FORESCOUT
Active Defense for the Enterprise of Things.

eyeSight
Comprehensive Device Visibility

AGENTLESS
Gain a unified, real-time inventory of network-connected devices.

ACCURATE
Profile all devices to gain context for building proactive security and compliance.

EFFECTIVE
Identify rogue, vulnerable or noncompliant devices and build policies to limit risk.

DEPENDABLE
Gain real-time assurance that security tools and compliance controls are working.

EFFICIENT
Automatically measure and report compliance posture and cyber risk exposure while minimizing human error and increasing efficiency.

Continuously discover, classify and assess all connected things across your enterprise

Forescout eyeSight delivers unparalleled insight into your entire Enterprise of Things (EoT) without disrupting critical business processes.

- Discover every IP-connected device
- Auto-classify devices and gain comprehensive context
- Assess policy compliance and device security posture

DISCOVER
See devices the instant they connect to the network

Continuously monitor as transient 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 the 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

DISCOVER

Continuous agentless discovery

Eliminate blind spots and minimize operational risk with complete visibility across your EoT:

- Laptops, tablets, smartphones, BYOD/guest systems, work-from-home devices
- IoT devices in campus networks, data centers, branches, remote sites and edge networks
- Public and private cloud instances across AWS, Azure and VMware environments
- Operational technology (OT) systems including medical, industrial and building automation
- Physical and SDN infrastructure including switches, routers, wireless access points and controllers

Leverage the flexibility of 20+ active and passive monitoring techniques across wired, wireless, VPN, virtual and software-defined networks. Avoid disrupting devices that are sensitive to active scanning 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 Flow analysis • NetFlow • Flexible NetFlow • IPFIX • sFlow	SDN integration • Meraki • Cisco ACI	Agentless macOS, Linux inspection • SSH
DHCP requests	Public/Private cloud integration • VMware • AWS • Azure	NMAP
HTTP user-agent	Query directory services (LDAP)	SNMP queries
TCP fingerprinting	Query web applications (REST)	HTTP queries
Protocol parsing	Query databases (SQL)	SecureConnector®
RADIUS requests	eyeExtend orchestrations	

CLASSIFY

Intelligent auto-classification

Zero Trust policies can only be enforced when grounded in complete device context. Manually gathering this context is nearly impossible, and Zero Trust policies implemented without full device context can put operations at risk. With deep packet inspection of over 150 IT and OT protocols, eyeSight provides in-depth profiling of all IT, IoT and OT devices. Multi-dimensional classification taxonomy identifies device function and type, operating system and version, and vendor and model, including:

- More than 600 different operating system versions
- Over 5,700 different device vendors and models
- Healthcare devices from over 400 leading medical technology vendors
- Thousands of industrial control systems and automation devices used across manufacturing, energy, oil and gas, utilities, mining and other critical infrastructure industries

EYESIGHT SOLVES FOR:

Visibility gaps caused by siloed teams and disparate security tools

Operational and business risks due to error-prone manual processes

Incomplete device intelligence hindering the execution of defensible Zero Trust policies

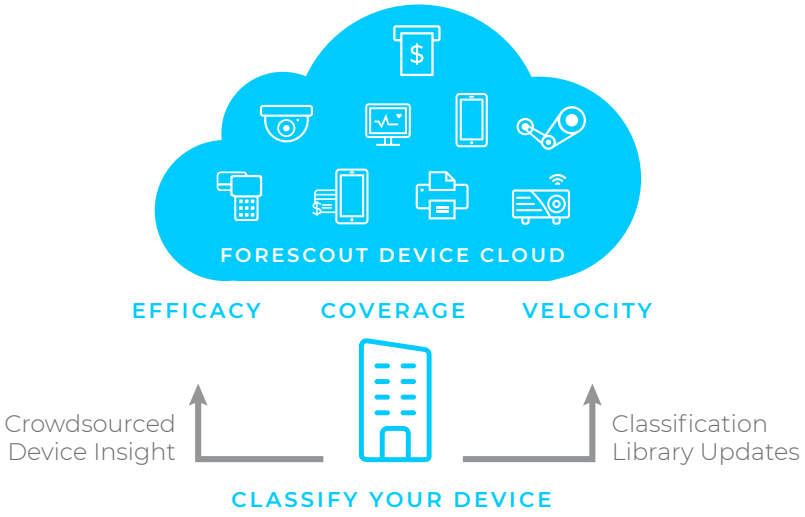
Security gaps when agent-based tools are not up to date or functioning properly

Undetected rogue devices or spoofing

Noncompliance that can quickly emerge between point-in-time scans

Auto-classification powered by Forescout Device Cloud

Device Cloud, the world's largest data lake of crowdsourced device intelligence, provides the most complete and accurate understanding of all device risks within the context of any organization.



Function +		Operating System +		Vendor & Model	
· Tablet	· Point of Sale	· Windows 7	· iOS	· Apple iPad	· GE Water Processor
· Wireless Access Pt.	· X-ray	· Windows Server 2016	· CentOS	· Apple iPhone	· Hitachi Power System
· Printer	· HVAC System	· OS X 10.7 Lion	· Android	· Apple Airport	· Hoana Medical
· VoIP Server		· OS X 10.10 Yosemite		· 3M Control System	

ASSESS

Device posture assessment

Another essential element of Zero Trust policies is to incorporate the security hygiene and risk profile of connecting devices. eyeSight continuously monitors the network to assess the configuration, security posture and risk indicators of connected devices and whether they adhere to compliance mandates and security standards. Zero Trust policies can be based on risk and compliance conditions such as:

- 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, especially IoT and OT systems, using default or weak passwords?
- Have rogue devices been detected, including those spoofing legitimate devices?
- Which of your connected devices are most vulnerable to the latest threats?

MONITOR

EoT visibility and compliance

Gain actionable insights from out-of-the-box and customizable dashboards to quickly pinpoint, prioritize and proactively mitigate risks across your connected things. Dynamic views help security analysts and SOC teams:

- Assess risk and compliance progress across all or any subset of policies
- Identify vulnerable and compromised devices to accelerate incident response
- Track compliance trends over time
- Personalize and share executive- and auditor-ready views of risk and compliance
- Quickly search and filter EoT assets by policy or device attributes

Segment, orchestrate and enforce

Extend the value of eyeSight with a suite of Forescout products to design and implement Zero Trust policies for network access control, IoT security, network segmentation and OT security. Visit www.forescout.com/platform/ to learn more about Forescout eyeSegment, eyeControl, eyeInspect and eyeExtend products.

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/eyeSight salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things.

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