ForeScout

Solution Brief

Operational Technology (OT)

See and secure devices from corporate and operations networks to production floors.

Business Challenges

- "By 2018, 66% of all networks will have an IoT security breach."[2]
  —IDC 2017
- "Top concerns of IIoT security and risk management leaders are the lack of security posture visibility and lack of asset visibility, which leave them "in the dark" on what assets to manage and prioritize."[3]
  —Gartner 2016

Technical Challenges

- 60% of respondents said that the biggest challenge was technical integration of legacy control systems with modern IT systems.[1]
  — SANS 2017 survey
- "Younger IT people don't realize that if something has been running without a reboot for seven years, don't touch it."[4]
  — Control Engineering, 2013

OT Security Defined:

"The practices and technologies used to protect people, assets and information involved in the monitoring and/or control of physical devices, processes and events."[5]

OT System examples:

SCADA (Supervisory Control and Data Acquisition)
PCN (Process Control Networks)
DCS (Distributed Control Networks)
MES (Manufacturing Execution Systems)
Telematics
Robotics
Facilities Management
Building Automation Systems
Fleet Management Systems

—Gartner, August 2017

Only 19 percent of respondents to a SANS Institute Control Systems security survey[1] could say that their control network had not been infected or infiltrated in the last 12 months. Can you identify what's on your operational technology (OT) network? Do you worry that needed security will impact your equipment's production uptime?

The Challenge

It is difficult enough being a prime target for security attacks. Now, imagine compounding those issues with the significant challenges that OT security customers face, including:

- **Lack of visibility into network activity and connected devices**. Operations staff in industrial environments often don't know what types of OT, IT (information technology), or IoT (Internet of Things) equipment they have. In addition, many maintenance processes are still performed manually or performed as part of a maintenance agreement through their equipment vendors. With these hidden devices and externally generated network activity taking place, how do you know when threat activities appear?
- **Convergence of legacy operational equipment and IT technologies**. While many organizations are embracing more OT equipment internet protocol (IP) advancements, many organizations still have significant investments in OT that predate the Internet. Introduce IT into the mix and you have an assortment of devices with different communications protocols, requirements and update cycles. What's more, they need to work together.
- **Constant pressure caused by audits and compliance obligations**. Safety and security for employees and customers have always been top priorities in industrial and utility companies, causing them to become highly regulated fields. Security mandates with compliance requirements (and fines) exist across most industries and agreed-upon standards must be met to help institutionalize best practices.
- **Necessity for continual uptime**. Nobody wants to disturb OT equipment because any downtime can turn into millions of dollars in lost productivity, highly vocal, disgruntled customers and regulatory fines. Machines must reach a high OEE (overall equipment effectiveness). There is no time to allow IT-style updates and patches that take down equipment.

Securing Industrial Networks with ForeScout

Why OT air gaps = IT security chasms

Not long ago, OT, such as manufacturing lines, environmental controls and industrial control systems (ICSs), and sensors used in critical infrastructure, was isolated by

Here's a partial list of OT applications and benefits.

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

Water and wastewater facilities.
Account for water usage, improve water quality and resource efficiency.

Utilities

Connected meters, substation automation and smart grids.
Automate meter reading and improve usage/production efficiencies.

Facilities Management

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

air-gapped networks. These command-and-control-type networks often ran legacy operating systems and proprietary network technologies that typically sacrificed security in favor of system performance and availability. This approach, often called "security through obscurity," no longer works. The economic and productivity advantages of IP connectivity quickly erased security air gaps as operational networks connected to external-facing IT networks. Today, vulnerable devices lack management agents and don't respond well to active security measures. Thus, security teams are unable to inventory them, let alone secure them.

OT networks need passive alternatives

While industrial equipment needs to be secured, the devices are not uniformly ready for active interrogation or authentication by security solutions without disruption. The solution is to first establish the visibility of all devices on the network in a passive manner. Next, selectively enable OT, IT and IoT assets that can submit to active security interrogation techniques. It is now possible for organizations to gain visibility and control of IP-based devices without impacting performance of the OT network.

The ForeScout Solution

ForeScout helps organizations secure OT devices 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 or active interrogation techniques. We take this a step further by discovering and classifying devices as well as validating their identities using multiple passive methods. This is essential for improving your endpoint compliance posture and defining your security and enforcement policies. In addition, CounterACT continuously monitors devices, ports and connections. With up-to-date context, incident responders can use a broad set of actions to address risk and potential threats.

Once you understand what each OT, IT and IoT device on your network is, its owner and purpose, the next step is to select those devices for further security measures. CounterACT enables a broad range of network access controls and alerts so that you can take appropriate actions.

Control For those devices that are selected to move forward with active security, CounterACT can allow, deny or limit network access based on device posture and security policies. By assessing and remediating malicious or high-risk endpoints, it mitigates the threat of data breaches and malware attacks that would otherwise put your organization at risk. In addition, by continuously monitoring devices on your network and controlling them in accordance with your security policies, CounterACT dramatically streamlines your ability to demonstrate compliance with industry mandates and regulations.

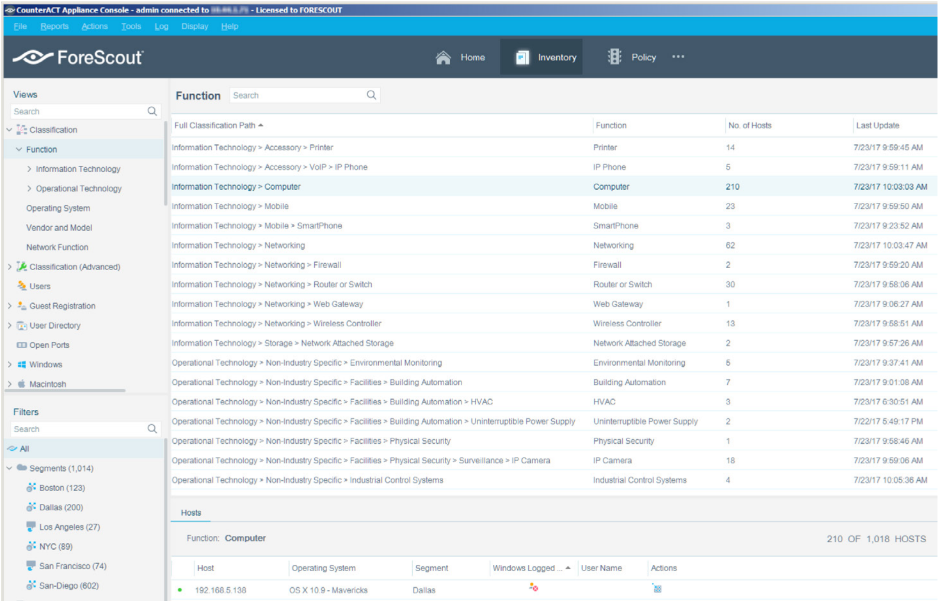
Orchestrate Without CounterACT, third-party management solutions are blind to unmanaged OT and IoT endpoints. ForeScout extends CounterACT's agentless visibility and control capabilities to leading network, security, mobility and IT management products via a rapidly growing number of ForeScout Extended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

Discover and Classify OT, IT and IoT Devices for Asset Management

Gain views of the network landscape and awareness of what was previously invisible. ForeScout gives real-time visibility to provide up-to-date device properties, classification, configuration and network context to use as-is or in collaboration with a configuration management database (CMDB) for a single-source-of-truth asset repository. Organizations can have a current view of network assets, track movement of devices and contain or remediate assets for security response. In an IDC survey[6] of CounterACT customers, an average of 24 percent more devices were seen with ForeScout CounterACT than were previously known by staff to exist.

> “From a single location, we can see all our network switches and IP ranges globally, and can tell which switch and which port connect to a particular host.
>
> We discovered it provides full visibility and compliance status of all devices on the network. That is something I didn’t have before.
>
> We have expanded the use of ForeScout CounterACT to the manufacturing network so that we now have a full view of all the devices in the entire company.”
>
> **— James Tu, Director of Information Security, International Rectifier**



Full Classification Path	Function	No. of Hosts	Last Update
Information Technology > Accessory > Printer	Printer	14	7/23/17 9:59:45 AM
Information Technology > Accessory > VoIP > IP Phone	IP Phone	5	7/23/17 9:59:11 AM
Information Technology > Computer	Computer	210	7/23/17 10:03:03 AM
Information Technology > Mobile	Mobile	23	7/23/17 9:59:50 AM
Information Technology > Mobile > SmartPhone	SmartPhone	3	7/23/17 9:23:52 AM
Information Technology > Networking	Networking	62	7/23/17 10:03:47 AM
Information Technology > Networking > Firewall	Firewall	2	7/23/17 9:59:20 AM
Information Technology > Networking > Router or Switch	Router or Switch	30	7/23/17 9:58:06 AM
Information Technology > Networking > Web Gateway	Web Gateway	1	7/23/17 9:06:27 AM
Information Technology > Networking > Wireless Controller	Wireless Controller	13	7/23/17 9:58:51 AM
Information Technology > Storage > Network Attached Storage	Network Attached Storage	2	7/23/17 9:57:26 AM
Operational Technology > Non-Industry Specific > Environmental Monitoring	Environmental Monitoring	5	7/23/17 9:37:41 AM
Operational Technology > Non-Industry Specific > Facilities > Building Automation	Building Automation	7	7/23/17 9:01:08 AM
Operational Technology > Non-Industry Specific > Facilities > Building Automation > HVAC	HVAC	3	7/23/17 6:30:51 AM
Operational Technology > Non-Industry Specific > Facilities > Building Automation > Uninterruptible Power Supply	Uninterruptible Power Supply	2	7/22/17 5:49:17 PM
Operational Technology > Non-Industry Specific > Facilities > Physical Security	Physical Security	1	7/23/17 9:58:46 AM
Operational Technology > Non-Industry Specific > Facilities > Physical Security > Surveillance > IP Camera	IP Camera	18	7/23/17 9:59:06 AM
Operational Technology > Non-Industry Specific > Industrial Control Systems	Industrial Control Systems	4	7/23/17 10:05:36 AM

Function: **Computer** 210 OF 1,018 HOSTS

	Host	Operating System	Segment	Windows Logged ...	User Name	Actions
●	192.168.5.138	OS X 10.9 - Mavericks	Dallas			

Figure 1. ForeScout CounterACT provides a consolidated and up-to-date asset inventory of IT, OT and IoT devices. Asset inventories can be categorized by operational function, vendor and operating system; rolled up to existing IT/security tools such as CMDB/ITSM/SIEM, and attached safely with context to relevant stakeholders such as Risk & Compliance.

Simplify compliance with regulatory requirements

ForeScout CounterACT can help protect confidential data and support compliance efforts with mandated policies and regulations such as FISMA, NERC, and ISO/IEC 27001.

ForeScout can:

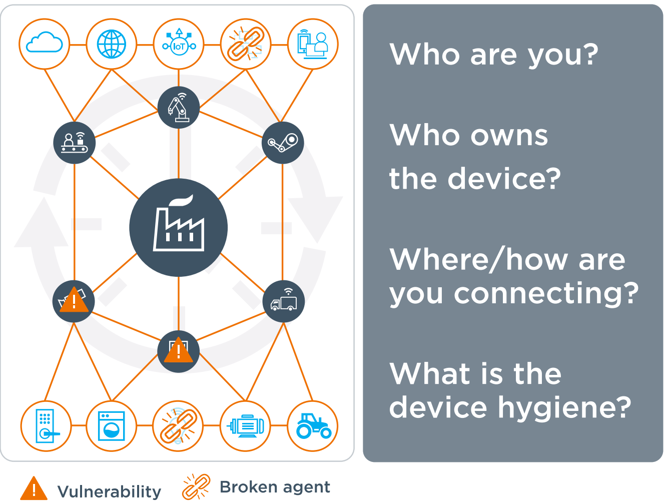
- Identify traditional OT devices as well as IT and IoT devices
- Continuously monitor the network for out-of-compliance activities
- Proactively monitor and alert for the introduction of non-compliant devices
- Contain the spread of malware across the network
- Guard against targeted threats that can result in stolen data and network downtime
- Perform posture assessments

With ForeScout CounterACT, your organization can automatically identify policy violations, remediate endpoint deficiencies and measure adherence to industry compliance mandates.

Example from National Institute of Standards and Technology 800 (53rev4 & 171)

Risk Management Framework and ForeScout CounterACT Control Mapping Data Sheet

AC-3	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.	3.1.1/3.1.2	Access Enforcement	ForeScout CounterAct will use the defined logical access to information and system resources in accordance with applicable access control policies established by the organization. With CounterACT Access Controls we recognize a few areas of management needed to establish this policy: Network device visibility and information. This must include device type user identity and role, device location, and its level of compliance with organizational security policies.



Who are you?

Who owns the device?

Where/how are you connecting?

What is the device hygiene?

Figure 2. A representation of ForeScout CounterACT performing access control to support compliance.

In addition to taking compliance actions based on security policies, CounterACT easily generates documentation to demonstrate mandate conformity to keep both internal and external auditors satisfied that your network is secure.

Want to learn more? Visit our:

Industries page

Government page

Case Studies

Request a Demo

Learn more at **www.ForeScout.com**

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

[1] SANS Security Industrial Control Systems Survey, June 2017
[2] Mobility 2016 Predictions Survey, June 2017
[3] Gartner Research Note, "Pragmatic Strategies to Improve Industrial IoT Security," November 2016
[4] http://www.controleng.com/single-article/it-vs-ot-bridging-the-divide, *Control Engineering*, August 2013
[5] Gartner Research Note, "Market Guide for Operational Technology Security," August 2017
[6] "The Business Value of Pervasive Device and Network Visibility with ForeScout," IDC survey, April 2017