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 that do not include management agents
- Validate device identities
- Classify devices and determine their owners
- Assess and monitor devices to determine anomalous behavior
- Prevent infected or non-compliant devices from spreading malware across the network

> By 2018 two-thirds of enterprises will experience IoT security breaches."
>
> **— IDC Chief Analyst Frank Gens**

Internet of Things (IoT)

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 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:

- IDC analysts predict that by 2018, two-thirds of enterprises will experience IoT security breaches.[1]
- Less than 10 percent of new devices connecting to corporate networks will be manageable by traditional methods by 2020.[2]
- There will be 20.8 billion connected things in use worldwide by 2020.[3]

Therefore, it should be no surprise that on Gartner's list of Top 10 IoT Technologies for 2017 and 2018, security ranks number one.[4]

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 IDC's global technology predictions for 2016
2 ForeScout analysis
3 Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Gartner Research, November 2015
4 *Top 10 IoT Technologies for 2017 and 2018*, Gartner Research, February 2016

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.[5] 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 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 ForeScout CounterACT® 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 discovering and 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, CounterACT continuously monitors IoT devices, ports and connections.

Control Once you understand each IoT device on your network, its owner and purpose, CounterACT 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. In addition, should you choose to isolate specific devices to a specific network segment or VLAN, CounterACT simplifies this process.

Orchestrate Without CounterACT, third-party management solutions are blind to unmanaged and IoT endpoints. ForeScout extends CounterACT's agentless visibility and control capabilities to leading network, security, mobility and IT management products via a rapidly growing number of 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

5 Intel Guide to IoT Infographic

> White hat hackers recently demonstrated that they could manipulate the flow of blood samples or drugs from within the hospital's lobby by breaching the security of the kiosk where patients checked in and initiating a pivot attack."
>
> **— Forbes, Feb 23, 2016**

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 are just a couple of the real-world use cases we address today.

Securing IoT devices on enterprise networks

Today's enterprise networks include agentless IoT devices and unmanaged Bring/Choose Your Own Devices (BYOD/CYOD). Each of these devices is a potential network attack or reconnaissance point. Here's one example of how ForeScout can detect, monitor and block a compromised IoT printer. This same scenario is equally relevant to any number of corporate-connected devices such as security cameras, HVAC/lighting controls or monitors and projectors.

1. IoT device connects to the network.
2. CounterACT 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. CounterACT blocks the compromised printer from the network and quarantines it, allowing IT to safely remove the device from the network and perform forensic analysis.

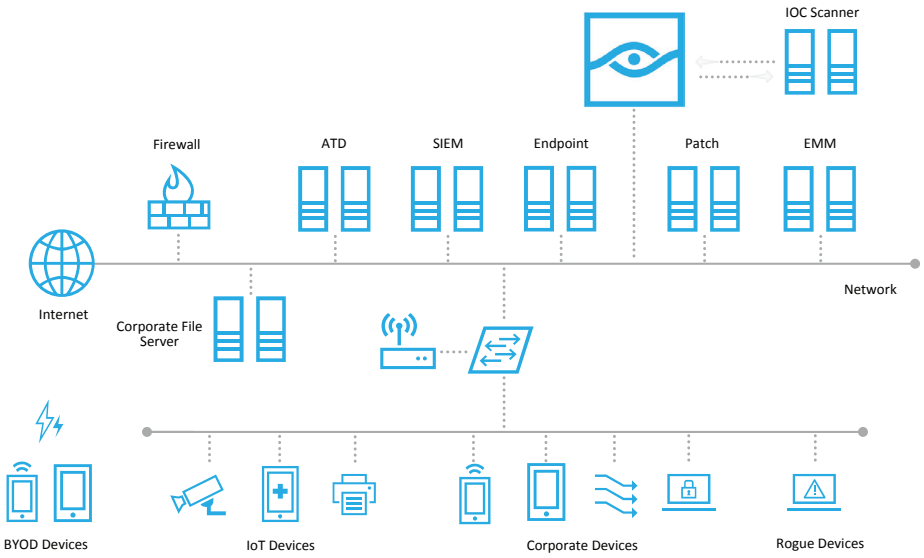

Figure 1: ForeScout's agentless IoT security process provides visibility, control and orchestration with third-party solutions, including SIEMs. It begins with discovery and classification of over 1,000 devices—including IoT and OT devices—by function, operating system, vendor and model.

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