Datasheet

ForeScout CounterACT®

Transforming Security Through Visibility™ Across the Extended Enterprise

Organizations continue to grapple with network security, not just on campus but in data centers and clouds. At the same time, their infrastructure is becoming increasingly complex due to the explosive growth and diversity of devices on their networks. A vast majority of the new devices are IoT and operational technology (OT) devices, and most can't accept security agents. To complicate matters, industrial networks and critical infrastructure networks are no longer isolated or air-gapped from IT networks. This increases business risks—especially when organizations don't have insight into what's connected to their networks.

Attackers are also taking advantage of these business trends. They have begun to focus on easy-to-target new attack surfaces. Once they get into your network, they move laterally, trying to gain access to sensitive information or cause business disruption.

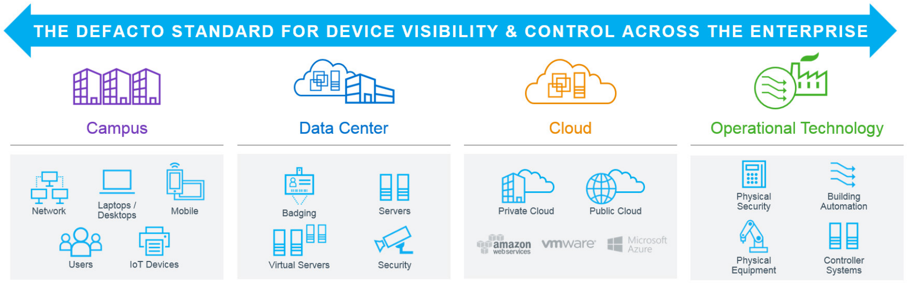
The Key Challenge: Limited Visibility

You can't secure what you can't see.™ What you need is comprehensive visibility across your extended enterprise—from campus and data center to cloud and operational technology networks. Without visibility of all connected devices, how can you truly secure the enterprise and implement important security measures? In other words, how can you effectively control access to your network, perform network segmentation, ensure device compliance, manage assets and respond to incidents?

Most security tools are great at sending alerts yet incapable of taking actions. The high volume of alerts—including many false positives—requires manual validation and remediation by resource-constrained security operations staff. You need a solution that reduces the attack surface and lets you automate remediation and incident response.

The ForeScout Platform

ForeScout CounterACT is the visbility platform that provides insight into virtually any connected device across your extended enterprise and gives you a single-pane-of-glass perspective. The platform deploys quickly into your existing environment and rarely requires infrastructure changes, upgrades or endpoint reconfiguration.



The ForeScout platform provides continuous visibility and control of every IP-connected device across your extended enterprise.

ForeScout's visibility platform provides See, Control and Orchestration capabilities. ForeScout pioneered an agentless approach to security which lets you discover devices in real time, then classify, assess and monitor these devices. Visibility extends to virtual devices such as VMs in private and public clouds. In addition, the platform provides agentless control and continuous monitoring across your heterogeneous environment. You can automatically trigger actions to notify, control and remediate.

Why Customers Choose CounterACT

- **Agentless:** No endpoint agents required to discover, classify and assess devices.
- **Heterogeneous support:** Works with leading network infrastructure vendors and third-party security solutions.
- **Real-time and continuous visibility:** See devices the instant they connect, ensuring accurate and up-to-date asset inventory.
- **Device intelligence for your extended enterprise:** See and assess devices that other solutions can't across campus, data center and clouds, IoT and OT.
- **802.1X and non-802.1X:** Flexible architecture to support a wide range of today's complex networks.
- **Automated control:** Automate an extensive range of actions through a robust policy engine.
- **Rapid time to value:** Easy to deploy and configure, enabling device visibility across the extended enterprise in hours.

> **"We have a geographically dispersed infrastructure and ForeScout delivered centralized, real-time visibility and control with regards to anything touching our network."**
>
> — Philip Egeberg, IT Security Manager at Daktronics

How ForeScout Helps You See More:

Passive discovery and profiling

- SNMP traps
- DHCP fingerprinting
- HTTP user-agent
- TCP fingerprinting
- NetFlow
- Poll Network Infrastructure via SNMP, CLI – get MAC/ARP tables and PoE details
- Monitor RADIUS requests
- MAC classification database
- vSphere and EC2 integration
- CMDB or other external data source

Active scanning techniques

- NMAP
- SMB
- RPC
- WMI
- SSH
- SNMP

Control Network Access:

Protect your campus with network access control

- Control access to enterprise resources based on device profiles and user roles
- Prevent infected or noncompliant devices from accessing the network and spreading malware
- Automatically enforce actions for identified situations without human involvement

Segment Your Network:

Enhance security and regulatory compliance with network segmentation.

- Gain visibility into what devices are talking to each other across campus, data center, cloud and OT
- Dynamically assign segments as the network and/or devices change
- Prevent select devices from communicating to other devices in different areas of the network

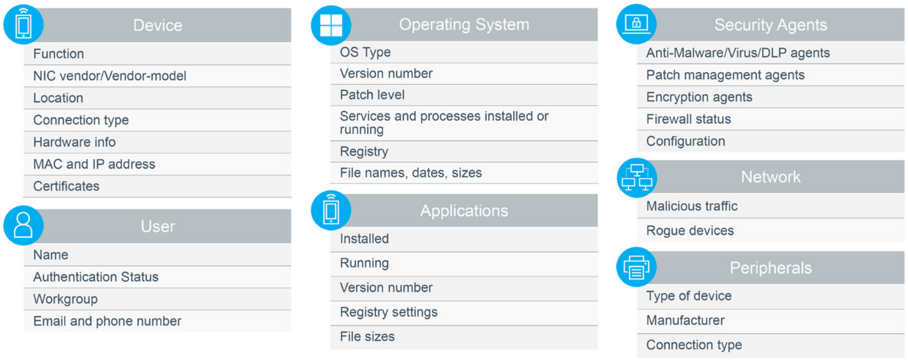
How ForeScout CounterACT Works

See. To know what's on your network, you must talk to your network. The ForeScout platform integrates with switches, wireless infrastructure, VPNs and cloud-based network management systems such as Cisco Meraki. In private and public clouds, we directly integrate with virtualization and cloud management infrastructure like VMware® and AWS®. Such multivendor integrations provide detailed visibility into virtually every conceivable type of device, whether IPv4 or IPv6, virtual machines or cloud instances, IoT or OT devices and more.

Industrial IoT and critical infrastructure systems create unique visibility challenges. Most of these devices can't support agents. They can be especially sensitive to active probing and scanning techniques, as they can cause system and business disruption. Our platform enables you to use passive-only discovery and profiling techniques that provide device visibility without introducing operational risk. It also can provide you with accurate and real-time inventory of OT devices.

With the ForeScout platform, you can discover and classify devices the instant they connect, and continuously monitor them afterwards—without requiring security agents or previous device knowledge. You classify your devices with the latest device classification profiles from ForeScout Research, whose analysts study more than three million devices in the ForeScout Device Cloud, thereby improving device classification efficacy and coverage.

You can quickly evaluate devices to determine users, system configuration, applications, presence of security agents and more (see graphic below). This knowledge lets you create context-aware security policies for compliance as well as network access and segmentation using ACLs, VLANS and virtual firewalls. You also assess the security posture of your devices, identifying out-of-date security software and operating systems, noncompliant configurations and more. CounterACT also detects suspicious or rogue devices.



Device
Function
NIC vendor/Vendor-model
Location
Connection type
Hardware info
MAC and IP address
Certificates

User
Name
Authentication Status
Workgroup
Email and phone number

Operating System
OS Type
Version number
Patch level
Services and processes installed or running
Registry
File names, dates, sizes

Applications
Installed
Running
Version number
Registry settings
File sizes

Security Agents
Anti-Malware/Virus/DLP agents
Patch management agents
Encryption agents
Firewall status
Configuration

Network
Malicious traffic
Rogue devices

Peripherals
Type of device
Manufacturer
Connection type

Examples of information that ForeScout can discover.

Control. ForeScout can automate policy-based access control and enforcement, allowing you to perform a range of actions to limit access to appropriate resources, find and fix endpoint security gaps and more. You can maintain and improve compliance with corporate policies or industry regulations. For example, CounterACT can remediate noncompliant endpoints by initiating antivirus software updates, triggering SCCM for patching endpoints, killing blacklisted apps, etc. Unlike other solutions that are limited to built-in remediation actions, you can run custom scripts on devices to let you keep up with changing needs. In addition, protecting your enterprise from risky BYOD devices belonging to employees and contractors becomes easy as you can place them on a guest network or route them to an automated onboarding portal for network access.

Depending upon your policies or the severity of the situation, you can enforce control by automating a vast range of network and host actions. For example, minor violations result in an alert, while serious violations might trigger an endpoint to be quarantined. Our Control capability puts a wide range of enforcement options into your hands, helping you close security gaps.

Enforce Device Compliance:

Improve device hygiene and compliance

- Achieve device compliance without the administrative burden or end user inconvenience of additional agents
- Control endpoint configurations according to organizational best-practice policies and regulatory mandates
- Continuously detect noncompliant devices and bring them back into compliance and/or automate poicy-based actions

Respond to Incidents:

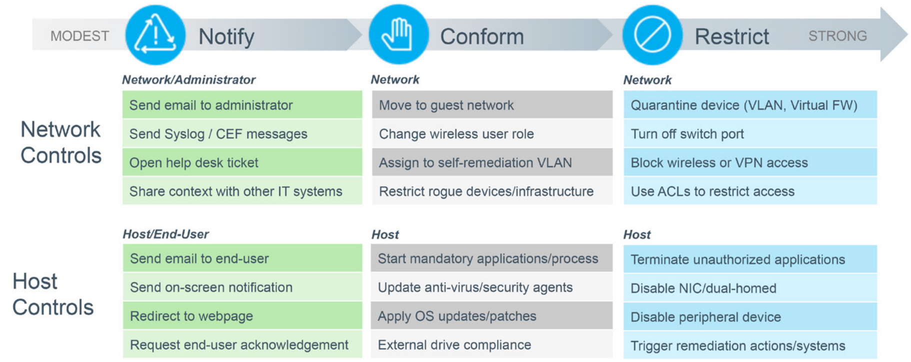
Accelerate incident response to mitigate threats and data breaches

- Identify and fix misconfigured, vulnerable or noncompliant devices to limit proliferation of threats
- Act on vulnerabilities, IOCs and other attributes provided by leading threat detection, VA and SIEM vendors
- Automate IT tasks natively or in concert with leading ITSM and security orchestration vendors to accelerate response

Manage Your Assets:

Improve security, IT efficiency and compliance with accurate ITAM

- Get an accurate picture of connected endpoints, infrastructure components and BYOD/IoT devices
- Receive rich contextual data for consumption by operations staff or third-party tools
- Orchestrate common, closed-loop processes with ITAM and other complementary IT services

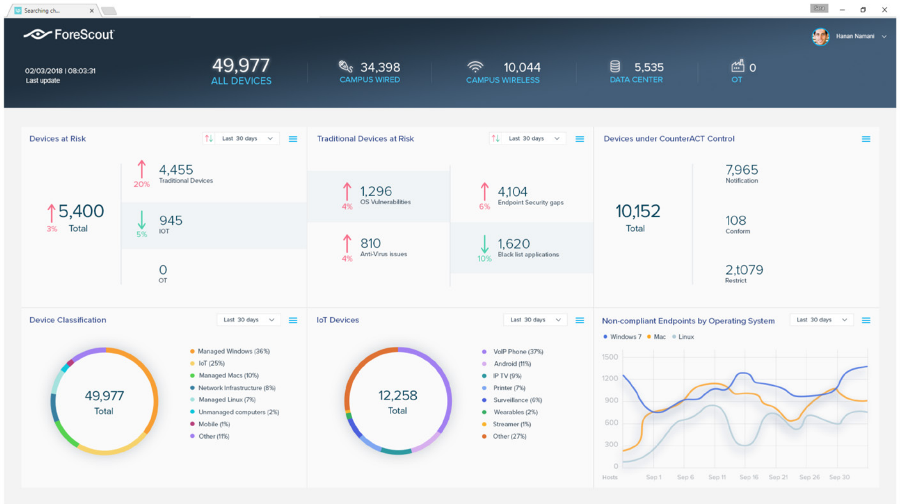


	Notify	Conform	Restrict
	Network/Administrator	*Network*	*Network*
Network Controls	Send email to administrator	Move to guest network	Quarantine device (VLAN, Virtual FW)
	Send Syslog / CEF messages	Change wireless user role	Turn off switch port
	Open help desk ticket	Assign to self-remediation VLAN	Block wireless or VPN access
	Share context with other IT systems	Restrict rogue devices/infrastructure	Use ACLs to restrict access
	Host/End-User	*Host*	*Host*
Host Controls	Send email to end-user	Start mandatory applications/process	Terminate unauthorized applications
	Send on-screen notification	Update anti-virus/security agents	Disable NIC/dual-homed
	Redirect to webpage	Apply OS updates/patches	Disable peripheral device
	Request end-user acknowledgement	External drive compliance	Trigger remediation actions/systems

Host and network control examples.

Orchestrate. ForeScout orchestrates information sharing and policy-based security enforcement operations with leading IT security and management products to automate security workflows and accelerate threat response without human intervention. ForeScout Extended Modules are available for NGFWs, ITSM, SIEM and more. They let you:

- Break down security silos and leverage your existing security investments
- Make your existing security tools and analysis richer and more context-aware, enabling a constant exchange of device hygiene, threat, behavior and compliance data
- Automate policy enforcement to accelerate response and substantially improve your security posture



Our Device Intelligence Dashboard is fully customizable to provide up-to-date device insight and compliance status to IT and SOC teams, your CIO/CISO and compliance officers.

Our orchestration capabilities allow you to leverage your existing investments in IT and management tools.

Centralized Management

CounterACT Enterprise Manager provides a single pane of glass to centrally manage and control multiple physical and/or virtual CounterACT appliances in large network environments. You gain overall visibility and control of devices as well as streamlined operations across your extended enterprise—from campus and data center to clouds and OT environments. You can manage your deployment easily with:

- A web dashboard that's customizable for varied personas, from security operations teams to IT executives, and for multiple use cases, from compliance management to incident response
- A fully integrated reporting engine that helps you monitor your level of policy compliance, help meet regulatory audit requirements and produce real-time inventory reports
- A user-friendly interface that allows you to easily view your devices by category and create and manage security policies for your extended enterprise
- Rapid analysis of policy flow and actions with a policy graph to fine-tune policies
- An asset inventory that provides a granular view of your networked devices such as users, classification, open ports, vulnerabilities and more—allowing you to take actions based on endpoint properties

ForeScout 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+
- DoD Information Network Approved Products List

Scale and Deployment

Manage large and heterogeneous deployments—with resiliency

- **Scalability:** Continuously monitor more than 2 million devices in a single deployment. Gain visibility and network controls across IPv4 and IPv6 devices.
- **Heterogeneous support:** Supports popular switches, routers, VPNs, firewalls, devices, operating systems (Windows, Linux, iOS, OS X, Android), patch management systems, antivirus systems, directories and ticketing systems—without infrastructure changes.
- **Nondisruptive:** Deploy without impacting users or devices. Introduce automated controls gradually, starting with appropriate actions for the most problematic locations.
- **Resiliency:** Configure automated failover or disaster recovery for service continuity—without requiring idle standby appliances.

Deploy with ease

- **Deployment options:** Deploy virtual or physical appliances across your centralized, distributed or hybrid environments.
- **Hybrid cloud support:** Gain consolidated visibility and control of your private and public clouds. Perform risk mitigation and response. Optimize resources and contain virtual machine sprawl.
- **Easy security policy creation:** Gain built-in policy templates, rules and reports. Drive consistent policies across multivendor and hybrid cloud environments.

The Forescout platform is easy to deploy and provides you with the scale you require.

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

[1] IT Central Station Review
[2] Predicts 2016: Security for the Internet of Things, December 9, 2015, Gartner Inc.
[3] IDC Business Value Analysis, December 2016