ForeScout®

Agentless Visibility

An unparalleled ability to see connected devices

Organizational Challenges

- Gain comprehensive visibility into known and unknown devices on the network
- Protect sensitive systems and data from unauthorized or non-compliant devices
- Minimize the human intervention required for secure network access control
- Comply with regulatory mandates
- Enable visitors and employees to use their own devices to easily and securely access the network
- Effectively manage BYOD, IoT and rogue devices

Technical Challenges

- Gain comprehensive visibility of devices—with or without security agents
- Discover, assess and monitor devices to detect anomalous behavior
- Identify and remediate devices that do not meet organizational policies and standards
- See wired or wireless devices as they connect to the network
- Confirm that encryption and data loss prevention agents are working
- Prevent unauthorized applications or peripheral devices on the network

If you can't see an unauthorized or non-compliant device on your network, you can't defend against it. ForeScout CounterACT® lets you see devices the instant they connect to your network, without requiring software agents or previous device knowledge. This unique, agentless approach makes a comprehensive range of devices visible—managed and unmanaged, corporate and personal, wired and wireless—even personally owned Bring Your Own Device (BYOD) systems, servers, switches, rogue hardware and Internet of Things (IoT) devices.

The Challenge

Conventional security solutions are only capable of detecting and assessing devices that are equipped with agents. This would be okay if all connecting devices had agents on board that would allow them to be managed by IT security. But the reality is that networks are being bombarded by BYOD and non-traditional devices connecting unseen and unknown—partners' and contractors' laptops, smartphones and tablets, IoT devices and hackers' rogue endpoints are all in the mix. With all the well-publicized network breaches constantly taking place, not to mention the billions of IoT devices that will soon be joining the billions already on networks worldwide, there is justifiable cause for concern among IT security professionals.

Another important issue that remains unresolved with most traditional endpoint management solutions is that many devices come and go on the network. Unless a solution offers real-time monitoring and continuous diagnostics rather than periodic scanning, unauthorized devices can do serious damage and be long gone before anyone even notices a problem.

The Solution

ForeScout CounterACT occupies a unique space among network security solutions because of its agentless approach to device visibility. A physical or virtual solution, it lets you instantly identify devices with IP addresses, including network infrastructure, BYOD systems, non-traditional IoT devices (handhelds, sensors and machines) and rogue endpoints (unauthorized switches, routers and wireless access points)—without requiring management agents or previous device knowledge.

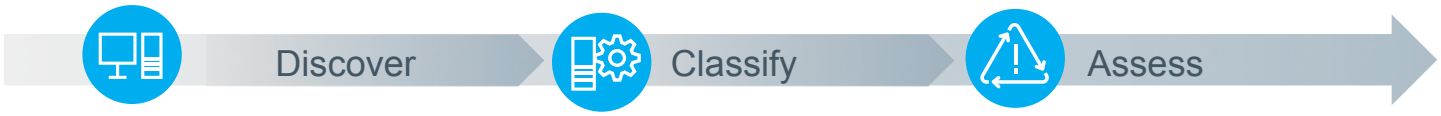
CounterACT's Breadth of Visibility

CounterACT sees devices in incredible detail, identifying and evaluating network devices and applications as well as determining the device user, owner, operating system, configuration, software, services, patch state and presence of security agents. CounterACT automatically classifies a growing number of IoT endpoints as it quickly clarifies and assesses the status and security posture of devices on your network. And it makes all of this possible with or without 802.1X infrastructure.

Equally important, CounterACT gains this in-depth visibility very quickly. In a recent evaluation by testing and research firm Miercom, CounterACT discovered and classified 100 percent of endpoints in all network environments tested. In addition, CounterACT fully discovered and classified 500 endpoints in less than five seconds.[1]

This is in stark contrast to traditional network access control solutions that typically offer few discovery and classification capabilities and are often limited to displaying a device's IP address.

Levels of Visibility

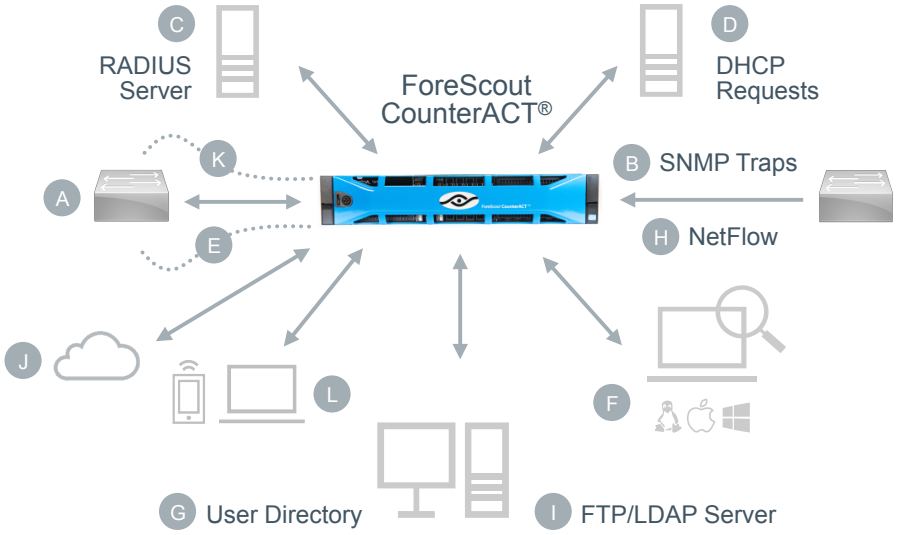


- Admission Event
  - Authentication event
  - SNMP traps
  - DHCP requests
  - Switch port change
  - MAC/IP
  - Network traffic
- Device Type and Ownership
  - Windows, Macintosh, Linux, mobile, network device, IoT, printer, VoIP and more
  - OS Type
  - Hardware properties such as NIC vendor (MAC address)
  - Switch information
  - Manageable (Domain/local/SecureConnector)
  - User information
  - Directory information
  - Device ownership (corporate, guest/contractor, BYOD)
  - Connection Type (LAN, WAN, Wireless, VPN)
  - IP assignment (DHCP, static)
  - Geographic location
- Compliance Policies
  - Authorized applications installed/running
  - Rogue applications installed/running
  - Antivirus agents status (installed/running) and database versions
  - Patch management agent status (installed/running)
  - P2P/IM clients installed/running
  - Number of devices on any port
  - Member of corporate domain
  - Network adapter (DeviceID, name, adapter type and speed)
  - Firewall status (installed/running)
  - Registry and configuration
  - Patch level

Multiple Methods

- **A** Poll switches, VPN concentrators, APs and controllers for list of devices that are connected
- **B** Receive SNMP traps from switches and controller
- **C** Monitor 802.1X requests to the built-in or external RADIUS server
- **D** Monitor DHCP requests to detect when a new host requests an IP address
- **E** Optionally monitor a network SPAN port to see network traffic such as HTTP traffic and banners
- **F** Run NMAP scan
- **G** Use credentials to run a scan on the endpoint
- **H** Receive NetFlow data
- **I** Import external MAC classification data or request LDAP data
- **J** Monitor virtual machines in public/private cloud
- **K** Classify devices using PoE with SNMP
- **L** Use optional agent

How ForeScout Sees Devices



CounterACT uses a wide array of methods, including proprietary processes, to discover and classify endpoints on the network without agents. It can also install a dissolvable agent on unmanaged devices to gain detailed device insights.

Extending Advanced Visibility and Control to Third-Party Tools

Based on ForeScout ControlFabric® technologies, CounterACT is easy to install because it usually doesn't require infrastructure changes or upgrades, endpoint agents or endpoint reconfiguration. CounterACT expands the capabilities—and meaning—of network access control. Several CounterACT capabilities raise the bar well above traditional NAC offerings:

- Agentless visibility lets you see unmanaged systems, including network infrastructure, BYOD and non-traditional IoT devices
- Continuous monitoring and assessment discovers new devices and those that drop on and off the network
- ForeScout ControlFabric Architecture and ForeScout Extended Modules share contextual information and extend the enforcement capabilities of CounterACT to a wide range of IT and security management products

Acronym Glossary:

Dynamic Host Configuration Protocol (DHCP)

File Transfer Protocol (FTP)

HyperText Transfer Protocol (HTTP)

Instant Messaging (IM)

Lightweight Directory Access Protocol (LDAP)

Local Area Network (LAN)

Media Access Control (MAC) address

Network Mapper (Nmap)

Point to Point (P2P)

Power over Ethernet (PoE)

Remote Authentication Dial-In User Service (RADIUS)

Simple Network Management Protocol (SNMP)

Switch Port Analyzer (SPAN)

Virtual Local Area Network (VLAN)

Virtual Private Network (VPN)

Voice over Internet Protocol (VoIP)

Wide Area Network (WAN)

Learn More

To learn more about how ForeScout offers the unique ability to see, devices the instant they connect to the network, control them and orchestrate information sharing and operation among disparate security tools, visit **www.ForeScout.com**.

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

[1] "An Independent Assessment of ForeScout CounterACT," Miercom, June 2016