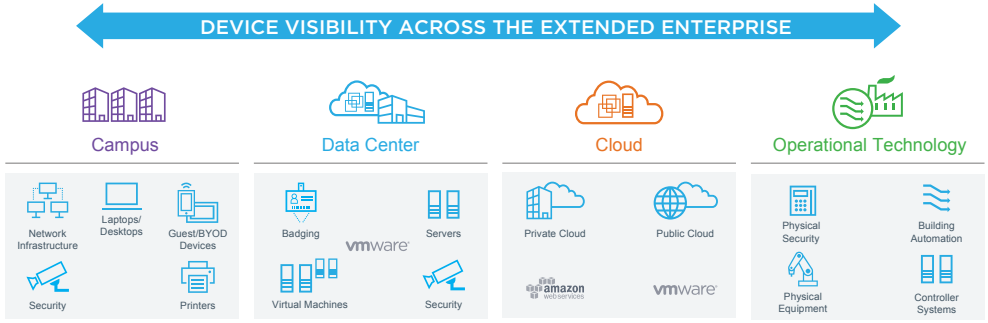
# ForeScout CounterACT® 8 What's New

Organizations are grappling with the explosive growth and diversity of devices on enterprise networks. An increasing majority of new devices are IoT and operational technology (OT) systems, most of which can't support software agents. As such, managing their security hygiene and compliance posture is challenging with traditional security methods.

As the convergence of IT and OT accelerates, networks with industrial and critical infrastructure systems are no longer air-gapped from IT networks. Hence, organizations face increased business risk as threats can jump between these domains. Bad actors take advantage of this IoT and OT attack surface to enter your network and move laterally to access sensitive information or cause business disruption.


By 2020, there will be 27 billion devices worldwide, 10 billion of which will connect to enterprise networks.[1]

Accurate device visibility is foundational to any security practice. The ForeScout device visibility platform provides insight into the diverse types of devices connected to your heterogeneous network—from campus and data center to cloud and operational technology networks. In other words, your extended enterprise. With one platform, you gain a consolidated view of traditional systems, mobile and IoT devices, virtual machines and cloud instances, and now, operational technology systems.




ForeScout visibility platform for the extended enterprise.

## CounterACT® 8 — Expanded Device Visibility Platform

CounterACT 8 raises the bar on device visibility and is a major step forward for organizations looking to keep pace with more than 5 billion[1] IP-connected devices on enterprise networks today. It includes foundational enhancements and innovative new capabilities to scale and deploy in the largest and most complex enterprise networks. New capabilities include:

- Better insight into some of the fastest-growing devices on enterprise networks, including IPv6-addressable systems and devices managed by cloud network controllers such as Cisco® Meraki
- Passive-only monitoring to inventory OT devices safely
- Cloud-based intelligence to auto-classify new devices
- IoT risk assessment to reduce your attack surface
- A customizable device intelligence dashboard to improve security operations and incident response
- Industry-leading scalability, enhanced deployment options and a new licensing model to manage up to 2 million devices in a single Enterprise Manager deployment

## Passive-only Monitoring — Inventory OT Devices Safely

Industrial IoT and critical infrastructure systems create unique visibility challenges. Most of these devices can't support agents, and they are especially sensitive to active probing and scanning techniques that can cause system and business disruption. To address these concerns, CounterACT 8 now allows you to use passive-only discovery and profiling techniques in such environments without actively scanning or interrogating connected devices.

ForeScout's passive discovery and profiling techniques glean information by inspecting network traffic, directly integrating with network infrastructure and monitoring various networking protocols. This enables you to gain device visibility without scanning or accessing connected devices, thereby minimize operational risk in OT environments. It removes traditional blind spots within your extended enterprise network and gives you an accurate and real-time inventory of these devices.

- **SNMP traps**
- **SPAN traffic**
- **NetFlow**
- **HTTP user-agent**
- **RADIUS requests**
- **DHCP fingerprinting**
- **MAC classification**
- **TCP fingerprinting**
- **Power over Ethernet**
- **Network infrastructure polling**

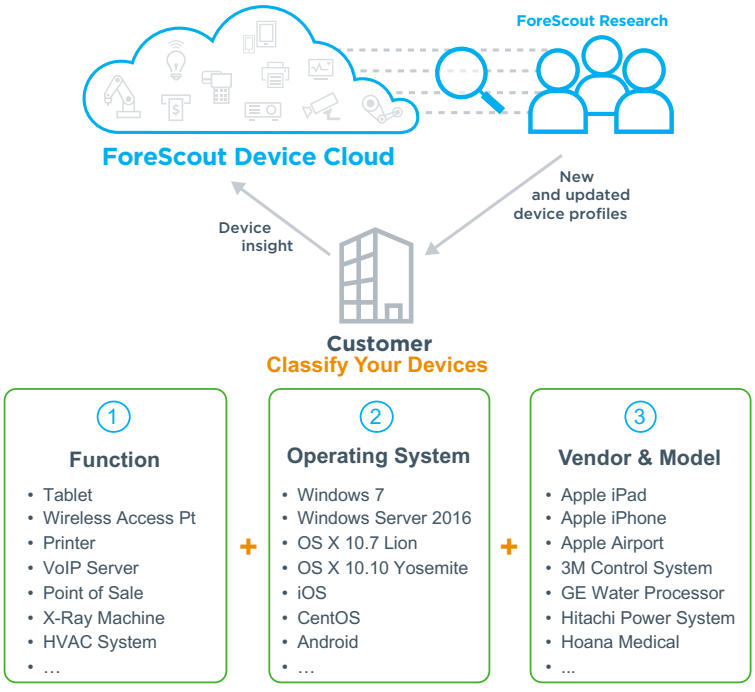
Passive monitoring for OT environments

## ForeScout Device Cloud — Auto-Classify New Devices

Discovering devices on your network is just part of the problem ForeScout addresses. Classification is the next important step to keep pace with new devices on your network. Auto-classifying devices is essential for creating security policies for network access, device compliance and network segmentation.

With CounterACT 8 and the ForeScout Device Cloud, you can benefit from crowd-sourced device insight from a growing community of over **500 enterprise customers** across more than 10 industries to auto-classify your devices. The ForeScout platform provides a rich taxonomy to auto-classify your devices by their type and function, operating system and version, and manufacturer and model.

ForeScout Research leverages intelligence from over 3 million real-world devices in our cloud to help improve classification efficacy and coverage in your environments. You can leverage new and updated auto-classification profiles published by ForeScout on a frequent basis. In addition, you can create custom classification policies to auto-classify devices unique to your environment.




Classify devices using the ForeScout platform.

## IoT Risk Assessment — Reduce Your Attack Surface

Attackers always look for the easiest way into your network. And, with IoT devices, weak and default credentials are the easiest attack surface to exploit. Botnets such as Mirai take advantage of these weak credentials and harvest millions of IoT devices to disrupt critical services. The ForeScout platform now allows you to assess and identify IoT devices with factory-default or weak credentials and automate policy actions to mitigate risk.

CounterACT 8 uses agentless assessment to identify IoT devices accessible via SSH, Telnet and SNMPv2 protocols. You can then use the ForeScout-provided IoT credentials library or your own custom credential library to identify devices using factory-default or commonly-used credentials and SNMP strings in IoT devices. For high-risk devices with weak credentials, you can use ForeScout policies to automate risk mitigation actions such as isolating or segmenting the devices until they are remediated.

**"By 2018, 66 percent of all networks will have an IoT security breach."**
–IDC 2017

**"81 percent of breaches involve the misuse of stolen, weak or default credentials."**
–Verizon 2017 Data Breach Investigations Report

## Device Intelligence Dashboard — Improve Security Operations and Incident Response

Security operations teams lack a comprehensive view into connected devices and their classification, connection and compliance context. This hampers incident response and compliance reporting. In addition to the CounterACT console, the ForeScout platform now includes a customizable web dashboard that provides a consolidated view of your device landscape and compliance across the extended enterprise. The dashboard works in concert with the Enterprise Manager and provides insight into the diverse types of devices connected to your heterogeneous network.


Consolidated view of device landscape for security operation centers.

Security operations centers (SOCs) can use the device intelligence dashboard for incident response. During a threat outbreak or security incident, SOC operators can quickly get the device context they need, including device classification, connection, compliance and risk status at their fingertips. This eliminates tedious manual processes to identify devices, where and how they are connected to the network, and their current security posture. It optimizes incident response processes and reduces your mean time to respond. You can also tailor device intelligence views for other IT functions such as compliance and risk reporting, asset management and executive reporting.

## Scalability, Deployment and Licensing — Scale to 2 Million Devices

With more than 5 billion[1] IP-connected devices on enterprise networks today, organizations need a scalable platform for visibility across their device landscape. The ForeScout platform provides a flexible management and deployment architecture with active customer deployments exceeding one million devices. CounterACT 8 raises the bar on scale, performance, deployment flexibility and license management to meet the stringent needs of large, complex enterprise environments.

- **Management scale.** To keep pace with device growth, CounterACT 8 provides twice the management capacity as before. You can now manage up to **2 million devices** in a single Enterprise Manager deployment across your extended enterprise.
- **Appliance scale.** Scale to **20,000 devices** in half the footprint to improve deployment density and optimize rack space. Additionally, monitor and analyze full **10Gbps** traffic with physical appliances.
- **Virtual deployments.** CounterACT 8 supports KVM as a third virtual appliance deployment option, in addition to VMware® and Hyper-V.
- **Intelligent IP distribution.** Automate IP distribution and management across a multi-appliance cluster to reduce administration overhead associated with allocating IP ranges to individual appliances.
- **ForeScout Flexx licensing.** This software-centric licensing model provides a centralized license pool with deployment flexibility and license portability to manage your devices across campus, data center, cloud and OT networks. The customer licensing portal enables you to optimize license administration, entitlement management and license compliance functions.
- **New physical appliances.** ForeScout 5100 series appliances offer higher capacity, support for ForeScout Flexx licensing and universal network connectivity options for agile and flexible deployments.


*For the latest ForeScout product announcements and updates, sign up for our RSS feed.*

[1] IDC, Worldwide Business Use Smartphone Forecast Update, 2015-2020; IDC, Worldwide Business Use Tablet Forecast Update, 2015-2020; IDC, Desk-Based, Notebook, Ultramobile and Mobile Phone Units (K) and Installed Base, by Country, 2014-2020; Gartner, Forecast: Internet of Things – Endpoints and Associated Services Worldwide, 2017; IDC, Worldwide and U.S. Server Forecast 2014-2018; IDC 2015 Server Virtualization and Cloud Multiclient Study

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


**Version 01_19**