FORESCOUT

Business Challenges

- Securely embrace IoT innovations
- Ensure resiliency and availability for operational technology teams
- Provide security and compliance for enterprise IT teams
- Defend intellectual property and sensitive data
- Comply with regulatory mandates pertaining to your company or industry
- Leverage existing network security investments

Technical Challenges

- Discover unknown devices on the network in real time that do not include management agents
- Validate device identities
- Classify devices and determine their owners
- Discover and fix IoT devices with weak or factory-default passwords
- Continuously assess and monitor devices to determine anomalous behavior
- Prevent infected or non-compliant devices from spreading malware across the network

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

IoT Security

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

During your last security audit, were you unable to identify what's on your network? Does OT (operational technology) share the same network as your information technology? Would you like to instantly discover IoT devices, place them on appropriate network segments or VLANs and know if a printer 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. 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 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 of U.S. organizations using some sort of IoT network (48%) have experienced a recent security breach.[1]
- Less than 10 percent of new devices connecting to corporate networks will be manageable by traditional methods by 2020.[2]
- There will be 29 billion connected things in use worldwide by 2020.[3]

Why OT air gaps = IT security chasms

Not long ago, operational technology (OT) such as manufacturing lines, environmental controls and industrial control systems and sensors used in critical infrastructure were isolated by air-gapped networks. These command-and-control-type networks often ran legacy operating systems and proprietary network technologies that typically sacrificed device security in favor of system performance and availability. This approach, often called "security through obscurity," no longer works.

1 Altman Vilandrie & Co. https://enterpriseiotinsights.com/20170602/security/20170602securitystudy-iot-security-breaches-tag23
2 ForeScout analysis
3 ABI Research, 2017

FORESCOUT

Here's 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.

Oil and Gas
Connected infrastructure from exploration and refining to distribution.
Reduce operating/distribution costs, optimize processes and enable proactive maintenance.

Manufacturing
Smart sensors, inventory management and digital control systems.
Respond faster to demand fluctuations, automate processes and optimize efficiency.

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.

Utilities
Connected meters and smart grids.
Automate meter reading and improve usage/production efficiencies.

The economic advantages of IP connectivity quickly obliterated security air gaps as operational networks connected to external-facing IT networks, resulting in major security challenges. Today, vulnerable devices that were formerly on air-gapped networks now reside on many corporate networks, and since they lack management agents, security teams are unable to inventory them, let alone secure them.

IoT innovation and corporate networks

The vast majority of IoT devices today are used by businesses, not consumers. In fact, business/manufacturing, healthcare and retail account for nearly 79 percent of networked devices today.[4] These 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, they are not capable of accommodating management agents, leaving them invisible to traditional security management systems. Nonetheless, they 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 majority of new devices connecting to networks today are unmanaged IoT endpoints. ForeScout helps organizations ensure IoT device security in three distinct ways:

See The ForeScout platform offers the unique ability to see devices the instant they connect to your network, without requiring software agents. We take this a step further by classifying devices and validating their identities. This key capability is essential for improving your endpoint compliance posture as well as defining your IoT security and enforcement policies. In addition, the ForeScout platform continuously monitors IoT devices, ports and connections.

Control Once you understand each IoT device on your network, its owner and purpose, The ForeScout platform enables a broad range of network access controls. You can restrict access to a non-compliant device, block Internet access, quarantine any device based upon anomalous behavior and/or notify its owner of a security concern. And should you choose to isolate various devices to a various network segment or VLAN, the ForeScout platform simplifies this process.

Orchestrate Without the ForeScout platform, third-party management solutions are blind to unmanaged and IoT endpoints. ForeScout extends our platform's agentless visibility and control capabilities to leading network, security, mobility and IT management products via more than 20 ForeScout Extended Modules.* This unique ability to orchestrate multivendor security allows you to:

- Share context and control intelligence among systems to enforce unified network security policy
- Reduce vulnerability windows by automating system-wide threat response
- Gain higher return on investment from your existing security tools while saving time through workflow automation

4 Intel Guide to IoT Infographic

FORESCOUT

Passive Monitoring Techniques

Passive-only monitoring techniques allow non-disruptive discovery of critical IoT and OT devices on the network without impacting performance or reliability. The ForeScout platform's passive techniques include:

- SNMP traps
- DHCP fingerprinting
- SPAN traffic
- HTTP user-agent
- TCP fingerprinting
- NetFlow
- Network infrastructure polling
- Power over Ethernet
- Radius requests
- MAC classification
- VMware® vSphere®
- Amazon® EC2®
- CMDB or external sources

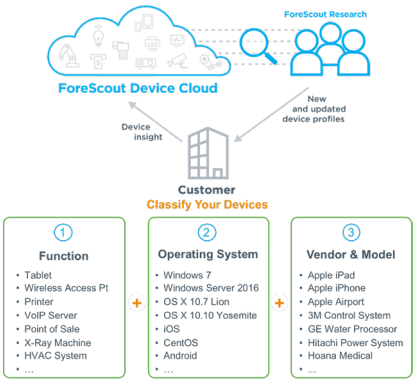
Passive-Only Monitoring — Inventory OT Devices Safely

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, the ForeScout platform 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 minimizing operational risk in OT environments. It removes traditional blind spots within your extended enterprise network and gives you an accurate, real-time inventory of these devices.

ForeScout Device Cloud — Auto-Classify New Devices

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



Classify IoT and OT devices using the ForeScout platform

The ForeScout platform includes ForeScout Device Cloud, allowing you to 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 millions of 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.

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

IoT Risk Assessment — Reduce Your Attack Surface

With IoT devices, weak and default credentials are an easy 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 allows you to assess and identify IoT devices with factory-default or weak credentials and automate policy actions to mitigate risk.

You can 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.

> Today we know what's on our network—including IoT devices. The ForeScout platform classifies the device and slips it onto the appropriate VLAN segment."
>
> — Ken Compres, Sr. Network Security Engineer/CSO, Hillsborough Community College

IoT Use Cases: Separating Facts from Fiction

Given the extraordinary value and broad-based adoption of IoT, many security vendors are quick to proclaim IoT security capabilities. While claims are plentiful, real use cases are much harder to find. Here is a real-world use case that shows how ForeScout Extended Modules orchestrate the visibility, continuous monitoring and control capabilities of the ForeScout platform with third-party security tools to increase IoT security.

The ForeScout platform can automatically detect and classify IoT devices such IP security cameras, conference room displays and VoIP phones, then place them on appropriate network segments. It continuously monitors IoT devices to ensure they behave as expected and can share data with security information and event monitoring (SIEM) solutions. This same scenario is equally relevant to any number of corporate-connected devices such as HVAC/lighting controls.

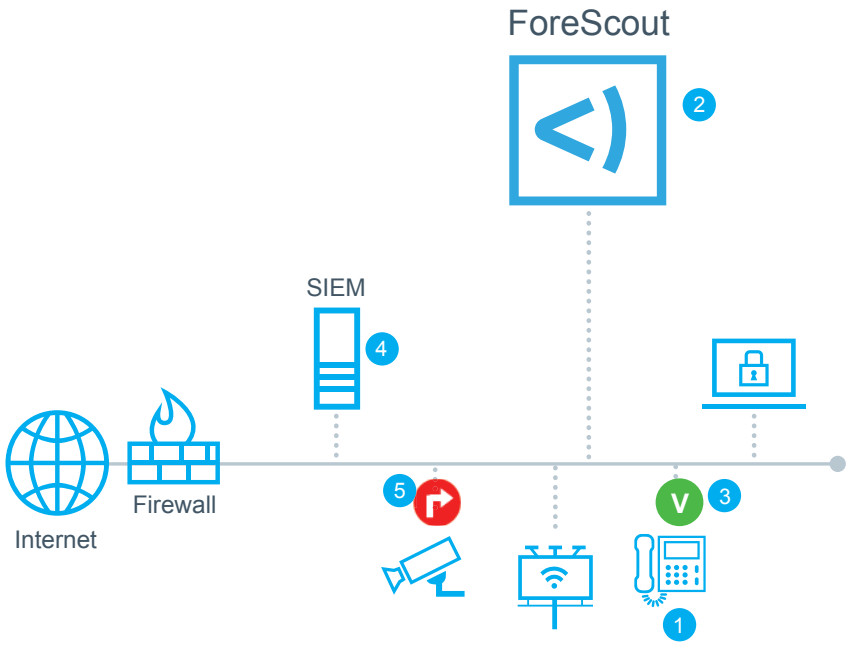


Figure 1: How the ForeScout platform applies policy-based network segmentation, monitoring and response to IoT devices. For more details about dynamic segmentation, read our Network Segmentation Solution Brief.

1. IoT device connects to the network.
2. ForeScout detects and classifies device as a printer.
3. Compromised printer attempts to access corporate file server.
4. Third-party Security Information and Event Management (SIEM) solution detects anomalous behavior.
5. ForeScout blocks the compromised printer from the network and quarantines it, allowing IT to safely remove the device from the network and perform forensic analysis.

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

*As of December 31, 2017