FORESCOUT

ForeScout for Operational Technology (OT)

Expand your visibility and reduce security risk for converged IT and OT networks in Industrial Controls, SCADA, Critical Infrastructure and Transportation

Highlights

You can't secure what you can't see™, especially in operational networks with a mix of devices and operating systems. True security begins with visibility, and ForeScout provides the needed framework to See, Control and Orchestrate the devices on your OT networks.

See

- Discover devices the instant they connect to your network using passive techniques
- Classify and profile devices without requiring agents
- Identify users and applications
- Assess device hygiene and continuously monitor security posture

Once you gain knowledge of each OT, IT and IoT device on your network, including its owner and purpose, a potential next step is to apply further security measures to selected devices by allowing active security. ForeScout can:

Control

- Allow, deny or limit network access based on device posture and security policies
- Notify end-users, administrators or IT systems about security issues
- Comply with security policies, industry mandates and best practices

Lack of asset visibility and device status knowledge continue to be top concerns for OT security and risk management leaders. Most industrial facilities lack a complete, up-to-date inventory of legacy and converged IT-centric assets despite the need for safety, security and compliance. With the diversity of technology, variety of devices and protocols, and the sensitivity of equipment, extreme caution needs to be taken to ensure that security solutions do not impose risk to physical safety and operational uptime. (Refer also to the Operational Technology Solution Brief.)

ForeScout for OT uses multiple non-disruptive methods to discover, classify and validate device identities as part of a comprehensive security solution. ForeScout for OT builds a strong security foundation to resolve:

- What is on the network and how to classify and manage it
- Who can access the network and under what context
- How to stay within compliance for regulatory and security frameworks
- How to orchestrate a security response in the event of an incident

And most importantly,

- How to improve security without compromising operational uptime

Reduce risk and enhance OT security with ForeScout

Extend your secure network environment throughout the entire organization

As threats expand beyond traditional IT networks, the need to extend security visibility expands to all networks. With ForeScout, you can reduce overall business risk from costly cyber-outages with continuous network-connected device identification and security monitoring. In addition, you can increase operational efficiencies by leveraging a consolidated security platform across campus, data center, cloud and OT environments.

Gain visibility of networked devices that were previously unseen or off limits

Increased visibility of connected devices and intelligence of device security posture help you to manage security risk. Without a proper security solution, a significant percentage of endpoints on networks go undetected primarily due to:

- Devices with disabled or broken agents
- Devices with IP addresses but not enough memory to communicate
- Transient devices undetected by periodic scans
- Devices not directly connected to the network
- Guest devices or bring-your-own devices (BYOD)

With ForeScout for OT, you see devices on the network the moment they connect to your network using non-disruptive techniques and without requiring security agents. Once established, visibility becomes a foundational step in managing your security and risk objectives.

Orchestrate

- Share context and control intelligence with existing security solutions and network infrastructure to enforce a unified network security policy
- Reduce vulnerability gaps by automating system-wide threat response
- Gain higher return on investment from your existing security tools while saving time through security orchestration

Discover and classify OT, IT and IoT devices for enhanced asset management

With this solution, you benefit from continuous asset identification and assessment, providing up-to-date device and network security posture—without requiring data calls. ForeScout's real-time visibility and intelligence provides 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. ForeScout can identify devices, infrastructure and operating systems, as well as obtain user and application information. In turn, organizations can gain a current view of network assets, track movement of devices and contain or remediate assets for a better security response, while lowering IT costs throughout the asset lifecycle.

Build policies that control access and develop relevant network segmentation

ForeScout's visibility and classification intelligence provide context to build network controls that can effectively defend against common intrusion practices.

- Implement policies to control device and user access with ForeScout network access control actions
- Split the network into zones that contain devices and data with similar compliance requirements for defensive network segmentation
- Apply tailored security policies by zone to achieve the right mix of passive and active security controls based on the needs of the underlying devices

Having policy-based, automated response to address common security issues frees up personnel for more complex and sensitive cyber-risk issues.

Respond better to incidents leveraging increased context

In scenarios where systems and devices generate many potential threat indicators, context helps provide suitable answers to speed time to resolution. To reduce false positives, you can provide device classification and assessment context from ForeScout to your security information and event management (SIEM) tools for better incident prioritization. If further action is needed, you can use network access controls to automatically block outbound command and control channels from a suspected system or device.

Through orchestration, ForeScout and ForeScout Extended Modules help you create a consolidated security platform across campus, datacenter, cloud and OT—a platform that helps you increase operational efficiencies and reduce overall business risk related to costly cyber outages.

How ForeScout Fits in Segmented OT Frameworks

Most OT networks map to some security best-practices frameworks or standards. Across these frameworks, common themes include the need to identify assets, control access to the network, utilize passive security techniques, and prioritize the uptime and availability of the operational network. These are the principles that define how The ForeScout platform operates in an operational environment.

The ForeScout Solution Within an Operational Technology Framework

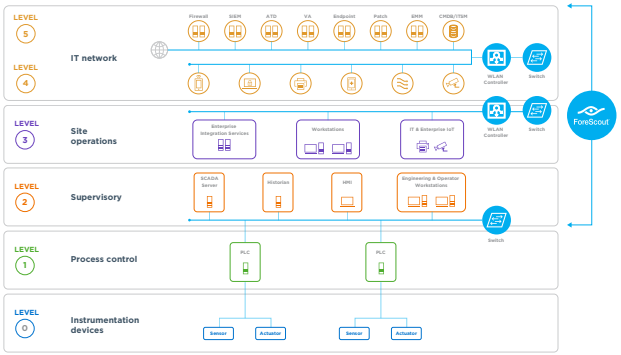

Figure 1. ForeScout determines the security posture of an operational network through passive techniques, without needing direct connection to devices.

Why Customers Choose ForeScout

Exceptional, continuous visibility. See devices that other solutions can't. According to an IDC study , respondents could see 24% more devices after deploying ForeScout.

Real-time information. Gain near real-time visibility and control of devices the instant they access your network.

Heterogeneous support. Works with common Operational Technology interfaces, wired and wireless IT network infrastructure, operating systems, endpoint software and third-party security solutions.

Agentless. No device agents required for authentication and access control.

Rapid time to value. Deploy quickly to gain network visibility in hours.

Compliance. Automatically identify policy violations, remediate endpoint deficiencies and adhere to compliance mandates.

> **Machine manufacturers understand the need for device security, as there are no longer air gaps in production networks. In a perfect world, every networked device should undergo vulnerability assessment testing and be monitored."**
> **— Billy Lewis, State Garden, Director of Information Technology**

Address device security gaps to maintain compliance

ForeScout provides a foundational security baseline for common regulatory compliance requirements such as NERC-CIP[2] , security frameworks such as SANS Institute or NIST[3], and industry certifications such as IEEE, IEC and ISO.

- Gain real-time endpoint compliance capabilities without security personnel interventions and without software agents
- Detect suspicious activity and take actions upon discovery
- Control device configurations according to your policies and regulatory mandates

In many cases ForeScout supports regulatory controls through hardware and software asset management, as well configuration and vulnerability management, or by helping to establish an electronic security perimeter.

How ForeScout Works

The ForeScout agentless security solution identifies and evaluates networked devices and applications the instant they connect to your network. Using non-disruptive approaches, ForeScout can see what's on your network from your campus, data center, virtual servers and cloud, extending to your OT environment. With this added visibility and intelligence, you can take steps to identify devices needing passive monitoring and act upon those that can support further security controls. Additionally, ForeScout can share relevant data with security and system management tools you already own to improve your security profile and enhance your existing investments.

As seen in Figure 2 below, ForeScout monitors network-connected devices by using a variety of non-disruptive data capture methods from relevant network devices, such as switches, firewalls, Virtual Private Network (VPN) concentrators and wireless controllers. These devices already connect to operational workstations and supervisory controllers, such as supervisory control and data acquisition (SCADA) servers and Human Machine Interface (HMI) stations on OT networks. Using the data captured, ForeScout discovers connected devices, classifies devices by type, identifies users and applications, assesses device hygiene and continuously monitors security posture. With this information, ForeScout continuously leverages layered ForeScout and customer-defined policies to take appropriate actions to secure the network.

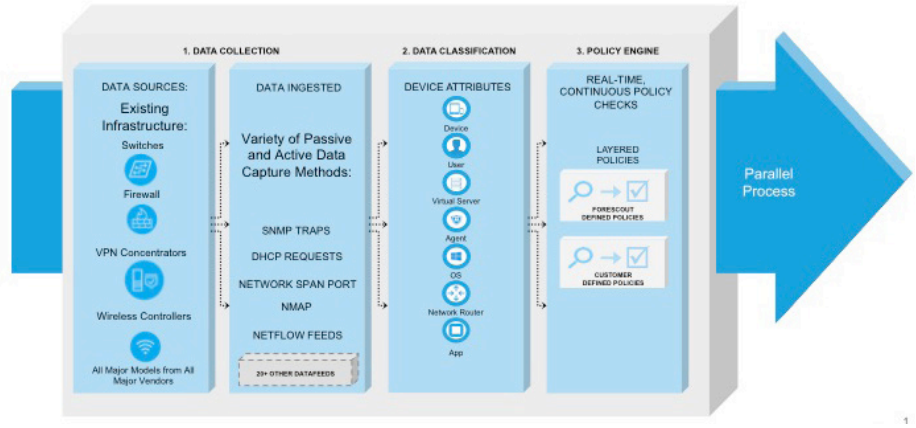

Figure 2. ForeScout uses passive techniques to discover, monitor and assess devices

Key ForeScout Features Address OT Security Needs

Classification engine with OT taxonomy

Take the guesswork out of identifying IT, IoT and OT devices by using out-of-the box or customizable OT classification intelligence in ForeScout's classification engine. Use passive, configurable profiling methods and rules to inspect and classify devices by OT operating system, device manufacturer, functional or operational grouping, or other criteria. This foundation of information lets you build a real-time asset inventory and apply context-based policies for compliance and segmentation to secure your network.

Visibility use cases for ForeScout passive capabilities:

- Real-Time Asset Intelligence
  - Real-Time Asset Discovery
  - Automated Asset Classification
  - New Asset Detected Alerting
  - Critical Asset Offline Alerting
- Network Isolation Validation
  - Unauthorized Asset on Virtual Local Area Networking (VLAN) Alerting
  - Unauthorized Traffic to Critical Asset/VLAN Alerting
  - Inter-VLAN Traffic Alerting
  - Internet-bound Traffic Alerting
- Traffic-Based Compliance Rules
  - Traffic Detected Outside Defined Rules Alerting

Passive profiling capabilities

For networked devices known to be sensitive to network probing, ForeScout's Passive Profiling excludes devices designated to not allow active security actions. ForeScout doesn't contact these groups of devices and exclusively uses passive methods to gain intelligence. With Passive Profiling, you can securely identify and monitor sensitive zones, as well as learn properties or states of devices without disrupting normal operational activities.

Orchestration

ForeScout orchestrates information sharing with leading IT and security management products that you may already own, allowing you to improve your security posture and enhance your existing investments. You can share increased depth and breadth of IT, IoT and OT device context discovered by ForeScout without disruption of your other systems:

- Enrich your configuration management database (CMDB) with information about industrial and critical infrastructure systems
- Provide device classification and assessment context to your SIEM tool to leverage this information for incident prioritization
- Develop policies and tag devices based on classification and assessment so your next- generation firewalls (NGFWs) can implement segmentation policies grouping OT devices accordingly

For specific details about the product and for technical specifications, visit: https://www.forescout.com/products/specifications/

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

[1] IDC, *The Business Value of Pervasive Device and Network Visibility and Control with ForeScout*
[2] North American Electric Reliability Corporation critical infrastructure protection
[3] National Institute of Standards and Technology