FORESCOUT

IoT Security

See and control IoT devices that are invisible to traditional security products

> Nearly half (48%) of U.S. organizations using some sort of IoT network have experienced a recent security breach.[1]
>
> — Altman Vilandrie & Co.

During your last security audit, were you unable to identify what's on your network? Would you like to instantly discover IoT devices, place them on appropriate network segments or VLANs and be alerted if a printer, digital video recorder or HVAC device starts behaving like a PC?

The Challenge

Without a cutting-edge IoT security solution—one that begins with agentless visibility—IoT devices are invisible (and potentially unwanted) guests on your network. Connected video surveillance systems, projectors, smart copiers and printers, industrial controls and HVAC systems are common in most businesses today. These devices become more intelligent and valuable when networked, but when compromised, they can quickly become hackers' favorite hardware.

The "things" on this ever-expanding list of devices share one common trait: they include lightweight operating systems that don't support the software agents that traditional security tools require to discover and manage them.

While industry analysts debate the pace of IoT's phenomenal growth, enterprise IT staff have a more immediate concern: identifying the agentless devices that already reside on their networks. This critical lack of visibility insight is concerning in light of these facts:

- Nearly half (48%) of U.S. organizations using some sort of IoT network have experienced a recent security breach.[1]
- Less than 10% of new devices connecting to corporate networks will be manageable by traditional methods by 2020.[2]

A partial list of IoT applications and benefits

Facilities Management

Heating/cooling/lighting controls, fire prevention and building security. *Reduce costs through optimized resource utilization and preventive maintenance.*

Healthcare

Remote device monitoring, presence status and inventory management. *Accelerate care, improve diagnostic accuracy and lower medical/insurance costs.*

Public Sector

Digital governance, smart cities and connected infrastructure. *Empower constituents, improve public safety, boost traffic flow and reduce lighting costs.*

Retail

Connected inventory, CRM/ customer loyalty and inventory management systems. *Optimize inventory availability, improve customer insight and personalize marketing.*

Supply Chain

Real-time inventory management, tracking, shipping and logistics. *Enable proactive problem resolution and boost operational efficiency.*

- There will be 29 billion connected things in use worldwide by 2020.[3]
- By 2023, the average CIO will be responsible for more than 3 times the endpoints they managed in 2018.[4]

IoT innovation and corporate networks

IoT devices are designed to capture and share information or automate functions—making them perfect candidates for IP-based network connectivity. Unfortunately, since they have minimal system resources and often include proprietary operating systems, most are not capable of accommodating management agents, leaving them invisible to traditional security management systems. Nonetheless, IoT devices are showing up on wired and wireless enterprise networks with little regard as to how they will be secured or the risk they pose to the businesses and government agencies that have so aggressively embraced them.

The Forescout Solution

The Forescout platform provides absolute device visibility and automated control to effectively manage cyber, operational and compliance risks while increasing security operations productivity. Passive-only profiling provides device visibility into sensitive IoT, OT and critical infrastructure systems without impacting system uptime, introducing operational risk or disrupting critical business processes. Automated controls boost productivity, eliminate security management siloes and accelerate incident response.

Device Visibility: Agentless discovery and classification in real time plus continuous posture assessment equals accurate situational awareness.

- **Discover** every physical and virtual device across campus, data center, cloud and industrial environments
- **Classify** diverse IT, IoT and OT/ICS devices in real time
- **Assess** and continuously monitor compliance of all devices without requiring agents or active interrogation

Automated Control: Use accurate situational awareness to automate policy-based controls and orchestrate actions.

- **Conform** with policies, industry mandates and best practices such as network segmentation
- **Restrict**, block or quarantine noncompliant or compromised devices
- **Automate** endpoint, network and third-party control actions

Reduce the risk of business disruption

The Forescout 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 minimizing operational risk. It removes traditional blind spots within your extended enterprise network and gives you an accurate, real-time inventory of these devices.

Increase security operations productivity

Discovering IoT devices on your network is just one of the important benefits of the Forescout platform. Classification is another. Auto-classifying IoT devices is essential for creating security policies for network access, device compliance and network segmentation. The Forescout platform:

- Provides a rich taxonomy to auto-classify devices by their type and function, operating system and version, and manufacturer and model
- Includes deep packet inspection of over 100 IT and OT protocols to power auto-classification of medical, industrial, building automation and IoT devices
- Improves classification efficacy, velocity and coverage using crowd-sourced device insights from more than 8 million devices in the Forescout Device Cloud

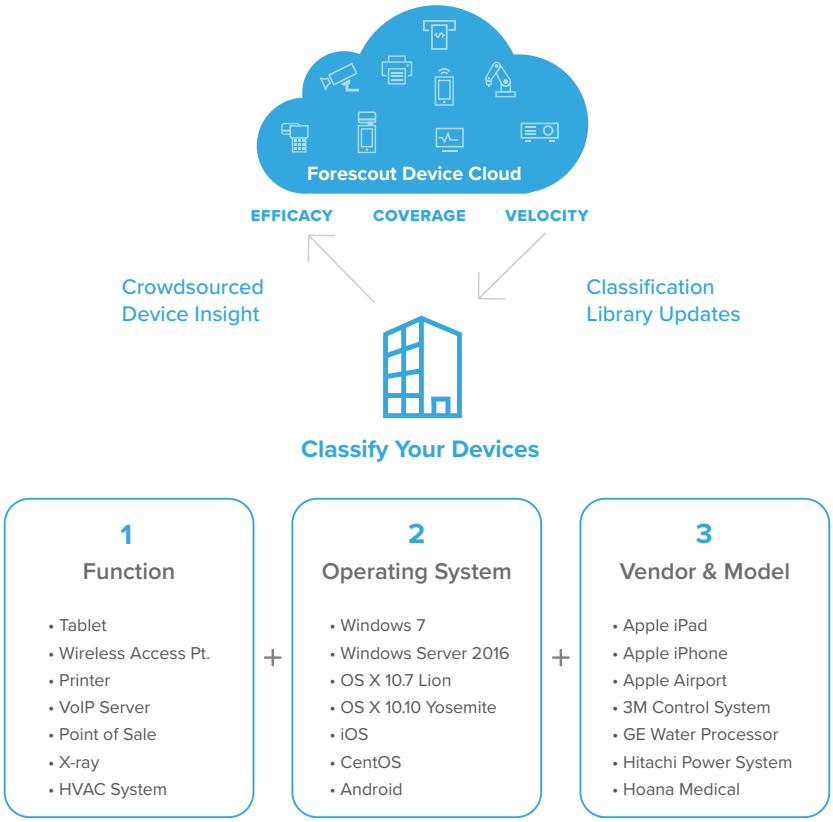


Figure 1: Auto-classify IoT and OT devices with the Forescout platform.

Assess and mitigate IoT risks

With IoT devices, weak and default credentials are easy attack surfaces 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 can:

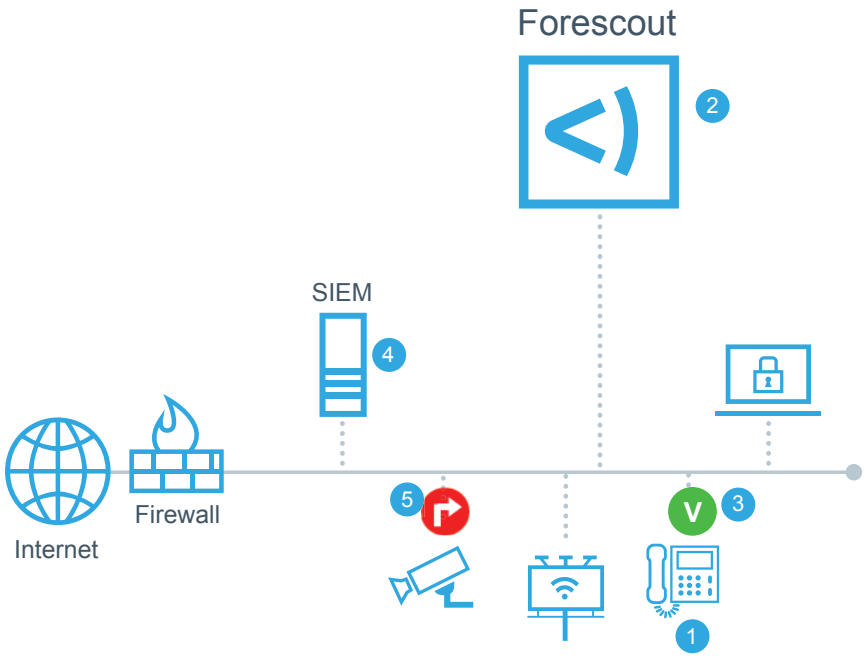
- Assess and identify IoT devices with factory-default or weak credentials
- Automate policy actions to mitigate risk and enforce strong passwords
- Isolate devices until they are remediated

In addition, this device visibility and control platform provides:

- Patent-pending rogue device detection to stop impersonators that use MAC address spoofing techniques
- Continuous monitoring to detect spoofing across wired and wireless networks and identify victim and impersonator devices
- Policy-based controls to block spoofing attempts and prevent malicious access

Use eyeExtend to orchestrate IoT security and enforce compliance

Forescout eyeExtend products orchestrate the visibility, continuous monitoring and control capabilities of the Forescout platform with third-party security tools to increase IoT security. Here's one example of the platform's orchestration capabilities:



Here's how:

1. IoT device connects to the network.
2. Forescout discovers the device, determines its type and ownership.
3. Forescout places corporate-owned devices in appropriate VLANs or applies ACLs to limit access. If not corporate-owned, device is denied access.
4. Forescout monitors anomalous behavior on IoT segment leveraging its eyeExtend integration and a SIEM.
5. Suspicious IoT device is moved to a restricted VLAN segment for further analysis.

Figure 2: How the Forescout platform applies policy-based network segmentation, continuous monitoring and response to IoT devices. Note: enforcement can also be provided via next-generation firewalls using Forescout eyeExtend products. For more detail, read our Network Segmentation Solution Brief.

The Forescout platform provides absolute device visibility and automated control to effectively manage cyber, operational and compliance risks while increasing security operations productivity.

***Notes**

1. Altman Vilandrie & Co. https://enterpriseiotinsights.com/20170602/security/20170602securitystudy-iot-security-breaches-tag23
2. Forescout analysis
3. ABI Research
4. Gartner Top Strategic IoT Trends and Technologies Through 2023, September, 2018

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at Forescout.com