

Forescout eyeManage

Centrally manage Forescout deployments across your extended enterprise


The Forescout platform helps organizations accelerate and optimize device visibility and control workflows throughout the extended enterprise. With such breadth and scale, having a single, centralized console to manage all aspects of your deployment eliminates jumping between different management tools. Forescout eyeManage communicates with Forescout appliances distributed throughout a network, aggregates device intelligence and provides a single pane of glass for overseeing all connected devices under Forescout management.

From eyeManage, customers can control devices, share risk and compliance insights with cross-functional stakeholders, and manage both policy creation and enforcement. Deployed as a physical or virtual appliance (on premises or in the AWS or Azure cloud), eyeManage installs out of band, avoiding latency or issues related to network disruption. Failover and recovery options through Forescout eyeRecover ensure availability of this business-critical application.



<p>Define Policy</p> <p>Create context-driven policies to minimize risk</p>	<p>Execute Controls</p> <p>Automate or initiate actions to manage risk</p>	<p>Share Dashboards</p> <p>Share risk & compliance insights with peers and executives</p>
<p>Search Inventory</p> <p>Quickly find any device connected to your networks</p>	<p>Manage Licenses</p> <p>Distribute licenses and manage software upgrades</p>	<p>Configure Deployment</p> <p>Provision and configure your Forescout deployment</p>

Figure 1. Centralized management for your complete Forescout deployment and operations.



Highlights

- <) Unify device inventory across campus, data center, cloud, IoT and OT
- <) Search and drill down from a centralized asset view
- <) Automate IP distribution, software upgrades and backups
- <) Expand deployment simply with zero-touch provisioning of new appliances
- <) Use pre-configured dashboards to quickly share visibility and compliance progress with executives
- <) Empower security operations with real-time snapshots of device posture
- <) Scale to 2M devices regardless of where those devices are deployed
- <) Centralize administration of licenses across the extended enterprise

Unified Device Management

In addition to managing appliances, eyeManage serves as a central console for managing devices, including validating asset inventory information, creating and managing security policies and executing native control actions. As Forescout eyeExtend products are added, eyeManage is also the central hub for communicating with other security and IT management products to orchestrate network and endpoint controls.

Asset inventory. All current activity, including processes, services, vulnerabilities, ports open or users logged in can be easily viewed in the inventory. eyeManage uncovers insights that can be used to track network activity, spot noncompliance and enhance policy creation. Device data gathered through discovery, classification and assessment capabilities in Forescout eyeSight can be viewed using asset views, allowing:

- Security staff to quickly locate and shut down switch ports to eliminate threats
- IT personnel to locate and contact users when maintenance is required on a device
- Help desk staff to link IP or MAC addresses and switch ports to devices in real time

Device	IP Address	Segment	MAC Address	Function	Operating System
h-2018-077	172.22.205.57	Network 5	048e0356f70	Computer	Windows 10
ipr-2018-011	172.22.205.56	Network 5	e8d61c3b2c2	Printer	Windows
ipcam-2018-118	172.22.205.95	Network 5	58aa4f5d597	IP Camera	Linux
h-2018-134	172.22.205.92	Network 5	0b8a4938f27	Computer	Windows 10
ipph-2018-125	172.22.205.91	Network 5	00627f5c242	IP Phone	Embedded Firmware
172.22.205.89	172.22.205.89	Network 5	726d6f60526	Computer	macOS 10.13 - High Sierra
h-2017-266	172.22.205.84	Network 5	048e939f621	Computer	Windows 10
h-2018-862	172.22.205.83	Network 5	048e939f62	Computer	Windows 10
ipcam-2018-098	172.22.205.82	Network 5	58aa4f5d590	IP Camera	Linux
ipr-2018-010	172.22.205.81	Network 5	e8d61c3b1b2	Printer	Windows
ipph-2018-130	172.22.205.80	Network 5	00627f5c126	IP Phone	Embedded Firmware
ipph-2018-110	172.22.205.76	Network 5	00627f5c398	IP Phone	Embedded Firmware
h-2018-103	172.22.205.74	Network 5	0b8a4938f18	Computer	Windows 10
h-2017-099	172.22.205.73	Network 5	048e939f612	Computer	Windows 10
h-2018-141	172.22.205.72	Network 5	58aa4f5d599	Computer	macOS 10.13 - High Sierra
ipph-2018-111	172.22.205.71	Network 5	00627f5c387	IP Phone	Embedded Firmware

Policy management. With the insights from the inventory at your fingertips, the Policy Manager in eyeManage enables you to create detailed, granular policies to protect your business. Policy templates help kick-start this process by guiding you to:

- ✓ Detect network devices based on classification
- ✓ Detect corporate, guest and unauthorized devices
- ✓ Understand compliance and guide remediation actions
- ✓ Detect and remediate threats to your network
- ✓ Track and identify unauthorized changes

Executing security controls. Networks are constantly changing with the addition of new device types, software, configurations and compliance requirements, as well as the evolving threat landscape. Dynamic policies help ensure controls continuously reflect the current state of the network and the devices connected to it. Security teams can use eyeManage to initiate control actions themselves as needed or choose to execute selected actions automatically.

User enforcement and education	Traffic control
Application control and remediation	Network restrictions
Operating system control and remediation	Device control

Figure 2: Actions can be automated or administrator-executed.

Security and IT management integrations. With the addition of eyeExtend products, many more control actions can be orchestrated from eyeManage. Adding eyeExtend for Palo Alto Networks® or eyeExtend for Splunk®, for example, enables information shared by these products to influence policies and control actions. eyeManage can help ensure information from the Forescout platform is delivered back to those eyeExtend products with bi-directional integrations. This information sharing can accelerate the resolution of security issues and streamline IT processes.

Monitoring and Risk Insight

Detailed views are essential for security architects who need granular data to build robust policies. But the executive team needs to prove to the board, auditors and customers how they measure up against regulations, or document their level of exposure to recently exploited vulnerabilities. Equally important, the SOC team monitoring the network also needs fast access to the current state of connected devices to ensure ongoing security. eyeManage elevates data from the Forescout platform to arm these teams with the insights they need to quickly respond.

Visualizing risk and compliance insights. Pre-configured device visibility and device compliance dashboards provide summaries of your device landscape, including overall compliance and security state across the extended enterprise. These snapshots of progress toward compliance goals that can be shared with executive teams and auditors for improved transparency and leadership confidence. You can also build specific views for security operations teams to reduce mean time to respond. Asset management teams can also build dashboards for a real-time inventory across distributed networks and geographies.

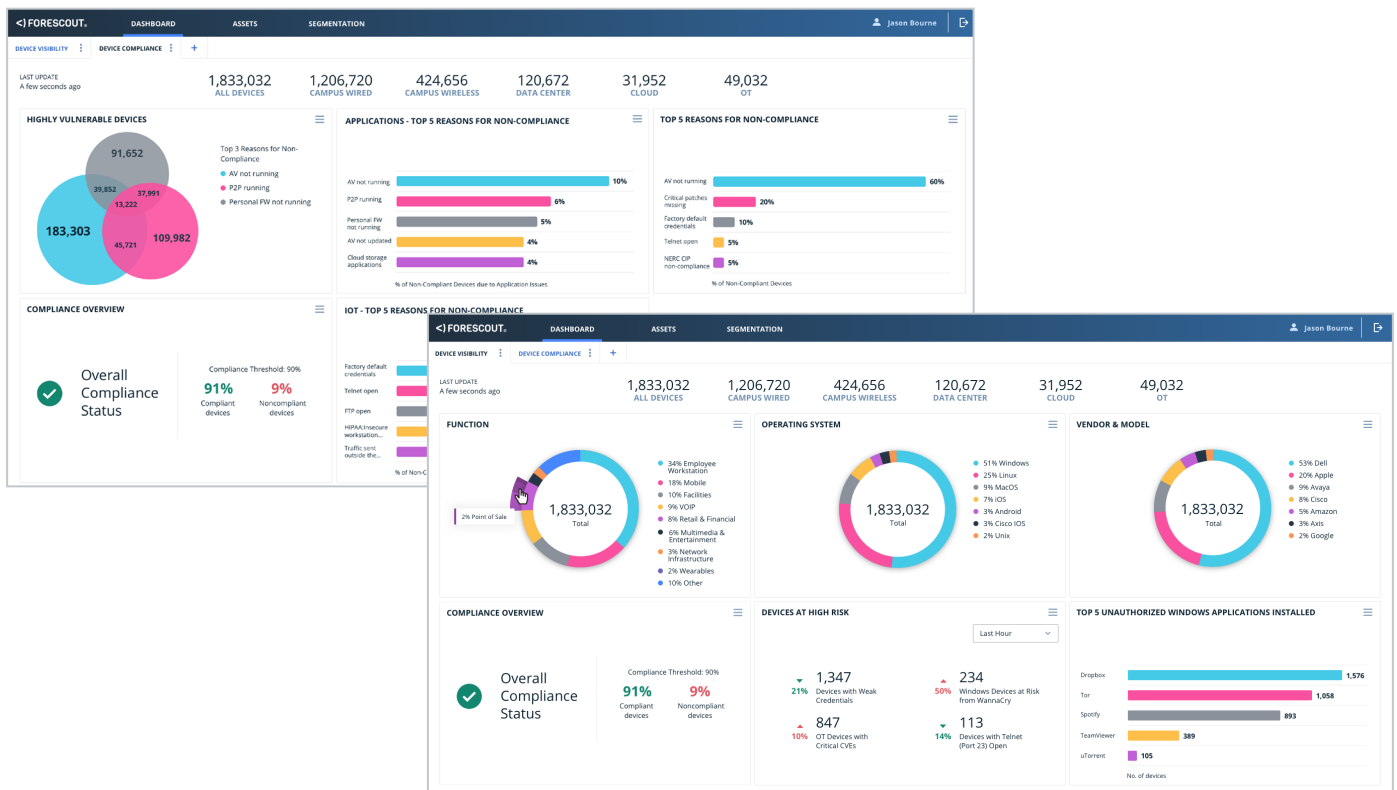


Figure 3: Real-time device visibility and device compliance dashboards visualize security state across the extended enterprise.

Centralized reporting. While dashboards present powerful summaries, more detail is often required to keep network administrators, executives, help desks, IT, security and other teams fully informed. eyeManage delivers reports, including current and trend information about policies, device compliance status, vulnerabilities, device details and network guests. Reports can be viewed, scheduled and saved to ensure automated and consistent reporting. Any language supported by your operating system can be used to generate reports, which can be saved in PDF and CSV formats.

Deployment Management at Scale

eyeManage combines management of your device landscape and your Forescout deployment in a single system. The scale, performance, deployment flexibility and license-management capabilities within eyeManage meet the stringent requirements of large, complex enterprise environments.

- **Scale to 2 million devices.** Organizations need a scalable platform for visibility across their device landscape. eyeManage provides a flexible management and deployment architecture for active customer deployments exceeding two million devices across physical, virtual, cloud and mixed environments.
- **Virtual appliance deployments.** Simplify and expedite product distribution and deployment, especially in distributed and remote sites, by deploying eyeManage as a virtual appliance. eyeManage can be deployed on VMware®, Hyper-V or KVM systems. The virtual appliance can also be deployed in AWS or Azure to further reduce your on-premises footprint.
- **Single-touch provisioning and expansion.** Configurations for Forescout appliances can be centrally managed at setup and pushed to the entire Forescout deployment. Updates can also be applied en masse, with a single keystroke, replicating settings to all Forescout appliances. As new appliances are added, they automatically inherit existing configurations.
- **Intelligent IP discovery and distribution.** Automate IP distribution and management across a multi-appliance cluster to reduce administration overhead associated with allocating IP ranges to individual appliances.
- **Centralized appliance administration.** Software upgrade files can be downloaded in eyeManage and installed according to your schedule. Backups can also be scheduled, and appliance restores initiated. Licenses associated with your Forescout deployment are also allocated and optimized through eyeManage.
- **Disaster recovery.** Automated failover and deployment resiliency are available through Forescout eyeRecover to ensure service continuity in single or multisite Forescout deployments. eyeRecover provides a choice of dedicated active-standby appliance pairs or failover clusters of active appliances that support intelligent reallocation of workloads from one or more failed nodes, clusters or entire sites. Administration is via the eyeManage console.



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](https://www.forescout.com)

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 02_20