Forescout eyeSight

Continuously discover, classify and assess devices to gain situational awareness and reduce risk

CIOs are assuming responsibility for securing increasing numbers of network-connected systems, especially IoT and OT devices. Since you can't secure what you can't see, this surge in numbers (and types) of devices is driving a collective sense of urgency for visibility into every connected physical and virtual device. That includes managed, unmanaged and unknown devices connected by employees, contractors and customers—or even by well-meaning operational staff. And no matter where all of these devices are on the network—in campus, data center, private and public cloud, and even medical, OT and ICS environments—they need to be properly detected, profiled and accounted for.

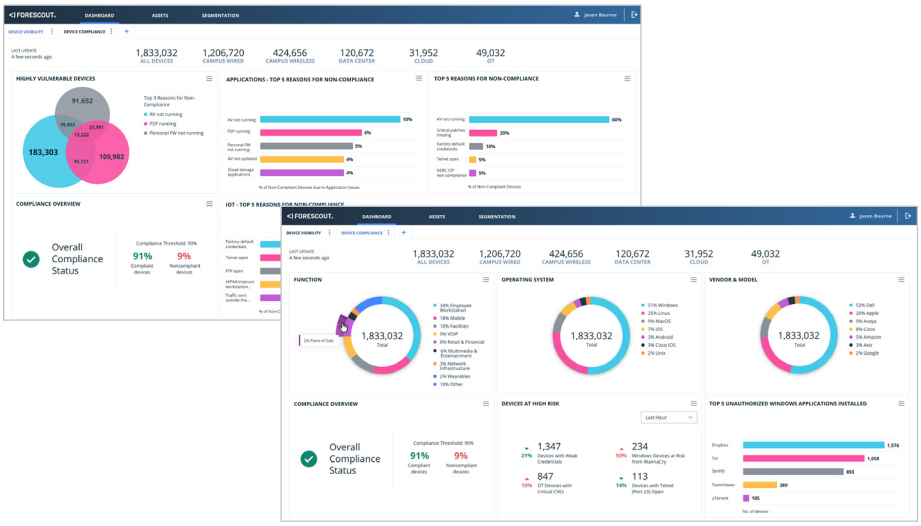


Figure 1: Out of the box Device Visibility and Device Compliance dashboards.

Forescout eyeSight gives you unparalleled insight into your entire device landscape without disrupting critical business processes. It starts by agentlessly discovering every IP-connected device across your extended enterprise networks. But discovery is just the first step toward complete visibility. To make the right policy and control decisions, comprehensive context is essential. After discovering connected devices, eyeSight then auto-classifies and assesses those devices against company policies. The powerful combination of these three capabilities—discovery, classification and assessment—delivers the device visibility to drive appropriate policies and actions.

eyeSight

Highlights

- Agentlessly gain a unified, real-time inventory of network-connected devices
- Accurately profile devices to gain required context for building proactive security and compliance policies
- Identify rogue, vulnerable or noncompliant devices and build policies to limit risk
- Gain real-time assurance that security tools and compliance controls are working
- Efficiently measure and report compliance posture and cyber risk exposure
- Automate common tasks to minimize human error and increase efficiency

DISCOVER

- See devices the instant they connect to the network
- Continuously monitor as devices come and go
- Get real-time asset inventory without business disruption

CLASSIFY

- Identify diverse types of IT, IoT and OT devices
- Harness the power of Forescout Device Cloud
- Improve auto-classification efficacy, coverage and velocity

ASSESS

- Identify security exposures and compliance gaps
- Assess adherence to internal and external mandates
- Gain situational awareness of cyber and operational risk

Continuous, Agentless Discovery

IoT and OT devices pose unique visibility challenges. The sheer volume of these devices creates a scale challenge because manual discovery is no longer feasible. Additionally, many of these devices can't support agents and are sensitive to active probing and scanning techniques that could cause system and business disruption. Using over 20 active and passive monitoring techniques (see Figure 2), eyeSight avoids potential visibility gaps by automatically discovering:

- Laptops, tablets, smartphones, BYOD/guest systems and IoT devices on campus networks
- Virtual machines, hypervisors and physical servers in data centers
- AWS, Azure and VMware instances across public and private clouds
- Medical, industrial and building automation devices on operational technology networks
- Physical and SDN infrastructure including switches, routers, VPNs, wireless access points and controllers

These visibility capabilities combine to minimize operational risk and eliminate visibility blind spots for a complete and continuous device inventory across the extended enterprise.

Figure 2: Active and passive discovery techniques.

PASSIVE TO INFRASTRUCTURE	PASSIVE TO END-DEVICE	ACTIVE TO END-DEVICE
SNMP traps	Network infrastructure polling	Agentless Windows inspection • WMI • RPC • SMB
SPAN traffic	SDN Integration • Meraki • Cisco ACI	Agentless macOS, Linux inspection • SSH
Flow Analysis • NetFlow • Flexible NetFlow • IPFIX • sFlow	Public/Private cloud integration • VMware • AWS • Azure	NMAP
DHCP requests	Query directory services (LDAP)	SNMP queries
HTTP user-agent	Query web applications (REST)	HTTP queries
TCP fingerprinting	Query databases (SQL)	SecureConnector®
Protocol parsing	eyeExtend orchestrations	
RADIUS requests		

Challenges

- Siloed teams, security tools and processes introduce visibility gaps
- Error-prone manual processes introduce operational and business risk
- Incomplete device intelligence gives IT little context to build defensible policies
- Inability to verify that security technologies are installed and operating properly wastes investment in those tools
- Undetected rogue devices cause unnecessary security and compliance risk
- Outdated, point-in-time scans cause a lack of confidence in compliance posture

Intelligent Auto-Classification

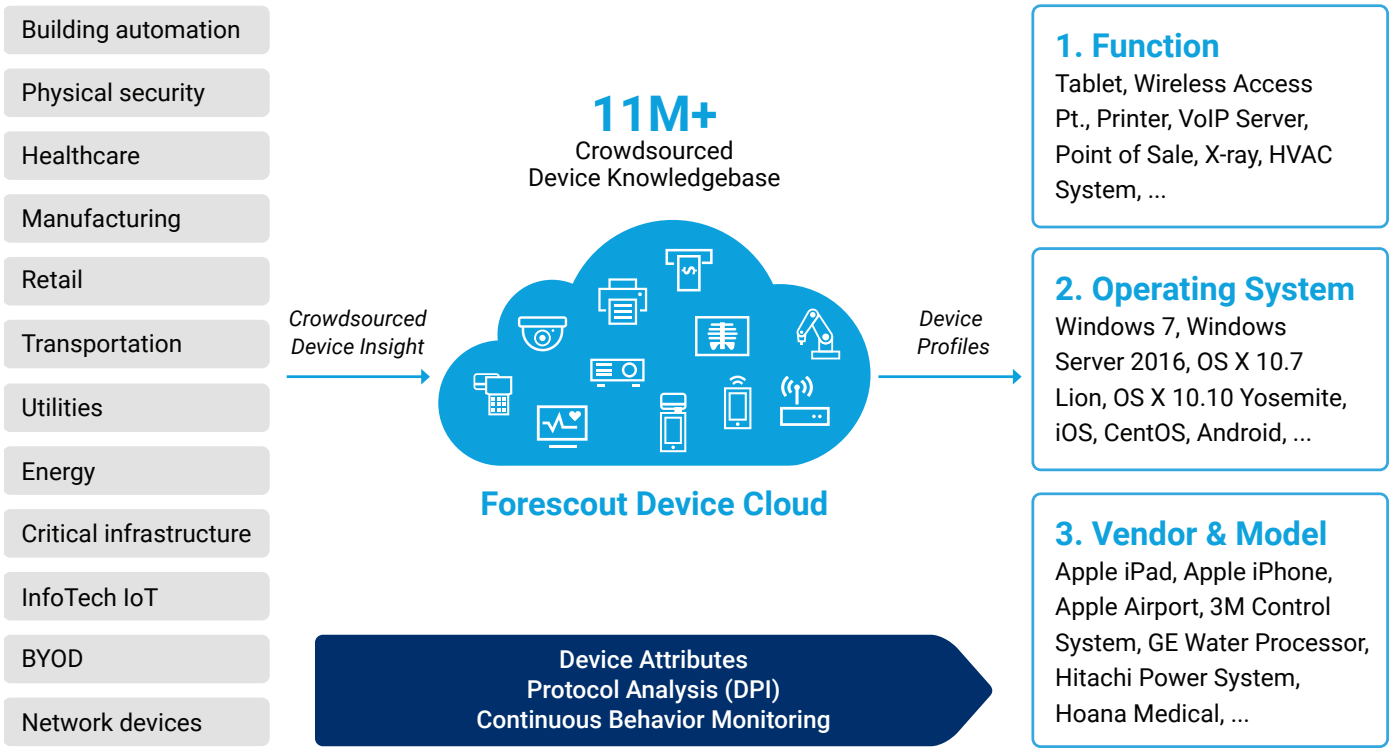
Complete context for every device is key to granular policy creation. You need to know the operational context or purpose of each device to decide how it is best secured and managed. The growth and diversity of devices makes manually gathering this context nearly impossible, and creating policies without proper context puts operations at risk. eyeSight 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. Deep packet inspection of over 100 IT and OT protocols allows eyeSight to gain in-depth insight about the identity of IoT and OT devices.

eyeSight auto-classifies:

- More than 600 different operating system versions
- Over 5,000 different device vendors and models
- Healthcare devices from over 350 leading 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 auto-classification in eyeSight, ensuring this rich source of context continues to keep pace with device growth and diversity. Forescout Research leverages intelligence from over 11 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.

Figure 3: Forescout Device Cloud.



As of January 15, 2020

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. eyeSight 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. eyeSight answers critical questions, including:

- 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 (and whether or not those devices are connected to the network)?
- Which of your connected devices are most vulnerable to the latest threats?

The Power of Device Intelligence

The device visibility that eyeSight provides through discovery, profiling, auto-classification and assessment is readily apparent in the Forescout console. High-level insights are automatically displayed in Device Visibility and Device Compliance dashboards, and you can easily create your own policy-based dashboards to share real-time progress towards your risk and compliance goals. These dynamic views help teams:

- Assess compliance across all policies, and the success of a particular policy or group of policies
- Identify vulnerable devices in the event of a breach to accelerate incident response
- Track adherence to specific compliance requirements over time
- Build executive- and auditor-ready views of risk and compliance as well as potential vulnerabilities
- In addition to the dashboard, the Asset View enables operators to quickly search and filter for assets related to a policy, or any property collected through classification. This greatly simplifies finding devices needing attention

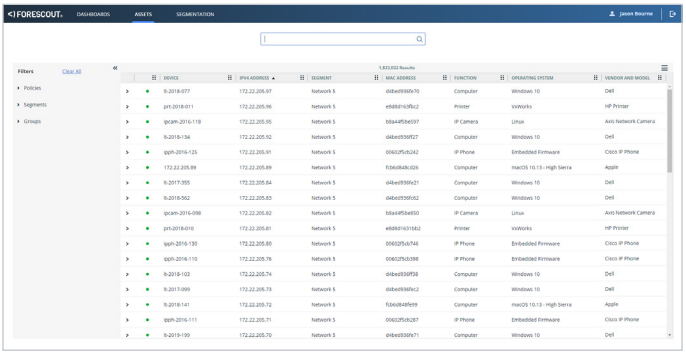


Figure 4: Web-based Asset View

The device visibility from eyeSight can also be shared with cross- functional IT stakeholders via notification actions and APIs. The eyeExtend portfolio of products shares this device context with other leading IT and security products to automate workflows and orchestrate system-wide response.

Without device context from eyeSight, organizations may lack the confidence to implement control policies. Taking action based on insufficient intelligence can put business operations at risk.

eyeSight gives you the in-depth insights you need to design and implement granular policies and automate actions for asset management, device compliance, network access, network segmentation and incident response. You can then establish effective policy-based controls and orchestrate actions with confidence using Forescout eyeSegment, eyeControl and eyeExtend products.

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