ForeScout CounterACT™
Network Access Control

Data Sheet

Highlights

Features

- **Easy to deploy.** No endpoint agents required for authentication and network access control.
- **Rapid time to value.** Visibility to your network in hours or days.
- **Comprehensive coverage.** Managed and unmanaged devices. Wired and wireless LANs. Servers, desktops, smartphones, tablets.
- **Powerful policy engine** helps you automate an extensive range of actions to control network access, remediate the endpoint, or alert help desk.

Benefits

- **Visibility.** See what is on your network — devices, endpoints, users, applications.
- **Security.** Protect sensitive data and block threatening activity.
- **Productivity.** Grant the right level of network access to each person and device, without intrusive intervention or staff involvement.
- **Reliability.** Improve network stability by identifying and removing rogue infrastructure.
- **Cost Savings.** Eliminate manual labor associated with opening or closing network ports for guest access, and eliminate troubleshooting and downtime caused by rogue network devices.

Network Access Control

ForeScout CounterACT™ is a continuous monitoring and mitigation platform that delivers real-time visibility and control of devices on your network. ForeScout CounterACT lets employees and guests remain productive on your network while you protect critical network resources from unauthorized access.

Based on ControlFabric™ technologies, ForeScout CounterACT is easy to install because it typically requires no infrastructure changes or upgrades, no endpoint agents, and no endpoint reconfiguration of any kind.

Network Security Risks and Blind Spots

The traditional network security focus has been on blocking external attacks with firewalls and intrusion prevention systems. These devices do nothing to protect your network against insider threats such as:

- **Visitors:** When guests and contractors come to your location, they bring their computers with them. To remain productive, guests need to access the Internet, and contractors may need additional resources. If you give these visitors unlimited access, you risk attack by malware or compromise of your sensitive data.
- **Wireless and mobile users:** Your employees want to use their smartphones and tablets on your network. If you don't have adequate control, these devices can infect your network or be a source of data loss.
- **Rogue devices:** Well-meaning employees can extend your network with inexpensive wiring hubs and wireless access points. These devices can cause your network to become unstable, and they can be a source of infection and data loss.
- **Malware and Botnets:** Studies show that even well-managed enterprises have infected computers because of zero-day attacks and/or out-of-date antivirus. Once your PCs are compromised, they can be used in "pivot attacks" whereby outsiders can scan your network and steal your data.
- **Compliance:** Endpoints can be misconfigured, virtual machines can appear on your network with improper settings or inappropriate software, and security controls can be de-activated. Non-compliant systems are security risks.

How ForeScout CounterACT Works

ForeScout CounterACT is different from most network access control (NAC) solutions because it is easy to deploy and provides rapid results. Everything is contained in a simple appliance and interoperates with most types of existing network infrastructure. No endpoint agents required for authentication and network access control.

ForeScout CounterACT physically deploys out-of-band on your network. From that position, CounterACT monitors network traffic and integrates with your networking infrastructure so it can see new devices the moment they try to access your network. CounterACT automatically grants access based on who the user is, what the device is, and the security posture of the device. After the device has been allowed onto your network, CounterACT can notify you of a security issue, fix the issue for you, or quarantine the endpoint until the issue can be addressed. CounterACT continuously protects your network by monitoring the behavior of devices and blocking attacks.

ForeScout

The ForeScout Difference

ForeScout CounterACT is dramatically easier and faster to deploy than traditional NAC products. Here is why:

- **Turnkey.** Everything is contained in a single physical or virtual appliance. Setup is fast and easy with built-in configuration wizards and templates.
- **Works with what you have.** CounterACT works with the majority of popular switches, routers, firewalls, endpoints, antivirus systems, directories, and other infrastructure. We typically require no infrastructure changes or equipment upgrades.
- **Agentless.** ForeScout CounterACT can identify, classify, authenticate and control network access of both managed and unmanaged (BYOD) endpoints without any help from agents or any kind of preconfigured endpoint software. Deep endpoint inspection can also be done without an agent as long as CounterACT has administrative credentials on the endpoint. In situations where CounterACT does not have administrative credentials (e.g. BYOD), deep inspection can be performed with the help of our optional SecureConnector agent.
- **Non-disruptive.** Unlike conventional NAC products that immediately disrupt users with heavy-handed access controls, ForeScout CounterACT can be deployed in a phased approach which minimizes disruption and accelerates results In the initial phase, CounterACT gives you visibility to your trouble spots. When you want to move forward with automated control, you can do so gradually, starting with the most problematic locations and choosing an appropriate enforcement action.
- **Open interoperability.** Unlike infrastructure vendors which offer minor interoperability and modest third-party coverage, ForeScout CounterACT offers extensive third-party vendor interoperability and an open integration architecture. Learn more about ForeScout ControlFabric.
- **Accelerated results.** ForeScout CounterACT provides useful results on Day 1 by giving you visibility to problems on your network. . Built-in wizards and policy templates help you configure security policies quickly and accurately.

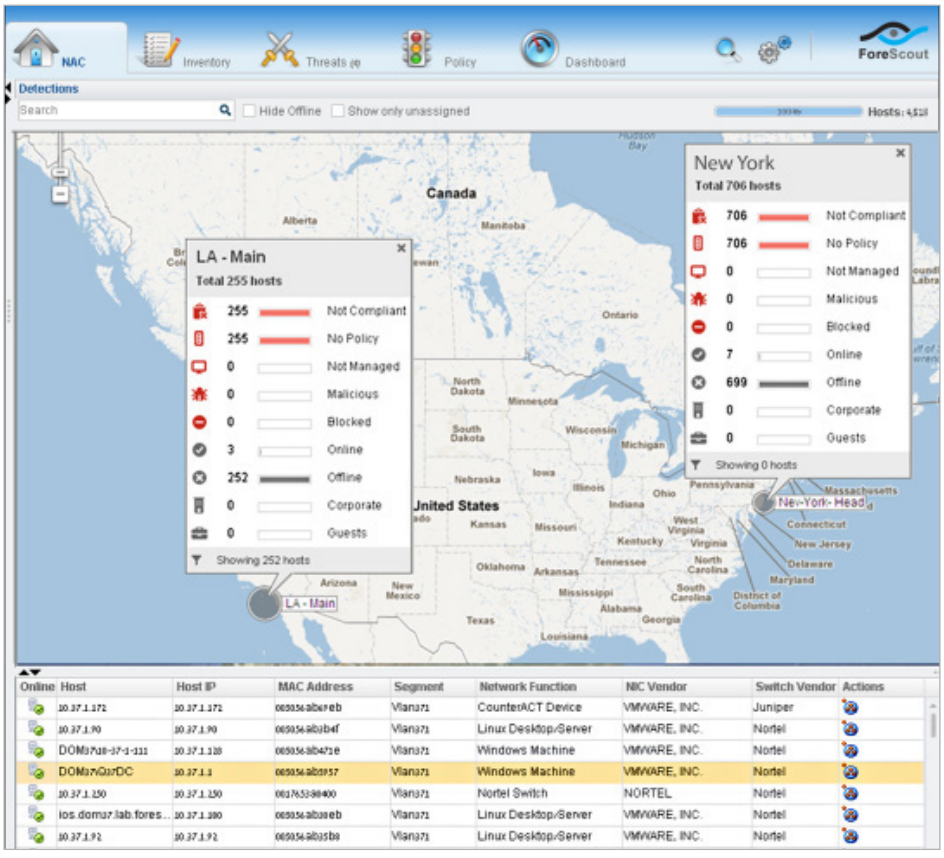

Figure 1: ForeScout CounterACT provides both high-level and detailed information about devices on your network.

Features

General		
ControlFabric™ architecture ForeScout CounterACT is the centerpiece of the ControlFabric architecture that enables ForeScout CounterACT and other solutions to exchange information and resolve a wide variety of network, security and operational issues.	**Visibility** ForeScout CounterACT's Asset Inventory provides real-time, multi-dimensional network visibility and control, allowing you to track and control users, applications, processes, ports, external devices, and more (see Figure 1).	**IT infrastructure integration** Unlike proprietary NAC products, CounterACT is fast and easy to install because it supports an extensive range of third-party networking and security hardware and software such as network switches, wireless access points, VPN, directories, etc.
Out-of-band deployment ForeScout CounterACT physically deploys out-of-band on your network which eliminates potential points of failure in your network.	**Policy management** ForeScout CounterACT lets you create security policies that are right for your enterprise. Configuration and administration is fast and easy thanks to CounterACT's built-in policy templates, rules and reports.	**Scalability** ForeScout CounterACT has been proven in customer networks exceeding 500,000 endpoints. CounterACT appliances are available in a variety of sizes (see last page for details).
Reporting ForeScout CounterACT has a fully integrated reporting engine that helps you monitor your level of policy compliance, fulfill regulatory audit requirements, and produce real-time inventory reports.		**Qualifications** ForeScout CounterACT is military grade with the following qualifications: • USMC ATO • US Army CoN (Certificate of Networthiness) • UC APL (Unified Capabilities Approved Product List) • Common Criteria EAL L4+

Endpoint		
Endpoint compliance ForeScout CounterACT can ensure that endpoints on your network are compliant with your antivirus policy, are properly patched, and are free of illegitimate software such as P2P.	**Threat detection** ForeScout CounterACT's patented ActiveResponse™ threat detection technology monitors the behavior of devices post-connection. ActiveResponse blocks zero-day, self-propagating threats and other types of malicious behavior. Unlike other approaches, ActiveResponse doesn't rely on signature updates to remain effective, translating to low management cost.	**Rogue device detection** ForeScout CounterACT can detect rogue infrastructure such as unauthorized switches and wireless access points by identifying whether the device is a NAT device, identifying whether the device is on a list of authorized devices, or identifying situations where a switch port has multiple hosts connected to it. CounterACT can even detect devices without IP addresses, such as stealthy packet capture devices designed to steal sensitive data.
Real-time mobile device control ForeScout CounterACT detects and controls hand-held mobile devices connected to your Wi-Fi network. Supports iPhone/iPad, Blackberry, Android, Windows Mobile, Kindle, Palm, others.	**Agentless** ForeScout CounterACT can identify, classify, authenticate and control network access without an agent. Deep endpoint inspection can also be done without an agent as long as CounterACT has administrative credentials on the endpoint. In situations where CounterACT does not have administrative credentials (e.g. BYOD), deep inspection can be performed with the help of our optional SecureConnector agent which is included with CounterACT at no additional charge.	

Access		
Guest registration ForeScout CounterACT's automated process allows guests to access your network without compromising your internal network security. CounterACT includes several guest registration options allowing you tailor the guest admission process to your organization's needs.	**Flexible Control Options** Unlike early generation NAC products that employed heavy-handed controls and disrupted users, ForeScout CounterACT provides a full spectrum of enforcement options that let you tailor the response to the situation. Low-risk violations can be dealt with by sending the end-user a notice and/or automatically remediating his security problem; this allows the user to continue to remain productive while remediation takes place (see Figure 2).	**802.1X or not** ForeScout CounterACT lets you choose 802.1X or other authentication technologies such as LDAP, Active Directory, Oracle and Sun. Hybrid mode lets you use multiple technologies concurrently, which speeds NAC deployment in large, diverse environments.
Role-based access ForeScout CounterACT ensures that only the right people with the right devices gain access to the right network resources. ForeScout leverages your existing directory where you assign roles to user identities.	**Authentication** CounterACT supports existing standards-based authentication and directories such as 802.1X, LDAP, RADIUS, Active Directory, Oracle and Sun.	**Built-in RADIUS** ForeScout CounterACT includes a built-in RADIUS server to make rollout of 802.1X easy. Or, leverage existing RADIUS servers by configuring CounterACT to operate as a RADIUS proxy.

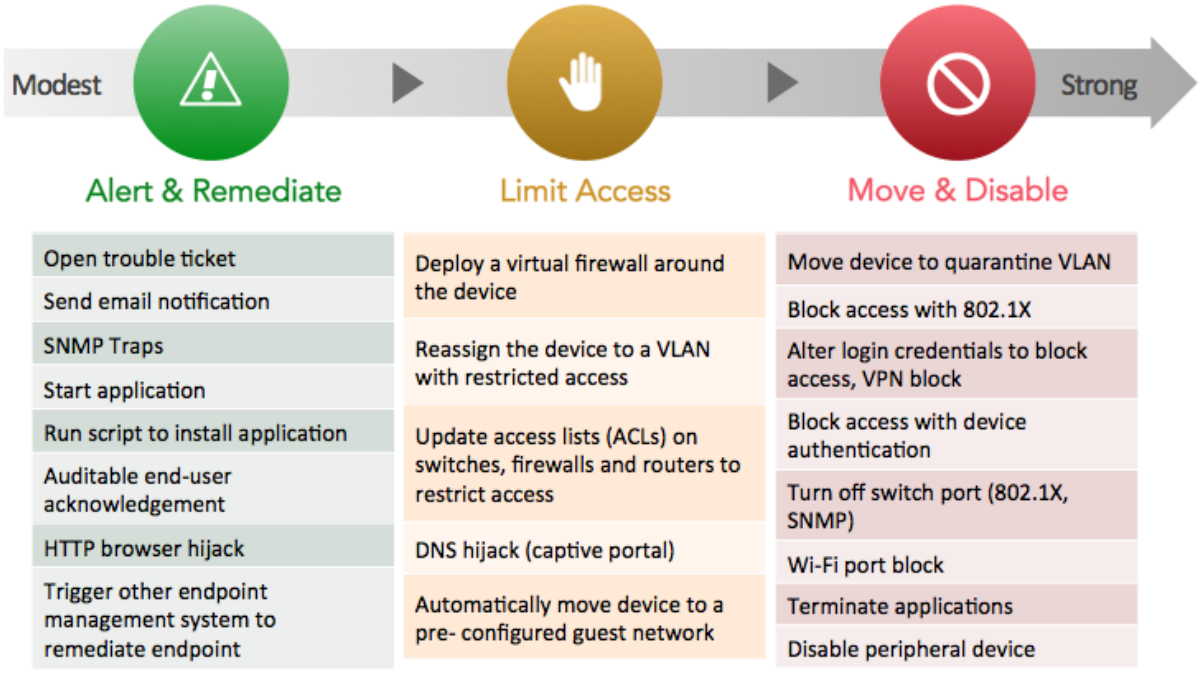

Figure 2: CounterACT handles the full spectrum of control actions.

Scalable Models

ForeScout CounterACT has been proven in customer networks exceeding 500,000 endpoints. CounterACT appliances are available in a range of sizes to accommodate networks of different sizes. Large networks that require multiple appliances can be centrally managed by ForeScout CounterACT Enterprise Manager. ForeScout CounterACT is available in either a physical or virtual appliance form factor. Each ForeScout CounterACT appliance includes a perpetual license for a specified number of network devices. Licenses are available for 100, 500, 1000, 2500, 4000, and 10,000 devices per appliance. For details on our licensing policy, see www.forescout.com/licensing. ForeScout CounterACT is fully integrated with functionality contained in a single product. This simple model avoids the administrative burdens and costs that are required to maintain multiple products, components, portals and licenses.

Physical appliance specifications are shown below. For virtual appliance specifications, visit http://www.forescout.com/product/scalable-models.

	CT-R	CT-100	CT-1000	CT-2000	CT-4000	CT-10000
Devices[1]	Up to 100	Up to 500	Up to 1000	Up to 2500	Up to 4000	Up to 10000
Bandwidth	100 Mbps	500 Mbps	1 Gbps	2 Gbps	Multi-Gbps	Multi-Gbps
Recommended Maximum Number of Managed Switches[2]	2	10	20	50	80	200
Network Ports **Copper** **Fiber**	 4 10/100/1000 N/A	 4 - 8 (depending on specific model) 10/100/1000 Available option (Up to 2 total)	 4 - 8 (depending on specific model) 10/100/1000 Available option (Up to 4 total)	 4 - 8 (depending on specific model) 10/100/1000 Available option (Up to 4 total)	 4 - 8 (depending on specific model) 10/100/1000 Available option (Up to 4 total)	 4 - 8 (depending on specific model) 10/100/1000 Available option (Up to 4 total)
I/O Support	1 serial port (RJ45)	1 serial port (DB9)	1 serial port (DB9)	1 serial port (DB9)	1 serial port (DB9)	1 serial port (DB9)
USB Ports	2, USB 2.0-compliant	2 back panel USB 2.0 + 1 front panel USB 2.0	2 back panel USB 2.0 + 1 front panel USB 2.0	2 back panel USB 2.0 + 1 front panel USB 2.0	2 back panel USB 2.0 + 1 front panel USB 2.0	2 back panel USB 2.0 + 1 front panel USB 2.0
VGA	1 (DB15)	1 (DB15)	1 (DB15)	1 (DB15)	1 (DB15)	1 (DB15)
CD-ROM	N/A	1	1	1	1	1
Hard Drives	1 HDD	3 HDD (RAID-1+HS)	3 HDD (RAID-1+HS)	3 HDD (RAID-1+HS)	3 HDD (RAID-1+HS)	3 HDD (RAID-1+HS)
Power Supply	1 @ up to 60w, 100-240VAC (External)	1 @ up to 750w 100-240VAC	2 @ up to 750w 100-240VAC	2 @ up to 750w 100-240VAC	2 @ up to 750w 100-240VAC	2 @ up to 750w 100-240VAC
Power Consumption (max)	45.3w	744w	744w	744w	744w	744w
Temperature **Operating** **Storage**	 5° to 40°C 0° to 70°C	 10°C to 35°C at 10% to 80% relative humidity (RH), with 26°C max dew point. –40°C to 65°C (-40°F to 149°F) with a maximum temperature gradation of 20°C per hour	 10°C to 35°C at 10% to 80% relative humidity (RH), with 26°C max dew point. –40°C to 65°C (-40°F to 149°F) with a maximum temperature gradation of 20°C per hour	 10°C to 35°C (50°F to 95°F) at 10% to 80% relative humidity –40°C to 65°C (-40°F to 149°F) with a maximum temperature gradation of 20°C per hour	 10°C to 35°C (50°F to 95°F) at 10% to 80% relative humidity –40°C to 65°C (-40°F to 149°F) with a maximum temperature gradation of 20°C per hour	 10°C to 35°C (50°F to 95°F) at 10% to 80% relative humidity –40°C to 65°C (-40°F to 149°F) with a maximum temperature gradation of 20°C per hour
Cooling Requirement	N/A	2891 BTU/Hr	2891 BTU/Hr	2891 BTU/Hr	2891 BTU/Hr	2891 BTU/Hr
Humidity	20% - 90%	20% to 80% (noncondensing) at a maximum wet bulb temperature of 29°C (84.2°F)	20% to 80% (noncondensing) at a maximum wet bulb temperature of 29°C (84.2°F)	10°C to 35°C at 10% to 80% relative humidity (RH), with 26°C max dew point	10°C to 35°C at 10% to 80% relative humidity (RH), with 26°C max dew point	10°C to 35°C at 10% to 80% relative humidity (RH), with 26°C max dew point
Chassis	1U desktop (steel slim line case)	1U 19" rack mount	1U 19" rack mount	2U 19" rack mount	2U 19" rack mount	2U 19" rack mount
Dimensions	Height: 55mm (2.17") Width: 335mm (9.84") Depth: 213mm (8.39")	Height: 42.92mm(1.69") Width: 482.34mm (18.99") Depth: 701.29mm (27.61")	Height: 42.92mm(1.69") Width: 482.34mm (18.99") Depth: 701.29mm (27.61")	Height: 87.30mm(3.44") Width: 482.4mm(18.99") Depth: 722.88mm (28.46")	Height: 87.30mm(3.44") Width: 482.4mm(18.99") Depth: 722.88mm (28.46")	Height: 87.30mm(3.44") Width: 482.4mm(18.99") Depth: 722.88mm (28.46")
Shipment	Size: 36.0 x 24.0 x 11.0" Weight: 4 pounds	Size: 36.0 x 24.0 x 11.0" Weight: 56 pounds	Size: 36.0 x 24.0 x 11.0" Weight: 57 pounds	Size: 36.0 x 24.0 x 11.0" Weight: 65 pounds	Size: 36.0 x 24.0 x 11.0" Weight: 66 pounds	Size: 36.0 x 24.0 x 11.0" Weight: 67 pounds

NOTE: All devices comply with FCC Part 15 of the FCC Rules, Class A; CANADA/USA: CSA 60950 and UL 60950 (Safety); ROHS.

[1]Device count, as determined by CounterACT, is the numerical sum of unique connections monitored by CounterACT made by on-site assets, off-site assets, and assets made known to CounterACT via third-party integrations. Network assets include user endpoints such as laptops, tablets and smartphones, network infrastructure devices such as switches, routers and access points, and non-user devices such as printers, IP phones, security/medical/manufacturing equipment etc. Device information is retained in CounterACT from initial discovery until such time the information is purged, based on aging preferences set in CounterACT.

[2] Each CounterACT appliance is licensed for a specified device count. However, the maximum number of devices that a CounterACT appliance can manage will vary based on several factors, including but not limited to, network environment, product configuration and use cases. When managing more than the recommended maximum number of L2/L3 switches, there is a tradeoff between managed switch count and total managed device count. For a more detailed explanation, including capacity planning guidelines, refer to the CounterACT Switch Plugin Configuration Guide.

Base Integrations

ForeScout CounterACT includes a wide variety of integrations with network and IT infrastructure (switches, wireless controllers, VPN, routers, directories), endpoints (Windows, Mac, Linux, iOS, Android, printers, other devices), and endpoint software (antivirus, instant messaging, WMI, etc.). These integrations are available at no additional charge in the form of easily installed plugins. These base integrations give you tremendous power to discover and classify endpoints; track users and applications; assess security posture; control network access; enforce endpoint compliance policy, and fix security gaps such as broken endpoint security agents.

Extended Integrations

ControlFabric extended integrations, developed and supported by ForeScout, bring additional value to the CounterACT appliance and are available as separately licensed modules that can be added to the CounterACT appliance. Current integration modules developed and supported by ForeScout include:

- Security Information and Event Management (SIEM)
- MDM Integration Module
- Advanced Threat Detection Integration Module
- Vulnerability Assessment Integration Module
- McAfee ePO Integration Module
- Splunk Integration Module

Custom Integrations

ForeScout's open ControlFabric Interface allows you or any third party to easily implement new integrations based on common standards-based protocols. The ControlFabric Interface can be enabled on the CounterACT appliance by purchasing the Open Integration Module. The Open Integration Module currently supports the following standards-based integration mechanisms: Web Services API, SQL, and LDAP.

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 enables organizations to continuously monitor and mitigate security exposures and cyber attacks. The company's CounterACT appliance dynamically identifies and evaluates network users, endpoints and applications to provide visibility, intelligence and policy-based mitigation of security problems. ForeScout's open ControlFabric architecture allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, extensible and scalable, as of January 1, 2015, they have been chosen by more than 1,800 of the world's most secure enterprises and government agencies in over 62 countries. Headquartered in Campbell, California, ForeScout offers its solutions through its global network of authorized partners. **Learn more at www.forescout.com.**

ForeScout Technologies, Inc.
900 E. Hamilton Ave.,
Suite 300
Campbell, CA 95008
U.S.A.

Contact Us
T 1-866-377-8771 (US)
T + 1-408-213-3191 (Intl.)
F + 1-408-371-2284 (Intl.)
www.forescout.com

Doc: 2013.0016 REV. 4