ForeScout CounterACT
Network Access Control

Highlights

Features

• **Easy to deploy.** No endpoint agents required. No infrastructure changes. Everything in a single appliance.

• **Rapid time to value.** Complete visibility to your entire network in hours or days.

• **100% 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 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.

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, and 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, and no hardware upgrades or reconfigurations. Everything is contained within a single appliance.

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 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.
“No matter what (BYOD) strategy is selected, the ability to detect when unmanaged devices are in use for business purposes will be required — and that requires NAC.”

Gartner, “NAC Strategies for Supporting BYOD Environments” 22 December 2011, Lawrence Orans and John Pescatore

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.](image-url)
## Features

<table>
<thead>
<tr>
<th>General</th>
<th>Visibility</th>
<th>IT infrastructure integration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ControlFabric™ technology</strong></td>
<td>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).</td>
<td>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).</td>
</tr>
<tr>
<td><strong>Out-of-band deployment</strong></td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
| **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. | 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 4+ |

### Endpoint

<table>
<thead>
<tr>
<th>Endpoint compliance</th>
<th>Threat detection</th>
<th>Rogue device detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Real-time mobile device control</strong></td>
<td><strong>Optional agent</strong></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>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 can be automatically installed when the device connects to the network and the user registers their identity.</td>
<td></td>
</tr>
</tbody>
</table>
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 to 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 (see Figure 3).

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.

Alert & Remediate
- Alert
  - Alert
  - LED/Email notification
- Restrict Access
  - Restrict Access
  - Deploy a Virtual Firewall around an infected or uncompliant device
- Move & Disable
  - Move & Disable
  - Deploy a Virtual Firewall around an infected or uncompliant device

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

Figure 3: Production LAN 802.1X & Non-802.1X
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.


<table>
<thead>
<tr>
<th>CT-R</th>
<th>CT-100</th>
<th>CT-1000</th>
<th>CT-2000</th>
<th>CT-4000</th>
<th>CT-10000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices¹</td>
<td>Up to 100</td>
<td>Up to 500</td>
<td>Up to 1000</td>
<td>Up to 2500</td>
<td>Up to 4000</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>100 Mbps</td>
<td>5– Mbps</td>
<td>1 Gbps</td>
<td>2 Gbps</td>
<td>Multi-Gbps</td>
</tr>
<tr>
<td>Network Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copper</td>
<td>4</td>
<td>4 – 8 (depending on specific model)</td>
<td>4 – 8 (depending on specific model)</td>
<td>4 – 8 (depending on specific model)</td>
<td>4 – 8 (depending on specific model)</td>
</tr>
<tr>
<td>Fiber</td>
<td>N/A</td>
<td>Available option (up to 2 total)</td>
<td>Available option (up to 4 total)</td>
<td>Available option (up to 4 total)</td>
<td>Available option (up to 4 total)</td>
</tr>
<tr>
<td>USB Ports</td>
<td>2, USB 2.0-compliant</td>
<td>4 back panel USB 2.0 + 1 front panel USB 1.1</td>
<td>4 back panel USB 2.0 + 1 front panel USB 1.1</td>
<td>4 back panel USB 2.0 + 1 front panel USB 1.1</td>
<td>4 back panel USB 2.0 + 1 front panel USB 1.1</td>
</tr>
<tr>
<td>VGA</td>
<td>1 (DB15)</td>
<td>1 (DB15)</td>
<td>1 (DB15)</td>
<td>1 (DB15)</td>
<td>1 (DB15)</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>N/A</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Hard Drives</td>
<td>1 HDD</td>
<td>3 HDD (RAID-1+HS)</td>
<td>3 HDD (RAID-1+HS)</td>
<td>3 HDD (RAID-1+HS)</td>
<td>3 HDD (RAID-1+HS)</td>
</tr>
<tr>
<td>Power Supply</td>
<td>1 @ up to 60W, 100-240VAC (External)</td>
<td>1 @ up to 650W, 100-240VACAC</td>
<td>2 @ up to 650W, 100-240VAC</td>
<td>2 @ up to 750W, 100-240VAC</td>
<td>2 @ up to 750W, 100-240VAC</td>
</tr>
<tr>
<td>Power Consumption (max)</td>
<td>45.3w</td>
<td>648w</td>
<td>648w</td>
<td>744w</td>
<td>744w</td>
</tr>
<tr>
<td>Temperature Operating</td>
<td>5° to 40°C</td>
<td>+10°C to +35°C (fluctuation not to exceed 10°C per hour)</td>
<td>+10°C to +35°C (fluctuation not to exceed 10°C per hour)</td>
<td>+10°C to +35°C (fluctuation not to exceed 10°C per hour)</td>
<td>+10°C to +35°C (fluctuation not to exceed 10°C per hour)</td>
</tr>
<tr>
<td>Storage</td>
<td>0° to 70°C</td>
<td>-40°C to +70°C</td>
<td>-40°C to +70°C</td>
<td>-40°C to +70°C</td>
<td>-40°C to +70°C</td>
</tr>
<tr>
<td>Cooling Requirement</td>
<td>N/A</td>
<td>2550 BTU/Hr</td>
<td>2550 BTU/Hr</td>
<td>2550 BTU/Hr</td>
<td>2550 BTU/Hr</td>
</tr>
<tr>
<td>Humidity</td>
<td>20% - 90%</td>
<td>90%, non-condensing at 35°C (non-operating)</td>
<td>90%, non-condensing at 35°C (non-operating)</td>
<td>90%, non-condensing at 35°C (non-operating)</td>
<td>90%, non-condensing at 35°C (non-operating)</td>
</tr>
<tr>
<td>Chassis</td>
<td>1U desktop (steel slim line case)</td>
<td>1U 19&quot; rack mount</td>
<td>1U 19&quot; rack mount</td>
<td>2U 19&quot; rack mount</td>
<td>2U 19&quot; rack mount</td>
</tr>
<tr>
<td>Dimensions</td>
<td>Height: 55mm (2.17&quot;)</td>
<td>Width: 335mm (9.84&quot;)</td>
<td>Depth: 213mm (8.39&quot;)</td>
<td>Height: 43.2mm (1.70&quot;)</td>
<td>Width: 430mm (16.93&quot;)</td>
</tr>
<tr>
<td>Shipment</td>
<td>Size: 13.19 x 12.6 x 12.8&quot;</td>
<td>Weight: 3.6 pounds</td>
<td>Size: 36 x 28 x 10&quot;</td>
<td>Weight: 55 pounds</td>
<td>Size: 36 x 28 x 10&quot;</td>
</tr>
</tbody>
</table>

¹Device count, as determined by CounterACT, is the sum of unique on-site connections made by network assets, connections made by off-site assets managed by CounterACT, 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.

Figure 4: 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.
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
• Mobile Security Module (integration with iOS and Android)

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 a ControlFabric Integration Module. The ControlFabric Integration Module currently supports the following standards-based integration mechanisms: Web Services API (available Q4 2013), SQL, LDAP, Syslog.

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 delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyber attacks. The company’s CounterACT appliance dynamically identifies and assesses all network users, endpoints and applications to provide complete visibility, intelligence and policy-based mitigation of security issues. ForeScout’s open ControlFabric technology 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, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com.