



CounterACT™

NETWORK ACCESS. **CONTROLLED.**™



"CounterACT is easy to deploy because it is clientless, it interrogates every single device that touches the network, and it doesn't disrupt our business."

Kenneth Corriveau, CIO, Omnicom Media Group

CounterACT combines clientless network access control (NAC) and signatureless intrusion prevention to ensure all connecting devices are in compliance with network security policies and are free of worms and self-propagating malware. CounterACT seamlessly integrates into any network environment without requiring costly upgrades or infrastructure changes, and enables enterprises to tailor enforcement actions to match the level of policy violations, eliminating disruptions during device interrogation.

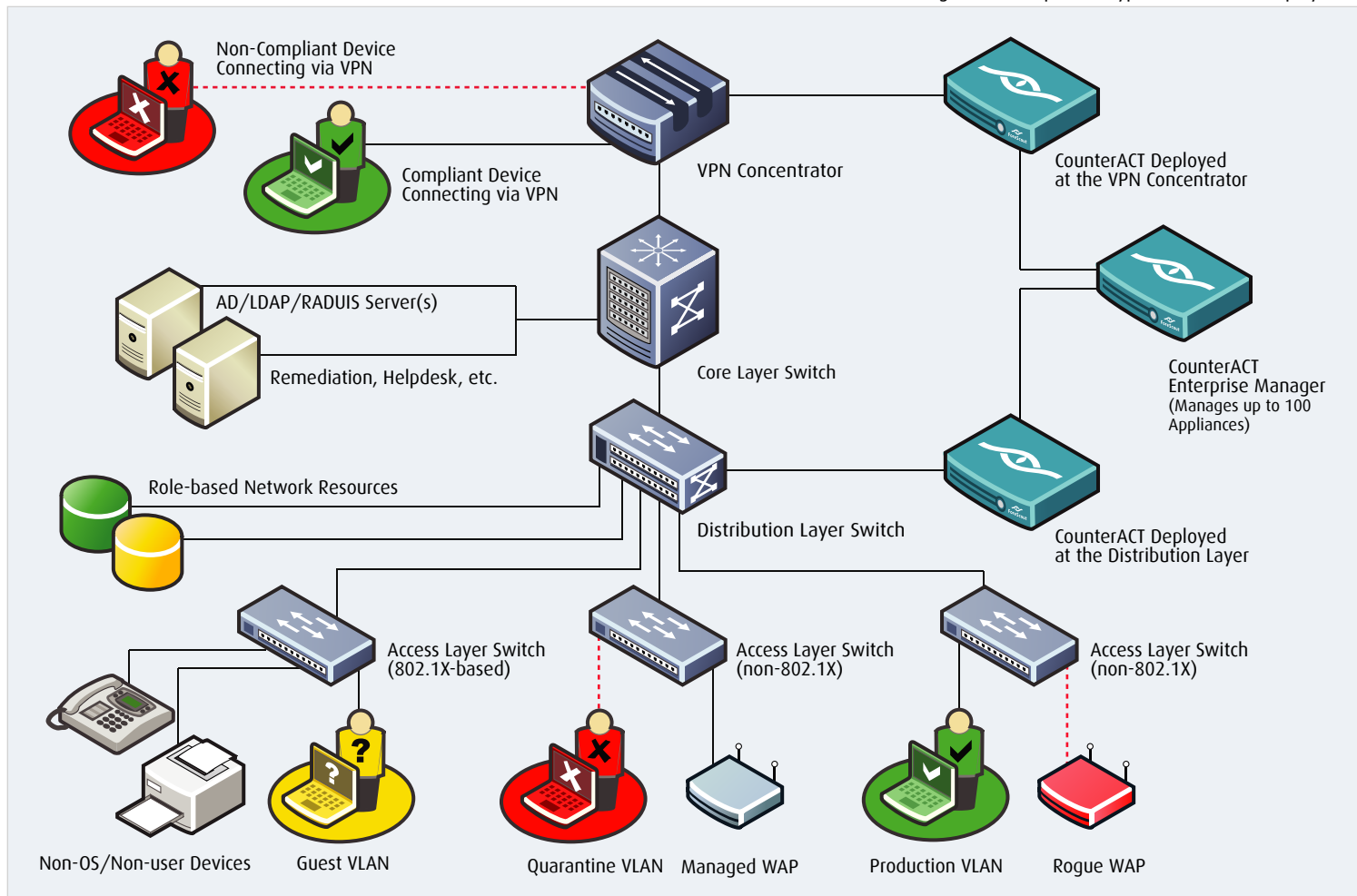
CounterACT solves the complex problem of enterprise-wide network policy enforcement across all devices connected to a network by ensuring that all endpoints are up-to-date with necessary patches, (i.e. Microsoft Security Updates or anti-virus definition files), and are free of unauthorized programs and malware. By detecting and instantly blocking critical threats (fast spreading worms and malware) upon connection, CounterACT allows users to connect to the network while their device is undergoing a deep interrogation, without disruptions or changes in end-user experience.

In addition to traditional security issues, today's enterprises are dealing with the influx of vulnerabilities introduced by contractors, guests and mobile/home employees who are able to bypass physical security and the traditional network security mechanisms designed to prevent non-compliant endpoints from accessing the network. CounterACT addresses this problem by enforcing network security policies across all managed and unmanaged network devices, including desktops and laptops as well as non-OS devices such as VoIP phones, handhelds and network printers, without the need for a software agent of any kind.

How It Works

Network administrators follow a step-by-step process to define security policies and associated enforcement actions that CounterACT will take when violations occur. Through a variety of detection mechanisms, CounterACT listens to the traffic as devices attempt to join the network, and determines whether the connecting endpoints are managed (employee) or unmanaged (guest, contractor or an unauthorized user). The appliance instantly scans the device for worms and malware, and blocks the device if it presents a threat. Based on the policy in place, CounterACT can immediately re-assign guest endpoints or non-OS devices into suitably designated VLANs. Managed devices are placed in their corresponding segment of the LAN and are granted role-based access to pre-determined network resources. CounterACT initiates an in-depth interrogation of the endpoint to determine its compliance status with defined network security policies, while the device gains access to the network. In case a device is found to be non-compliant, CounterACT takes appropriate action associated with the specific policy violation. CounterACT continues to monitor devices for compliance throughout their connection to the network.

Figure 1: Example of a typical CounterACT deployment



Endpoint X-Ray™

CounterACT features the most granular device interrogation engine in the industry. This includes both a quick inspection for self-propagating threats at point of connection and a deep interrogation of the device to ensure policy compliance. By tapping directly into the registry and file system of a device, CounterACT determines virtually everything about the state of an endpoint ranging from the presence of a desktop firewall, the state of OS patches, last update of anti-virus definitions or the presence of specific files or specific entries in the registry of the system. CounterACT ships with an extensive library of tests which are configured through an intuitive, user-friendly interface.

NAC FastPass™

CounterACT provides flexible access based upon the specific security requirements of each customer. With NAC FastPass, CounterACT does not require connecting devices to wait while they are being interrogated for compliance by eliminating the usual mandatory "quarantine upon connection" stage. At the point of connection, CounterACT ensures that devices are not infected with any form of self-propagating malware or worms with its integrated signatureless intrusion prevention module. Once confirmed that no active threats are present, it instantly allows users to gain access to network resources while the deep interrogation of the device for policy compliance is being completed. Alternatively, CounterACT can be configured to quarantine by default until all policy checks are complete, providing a flexible platform based upon specific security requirements.

Truly Clientless NAC

CounterACT does not require a persistent or downloaded software agent to be installed on any connecting devices in order to perform its in-depth interrogation for compliance with network policies. This ensures universal discovery of all endpoints connecting to the network including non-user devices such as network printers, rogue and legitimate wireless access points, VoIP phones and PDAs. Upon connection, CounterACT instantly determines the type of device, ensures it does not present a threat, and has the ability to place it in its appropriate logical location on the network.

Tailored Enforcement

ForeScout's NAC solution features a full spectrum of enforcement options to enable organizations to custom-fit responses to network policy violations. CounterACT enables tailored access for all devices and users to ensure all endpoints meet enterprise-wide security requirements. For example, low-risk violations, such as outdated

anti-virus definitions, can be dealt with by providing the end-user with self-remediation options while allowing limited access to the network and keeping the user productive while remediation takes place. Serious violations, such as unauthorized access to restricted network resources or worm infections, can be blocked from the network entirely; or in the case of a self-propagating threat, CounterACT can simply block the service or propagation port on the infected machine.

Non-Disruptive Deployment

CounterACT seamlessly integrates with any network environment and does not require any infrastructure changes or costly equipment upgrades. Typically spanned from a distribution layer switch for a highly scalable deployment, CounterACT is completely out-of-band and features downstream enforcement to control devices at the access layer. The non-inline deployment method eliminates latency and point-of-failure issues, without requiring costly infrastructure upgrades. CounterACT also enables policy deployment in monitor mode to allow administrators the ability to assess the effect of a policy on the network before activating enforcement. This ensures that network operations are not disrupted by lack of employee knowledge of new policy or a mis-configured policy. CounterACT also features a high-availability option to further reinforce its non-disruptive deployment capability.

Managing the Unmanaged

Because CounterACT does not require a software client, unmanaged devices (i.e. various types of network guests) are subject to the same policy enforcement as the managed endpoints. At the point of connection, CounterACT instantly determines whether the endpoint is an unknown device. Once the determination is made, CounterACT provides several options including automated assignment to a quarantine VLAN or engaging the end user and requesting permission to scan the device. If permission is granted (through the user re-logging into the device) CounterACT interrogates the device for policy compliance and automatically directs it to a pre-determined network segment with the appropriate access privileges.

Integrated Signatureless IPS

CounterACT features the only integrated signatureless intrusion prevention system that does not require manual updates of pattern files or definitions. By interacting with an attacking source, CounterACT detects and blocks devices infected with self-propagating malware or worms in real-time before they contaminate the network.

Figure 2: Tailored enforcement actions to policy violations.

ALERT AND INFORM	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		Block access with 802.1X
SNMP Traps	Reassign the device into a VLAN with restricted access to resources and services	Alter the end user's login credentials to restrict or completely block access
Syslog		Block access with device authentication
HTTP Browser Hijack		Turn off physical switch port
Auditable End-User Acknowledgement	Update access lists on switches, firewalls and routers to restrict access	Terminate unauthorized applications
Self-Remediation		Automatically move device to a pre-configured guest network
SMS, PatchLink Integrated Remediation		

Transparent Enforcement

CounterACT does not introduce any changes to end-user behavior. Compliant users are not aware that the NAC system is in place until a policy violation occurs, regardless of whether it is at the point of connection to the network or at any time during the network session. In case a violation occurs, CounterACT takes appropriate action to secure the network from a potential threat and quarantine the device if necessary, inform the end-user of a problem, present self-remediation options or notify the appropriate IT staff to mitigate the issue. End-users with compliant devices never know that CounterACT is deployed.

3rd Party Integration

CounterACT streamlines policy enforcement by integrating with a wide range of network devices and systems. ForeScout works with industry-leading vendors to provide integration with switches (e.g., Cisco), helpdesk systems (e.g., Remedy), patch management systems (e.g., PatchLink), firewalls (e.g., Check Point), VPN devices (e.g., Cisco VPN3K) and vulnerability assessment systems (e.g., Qualys). CounterACT also features remote monitoring and management of the appliances by third-party utilities through its extensive API. Custom integration options are available for most proprietary and legacy systems.

802.1X Integration

CounterACT works seamlessly in networks with full or partial 802.1X deployments. In an environment where 802.1X is present, ForeScout leverages the admission control aspect of this standard in conjunction with the other authentication methods employed by CounterACT. If 802.1X is not present, CounterACT can provide the same level of device authentication and work with the switching infrastructure to enforce admission control policies. CounterACT enhances this functionality by providing multiple admission criteria checks (user authentication, MAC address, etc) as well as tailored enforcement options which allow for both limited and full blocking of the non-compliant device.

VPN Enforcement

VPN users are subject to the same policies as the rest of the devices on the network. This ensures that all connecting devices comply with the security policies, regardless of whether the user is connecting with a company-issued device or personal home computer. CounterACT also features the same extensive enforcement options over the VPN as those available on the LAN.

About ForeScout

ForeScout's clientless network access control (NAC) solutions enable customers to gain complete control over network security without disrupting end-user productivity. ForeScout's flagship product, CounterACT, combines NAC and signature-less intrusion prevention in a single network appliance that interrogates and controls access of every device and seamlessly integrates with any existing IT infrastructure. ForeScout's NAC is completely transparent and enables enterprises to tailor enforcement to match the level of policy violations, eliminating disruptions during device interrogation. Today, Fortune 1000 corporations and government agencies have deployed ForeScout appliances globally to control access to their networks and resources, defend against hackers and self-propagating malware, and ensure business continuity.

	CT-R	CT-100	CT-1000	CT-2000
Concurrent Devices	50	250	1000	2500
Bandwidth	100 Mbps	100 Mbps	1 Gbps	1 Gbps
Network Ports	4	6	8	8
Fiber Ports	N/A	Available option (up to 2 total)	Available option (up to 4 total)	Available option (up to 4 total)
VLAN Support	Unlimited	Unlimited	Unlimited	Unlimited

Management and Reporting

Each CounterACT appliance comes with a Java-based management interface. When multiple CounterACTs are present (up to 100 appliances), these devices can be managed as one through a central CounterACT Enterprise Manager. Network administrators use the Enterprise Manager to define and distribute network policies throughout the LAN to all CounterACT appliances. Enterprise Manager collects security event data for intuitive reporting, and shares relevant security information gathered from individual appliances with the rest of the CounterACTs on the network.

Vulnerability Assessment

CounterACT provides proactive threat prevention by scanning the network for potential vulnerabilities and takes appropriate actions in response to discovered threats and policy violations. Once the security risks are identified, CounterACT provides one-click protection against threats through an intuitive user interface. Additionally, CounterACT integrates with leading third party vulnerability assessment systems.

Network Information Portal

CounterACT features a powerful search engine that reports on all security events such as policy violations and malware threats, and correlates all relevant event data with specific users and devices for granular forensic capabilities.

Additionally, the Network Information Portal features a flexible, user-friendly interface which provides the ability to search the captured information of all connected devices. The information gathered is a complete inventory of all connected network devices and the relevant events and activity associated with them.


ForeScout
NETWORK ACCESS. CONTROLLED.™

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