

Forescout eyeManage

Zentrale Verwaltung von Forescout in Ihrem gesamten Unternehmen


Mit der Forescout-Plattform können Unternehmen die Gerätetransparenz- und Kontroll-Abläufe im gesamten Unternehmen beschleunigen sowie optimieren. Ein solcher Umfang macht eine zentrale Konsole unverzichtbar, mit der alle Aspekte Ihrer Forescout-Appliances verwaltet werden und die den Wechsel zwischen unterschiedlichen Verwaltungstools überflüssig macht. Forescout eyeManage kommuniziert mit den im Netzwerk verteilten Forescout-Appliances, aggregiert Geräteinformationen und stellt eine zentrale Übersicht aller verbundenen Geräte bereit, die von Forescout verwaltet werden.

Über eyeManage können Kunden Geräte kontrollieren, Risiko- und Konformitätsinformationen mit funktionsübergreifenden Verantwortlichen austauschen und sowohl die Richtlinienerstellung als auch die Durchsetzung verwalten. eyeManage wird als physische oder virtuelle Appliance (in der Private Cloud oder AWS- bzw. Azure-Public-Cloud) parallel zum bestehenden Netzwerk installiert, um Latenzprobleme und Netzwerkstörungen zu vermeiden. Dank der über Forescout eyeRecover bereitgestellten Failover- und Recovery-Optionen wird die Verfügbarkeit dieser geschäftskritischen Anwendung gewährleistet.



<p>Richtlinien definieren</p> <p>Erstellung kontextgesteuerter Richtlinien zur Verringerung von Risiken</p>	<p>Kontrollen durchführen</p> <p>Automatisierung oder Initiierung von Maßnahmen zur Eindämmung von Risiken</p>	<p>Dashboards freigeben</p> <p>Teilen von Informationen zu Risiken und Konformität mit Mitarbeitern und Führungskräften</p>
<p>Bestand durchsuchen</p> <p>Schnelles Auffinden aller Geräte, die mit Ihrem Netzwerk verbunden sind</p>	<p>Lizenzen verwalten</p> <p>Verteilung von Lizenzen und Verwaltung von Software-Upgrades</p>	<p>Bereitstellung konfigurieren</p> <p>Implementierung und Konfiguration Ihrer Forescout-Umgebung</p>

Abbildung 1. Zentrale Verwaltung und Betrieb Ihrer kompletten Forescout-Instanzen.



eyeManage

Kernpunkte

- <) Zentralisierung des Geräteinventars im Campus, Rechenzentrum, Cloud, IoT und OT
- <) Such- und Filtermöglichkeiten über eine zentrale Geräteübersicht
- <) Automatisierte IP-Zuweisung, Software-Upgrades und Backups
- <) Einfache Erweiterung der Bereitstellung mit automatisierter Implementierung neuer Appliances
- <) Vorkonfigurierte Dashboards zur Anzeige von Geräte- und Konformitätsinformationen vereinfacht die Weitergabe an Führungskräfte
- <) Erhöhung der Sicherheit durch Zustandsinformationen der Geräte in Echtzeit
- <) Skalierbar bis zu 2 Mio. Geräten unabhängig davon, wo diese Geräte eingesetzt werden
- <) Zentrale, unternehmensweite Lizenzverwaltung

Einheitliche Geräteverwaltung

Neben der Verwaltung von Appliances dient eyeManage als zentrale Konsole zur Verwaltung von Geräten, einschließlich der Überprüfung von Inventar-Bestandsinformationen, Erstellung und Verwaltung von Sicherheitsrichtlinien sowie Ausführung systemeigener Kontrollaktionen. Wenn Forescout eyeExtend-Produkte hinzugefügt werden, dient eyeManage auch als zentrale Schnittstelle für die Kommunikation mit anderen Sicherheits- und IT-Verwaltungsprodukten zur Koordinierung von Netzwerk- und Endgerätekontrollen.

Bestandsdatenbank: Alle aktuellen Aktivitäten einschließlich Prozessen, Services, Schwachstellen, offenen Ports oder angemeldeten Benutzern können im Inventar übersichtlich angezeigt werden. eyeManage deckt Informationen auf, mit denen Netzwerkaktivitäten verfolgt, Konformitäts Verstöße aufgedeckt und die Sicherheitsregeln optimiert werden können. Gerätedaten, die mit den Erkennungs-, Klassifizierungs- und Bewertungsfunktionen von Forescout eyeSight erfasst wurden, können in Bestandsübersichten durch verschiedene Filter angezeigt werden:

- Sicherheitsmitarbeiter können Switch-Ports schnell lokalisieren und deaktivieren, um Bedrohungen zu stoppen.
- IT-Mitarbeiter können Benutzer lokalisieren und kontaktieren, wenn Wartungsmaßnahmen für ein Gerät notwendig werden.
- Helpdesk-Mitarbeiter können die Zuordnung von IP-, MAC-Adressen oder Switchports in Echtzeit abrufen.

Device	IP Address	Segment	MAC Address	Function	Operating System
R-2018-077	172.22.205.97	Network 5	d48e939870	Computer	Windows 10
prh-2018-011	172.22.205.96	Network 5	e1881f1278c2	Printer	Windows
ipcam-2016-118	172.22.205.95	Network 5	53aa475a1937	IP Camera	Linux
R-2018-134	172.22.205.92	Network 5	d48e939870	Computer	Windows 10
ipph-2016-125	172.22.205.91	Network 5	00022f5b3242	IP Phone	Embedded Firmware
172.22.205.89	172.22.205.89	Network 5	f86d8481d26	Computer	macOS 10.13 - High Sierra
R-2017-885	172.22.205.84	Network 5	d48e939870	Computer	Windows 10
R-2018-562	172.22.205.83	Network 5	d48e939870	Computer	Windows 10
ipcam-2016-098	172.22.205.82	Network 5	53aa475a1937	IP Camera	Linux
prh-2018-010	172.22.205.81	Network 5	e1881f1278c2	Printer	Windows
ipph-2016-130	172.22.205.80	Network 5	00022f5b3242	IP Phone	Embedded Firmware
ipph-2016-110	172.22.205.76	Network 5	00022f5b3242	IP Phone	Embedded Firmware
R-2018-103	172.22.205.74	Network 5	d48e939870	Computer	Windows 10
R-2017-099	172.22.205.73	Network 5	d48e939870	Computer	Windows 10
R-2018-141	172.22.205.72	Network 5	f86d8481d26	Computer	macOS 10.13 - High Sierra
ipph-2016-111	172.22.205.71	Network 5	00022f5b3242	IP Phone	Embedded Firmware

Richtlinienverwaltung: Mit den Inventarinformationen lassen sich im Richtlinien-Manager von eyeManage detaillierte Richtlinien erstellen, die Ihr Unternehmen zuverlässig schützen. Richtlinienvorlagen für folgende Einsatzbereiche beschleunigen diesen Prozess:

- ✓ Erkennung von Netzwerkgeräten anhand der Klassifizierung
- ✓ Erkennung von unternehmenseigenen, nicht autorisierten sowie Gast-Geräten
- ✓ Bewertung der Compliance sowie Koordinierung von Abhilfemaßnahmen

- ✓ Erkennung und Behebung von Bedrohungen für Ihr Netzwerk
- ✓ Überwachung und Aufdeckung unberechtigter Änderungen

Ausführung von Sicherheitskontrollen: Netzwerke sind ständigen Veränderungen durch neue Gerätetypen, Software, Konfigurationen und Konformitätsanforderungen unterworfen. Hinzu kommt eine sehr wandlungsfähige Bedrohungslage. Mit dynamischen Richtlinien kann gewährleistet werden, dass die permanente Kontrolle des Netzwerkzustands und der Geräte, die mit ihm verbunden sind, sichergestellt wird. Sicherheitsteams können mithilfe von eyeManage Kontrollaktionen nach Bedarf manuell initiieren oder die ausgewählten Aktionen automatisch ausführen lassen.

Durchsetzung von Benutzermaßnahmen und	Datenverkehrkontrolle
Applikationskontrolle und Problembehebung	Netzwerkbeschränkungen
Kontrolle und Problembehebung für das Betriebssystem	Gerätekontrolle

Abbildung 2. Aktionen können automatisiert oder vom Administrator durchgeführt werden.

Sicherheits- und IT-Verwaltungsintegrationen: Durch den Einsatz von eyeExtend-Produkten können viele weitere Kontrolloperationen über eyeManage koordiniert werden. Beispielsweise können mit Hilfe von eyeExtend für Palo Alto Networks® oder eyeExtend für Splunk® Informationen aus diesen Produkten weitergegeben werden, die sich auf Richtlinien und Kontrollaktionen auswirken. Außerdem lässt sich mit eyeManage gewährleisten, dass Informationen aus der Forescout-Plattform über bidirektionale Integrationen zurück an diese eyeExtend-Produkte übertragen werden. Dieser Informationsaustausch kann die Behebung von Sicherheitsproblemen beschleunigen und IT-Prozesse optimieren.

Monitoring und Risikoinformationen

Detaillierte Ansichten sind für Sicherheitsarchitekten unverzichtbar, die anhand detaillierter Daten zuverlässige Richtlinien erstellen sollen. Doch Führungskräfte müssen dem Vorstand, Wirtschaftsprüfern und Kunden demonstrieren können, dass bestimmte Regularien eingehalten werden, oder dokumentieren, inwieweit gegen Schwachstellen vorgegangen wurde. Ebenso wichtig ist, dass das SOC-Team bei der Überwachung des Netzwerks zeitnahen Zugriff auf die Echtzeitdaten der angeschlossenen Geräte abrufen kann. eyeManage nutzt Daten der Forescout-Plattform, um all diesen Verantwortlichen die notwendigen Informationen für schnelle Erkennung und Reaktion bei Risiken zu liefern.

Visualisierung von Risiko- und Konformitätsinformationen: Vordefinierte Geräteübersichts- und Konformitäts-Dashboards liefern Zusammenfassungen zu Ihrer Betriebslage, einschließlich Informationen zur allgemeinen Konformitäts- und Sicherheitslage im gesamten Unternehmen. Hierdurch erhalten Sie Momentaufnahmen über die Fortschritte zur Erreichung der Konformitätsziele, die an das Management und Wirtschaftsprüfer weitergegeben werden können und somit Transparenz sowie Vertrauen schaffen.

Die Ansichten der Security Operations-Teams lassen sich anpassen, um die mittlere Reaktionszeit zu verringern. Außerdem können die für die Geräteverwaltung und Inventarisierung verantwortlichen Mitarbeiter Echtzeit-Dashboards zur Bestandsaufnahme in großen, geografisch verteilten Netzwerken erstellen.

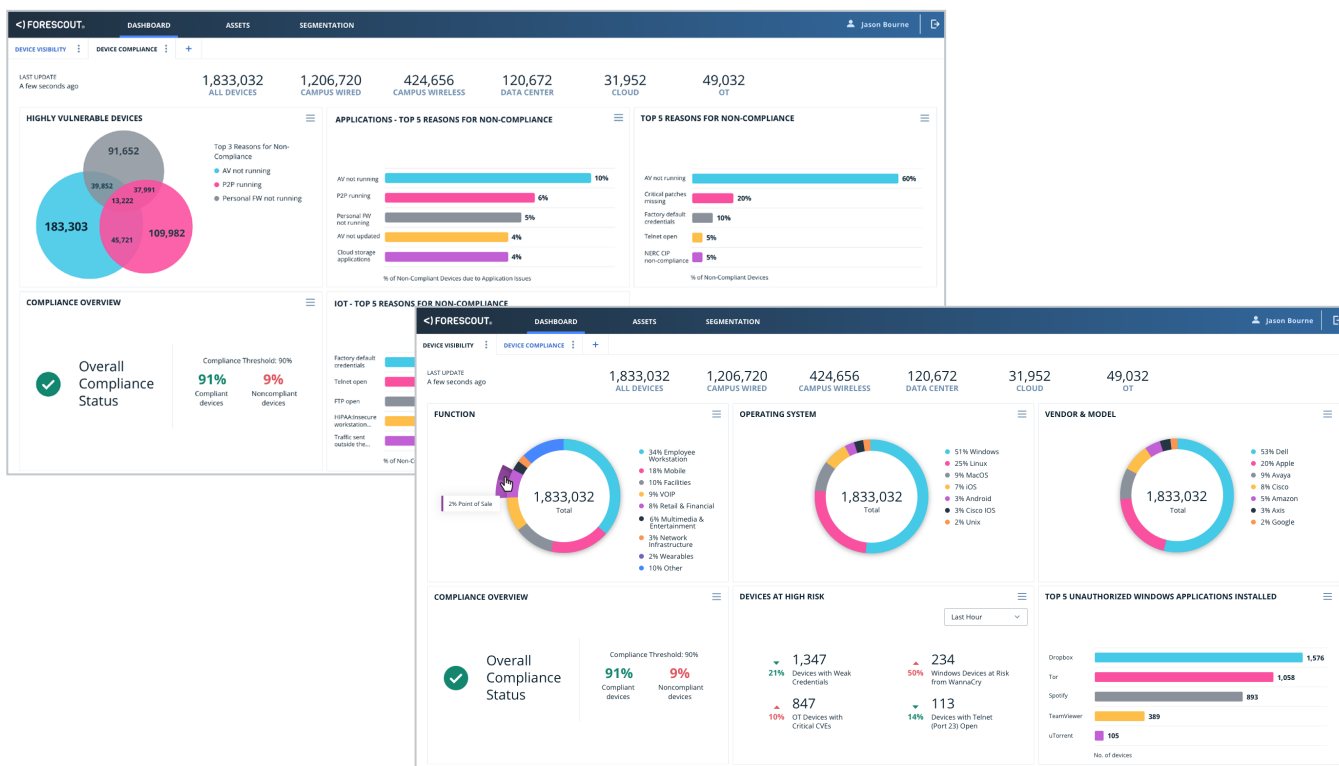


Abbildung 3. Dashboards für Gerätetransparenz und -konformität zeigen in Echtzeit den unternehmensweiten Sicherheitsstatus.

Zentrale Berichterstattung: Auch wenn Dashboards leistungsstarke Zusammenfassungen bieten, sind häufig weitere Details erforderlich, damit Netzwerkadministratoren, Führungskräfte, Helpdesk-Mitarbeiter sowie IT-, Sicherheits- und weitere Teams umfassend informiert sind. eyeManage erstellt Berichte, darunter aktuelle und Trend-Informationen über Richtlinien, Geräte-Compliance-Status, Schwachstellen, Gerätedetails und Netzwerk Gäste. Die Berichte können angezeigt, geplant und gespeichert werden, sodass die automatisierte und einheitliche Berichterstattung gewährleistet ist. Berichte können in jeder von Ihrem Betriebssystem unterstützten Sprache generiert und im PDF- und CSV-Format gespeichert werden.

Skalierbare Verwaltung

eyeManage verbindet die Verwaltung der Geräteumgebung und Ihre Forescout-Instanzen in einem einzigen System. Die Skalierung, Leistung, Einsatzflexibilität und Lizenzverwaltungsfunktionen von eyeManage genügen auch den anspruchsvollen Anforderungen großer und komplexer Unternehmensumgebungen.

- **Skalierung bis zu 2 Millionen Geräte:** Unternehmen benötigen eine skalierbare Plattform, die einen Überblick über den gesamten Gerätebestand liefert. Deshalb bietet eyeManage eine flexible Verwaltungs- und Installationsarchitektur für aktive Kundenbereitstellungen mit mehr als 2 Millionen Geräten in physischen, virtuellen und Cloud- und Hybridumgebungen.
- **Virtuelle Appliance-Bereitstellungen:** Der Einsatz von eyeManage als virtuelle Appliance ermöglicht die vereinfachte und schnellere Produktverteilung und Installation, insbesondere bei verteilten und entfernten Standorten. eyeManage kann auf VMware®, Hyper-V- oder KVM-Systemen genutzt werden.
- **Einfache Installation und Erweiterung:** Konfigurationen für Forescout-Appliances können bei der Einrichtung zentral festgelegt und für alle Forescout-Appliances freigegeben werden. Auch Updates können mit einem einzigen Mausklick angestoßen und auf allen Forescout-Appliances verteilt werden. Wenn neue Appliances hinzugefügt werden, enthält diese automatisch die bestehenden Konfigurationen.
- **Intelligente Erkennung und Verteilung von IP-Adressen:** Sie können die IP-Verteilung und -Verwaltung in einem Cluster mit mehreren Appliances automatisieren, um den Verwaltungsaufwand bei der Zuweisung von IP-Bereichen für einzelne Appliances zu reduzieren.
- **Zentralisierte Appliance-Verwaltung:** Software-Upgrade-Dateien können in eyeManage heruntergeladen und gemäß eines Zeitplans installiert werden. Zudem können Backups und Wiederherstellungsoperationen geplant und durchgeführt werden. Auch die Lizenzen für Ihre Forescout-Umgebung werden in eyeManage zugewiesen und optimiert.
- **Disaster Recovery:** Forescout eyeRecover bietet automatisiertes Failover und Ausfallsicherheit, sodass der Dauerbetrieb der Forescout-Umgebung an allen Unternehmensstandorten gewährleistet ist. Dabei bietet eyeRecover eine Auswahl an dedizierten Active-Standby-Gerätepaaren oder Failover-Clustern, die eine intelligente Neuzuweisung der Arbeitslast von einem oder mehreren ausgefallenen Knoten, Clustern oder ganzen Standorten erlauben. Die Verwaltung erfolgt über die eyeManage-Konsole.



Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

E-Mail: info-dach@forescout.com
Telefon international:
+1-408-213-3191
Support +1-708-237-6591

Weitere Informationen unter [Forescout.de](https://forescout.de)

© 2020 Forescout Technologies, Inc. Alle Rechte vorbehalten. Forescout Technologies, Inc. ist ein Unternehmen aus Delaware. Eine Liste unserer Marken und Patente finden Sie unter <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Andere genannte Marken, Produkte oder Servicenamen können Marken oder Servicemarken ihrer jeweiligen Eigentümer sein.
Version 02_20