Datasheet

ForeScout CounterACT

Network Access Control

ForeScout CounterACT™ is an automated security control platform that lets you see, monitor and control everything on your network—all devices, all operating systems, all applications, all users. ForeScout CounterACT lets employees and guests remain productive on your network while you protect critical network resources and sensitive data.

Based on third-generation network access control (NAC) technologies, ForeScout CounterACT is easy to install because it requires no software, no agents, no hardware upgrades or reconfigurations. Everything is contained within a single appliance.

ForeScout
Access ability.

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Botnets -** Studies show that even well-managed enterprises have infected computers because of zero-day attacks and/or out-of-date antivirus.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.

ForeScout CounterACT Benefits

ForeScout CounterACT automatically enforces network access policies you choose for your organization. If you choose to ban guests and unknown computers from your network, CounterACT can do that. If you choose to allow guests and handheld wireless devices Internet access without opening up your entire network to them, CounterACT can do that as well. This powerful level of control gives you:

» **Visibility** - See everything 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.

ForeScout CounterACT Features

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.

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.

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 and Nokia Symbian.

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 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.

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..

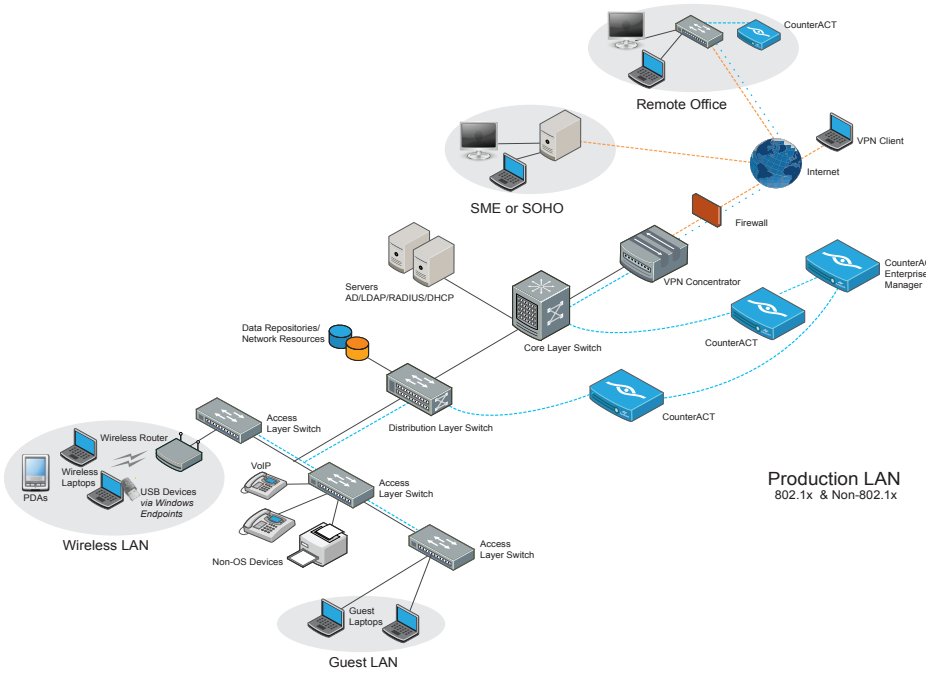
Flexible Control Options. Unlike early generation NAC products that employed heavy-handed controls and disrupted users, ForeScout CounterACT provides a full spectrum of enforcement options that let you tailor the response to the situation. Low-risk violations can be dealt with by sending the end-user a notice and/or automatically remediating his security problem; this allows the user to continue to remain productive while remediation takes place.

Out-of-band deployment. ForeScout CounterACT deploys out-of-band which eliminates issues regarding latency and potential points of failure in your network.

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 your existing network infrastructure. No software or agents to install, no hardware to upgrade.

ForeScout CounterACT deploys out-of-band by attaching to the span port of one of your existing switches. 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 all devices and blocking attacks.



ALERT & REMEDIATE	RESTRICT ACCESS	MOVE & DISABLE
Open trouble ticket	Deploy a Virtual Firewall around an infected or non-compliant device	Reassign device from production VLAN to quarantine VLAN
Send email notification	Reassign the device into a VLAN with restricted access	Block access with 802.1X
SNMP Traps	Update access lists on switches, firewalls and routers to restrict access	Alter login credentials to block access
Syslog	Automatically move device to a pre-configured guest network	Block access with device authentication
HTTP browser hijack		Turn off switch port (802.1X or SNMP)
Auditable end-user acknowledgement		Terminate unauthorized applications
Self-remediation		Disable peripheral device
Integrate with SMS, WSUS, SCCM, Lumension, BigFix		

The ForeScout Difference

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

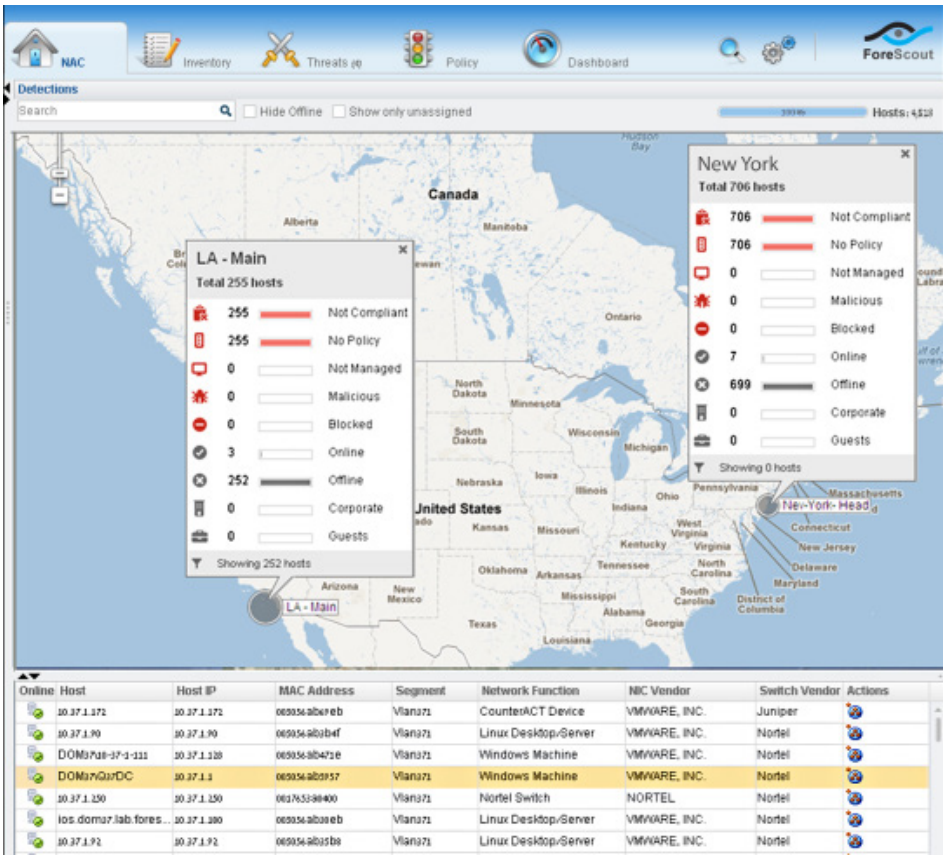
» **One box, one day to install.** Everything is contained in a single appliance. Setup is easy with built-in configuration wizards.

» **ForeScout works with what you have.** All your existing switches, routers, firewalls, endpoints, patch management systems, antivirus systems, directories, ticketing systems—ForeScout CounterACT works with them. We require no infrastructure changes or equipment upgrades.

» **No software.** ForeScout CounterACT is agentless, which means it works with all types of endpoints—managed and unmanaged, known and unknown, authorized and rogue. No client installation is required.

» **Non-disruptive.** Unlike first generation 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.

» **Accelerated results.** ForeScout CounterACT provides useful results on Day 1 by giving you visibility to problems on your network. The built-in knowledge base helps you configure security policies quickly and accurately.



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

CounterACT Features (continued)

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 wizard and knowledge base of device classifications, rules and reports.

Scalability. ForeScout CounterACT has been proven in customer networks exceeding 250,000 endpoints. CounterACT appliances are available in a range of sizes to accommodate networks of all sizes.

Optional agent. ForeScout CounterACT does not require an agent on the endpoint, which is important when dealing with BYOD. If you wish, you can install ForeScout's lightweight agent on Windows, Mac, Linux, iOS and Android devices. Agents and can be automatically installed when the device connects to the network and the user registers their identity.

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, antivirus, patch management, ticketing, SIEM, vulnerability assessment, and mobile device management (MDM) .

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.

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.

Authentication. CounterACT supports existing standards-based authentication and directories such as 802.1x, LDAP, RADIUS, Active Directory, Oracle and Sun.

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.

Endpoint compliance. ForeScout CounterACT can ensure that every endpoint on your network is compliant with your antivirus policy, is properly patched, and is free of illegitimate software such as P2P.

Scalable Models

ForeScout CounterACT has been proven in customer networks exceeding 250,000 endpoints. CounterACT appliances are available in a range of sizes to accommodate networks of all 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. ForeScout CounterACT is fully integrated with all 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
Concurrent Devices	100	500	1000	2500	4000	10,000
Bandwidth	100 Mbps	500 Mbps	1 Gbps	2 Gbps	Multi-Gbps	Coming soon. Virtual appliance VCT-10000 available now.
Network Ports						
Copper	4 10/100/1000	4 - 8 (depending on specific model) 10/100/1000	4 - 8 (depending on specific model) 10/100/1000	4 - 8 (depending on specific model) 10/100/1000	4 - 8 (depending on specific model) 10/100/1000	
Fiber	N/A	Available option (Up to 2 total)	Available option (Up to 4 total)	Available option (Up to 4 total)	Available option (Up to 4 total)	
I/O Support	1 serial port (RJ45)	1 serial port (RJ45)	1 serial port (RJ45)	1 serial port (RJ45)	1 serial port (RJ45)	
USB Ports	2, USB 2.0-compliant	4 back panel USB 2.0 + 1 front panel USB 1.1	4 back panel USB 2.0 + 1 front panel USB 1.1	4 back panel USB 2.0 + 1 front panel USB 1.1	4 back panel USB 2.0 + 1 front panel USB 1.1	
VGA	1 (DB15)	1 (DB15)	1 (DB15)	1 (DB15)	1 (DB15)	
CD-ROM	N/A	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)	
Power Supply	1 @ up to 60w, 100-240VAC (External)	1 @ up to 650w 100-240VAC	2 @ up to 650w 100-240VACC	2 @ up to 750w 100-240VAC	2 @ up to 750w 100-240VAC	
Power Consumption (max)	45.3w	648w	648w	744w	744w	
Temperature						
Operating	5° to 40°C	+10°C to +35°C (fluctuation not to exceed 10°C per hour)	+10°C to +35°C (fluctuation not to exceed 10°C per hour)	+10°C to +35°C (fluctuation not to exceed 10°C per hour)	+10°C to +35°C (fluctuation not to exceed 10°C per hour)	
Storage	0° to 70°C	-40°C to +70°C	-40°C to +70°C	-40°C to 70°C	-40°C to 70°C	
Cooling Requirement	N/A	2550 BTU/Hr	2550 BTU/Hr	2550 BTU/Hr	2550 BTU/Hr	
Humidity	20% - 90%	90%, non-condensing at 35°C (non-operating)	90%, non-condensing at 35°C (non-operating)	90%, non-condensing at 35°C (non-operating)	90%, non-condensing at 35°C (non-operating)	
Chassis	1U desktop (steel slim line case)	1U 19" rack mount	1U 19" rack mount	2U 19" rack mount	2U 19" rack mount	
Dimensions	Height: 55mm (2.17inches) Width: 335mm (9.84inches) Depth: 213mm (8.39inches)	Height: 43.2mm (1.70 inches) Width: 430mm (16.93 inches) Depth: 665.5mm (26.2 inches)	Height: 43.2mm (1.70 inches) Width: 430mm (16.93 inches) Depth: 665.5mm (26.2 inches)	Height: 87.30mm (3.44 inches) Width: 430mm (16.93 inches) Depth: 704.8mm (25.75 inches)	Height: 87.30mm (3.44 inches) Width: 430mm (16.93 inches) Depth: 704.8mm (25.75 inches)	
Shipment	Size: 13.19 x 12.6 x 12.8 inches Weight: 3.6 pounds	Size: 36 x 28 x 10 inches Weight: 55 pounds	Size: 36 x 28 x 10 inches Weight: 55 pounds	Size: 36 x 28 x 10 inches Weight: 71 pounds	Size: 36 x 28 x 10 inches Weight: 71 pounds	

Table 1: CounterACT Platform Specifications.
NOTE: All devices comply with FCC Part 15 of the FCC Rules, Class A; CANADA/USA: CSA 60950 and UL 60950 (Safety); ROHS.

About ForeScout

ForeScout Technologies is a leading provider of automated security control solutions for Global 1000 enterprises and government organizations. With ForeScout, organizations can accelerate productivity and connectivity by enabling people to access corporate network resources where, how and when needed without compromising security.

ForeScout's automated solutions for network access control, mobile security, threat prevention and endpoint compliance empower organizations to gain access agility while preempting risks and eliminating remediation costs. ForeScout CounterACT has been chosen by over 1300 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. The company delivers its solutions through its network of authorized partners worldwide. Learn more at http://www.forescout.com

Scan this code with your smartphone QR reader to get more info about Forescout CounterACT for NAC

ForeScout

10001 N. De Anza Blvd., Cupertino, CA 95014 Tel: +1 (408) 213-3191 info@forescout.com www.forescout.com