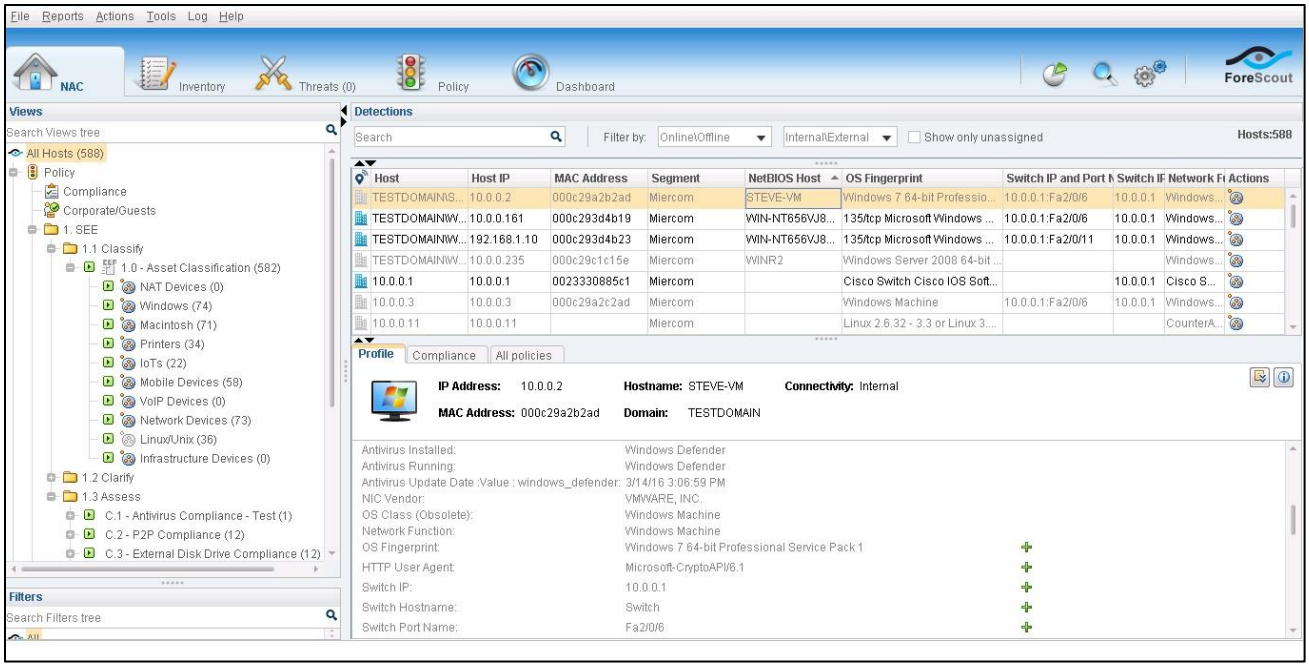
In the first tests, CounterACT was expected to promptly discover an endpoint attempting to access the network, then profile and accurately classify the endpoint.

Test: Endpoint Discovery
Task: Detect an agentless endpoint attempting to connect to the network.
Result: √ Pass A single non-corporate endpoint was connected and was immediately detected by CounterACT, which displayed it on the console as an unregistered Guest endpoint.

Then, using different tests, CounterACT was evaluated for efficiently detecting and classifying agentless corporate, BYOD and guest endpoints.

Test: Endpoint Classification - Corporate
Task: Classify newly detected corporate endpoint by device type (Windows, MAC OSX, Linux, Mobile, etc.); connected via wired, wireless or VPN
Result: √ Pass Two devices were connected to the network via wired and VPN. The devices were both recognized as corporate endpoints when attempting network access. They were accurately classified as MAC OSX and Windows, respectively.

Test: Endpoint Classification - BYOD and Guest
Task: Upon detection, classify BYOD and Guest endpoints by device type and host properties.
Result: √ Pass Both BYOD and Guest endpoints were detected immediately when accessing the network and classified as Windows devices. Correct host properties of both devices were also displayed. The endpoints were redirected to a captive portal login page for guest registration or BYOD authentication.



The list of "host properties" that CounterACT can determine for endpoints is impressive. Below is a brief list of properties that we observed during testing. Some of the reported properties depend, of course, on the type of endpoint and/or brand of infrastructure equipment, as well as the extent of traffic observed by CounterACT for a particular endpoint.

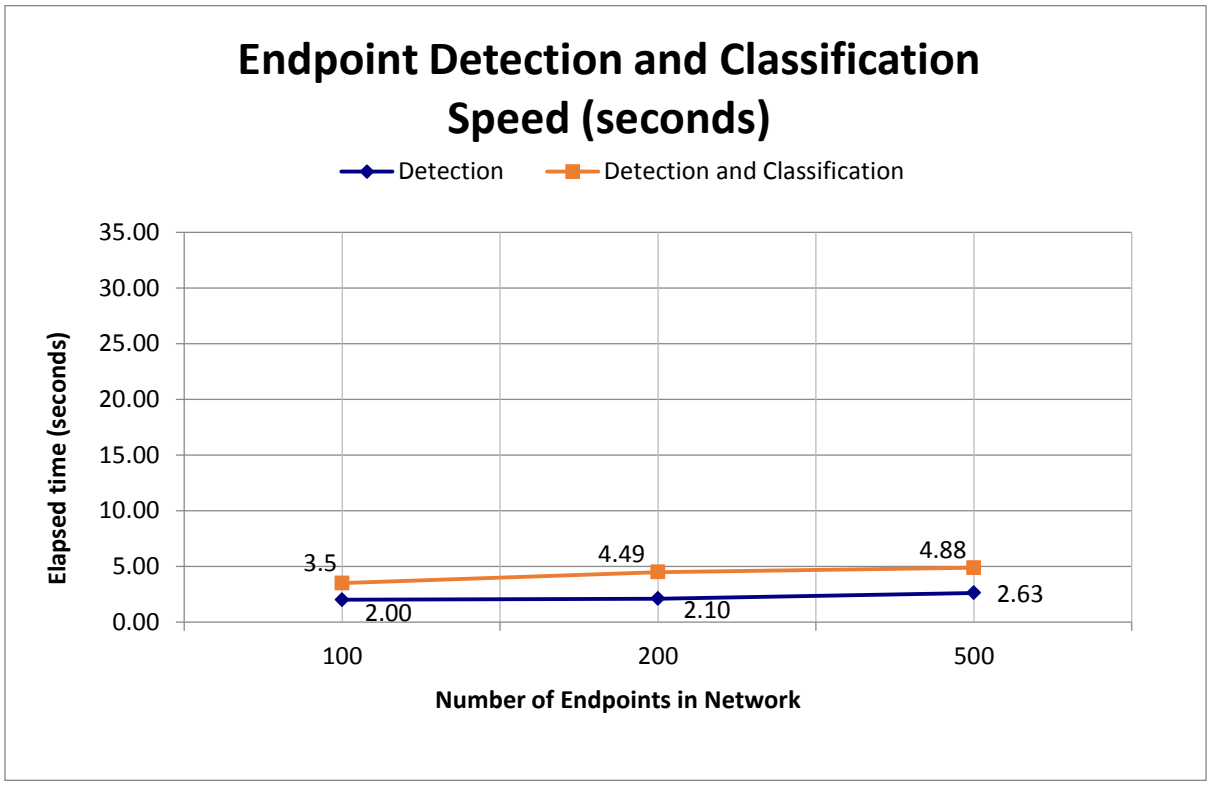
Examples of host properties reported by CounterACT include:

- IP Address
- MAC Address
- NetBIOS Domain
- NetBIOS Hostname
- Windows/OSX/Linux Manageable Domain
- Windows/OSX/Linux Manageable (agent)
- NIC Vendor
- Network Function
- DHCP Server Address
- DHCP Attributes like device class, OS fingerprint, hostname, request/options fingerprint, etc.
- OS Class
- OS Fingerprint
- HTTP User Agent
- Connectivity Status – Switch, Wireless or VPN
- Switch IP and Port Name
- Switch Port Alias
- Switch Port VLAN ID and Name
- Switch Port VoIP Device
- Switch Port PoE Information
- Open Ports
- LDAP Information

Time to discover and classify. We tested the speed at which CounterACT can discover and classify an entire network landscape of varying endpoint numbers and types. The cumulative speed for visibility and classification was recorded. In all cases, there were 30 actual physical endpoints and five simulated Linux and Windows platforms.

Test: Time to Discover and Classify an Entire Network
Task: To measure how long it takes to detect and classify different numbers of concurrently connecting endpoints. Tests were conducted for different network set-ups with 100, 200, and 500 endpoints.
Result: √ Pass 100 percent of the endpoints in each network scenario were detected and classified. All CounterACT discovery techniques and classification policies were enabled. Some endpoints were assigned static IPs, and CounterACT, using IP/MAC mapping from switches, SPAN traffic monitoring and NMAP scanning of known IPs, was able to readily detect and classify the static-IP endpoints as well.

The following chart shows the times it took CounterACT to conduct discovery and classification in each network scenario tested.



The above data points reflect the best speeds observed for each network size tested for multiple iterations. An unprecedented detection rate in the NAC industry was recorded for 500 devices in less than 5 seconds, proving scalability. There is a correlation between the number of endpoints and speed of detection and classification, although the increase is not necessarily linear.

We also measured the speed of endpoint discovery and classification for a single endpoint, and how easy it was to provision network access for a Guest endpoint.

Test: Time to Discover an Endpoint on Connection
Task: To promptly detect a new endpoint that is attempting network access.
Result: √ Pass The endpoint was discovered in less than 1 second.

Test: Time to Discover and Classify an Endpoint on Connection
Task: To promptly detect and classify a new endpoint.
Result: √ Pass CounterACT detected the endpoint in less than 1 second and was accurately able to classify the endpoint as Windows machine. CounterACT further clarified the endpoint as an agentless corporate endpoint by connecting to it via admin credentials.

Test: Provide Appropriate Network Access for a Guest Endpoint
Task: To provide appropriate network access for an endpoint that has no corporate credentials and no agent.
Result: √ Pass CounterACT immediately detected the Guest endpoint and placed it in the Guest VLAN. The endpoint was redirected to a Guest Captive Portal login page where the user was asked to register. User successfully registered as a guest and was provided Internet access only for 8 hours. CounterACT supports various guest flows like hotspots, self-service and sponsor portals. Automating guest access management eliminates manual administrative tasks and improves IT efficiency.

5 – Endpoint Posture Assessment and Policy Configuration

CounterACT does not require endpoint agents for posture assessment. CounterACT provides full visibility into the security posture of the corporate network. CounterACT inspects the endpoints based on the compliance policies to meet the network security standards.

Once the security posture of an endpoint is identified, CounterACT provides best-in-class host and network controls for non-compliant endpoints. The level of control varies from mild to moderate to strong, depending on the enterprise and its network and endpoint compliance policies.

CounterACT offers a wizard to help an administrator use pre-built policy templates, and also provides easy-to-configure custom policies. First, we evaluated the ease of policy creation and use. Then we looked at the complete endpoint compliance status of our network. We observed early on that the automation provided by CounterACT plays a major role in efficiently maintaining endpoint compliance.

Ease of Policy Set-up. With minimal training, we found policy creation with CounterACT to be fairly straightforward. CounterACT's if/else Boolean logic policy structure makes it easy to configure a new custom policy or update an existing policy.

The following tests assessed the ease of setting up policies to provide immediate visibility into the endpoint compliance status and trigger automatic control actions to mitigate the security risks.

Test: Posture Assessment of Corporate Endpoints
Task: To provide real-time visibility and accurate assessment of "corporate" endpoints: whether they comply with the policies that apply to the particular device type or group.
Result: √ Pass 100 percent of corporate endpoints were detected and correctly classified. Those endpoints were assessed against the configured compliance policies. Those that did not were prompted to comply with all appropriate policies.

Test: Windows/Mac Operating System (OS) Update Compliance Policy
Task: Set up a policy in CounterACT for checking endpoints' OS update status. Installing the latest OS updates can help prevent network breaches.
Result: √ Pass Under the policy tab of CounterACT, a wizard guides the user through a policy set-up. We found this tool and the process to be effective and straightforward. CounterACT uses a built-in vulnerability database to provide visibility onto the corporate Windows and MAC OS X endpoints that are not fully patched. In our test, CounterACT detected both Windows and MAC OS X corporate endpoints with missing patches, and automatic actions were triggered to update the non-compliant corporate endpoints. Users were notified about their endpoint compliance status by triggering an endpoint HTTP notification. CounterACT can also trigger third-party patch management systems to bring the endpoints to a compliant state.

Test: Peer-to-Peer (P2P) and Instant Messaging (IM) Compliance Policy

Task: Set up a policy in CounterACT for checking whether endpoints are running peer-to-peer or IM applications. These are often restricted or forbidden in many organizations due to inherent security vulnerabilities.

Result: √ Pass

Under the policy tab of CounterACT, a wizard guides the user through a policy set-up. We found this tool and process to be effective and straightforward to use.

In our test, CounterACT detected a corporate endpoint that had a P2P application installed. CounterACT was successfully able to shut down the unauthorized application, and the user was notified via HTTP notification about their endpoint compliance status.

Test: Antivirus Software Compliance Policy

Task: Set up a policy in CounterACT for checking endpoint antivirus software

Result: √ Pass

Under the policy tab of CounterACT, a wizard guides the administrator through policy set-up. We found this tool and the process to be effective and straightforward.

In the AV compliance policy, CounterACT provided visibility into the corporate endpoints that were missing AV software, endpoints with up-to-date AV software, and endpoints with out-of-date (in last 1 week) AV software.

Automatic actions to install AV software and update AV software were triggered for non-compliant endpoints. Users were notified about their endpoint compliance status by triggering an endpoint HTTP notification.

Test: Posture Assessment of BYOD or Guest Endpoints by Dissolvable Agent

Task: To provide real-time visibility and accurate assessment of ten BYOD and Guest endpoints attempting to connect to the corporate network.

Result: √ Pass

100 percent of BYOD and Guest endpoints were detected and correctly classified. All were prompted with a captive portal log-in page.

Guests were required to register and then were sent a user name and password for login by email. After logging in, they were provided with only Internet access.

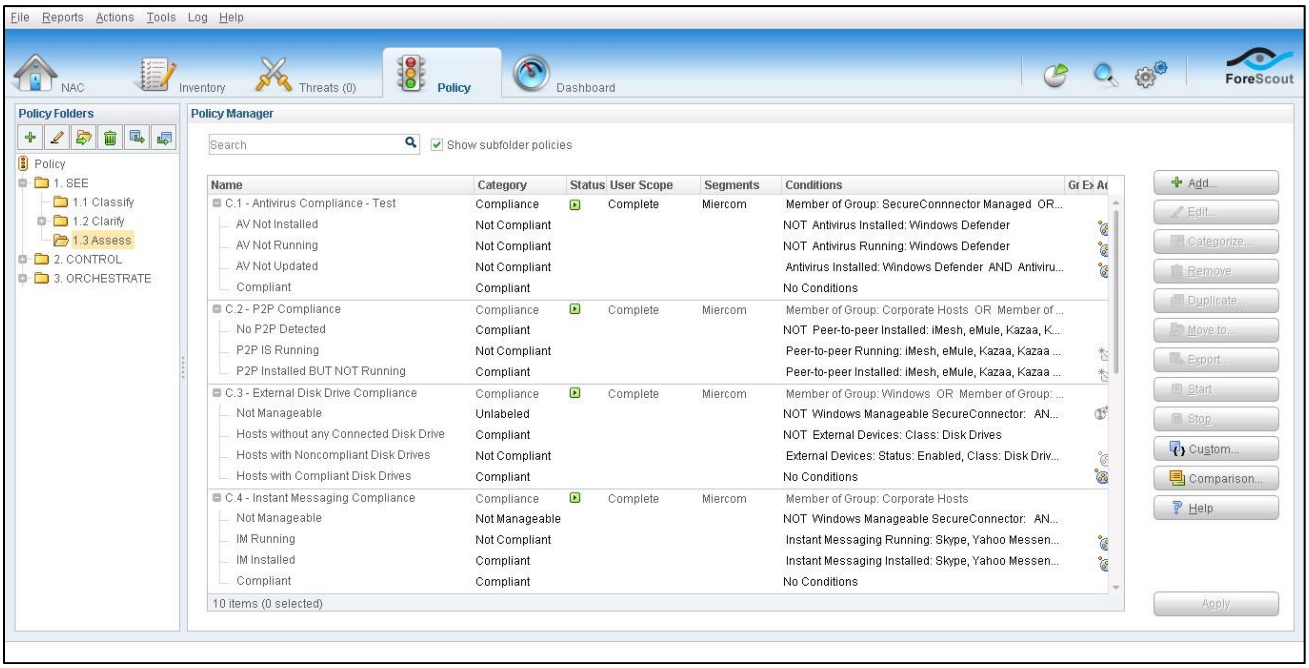
BYOD users logged in immediately with their corporate credentials. Once authenticated, they were prompted to install a lightweight dissolvable agent to gain corporate network access. The dissolvable agent ensured that BYOD endpoints were checked for security compliance, and only compliant BYOD endpoints were allowed on the network.

Checking BYOD endpoints for posture/compliance is not a requirement, it is a best practice. You may optionally choose to only authenticate with corporate credentials from the login page on BYOD endpoints and appropriate network access may be granted.

Test: Ease of Updating a Policy
Task: Update an existing compliance policy in CounterACT using the policy wizard.
Result: √ Pass Under the policy tab of CounterACT, a wizard guides the user through a policy set-up, as well as updating or modifying. We found this interface to be effective and straightforward. In our test, we modified the AV policy to check for Windows AV on corporate endpoints instead of McAfee, and this process was very quick and easy. We also updated the Action in the P2P policy from HTTP notification to send an email to the user. The policy update was easy and only took a few clicks.

Policy Granularity. A policy can be customized for different purposes depending on the organization's needs. CounterACT offers pre-built policy templates for assessing endpoint/ network security posture. There is an option to customize security policies, via the policy wizard. Pre-built policies address issues such as antivirus, personal firewall, unauthorized applications, software updates and more. Custom policies can include prescheduled events, timing-forced compliance, remediation actions and many more.

The wizard options under the Policy tab allow either the host or the network to respond to policy infractions – on a scale of mild, moderate or strong actions.



6 – Control

CounterACT has host and network control options. Host control actions take place on the host whereas network control actions occur at the network level. Controls can be applied manually to an individual endpoint or as automatic actions applied as outcomes of CounterACT policies. The controls vary from mild to strong. Examples of host and network control usage are shown below:

Host-based Controls:

- **Mild Control**: If OS updates are not a priority, the policy action response could be a self-remediation request. For example, an HTTP notification would appear on the user's screen, noting the policy violation and instructing them to update their OS.
- **Moderate Control**: If the OS updates are viewed as important, the control response could be to force the OS update on non-compliant endpoints.
- **Strong Control**: If a policy violation is severe such as an endpoint running a blacklisted application, the control response could be terminating that application on the endpoint. Additionally, a notification of the endpoint and the violation could be sent to the administrator.

Below are examples of host-based control options:

Mild Control "Alert"	**Moderate Control** "Apply"	**Strong Control** "Disable"
- Email to user - On-screen notification - Redirect to a Web page - Request end-user acknowledgment	- Install required applications - Update antivirus - Update agent - Apply OS updates - Apply patches	- Terminate unauthorized applications - Disable connection - Disable peripherals

Network-based Control.

- **Mild Control**: The administrator and IT staff are notified of a compliance violation and a system event is logged. If a rogue device is attempting to access the network, the administrator is immediately notified in order to prioritize the mitigation action.
- **Moderate Control**: The administrator can restrict the endpoints' network access in real-time. If a compliance policy determines that AV software has been disabled on a host, the host network access is changed to remediation resources only until the host AV is enabled and updated.
- **Strong Control**: If an endpoint type is not allowed by the enterprise such as a video camera, the switch port can be turned off or have limited network access.

Below are examples of network-based control options:

Mild Control "Alert"	Moderate Control "Apply"	Strong Control "Disable"
- Email to administrator - Register a system log message - Generate a help-desk ticket - IT system notification	- Assign user to Guest VLAN - Change wireless user role - Quarantine for self-remediation - Restrict rogue devices - Restrict changes to infrastructure	- Quarantine device - Turn off switch port - Block wireless/VPN - Access control list to restrict endpoint access

Test cases were conducted to confirm the effectiveness of various policy-based controls.

Test: Detect and Disable a Rogue Device
Task: Detect and disable a rogue device. Note: CounterACT views as a threat rogue devices such as switches, hubs and wireless access points, which are not managed or known to IT.
Result: √ Pass A Rogue wireless access point was connected to the network. CounterACT quickly determined the endpoint as a non-corporate NAT device. CounterACT shutdown the switch interface to which the rogue endpoint was connected.

BYOD/Guest endpoints are segmented in a restricted network until they either register as a guest or authenticate using corporate credentials. The following test looks at whether CounterACT appropriately identifies devices and provides them the means to gain corporate access by pushing a dissolvable client onto them.

BYOD devices should authenticate using their corporate credentials to get appropriate network access. Guest devices that properly sign in should have Internet access only.

Test: Handling of BYOD/Guest Device
Task: Isolate a BYOD/Guest device and provide appropriate access.
Result: √ Pass The BYOD and Guest endpoints were correctly identified and assigned appropriate network access. • The Guest endpoint without credentials was properly put in the Guest network without access until registered. • The Guest endpoint, once registered, was seen on the Guest network as "Signed-in as Guest." • Users with the BYOD devices that authenticated using corporate credentials were as asked to install a lightweight dissolvable agent, verified for corporate compliance and then given network access. **Mild and moderate controls** such as the log-in portal and VLAN reassignment allow the endpoint user to log in to an authorized network. Employee BYOD devices use their employee credentials for authentication and can be forced to accept a dissolvable client to check endpoint compliance. **Strong controls** can be used to disconnect network access for device types not approved for network access.

An endpoint is not allowed to be connected to two different networks simultaneously. Such a situation poses a security risk, possibly enabling unauthorized access through this endpoint from one network to another. This test checks whether CounterACT detects the dual-network connection and applies the appropriate policy-directed mitigation action (for mild, moderate and strong scenarios).

Test: Detect and Address a Dual-Homed Device
Task: Detect a corporate device that is connected to two networks – a corporate network and a less secure network. Disable the adapter that connects to the unsecured network.
Result: √ Pass The two network- connected dual-homed endpoints were detected and CounterACT sent the instructions to kill the unsecured network adapters to only allow corporate network access.

7 – Deployment and Management

Deployment

CounterACT was evaluated for its deployment flexibility, diverse vendor infrastructure integration, support for managed and unmanaged endpoints and authentication directory integration. CounterACT readily deploys into a mixed-vendor enterprise networks.

Our test bed consisted of Cisco switches, a Check Point firewall, a Microsoft domain controller/DHCP server with Active Directory, and Cisco wireless access points. CounterACT was easily deployed into this network environment, even integrating readily with Microsoft Active Directory – an LDAP server. We observed no dependency between CounterACT and the hardware comprising our test-bed network during deployment.

As already noted CounterACT was able to detect, classify and assess all of the endpoints in our network, both physical and simulated. Our simulated endpoints were appropriately shown as Linux and Windows platforms. The actual physical endpoint devices, in addition to network infrastructure equipment, consisted of a spectrum of Android and Apple smartphones, tablets, laptops and desktops – both wired and wireless.

We have included an impressive table (see page 8) of network-infrastructure equipment provided by ForeScout Technologies, Inc. listing vendors by equipment categories that are explicitly supported.

Agentless Device Support

Our testing found that CounterACT is able to do endpoint posture compliance policies "agentless." The mechanisms used by CounterACT to do this vary. For example, for a corporate Windows device, this is possible by using the Windows Management Instrumentation (WMI) protocol. For a corporate MAC OS X or Linux device, this is possible using SSH key exchange.

Management

In addition to detecting, classifying and assessing endpoints based on preset or custom policies, we assessed the CounterACT console for its organization, effectiveness and clarity.

The CounterACT console is the single-pane window into full network visibility. It gives an administrator a top-level view of all the endpoints, all policies, and all categories of device assignment based on these policies. The simple and intuitive search feature allows endpoints or policies to be filtered based on a specified property or group.

These tests were a subjective assessment of how easily an administrator can navigate the console to find endpoints and policies as well as perform updates.

Test: Search and Filter by Endpoints
Task: Search and filter for a specific endpoint by name, property or group.
Result: √ Pass Using the *Views* panel, a search box is available for searching all hosts. We entered an endpoint IP address and the correct endpoint was immediately located, displaying the host name, IP address, segment, MAC address, any comments, Switch IP and ports, device type and actions available. When we right-clicked on the endpoint, we could see all action triggers and statuses. For example, there was an HTTP notification triggered by an out-of-date anti-virus version, and the action status showed "pending" until the user confirmed receipt of this alert.

The ability to search endpoints by policy offers an administrator full visibility, from current network compliance to security policies. This test evaluates the ease of navigation to a specific policy and how CounterACT displays information regarding it. Policies should be searchable and filterable by many parameters or groups.

Test: Search and Filter by Policy
Task: Search and filter for a specific endpoint by policy.
Result: √ Pass Using the *Views* panel, a hierarchical tree of policies is displayed under *Policy*. For example, under *Compliance* is Antivirus Compliance policy. In parentheses are the number of endpoints to which this policy applies. By clicking on the policy, all endpoints with this policy are displayed by host name, IP address, segment, compliance status, MAC address, switch and port information, device type and actions available.

The following test evaluates the flexibility of navigation for editing policies.

Test: Policy Transparency
Task: While creating a policy or searching endpoints or policy groups, attempt to change a policy.
Result: √ Pass The user is able to see, update or create a policy from multiple areas of the console. Under the NAC tab, a policy can be seen and changed using the *View/Edit Policy* panel while searching endpoints or policy groups. Under the Policy tab, a policy can be created or changed using the Policy Wizard. In either approach, policy visibility is transparent and policies are simple to edit in the console.

Test: CounterACT Software Upgrade
Task: Conduct a software upgrade from the CounterACT console.
Result: √ Pass We found that software upgrades can be installed in two different ways: through the *Tools* drop-down menu within the console or by selecting the Settings icon in the upper-right of the GUI. Installation is straightforward and, when checking for updates, the user is prompted by the CounterACT *Update* page.

ForeScout Extended Modules support third-party security vendors' integration for sharing information and utilization of controls. Extended Modules are installed from the CounterACT console.

This test assesses the ease of navigation to install a new module and upgrade an existing module from the console.

Test: Extended Module Installation
Task: Install an Extended Module from the CounterACT console. Upgrade an existing VPN module that was installed previously.
Result: √ Pass This is a straightforward process using the *Plug-ins Installation Manager* of CounterACT. We readily installed a third-party module – a ForeScout Extended Module for a prominent vendor's ATD. And then, using the *Settings* > *Plugins* > *Update* process, we were readily able to update the existing VPN module that was previously installed.

8 – Conclusion

Following are the key observations and conclusions from Miercom's independent assessment of ForeScout CounterACT.

- **Visibility, control and situational awareness**. While most NAC (Network Access Control) solutions give an administrator the ability to manage endpoint authentication and access, CounterACT can "see" in real-time endpoints that enter the network, as well as those which do not comply with corporate policies. The CounterACT console provides a single pane of glass view into endpoints and policy compliance. An administrator can see which endpoints belong to the corporate or guest network, which have agents installed, and which are currently compliant with assigned policies.
- **Real-time updates**. The CounterACT console shows all changes in real-time. If a policy changes, non-compliant endpoints that are affected by the change are readily identified. CounterACT automatically notifies and updates users and IT staff of policy violations, network statuses, and appropriate control actions for each endpoint on the network.
- **Simplified control, automation and time savings**. Setting up policies for hosts and the network is straightforward via CounterACT's console and wizards. Endpoint policies are readily understood and easily modified. Instead of manually querying endpoints and determining their individual policy compliance, CounterACT automates this process, saving administrators and IT staff time and resources by mitigating problems.
- **No impact on endpoint or network performance**. Endpoint performance should not be affected by CounterACT. There was no appreciable CPU usage increase on endpoints during connection, while installing a dissolvable client, or when notified of non-compliance. Also, on a SPAN link, CounterACT observes network traffic passively, with little to no impact on network performance.

9 – About "Miercom Performance Verified" Testing

This report was sponsored by ForeScout Technologies, Inc. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Performance Verified assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by Miercom.

10 – About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

11 – Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.