ForeScout CounterACT®

Gain real-time monitoring, control and policy-based remediation of managed, unmanaged and non-traditional devices.

ForeScout CounterACT® is an agentless security appliance that dynamically identifies and evaluates network endpoints and applications the instant they connect to your network. CounterACT quickly determines the user, owner and operating system, as well as device configuration, software, services, patch state and the presence of security agents. Next, it provides remediation, control and continuous monitoring of these devices.

CounterACT performs these actions on corporate-issued, personally owned bring-your-own-device (BYOD) endpoints and non-traditional devices—without requiring software agents or previous device knowledge. It deploys quickly into your existing environment and rarely requires infrastructure changes, upgrades or endpoint reconfiguration.

Why Customers Choose CounterACT

Heterogeneous support. Works with popular network infrastructure, operating systems, endpoint software and third-party security solutions.

Agentless. No endpoint agents required for authentication and network access control.

Exceptional visibility. See devices that other solutions can't:

- Desktops, laptops, servers, routers, smartphones and tablets
- Wired/wireless LANs and printers
- IoT devices (projectors, industrial controls, healthcare, manufacturing, POS devices and more)

Automated control. Automate an extensive range of actions:

- Grant, deny or limit network access based on device posture and security policies
- Quarantine and remediate malicious/high-risk endpoints

Rapid time to value. Deploy quickly to gain network visibility in hours.

Policy enforcement. Enforce network access control, endpoint compliance and mobile device security.

Productivity. Grant appropriate network access to persons and devices—without intrusive intervention or staff involvement.

Reliability. Improve network stability by identifying and removing rogue infrastructure.

Cost savings. Eliminate manual labor associated with opening/closing network ports for guest access.

Compliance. Automatically identify policy violations, remediate endpoint deficiencies and measure adherence to compliance mandates.

Network Security Risks and Blind Spots

Traditional network security has focused on blocking external attacks with firewalls and intrusion prevention systems. However, these security tools do nothing to protect your network against the deluge of insider threats that are increasingly causing security incidents and breaches. Threats include:

- **Visitors:** Guests and contractors bring their computers to your business. Both need Internet access, and contractors may require additional resources. If you give these visitors unlimited access, you expose your network to attack.
- **Wireless and mobile (BYOD) users:** Employees want to use their personally owned smartphones, tablets and notebooks on your network. Without adequate control, these devices can infect your network or be a source of data loss.
- **Internet of Things (IoT) devices:** Non-traditional devices continue to expand your attack surface by adding unmanaged devices such as IP-attached projectors, thermostats, lighting controls, security cameras and more.
- **Rogue devices:** Well-meaning employees can extend your network with inexpensive wiring hubs, departmental servers, routers and wireless access points that can cause network instability and vulnerability.
- **Malware and botnets:** Once your network is compromised, network-attached devices can be used in "pivot attacks" in which outsiders scan your network and steal your data.
- **Compliance:** Misconfigured endpoints and virtual machines may include improper settings or inappropriate software. What's more, they may be intentionally disabled by the user or by malware—deactivating security controls.

You can't protect what you can't see

Limited visibility results in security blind spots. Most endpoint security systems require up-to-date agents on each device to see and manage them. IT security managers typically have no visibility into the existence of unmanaged BYOD endpoints and the growing numbers of IoT devices that are showing up on networks every day.

How ForeScout CounterACT® Works

ForeScout CounterACT provides the unique ability to see IP-attached networked devices, control them and orchestrate information sharing and operation among disparate security tools. Here's how:

See The CounterACT appliance deploys out of band on your network. From there, it continuously monitors network traffic and integrates with your networking infrastructure to identify devices as soon as they access the network. CounterACT has a unique ability to see a vast array of IP-attached endpoints, users and applications. In fact, CounterACT's sophisticated technologies discover devices that are invisible to competitive products.

CounterACT doesn't stop there. Next, it accurately classifies endpoints on your network through passive and active interrogation techniques. CounterACT can identify the device type, location, user, and whether the device is a member of your domain, as well as other basic information. It also obtains detailed information about the security posture of the device by using administrative credentials to query corporate-owned devices.

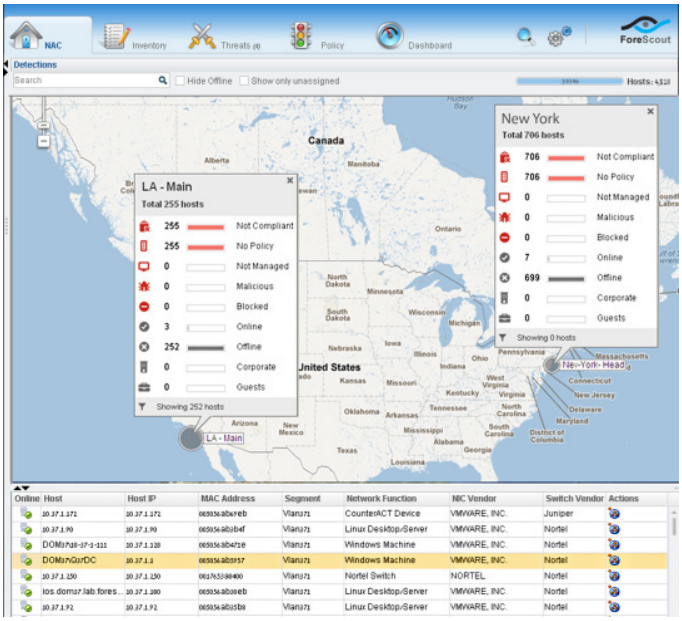

Figure 1: ForeScout CounterACT provides both high-level and detailed information about devices on your network.

Control. Once CounterACT discovers a security problem on an endpoint, its sophisticated policy manager can automatically execute a range of responses depending on the severity of the problem. Minor violations might result in a warning message sent to the end-user. Employees and contractors who bring their own devices can be redirected to an automated onboarding portal. Serious violations could result in actions such as blocking or quarantining the device, reinstallation of a security agent, re-starting of an agent or process, triggering the endpoint to fetch an operating system patch, or performing other remediation actions.

Analysts, Customers and Partners Choose CounterACT

- ForeScout has been named a Leader in the Gartner Network Access Control Magic Quadrant** for its ability to execute and completeness of vision (four consecutive reports)
- SC Magazine Best NAC Solution, June 2015
- SC Magazine Best Buy, October 2014

> We needed a NAC solution that was fast to deploy, without risk of business interruption. In addition, it needed to support our mixed Aruba® and Cisco® IT infrastructure. ForeScout CounterACT offered us all of this and much more—including impressive integration capabilities with our existing FireEye® and ArcSight® security tools. This is why we call CounterACT the 'Swiss Army knife' of our information security department, as it facilitates multiple, automated security checks and compliance controls in the most efficient way.
>
> **— Ali Kutluhan Aktaş, Head of Information Security/Risk Management at KKB**

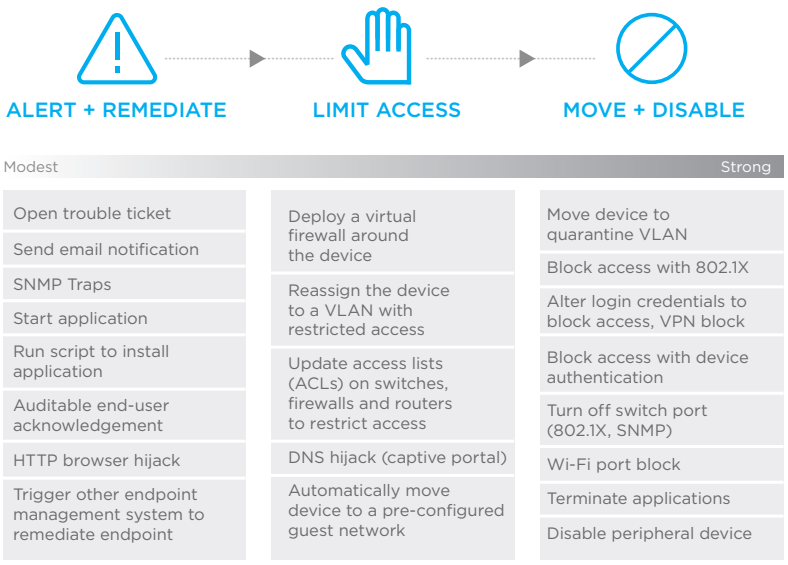

Figure 2: ForeScout CounterACT handles the full spectrum of control actions.

The Value of ControlFabric Architecture

ControlFabric Architecture is the glue that bonds ForeScout CounterACT capabilities with those of third-party network, security, mobility and IT management products. It tears down security management silos to:

- Unify system-wide security management
- Achieve greater operational efficiencies
- Accelerate threat response
- Boost your security return on investment
- Greatly improve your network security and compliance posture

Orchestrate. CounterACT leverages the ForeScout ControlFabric® Architecture to orchestrate information sharing and operation among the security and system management tools you already own. ControlFabric Architecture allows you to achieve this through custom integrations or plug-and-play software modules. Co-developed with ForeScout Technology Partners, ForeScout Base and Extended Modules bring the power of CounterACT to more than 70 leading network, security, mobility and IT management products* to:

- Share contextual insight with IT security and management systems
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

Features

General

Out-of-band deployment: Deploys out of band on your network without adding latency or a potential network failure point.

Visibility: The Asset Inventory feature 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).

Open interoperability: CounterACT works with popular switches, routers, VPNs, firewalls, endpoints, operating systems (Windows®, Linux, iOS, OS X and Android), patch management systems, antivirus systems, directories and ticketing systems—without infrastructure changes or equipment upgrades.

Reporting: A fully integrated reporting engine helps you monitor your level of policy compliance, fulfill regulatory audit requirements and produce real-time inventory reports.

Scalability: Proven in customer networks exceeding 1,000,000 endpoints. CounterACT appliances are available in a variety of sizes.

Certifications: CounterACT is military-grade with the following certifications:

- USMC Authority to Operate (ATO)
- U.S. Army CoN (Certificate of Networthiness)
- UC APL (Unified Capabilities Approved Product List)
- Common Criteria Evaluation Assurance Level (EAL) L4+

Non-disruptive: Deploy without impacting users or devices. When you want to move forward with automated control, you can do so gradually, starting with the most problematic locations and choosing appropriate enforcement actions.

Policy management: Create security policies that are right for your enterprise. Configuration and administration are fast and easy thanks to built-in policy templates, rules and reports.

ControlFabric Architecture: ControlFabric® Architecture offers extensive third-party vendor interoperability and an open integration architecture.

Endpoint

Agentless: Identify, classify, authenticate and control network access without an agent. Perform deep endpoint inspection without an agent as long as CounterACT has administrative credentials on the endpoint. In situations where CounterACT does not have administrative credentials, such as BYOD, deep inspection can be performed with the help of our optional SecureConnector agent, which is included with CounterACT at no additional charge.

Endpoint compliance: Ensure that endpoints on your network are compliant with your antivirus policy, properly patched and free of illegitimate software. CounterACT automatically identifies policy violations, remediates endpoint security deficiencies and measures adherence to regulatory mandates.

Threat detection: Continuous monitoring provides more timely and accurate insights than point-in-time vulnerability scans, as some devices may drop on and off the network.

Rogue device detection: Detect rogue infrastructure such as unauthorized switches and wireless access points. CounterACT can even detect devices without IP addresses, such as stealthy packet capture devices designed to steal sensitive information.

Access

Guest registration: Allow guests to access your network without compromising your internal network security. Several guest registration options let you tailor the guest admission process to your organization's needs.

Role-based access: CounterACT ensures that the right people with the right devices gain access to the right network resources.It leverages your existing directory where you assign roles to user identities.

Flexible control options: Unlike "old school" NAC products that employ heavy-handed controls and disrupt users, CounterACT provides a full spectrum of enforcement options that let you tailor the response to the situation. Resolve low-risk violations by sending the end-user a notice or automatically remediating the security problem; this allows the user to remain productive while remediation occurs (see Figure 2).

802.1X authentication, or not: Choose 802.1X or other authentication technologies such as LDAP, Active Directory®, RADIUS®, Oracle® and Sun. Hybrid mode lets you use multiple technologies concurrently, which speeds NAC deployment in large, diverse environments.

Built-in RADIUS: A built-in RADIUS server makes rollout of 802.1X easy. Or, leverage existing RADIUS servers by configuring CounterACT to operate as a RADIUS proxy.

Scalable Models

CounterACT has a proven track record in customer networks exceeding 1,000,000 endpoints. It's available in a range of physical and virtual appliance options to meet the specific needs of your business. Large networks that require multiple appliances can be centrally managed by CounterACT Enterprise Manager. Each CounterACT appliance includes a perpetual license for a specified number of network devices. For licensing policy details, visit www.forescout.com/licensing.

Centralized Management and Control

CounterACT Enterprise Manager can be deployed as a physical or virtual appliance to provide centralized management and control of CounterACT implementations. It oversees CounterACT activities and policies and collects information about identification, notification, restriction and remediation actions taken by CounterACT. This information is available for display and reporting at the CounterACT Console.

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

*As of January 2016.
**Gartner, Inc., "Magic Quadrant for Network Access Control", Lawrence Orans and Claudio Neiva, 10 December 2014. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Version 11_16