FORESCOUT

Agentless Device Visibility and Control

Foundational capabilities for effective cybersecurity

> "Visibility is the key in defending any valuable asset. The more visibility you have into your network across your business ecosystem, the better chance you have to quickly detect the telltale signs of a breach in progress and to stop it."[1]
>
> **— Dr. Chase Cunningham, Principal Analyst, Forrester Research**

Device Visibility and Control: Why You Need It

The ability to discover, classify, assess and control every device that connects to your network is the essential precondition for securing your systems and your business. Only with real-time knowledge of every physical and virtual endpoint on every segment; granular insight on configuration and security state; and automated, policy-based access control can you reliably ensure system and data security, respond quickly and accurately to incidents, achieve compliance, manage business and infrastructure risk and optimize security efficiency. Attackers are continuously searching for unmanaged and unsecured devices, and they will eventually find and exploit your blind spots. Visibility and control are the cornerstones of security and compliance.

Why Visibility and Control Are Hard to Acquire

The conventional method of managing network endpoints was a software agent installed on every device. This worked well enough when most endpoints were static, company-owned PCs or servers, but mobility, diversity of device types and virtualization have made contextual visibility and control far more complicated. In today's enterprise environments, cloud and data center segments hum with dynamically provisioned workloads running on virtual machines and connected by virtualized networks. Campus segments teem with user-owned BYOD laptops, tablets and smartphones that don't have security agents as well as Internet of Things (IoT) devices that can't support them. Operational technology (OT) segments add vast numbers of devices that don't support agents, communicate with proprietary protocols, manage mission-critical processes, and are intolerant of internal intrusion. IT organizations urgently need an agentless solution that can provide comprehensive visibility and control across all of these varied environments.

The Forescout Solution: Agentless Device Visibility and Control

Forescout Technologies has pioneered an agentless approach to network security that addresses the challenges of device visibility and control in today's dynamic and diverse environments. The Forescout device visibility and control platform provides a continuous, unified view of all your devices across campus, data center, cloud and OT networks.

The Forescout platform discovers:

- Campus network devices: Laptops, tablets, smartphones, BYOD/guest systems and IoT devices
- Data center infrastructure: Virtual machines, hypervisors, physical servers and virtual and physical networking
- Public and private cloud infrastructure: AWS®, Microsoft® Azure® and VMware® virtual machines
- OT and industrial control systems (ICS): Medical, industrial and building automation devices
- Physical and software-defined network infrastructure: Switches, routers, firewalls, VPNs, wireless access points and controllers

Device Visibility Across the Extended Enterprise

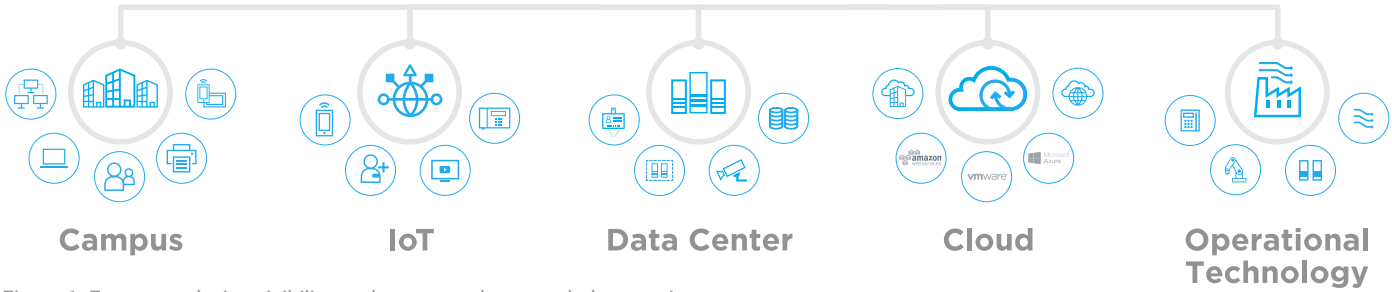


Figure 1: Forescout device visibility scales across the extended enterprise.

> "Assessments and visibility of risk/trust and the exchange of context become the immune system for digital business."[2]
>
> **— Neil MacDonald, VP, Analyst, Gartner**

What We Do

Forescout gives IT organizations the ability to:

- Discover every IP-connected device on every network: physical and virtual devices across campus, data center, cloud and industrial environments
- Classify diverse IT, IoT and OT/ICS devices as well as virtual machines (VMs) and cloud instances in real time based on identification of device type and function, vendor, model, operating system and version
- Assess and continuously monitor device security state for policy compliance
- Conform to 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

How We Discover Every IP-Connected Device and OT System on Every Segment

The Forescout platform provides more than 20 configurable information-gathering techniques that leverage deep integration with leading IT and OT network switches, routers, wireless access points, firewalls, VPN concentrators and data center and cloud solution providers. It listens passively to network traffic, parsing many different protocol streams, and can interact directly with both network infrastructure and endpoints. Forescout visibility techniques include:

- **Methods that are passive to both the network and the end device**. Examples include receiving SNMP traps from switches and wireless controllers, monitoring a SPAN port and parsing protocol streams in the traffic (Forescout provides deep packet inspection for more than 100 IT and OT protocols), collecting and analyzing flow data, or evaluating DHCP requests and HTTP user agent traffic. If 802.1X is implemented, Forescout can monitor a RADIUS server whether built-in or external.
- **Methods that are active on the network infrastructure.** Examples include: polling switches, VPN concentrators, wireless controllers, and private and public cloud controllers for a list of connected devices and VMs. For user and device data, the Forescout platform queries directory services, web applications or external databases.
- **Methods that are active on the end device.** Examples include: Scanning network segments for connected devices using NMAP, remotely inspecting Windows devices using WMI or Mac and Linux devices using SSH, and endpoint profiling using SNMP queries.

Device Visibility Techniques

PASSIVE TECHNIQUES
SNMP traps
SPAN traffic
DHCP requests
HTTP user-agent
TCP fingerprinting
DICOM protocol parsing (medical imaging devices)
ICS OT protocol parsing (60+protocols)
Flow analysis
Netflow
Flexible Netflow
IPFIX
sFlow
DHCP requests (via ip-helper)
HTTP user-agent (via URL redirect)
RADIUS requests
MAC OUI

ACTIVE TO INFRASTRUCTURE
Physical network infrastructure polling
Controller-based network infrastructure integration
Meraki
Cisco ACI
Private cloud (virtual infrastructure) integration
VMware
Private cloud integration
AWS
Azure
Query directory services (LDAP)
Query web applications (REST)
Query external databases (SQL)
Orchestrations (ITSM, UEM, EPP, EDR, VA)
ACTIVE TO END-DEVICE
Agentless inspection Windows (WMI, RPC, SMB)
Agentless inspection Windows (WMI, RPC, SMB)
NMAP
SNMP Queries to endpoint
Agent-based inspection (SecureConnector)

Figure 2: Forescout device visibility methods.

The Advantages of Multiple Device Visibility Methods

Because it offers many different discovery methods that are easily configured at set-up (and easily modified afterwards), the Forescout platform is uniquely flexible, efficient and effective.

Passive-only discovery, classification and assessment for OT networks: OT networks are often inappropriate environments for active probing and scanning techniques that could potentially disrupt process control systems and business operations. Once devices are better understood, active methods can be selectively applied. The Forescout platform provides device visibility across OT networks through a completely passive combination of SPAN traffic mirroring and deep packet inspection across nearly 100 OT-specific protocols. Forescout supports industry-standard protocols such as BACnet, CIP, DNP3, Ethernet/IP, ICCP, IEC 60870-5-104, IEC 60850, IEEE C37.118, Modbus/TCP, OPC, PROFINET and Siemens S7. We also support the proprietary protocols of leading manufacturers such as ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, Schneider Electric and Yokogawa.

Cost-effective deployment in large environments: The ability to use remote visibility techniques can reduce the overall cost of deployment by allowing small sites to be monitored without the need for a local appliance.

Insight beyond discovery: classification and assessment: The ability to layer passive and active profiling techniques allows the Forescout platform to do much more than simply identify a connecting device by MAC and IP address. Classification is the process of acquiring and correlating many layers of context to create a richly detailed profile of each device. Assessment is the process of comparing discovered device-state properties against security policy as the basis for access control and remediation decisions. Both processes deserve closer examination.

Intelligent Auto-Classification

Complete context for every device is key to granular policy creation. You need to know the operational context or purpose of each device to decide how it is best secured and managed. The growth and diversity of devices makes manually gathering this context nearly impossible, and creating policies without proper context puts operations at risk. Forescout auto-classifies traditional, IoT and OT devices using a multi-dimensional classification taxonomy to identify device function and type, operating system and version, and vendor and model.

The platform auto-classifies:

- More than 500 different operating system versions
- Over 5,000 different device vendors' products and models
- Healthcare devices from over 350 medical technology vendors
- Thousands of industrial control and automation devices used across manufacturing, energy, oil and gas, utilities, mining and other critical infrastructure industries

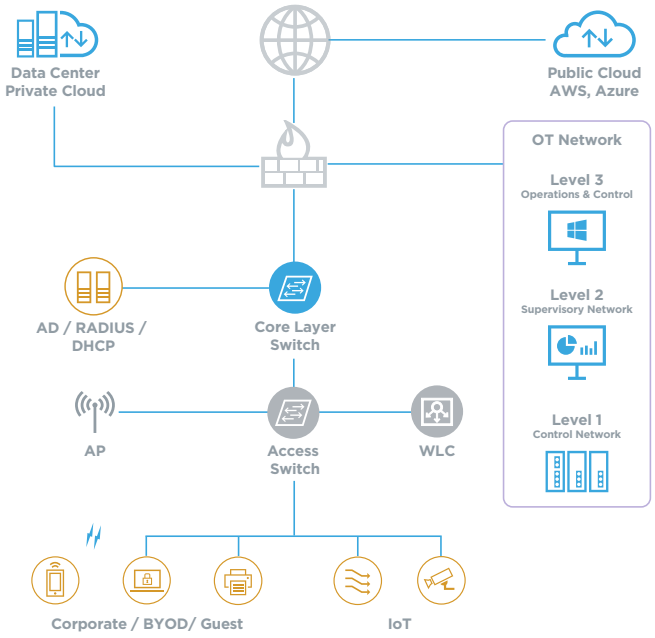
The Forescout Device Cloud powers the platform's auto-classification, ensuring this rich source of context continues to keep pace with device growth and diversity. Forescout Research leverages intelligence from over 8 million real-world devices* in our Device Cloud and publishes new profiles on a frequent basis to improve classification efficacy, coverage and velocity across your entire device landscape.

Device Posture Assessment

Device classification delivers operational context as to the purpose of a device—in effect, telling you what that device is. For complete context, however, another lens is required in order to gauge the health and hygiene of each device. Forescout continuously monitors the network and assesses the configuration, state and security posture of connected devices to determine their risk profiles and whether they adhere to security and regulatory compliance policies. It answers critical questions, including:

- Are devices running approved operating systems, including the latest OS patches?
- Is security software installed, operational and up-to-date with the latest patches?
- Are any devices running unauthorized applications or violating configuration standards?
- Are devices using default or weak passwords (a particular risk for IoT devices)?
- Have rogue devices been detected, including those impersonating legitimate devices via spoofing techniques?
- Which of your connected devices are most vulnerable to the latest threats?

Device Classification and Assessment



WHO?
- User
- Name
- Email
- Title
- Group
- Subscription/ Account
- IAM Owner/ Role

WHAT?
- Function
- OS
- Vendor/Model
- IP Address
- Browser Agent
- Ports
- Virtual/Physical
- Mac Address

POSTURE?
- Apps
- Services
- Processes
- Versions
- Registry
- Patches
- Encryption
- Antivirus

WHERE?
- Switch
- Controller
- Switch Port/ SSID/VLAN
- AWS/Azure
- Region
- VNet/VPC
- Purdue Level

Figure 3: The Forescout platform quickly classifies devices by type, clarifies whether they are corporate-managed, unmanaged, IoT/OT, physical or virtual, and helps you assess their compliance status.

Using Visibility to Enable Control

The Forescout platform includes a policy engine that continuously checks devices against a set of customizable policies that dictate and enforce device behavior on the network, providing continuous, real-time monitoring for up to two million devices. Policies are triggered in real time by events that occur either on a specific device or in the network. These can be network admission events, such as plugging into a switch port or changing an IP address. In addition, they can be authentication events like those received by a RADIUS server. Policies can also be invoked by changes in device attributes. Figure 4 illustrates the range of control actions available to the Forescout platform when a policy is triggered.

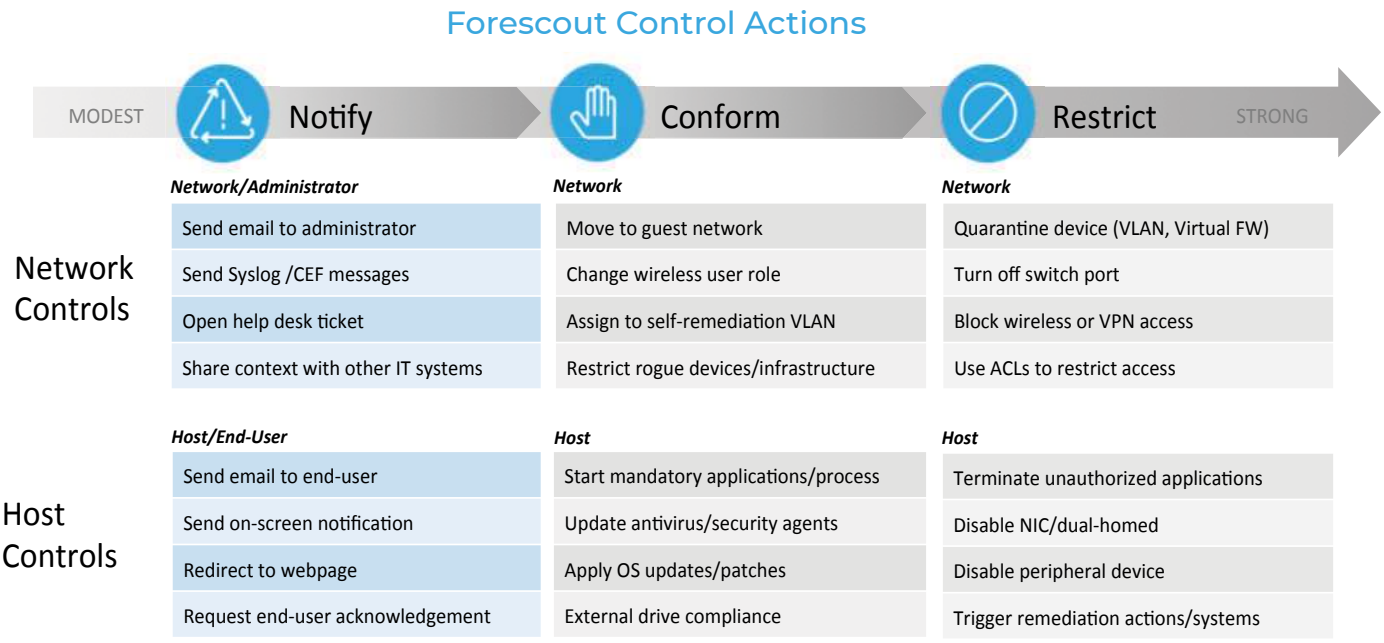


Figure 4: Customizable control actions allow you to enforce the appropriate level of control—from modest to stringent—based upon your security policies.

The policy engine leverages two ranges of control functions. The first is native to Forescout. The second is accessed through data exchange and control orchestration integrations with leading security and IT management products.

Native Control Functions

Forescout's native functionality includes network- and host-based controls. Controls in the network provide policy-based segmentation, enabling or restricting access according to user identity, role and device state. Host-based controls enforce device hygiene to start and stop applications, update antivirus and other host-based security agents or disable peripheral devices. The policy engine applies these policies automatically regardless of a device's location or movement across the corporate network and into the data center or cloud.

Extended Control Functions

The Forescout platform automates policy enforcement, accelerates system-wide response and mitigates risk by sharing real-time device context and orchestrating workflows across many different types of security and IT management products. Forescout offers integrations with leading vendors in these categories:

- Advanced threat detection
- Client management tools
- Enterprise mobility management
- Endpoint protection, detection & response
- IT service management
- Next-generation firewalls
- Privileged access management
- Security information and event management
- Vulnerability assessment

Through these integrations, Forescout orchestrates infrastructure-wide security, providing policy-driven controls based on user, device, application and traffic classification. It enforces granular access policies with precise and flexible control over resources, enabling IT organizations to implement dynamic network segmentation and create context-aware security policies based on real-time situational awareness.

Control Actions We Can Take

With deep roots in network access control, Forescout offers a combination of native and extended control functionality, giving the Forescout platform an extraordinarily broad range of device-control capabilities that, in turn, provide IT organizations with a powerful arsenal of network security tools.

The Forescout platform enforces network access to enterprise resources based on user profile (guest, employee, contractor), device classification and security posture by:

- Enabling differentiated access for guest and BYOD devices
- Enforcing network access policies with or without 802.1X authentication
- Taking action against suspicious, rogue or shadow IT devices on the network
- Limiting or blocking network access for compromised or malicious devices
- Quarantining or isolating noncompliant devices until compliance deviations have been addressed

The Forescout platform improves device compliance by automating compliance assessment and enforcing remediation controls for continuous compliance with internal security policies, external standards and industry regulations. Important capabilities include:

- Ensuring endpoints are properly configured and initiating remediation for critical configuration violations, including weak or default passwords
- Ensuring required applications and security agents are installed, running and up-to-date
- Disabling or blocking unauthorized applications that could introduce risk or put an unnecessary burden on network bandwidth or resource productivity
- Identifying high-risk vulnerabilities and missing critical patches and initiating remediation actions
- Proactively targeting remediation actions such as installing required security software, updating agents or applying security patches
- Implementing policies and automating controls for configuration compliance in cloud deployments, including AWS, Azure and VMware

The Forescout platform implements dynamic network segmentation by applying segmentation policies across disparate enforcement technologies in your extended enterprise through a common policy framework. The Forescout platform:

- Dynamically assigns devices to segmentation groups based on device properties, classification and security posture
- Applies segmentation enforcement via VLANs, ACLs, WLAN controls and tagging in campus and OT networks
- Applies segmentation controls via security groups/tags in public and private cloud environments such as AWS and VMware NSX®
- Segments noncompliant and vulnerable devices into separate zones—especially those that can only be patched or remediated within scheduled maintenance windows—to enable business continuity while reducing your attack surface
- Enforces segmentation policies to separate specific devices and critical data flows from the rest of the network, as required by regulations such as HIPAA, GDPR, PCI and SWIFT CSP

The Forescout platform accelerates incident response by quickly and effectively containing threats and responding to security incidents to minimize disruption to operations and damage to the business. This device visibility and control solution:

- Identifies high-risk devices that haven't been contained or remediated
- Works with ATD solutions to identify indicators of compromise (IOCs) on devices at time of connect to reduce mean time to respond (MTTR)
- Quickly isolates and contains compromised or malicious devices to avoid lateral propagation of malware
- Automates incident response and initiates remediation workflows on compromised devices
- Reduces MTTR by providing valuable device context (device connection, location, classification and security posture) to cross-functional incident response teams and siloed technologies

Security Starts with Visibility

There's a reason military commanders always seek to take and hold the high ground, because an elevated position renders approaching forces visible from afar, allowing defenders to respond before the attack begins. The Forescout platform offers IT organizations a commanding view of the network terrain they must defend. By continuously discovering, classifying, assessing and controlling every device no matter where it connects, Forescout makes the IT security battleground visible, intelligible and manageable.

Evaluate the Forescout Platform for Yourself

The best way to gain a better understanding of Forescout's agentless device visibility and control capabilities is to see them firsthand. Forescout offers many ways to gain greater insight into the Forescout platform, including:

Take a test drive: Experience the before-and-after difference of the Forescout platform with a hands-on test drive that takes you through six powerful use cases.

Get your Forescout Absolute Visibility and Risk Report: Gain a detailed device visibility and risk assessment. Contact your local Forescout representative for more information.

Request a demo: Visit the Forescout demo page to request a personal demo and access a full complement of on-demand demos and video options.

Use the Forescout Business Value ROI Tool: Quantify the business value the Forescout platform can provide to your organization (as calculated by IDC's Business Value Model) in just 10 minutes.

*As of March 31, 2019

1 The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, January 2018

2 Zero Trust Is an Initial Step on the Roadmap to CARTA, Gartner, December, 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