ForeScout

# CounterACT™

Network Access. Controlled.

Datasheet

# **CounterACT** Network Access Solutions.
# Securing the Global Enterprise.

## Highlights

### Network Visibility

- Out-of-band System
- Built-in Threat Detection
- High Degree of IT Infrastructure Integration
- Client and Clientless Operation

### Network Access Control & Compliance Management

- Powerful Policy Creation and Compliance Management
- Non-disruptive, Highly Automated Remediation

## Network Visibility

Industry analysts have called CounterACT one of the most advanced network sensors in the industry. It reveals who and what is connected to your network with pinpoint accuracy, and continuously monitors for changes.

## Feature/Benefits

**Out-of-Band.** Deploys outside of the switch and monitors network traffic as a mirror to the switch port.

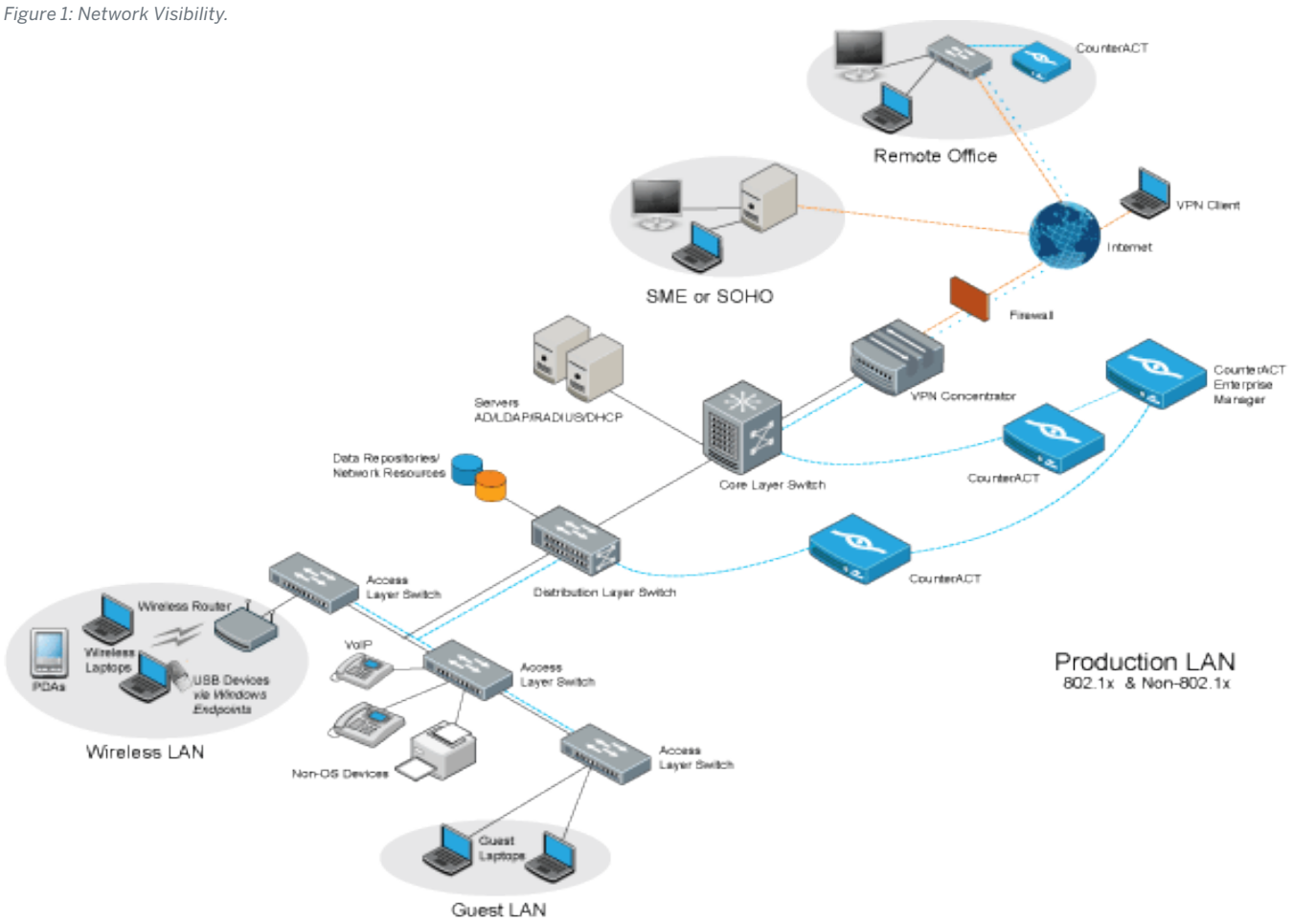
**Built-In Threat Detection.** Patented threat detection engine protects the network against zero-day self-propagating threats and helps to ensure that every device that attempts to attach to the network is free of viruses and malware.

**IT Infrastructure Integration.** Leverages and supports all existing IT infrastructure investments (see figure 1). Integrates with all major enterprise switches, both 802.1x and non-802.1x. Provides complete User-to-IP-to-Switch-to-Switch-Port mapping. Pinpoints location (IP→switch→location), user identity (LDAP→authentication) and endpoint system status (patch updates→AV, etc.). Leverages the switch's built-in security mechanism including VLAN assignment and switch post-blocking.

**Clientless Operation.** Detects and protects any device with an IP address without the need for a client residing on each endpoint. This includes the detection of devices like VoIP phones, printers, healthcare equipment, manufacturing machinery, etc.

**Secure Connector Dissolvable Client.** Persistent, multi-platform client delivers added peripheral protection for guest/contractor laptops and can be used to detect and disable portable data storage devices such as USB memory sticks on a per-policy basis.

*Figure 1: Network Visibility.*



## Network Access Control & Compliance Management

CounterACT has been lauded as the most effective, people-friendly and productivity-enabling NAC solution on the market. It automates network access and brings devices into security policy compliance without disrupting the user.

### Feature/Benefits

**Policy Creation Engine.** Offers flexibility to create the right network policies for each individual enterprise. For corporate policies, CounterACT offers out-of-the-box templates and a simple, easy-to-use wizard-based process that guides the IT staff through every step of policy creation. For regulatory standards-based audits (PCI, SOX, HIPAA, FISMA, etc.), CounterACT offers kits that help streamline the compliance audit and reporting process.

**Policy Compliance Engine.** Leverages IT infrastructural and CounterACT's built-in enforcement mechanisms to automate user and device compliance checks and to speed remediation or containment of out-of-compliant devices (see figure 2).

» ***Audit Mode***
Allows IT staff to simulate and fully understand the impact of a specific policy on devices and users before enforcements are turned on.

» ***Notifications (Alert/Inform)***
Notifying the user of policy violations is the first step towards remediation. Automated notifications and actions –such as trouble ticketing, emails, browser hijacks and redirects – significantly reduce costly help desk overhead.

» ***Access Control, Enforcement & Auto-Remediation.***
CounterACT limits non-compliant device access to specified resources, thus enabling users to remain productive while their device-compliance violations are addressed. For example, if a user device is found to have an out-of-date anti-virus (AV) definition file, it can be moved to a VLAN, allowing the user to access email and Internet while blocking the device from other critical resources. CounterACT can then work with existing services to provide guided remediation and/or cue the AV server to auto-update a specific device. Once remediation is complete and the device is found to be in compliance, complete access to the production network may be granted or restored.

CounterACT integrates with a number of remediation services, including patch management, anti-virus, anti-spyware, vulnerability management, and more. These third-party integrations allow CounterACT to orchestrate and automate the process of correcting policy violations. For example, if a device misses a critical patch, CounterACT detects the policy violation and automatically cues the patching engine (Microsoft WSUS or SMS) to update the specific system. Often this can be done without the user's involvement, retaining update report information for future security audits.

» ***Blocking***
CounterACT provides the ability to completely block the access of any device on the network. This can be accomplished by simply turning off the switch port or by leveraging CounterACT's built-in virtual firewall. The virtual firewall provides the ability to quarantine a device or a specific device port where malicious activity has been detected.

» ***Post Connection Monitoring.***
After initial connection is made, access control policies are enforced on an on-going basis. CounterACT continuously monitors the network for policy violations and/or the introduction of self-propagating threats from connected devices. This advanced capability ensures that the network is always safe and devices are always in compliance with established network security policies.

» ***Reporting.***
CounterACT has a fully integrated reporting engine that allows report-generation filters to be applied to both current and historical data. The reports help IT staff monitor and control device compliance and fulfill regulatory audit requirements.

*Figure 2: Tailored Enforcement Actions.*

| ALERT/INFORM & REMEDIATE | RESTRICTIVE ACCESS | MOVE AND DISABLE |
|---|---|---|
| Open Trouble Ticket | Deploy a Virtual Firewall around an infected or non-compliant device | Reassign device from production VLAN to a quarantine VLAN |
| Send Email | | |
| SNMP Traps | Reassign the device into a VLAN with restricted access to resources and services | Block access with 802.1X |
| Syslog | | Alter the end user's login credentials to restrict or completely block access |
| HTTP Browser Hijack | Update access lists on switches, firewalls and routers to restrict access | |
| Auditable End-User Acknowledgement | | Block access with device authentication |
| Self-Remediation | Automatically move device to a pre-configured guest network | Turn off physical switch port |
| SMS, PatchLink Integrated Remediation | | Terminate unauthorized applications |

## Deployments

CounterACT has the best track record in the industry for successful, fast and non-disruptive NAC deployments.

## Feature/Benefits:

**Integration.** CounterACT integrates with numerous third-party solutions, installs in a few hours and begins delivering real value within a day.

**Non-Disruptive Roll Outs.** CounterACT initial rollouts follow the same well-articulated, non-disruptive management process used to establish network access control and monitor/maintain compliance.

**Customer Driven, Global Deployment Proven.** ForeScout continues to respond to customer requirements, meeting the availability, scalability, and access control demands of the world's largest organizations in the financial, educational, federal, military, health and manufacturing sectors. CounterACT protects over 500 of the world's largest and most secure enterprises and military installations with global deployments spanning 37 countries.

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.

| | CT-R | CT-100 | CT-1000 | CT-2000 | CT-4000 |
|---|---|---|---|---|---|
| Concurrent Devices | 50 | 250 | 1000 | 2500 | 4000 |
| Bandwidth | 100 Mbps | 1 00 Mbps | 1 Gbps | 2 Gbps | Multi-Gbps |
| Network Ports<br>Copper<br>Fiber | 4<br>N/A | 6<br>Available option<br>(Up to 2 total) | 8<br>Available option<br>(Up to 4 total) | 8<br>Available option<br>(Up to 4 total) | 8<br>Available option<br>(Up to 4 total) |
| I/O Support | 1 serial port (DB9) | 1 serial port (DB9)<br>PS/2 keyboard<br>& mouse port | 1 serial port (RJ45)<br>PS/2 keyboard<br>& mouse port | 1 serial port (RJ45)<br>PS/2 keyboard<br>& mouse port | 1 serial port (RJ45)<br>PS/2 keyboard<br>& mouse port |
| USB Ports | 2, USB 2.0-compliant | 3, USB 2.0-compliant | 3, USB 2.0-compliant | 2, USB 2.0-compliant | 2, USB 2.0-compliant |
| VGA | 1 (DB15) | 1 (DB15) | 1 (DB15) | 1 (DB15) | 1 (DB15) |
| CD-ROM | N/A | 1 | 1 | 1 | 1 |
| Hard Drives | 1 HDD | 1 HDD | 2 HDD (RAID-1) | 2 HDD (RAID-1) | 2 HDD (RAID-1) |
| Power Supply | 1 @ up to 60W,<br>100-240VAC (External) | 1 @ up to 400W,<br>100-240VAC | 2 @ up to 650W,<br>100-240VAC | 2 @ up to 750W,<br>100-240VAC | 2 @ up to 750W,<br>100-240VAC |
| Temperature<br>Operating<br>Storage | 0°C to 45°C<br>(32°F ~ 113°C)<br>-20°C to 70°C<br>(-40°F ~ 158°C) | +10°C to +35°C<br>(fluctuation not to<br>exceed 10°C per hour)<br>-40°C to +70°C | -10°C to 35°C<br>(derated 0.5°C for every<br>1000 ft; 10,000 ft. max)<br>-40°C to 70°C | -10°C to 35°C<br>(derated 0.5°C for every<br>1000 ft; 10,000 ft. max)<br>-40°C to 70°C | -10°C to 35°C<br>(derated 0.5°C for every<br>1000 ft; 10,000 ft. max)<br>-40°C to 70°C |
| Humidity | 95% non-condensing<br>@ 35°C | 90% non-condensing<br>at 35°C | 90% non-condensing<br>at 30°C | 90% non-condensing<br>at 30°C | 90% non-condensing<br>at 30°C |
| Chassis | 1U desktop<br>(steel slim line case) | 1U 19" rack mount | 1U 19" rack mount | 2U 19" rack mount | 2U 19" rack mount |
| Dimensions | Height: 44mm<br>(1.73 inches)<br>Width: 210mm<br>(8.27 inches)<br>Depth: 150mm<br>(5.91 inches) | Height: 43.25mm<br>(1.703 inches)<br>Width: 430mm<br>(16.93 inches)<br>Depth: 692mm<br>(27.25 inches) | Height: 43.2mm<br>(1.7 inches)<br>Width: 430mm<br>(16.93 inches)<br>Depth: 654.4mm<br>(25.76 inches) | Height: 87.30mm<br>(3.44 inches)<br>Width: 430mm<br>(16.93 inches)<br>Depth: 704.8mm<br>(25.75 inches) | Height: 87.30mm<br>(3.44 inches)<br>Width: 430mm<br>(16.93 inches)<br>Depth: 704.8mm<br>(25.75 inches) |
| Shipment | Size: 14 x 12 x 15 inches<br>Weight: 8 pounds | Size: 10 x 28 x 36 inches<br>Weight: 37 pounds | Size: 10 x 28 x 36 inches<br>Weight: 54 pounds | Size: 10 x 28 x 36 inches<br>Weight: 68 pounds | Size: 10 x 28 x 36 inches<br>Weight: 70 pounds |
| Deployment Method | | | Layer 2 or Layer 3 | | |

10001 N. De Anza Boulevard, Suite 220 . Cupertino, CA 95014
Tel: 1.866.377.8771 . Fax: 1.408.213.2283 . www.forescout.com

© 2008 ForeScout Technologies, Inc. Products protected by US Patent #6,363,489, March 2002. All rights reserved. ForeScout Technologies, the ForeScout logo, CounterACT, CounterACT Edge and Active Response are trademarks of ForeScout Technologies, Inc. All other trademarks are the property of their respective owners. CT6.3-DS-V005-1108