


FORESCOUT

Organizational Challenges

- Gain comprehensive visibility into known and unknown devices on the network
- Ensure resiliency and availability for operational technology teams
- Protect sensitive systems and data from unauthorized or non-compliant devices
- Effectively manage BYOD, IoT, OT and rogue devices
- Discover and secure cloud-based workloads provisioned by business units

Technical Challenges

- Gain comprehensive visibility of devices—with or without security agents
- Discover and profile IoT devices and OT systems without disrupting critical services
- Continuously monitor wired or wireless devices as they come and go from the network
- Detect anomalous behavior on any connected device
- Confirm that encryption and data loss prevention agents are working
- Prevent unauthorized applications or peripheral devices on the network
- Gain visibility of virtual instances and cloud resources

Agentless Visibility for the Extended Enterprise

An unparalleled ability to see and classify connected devices



If you can't see every device on your network, you can't defend against it. The ForeScout device visibility platform lets you see devices the instant they connect to your network, without requiring software agents or previous device knowledge. Our unique, agentless approach makes a comprehensive range of devices visible—managed and unmanaged, physical and virtual, corporate and personal, wired and wireless—even rogue hardware, IoT devices and operational technologies.

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.

The definition of the network itself has also changed. It's no longer a campus network supporting physical endpoints. Today's extended enterprise includes highly distributed networks with virtual instances in the data center, cloud workloads and growing list of operational technologies. These "devices" join and leave the extended enterprise with increased frequency, making it essential to monitor and assess all of them all the time. Given the expanded scope of this challenge, IT and security personnel need a heterogeneous visibility and control solution—one that provides a single-pane-of-glass-view across the extended enterprise, versus a collection of disjointed tools.

The Solution

The ForeScout device visibility platform occupies a unique space among network security solutions because of its agentless approach to device visibility that allows customers to discover up to 60 percent more devices than previously known.* 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 devices, switches, routers and wireless access points)—without requiring management agents or previous device knowledge.



ForeScout customers have increased the number of devices they know to be on their networks by an average of 24%.*

— IDC white paper, *The Business Value of Pervasive Device and Network Visibility and Control with ForeScout*

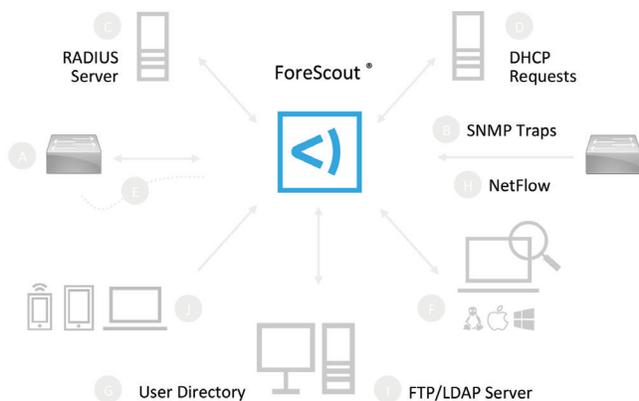
ForeScout's Breadth of Visibility

 <p>Who Are You?</p>	 <p>Who Owns Your Device?</p>	 <p>What Type of Device?</p>	 <p>Where/How Are You Connecting?</p>	 <p>What Is the Device Hygiene?</p>
<ul style="list-style-type: none"> • Employee • Partner • Contractor • Guest 	<ul style="list-style-type: none"> • Corporate • BYOD • Rogue 	<ul style="list-style-type: none"> • Windows, Mac • iOS, Android • Virtual Machine • Non-user devices, IoT, OT 	<ul style="list-style-type: none"> • Switch/Port/PoE • Wireless/Controller • VPN • IP, MAC • VLAN 	<ul style="list-style-type: none"> • Configuration • Software • Services • Patches • Security Agent

Agentless discovery and classification are essential first steps to knowing who and what is connected to the network. The ForeScout platform answers essential questions about connected devices and continuously monitors their compliance status to enforce policy-based access control.

The ForeScout platform 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. It automatically classifies a growing number of IoT devices and OT systems 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.

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 or MAC address and host name.

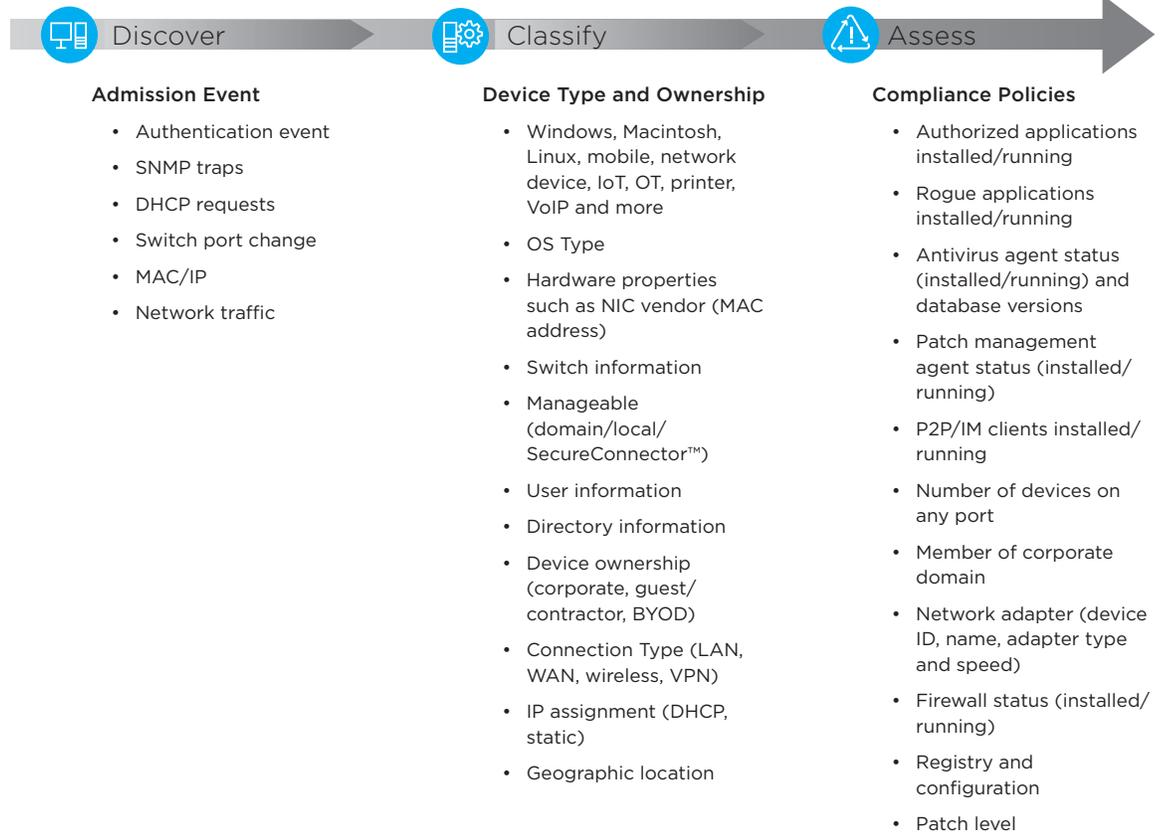


Multiple Methods

- 1 Poll switches, VPN concentrators, APs and controllers for list of devices that are connected
- 2 Receive SNMP traps from switches and controller
- 3 Monitor 802.1X requests to the built-in or external RADIUS server
- 4 Monitor DHCP requests to detect when a new host requests an IP address
- 5 Optionally monitor a network SPAN port to see network traffic such as HTTP traffic and banners
- 6 Run NMAP scan
- 7 Use credentials to run a scan on the endpoint
- 8 Receive NetFlow data
- 9 Import external MAC classification data or request LDAP data
- 10 Use optional agent

The ForeScout platform uses a wide variety passive discovery and active scanning techniques to identify IP-connected devices without requiring agents.

Levels of Visibility

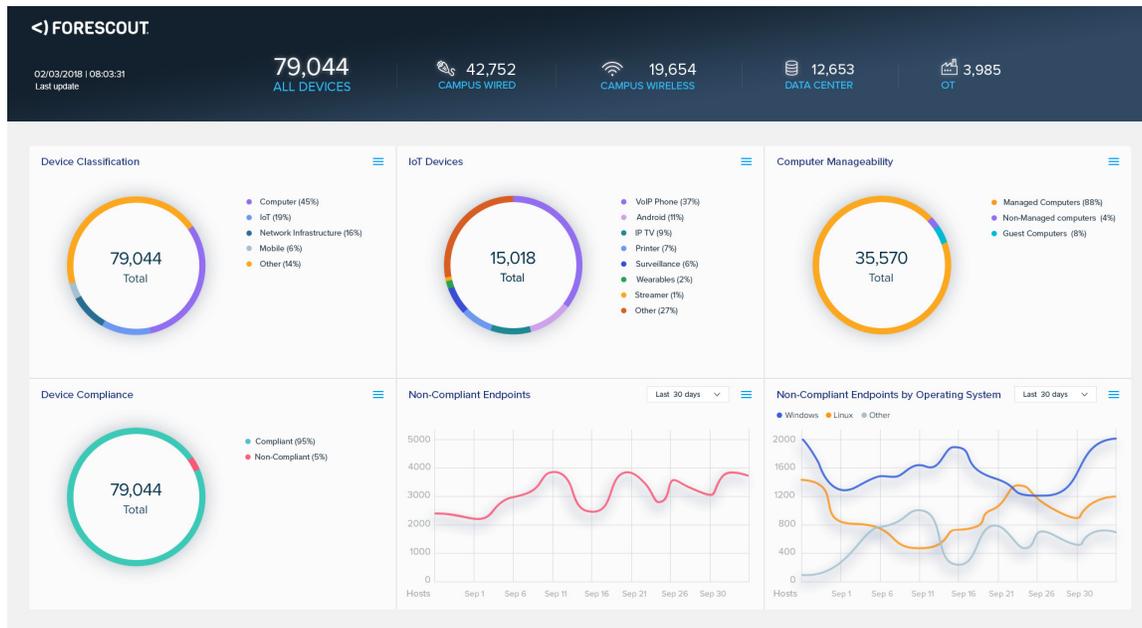


Accurate, in-depth visibility requires three core capabilities: discovery, classification and security posture assessment. The ForeScout device visibility platform provides exceptional detail in these categories.

The ForeScout Device Cloud – Auto-Classify New Devices

Auto-classifying devices is essential for creating security policies for network access, device compliance and network segmentation. However, the explosive growth in new device types and operating systems joining enterprise networks makes it difficult to identify and classify these devices—particularly IoT devices and OT systems that don't support software agents.

The ForeScout device visibility platform includes ForeScout Device Cloud, allowing you to benefit from crowdsourced device insight from a growing community of over 500 enterprise customers across more than 10 industries. ForeScout Research leverages intelligence from over 3 million real-world devices in our cloud, publishing these new profiles on a frequent basis to help improve classification efficacy and coverage in your environments.



ForeScout Device Intelligence Dashboard

Visualizing Device Intelligence

The ForeScout device visibility platform provides your security operations center (SOC) and incident response teams with a consolidated, up-to-date view of your device landscape along with classification, connection and compliance context. The ForeScout Device Intelligence Dashboard is easily customizable for other IT functions such as risk, compliance and executive reporting.

Support for Virtual and Cloud Environments

The ForeScout platform's heterogeneous support offers out-of-the-box integration with leading virtual switches, physical switching and wireless infrastructure. This ability to run in both physical and virtual environments helps you centrally manage and enforce consistent security policies across campus and cloud environments using the same solution and management console. ForeScout currently supports Amazon EC2 (Elastic Compute Cloud) and VMware vSphere, with additional cloud-based support coming soon.

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

* Based on actual ForeScout customer experience.
** As of June 30, 2018

© 2019 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 01_19**