

# Forescout eyeManage

## Gestione a livello centralizzato delle distribuzioni di Forescout nell'azienda estesa

La piattaforma Forescout permette alle aziende di accelerare e ottimizzare la visibilità dei dispositivi e di controllare i flussi di lavoro in tutta l'azienda estesa. Su una scala così vasta, una singola console centralizzata per gestire tutti gli aspetti della tua distribuzione elimina la necessità di passare continuamente da uno strumento di gestione all'altro. Forescout eyeManage comunica con le appliance di Forescout distribuite nella rete, aggrega le informazioni sui dispositivi e offre un singolo pannello di controllo per supervisionare tutti i dispositivi connessi sotto la gestione Forescout.

Da eyeManage i clienti possono controllare i dispositivi, condividere i rischi e le analisi della conformità con le parti interessate di diverse aree funzionali e gestire sia la creazione delle policy che la loro imposizione. Distribuito come appliance fisica o virtuale in sede, nel cloud di AWS o di Azure, eyeManage si installa fuori banda, evitando la latenza e i problemi legati alle interruzioni della rete. Le opzioni di failover e ripristino tramite Forescout eyeRecover assicurano la disponibilità di quest'applicazione critica per l'azienda.



<p><b>Definisci le policy</b></p> <p>Crea policy basate sul contesto per ridurre al minimo i rischi</p>	<p><b>Esegui i controlli</b></p> <p>Automatizza o avvia le azioni per gestire il rischio</p>	<p><b>Dashboard condivise</b></p> <p>Condividi gli approfondimenti su rischi e conformità con colleghi e dirigenti esecutivi</p>
<p><b>Inventario delle ricerche</b></p> <p>Trova rapidamente qualsiasi dispositivo connesso alle tue reti</p>	<p><b>Gestisci le licenze</b></p> <p>Distribuisce le licenze e gestisci gli upgrade del software</p>	<p><b>Configura la distribuzione</b></p> <p>Configura la tua distribuzione Forescout</p>

Figura 1. La gestione centralizzata per tutte le tue distribuzioni e operazioni Forescout.



### In breve

- <) Unifica l'inventario dei dispositivi fra ambiente fisico, data center, cloud, IoT e OT
- <) Esegui ricerche e analisi approfondite da una console di visualizzazione delle risorse centralizzata
- <) Automatizza la distribuzione IP, gli upgrade del software e i backup
- <) Amplia la distribuzione in modo semplice con la configurazione delle nuove appliance senza intervento
- <) Usa dashboard preconfigurate per condividere rapidamente i dati di visibilità e conformità con i dirigenti esecutivi
- <) Aiuta le operazioni di sicurezza con istantanee in tempo reale sulla condizione dei dispositivi
- <) Proteggi fino a due milioni di dispositivi a prescindere da dove sono impiegati
- <) Centralizza l'amministrazione delle licenze nell'azienda estesa

## Gestione unificata dei dispositivi

eyeManage funge da console centrale per gestire non solo le appliance ma anche i dispositivi e comprende la convalida delle informazioni dell'inventario delle risorse, la creazione e gestione delle policy di sicurezza e l'esecuzione di azioni di controllo native. Mano a mano che vengono aggiunti altri prodotti Forescout eyeExtend, eyeManage è inoltre il fulcro centrale delle comunicazioni con i prodotti di sicurezza e di gestione IT per coordinare i controlli della rete e degli endpoint.

**Inventario delle risorse.** Tutte le attività correnti, compresi processi, servizi, vulnerabilità, porte aperte o utenti connessi, possono essere facilmente visualizzati nell'inventario. eyeManage offre delle informazioni utilizzabili per monitorare l'attività della rete, individuare la non conformità e potenziare la creazione delle policy. I dati dei dispositivi, raccolti tramite le capacità di rilevamento, classificazione e valutazione in Forescout eyeSight, possono essere consultati in apposite visualizzazioni. In tal modo:

- il personale di sicurezza può individuare e chiudere rapidamente le porte degli switch per eliminare le minacce;
- il personale informatico può individuare e contattare gli utenti quando un dispositivo ha bisogno di manutenzione;
- il personale dell'help desk può collegare gli indirizzi IP o MAC e le porte degli switch ai dispositivi in tempo reale.

Filters	Device ID	IP Address	MAC Address	Vendor	Model	Function	Operating System
• Filtri	9-2018-077	172.22.205.97	945e939f7670	Network S	Computer	Windows 10	
• Segmento	9m-2018-011	172.22.205.96	e4581c2f8c2	Network S	Printer	Windows	
• Gruppo	9cam-2016-118	172.22.205.95	3a3a4f5a0197	Network S	IP Camera	Linux	
	9-2018-134	172.22.205.92	945e939f7670	Network S	Computer	Windows 10	
	9ph-2018-125	172.22.205.91	00002f5b766	Network S	IP Phone	Embedded Firmware	
	172.22.205.89	172.22.205.89	f956d848d24	Network S	Computer	macOS 10.13 - High Sierra	
	9-2017-955	172.22.205.84	945e939f7670	Network S	Computer	Windows 10	
	9-2018-562	172.22.205.83	945e939f7670	Network S	Computer	Windows 10	
	9cam-2016-098	172.22.205.82	33a44f5a0197	Network S	IP Camera	Linux	
	9m-2018-010	172.22.205.81	e4581c2f8c2	Network S	Printer	Windows	
	9ph-2016-130	172.22.205.80	00002f5b766	Network S	IP Phone	Embedded Firmware	
	9ph-2016-110	172.22.205.76	00002f5b766	Network S	IP Phone	Embedded Firmware	
	9-2018-103	172.22.205.74	945e939f7670	Network S	Computer	Windows 10	
	9-2017-099	172.22.205.73	945e939f7670	Network S	Computer	Windows 10	
	9-2018-141	172.22.205.72	f956d848d24	Network S	Computer	macOS 10.13 - High Sierra	
	9ph-2016-111	172.22.205.71	00002f5b766	Network S	IP Phone	Embedded Firmware	

**Gestione delle policy.** Con i dati dell'inventario a portata di mano e la gestione delle policy in eyeManage, puoi creare policy dettagliate e granulari per proteggere l'impresa. I modelli delle policy permettono di iniziare questo processo guidandoti nel:

- ✓ rilevare i dispositivi della rete in base alla classificazione;
- ✓ rilevare i dispositivi aziendali, ospiti e non autorizzati;
- ✓ valutare la conformità e indirizzare le azioni di risanamento;
- ✓ rilevare ed eliminare le minacce alla tua rete;
- ✓ monitorare e identificare le modifiche non autorizzate.

**Esecuzione dei controlli di sicurezza.** Le reti cambiano costantemente con l'aggiunta di nuovi tipi di dispositivo, software, configurazioni e requisiti di conformità, oltre che con l'evoluzione del panorama delle minacce. Le policy dinamiche assicurano che i controlli riflettano continuamente lo stato corrente della rete e i dispositivi a essa connessi. Gli addetti alla sicurezza possono usare eyeManage per avviare le azioni di controllo loro stessi quando necessario oppure scegliere di eseguire automaticamente le azioni selezionate.

Imposizione e formazione degli utenti	Controllo del traffico
Controllo delle applicazioni e risanamento	Restrizioni della rete
Controllo e risanamento del sistema operativo	Controllo dei dispositivi

Figura 2. le azioni possono essere automatizzate oppure eseguite dall'amministratore.

**Integrazioni fra sicurezza e gestione IT.** Con l'aggiunta dei prodotti eyeExtend, molte più azioni di controllo possono essere coordinate da eyeManage. Aggiungendo per esempio eyeExtend per Palo Alto Networks® oppure eyeExtend per Splunk®, si possono condividere le informazioni provenienti da questi prodotti per influenzare le policy e le azioni di controllo. eyeManage assicura che le informazioni della piattaforma Forescout vengano reinviata ai prodotti eyeExtend con integrazioni bidirezionali. Tale condivisione delle informazioni accelera la risoluzione dei problemi di sicurezza e semplifica i processi IT.

## Monitoraggio e approfondimenti sui rischi

Le viste dettagliate sono essenziali per gli architetti della sicurezza, che necessitano di dati granulari per costruire delle policy robuste. Ma i dirigenti esecutivi devono dimostrare a CdA, verificatori e clienti il rispetto dei regolamenti o di documentare il livello di esposizione alle vulnerabilità sfruttate di recente. Non meno importante è l'esigenza degli addetti del SOC che monitorano la rete di accedere velocemente allo stato corrente dei dispositivi connessi, per assicurare la continuità della protezione. A questo scopo eyeManage preleva dalla piattaforma Forescout le informazioni necessarie ai dirigenti per rispondere rapidamente.

**Visualizzazione delle informazioni sui rischi e la conformità.** Speciali dashboard preconfigurate che raccolgono dati sulla visibilità e la conformità forniscono un quadro chiaro sul panorama dei dispositivi, compreso lo stato complessivo di conformità e sicurezza dell'intero ambiente aziendale. Queste istantanee dei progressi compiuti verso gli obiettivi di conformità possono essere condivise con dirigenti esecutivi e verificatori per aumentare trasparenza e fiducia nei responsabili.

Le visualizzazioni possono essere create appositamente per gli addetti alla sicurezza in modo da ridurne il tempo medio di risposta. I gruppi di gestione delle risorse possono creare le dashboard per tenere sotto controllo in tempo reale l'inventario delle risorse su reti distribuite e varie località geografiche.

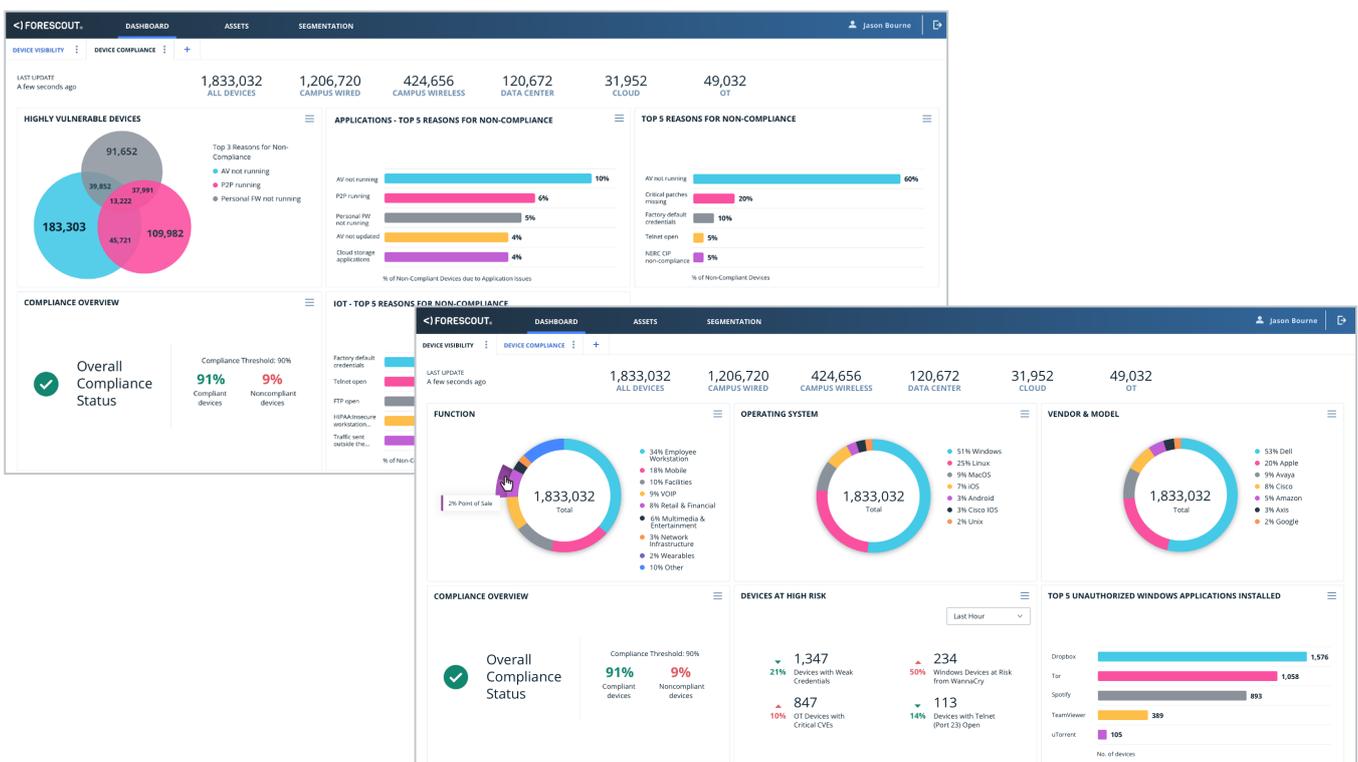


Figura 3. Dashboard che raccolgono dati sulla visibilità e la conformità in tempo reale visualizzano lo stato della sicurezza dell'intero ambiente aziendale.

**Reportistica centralizzata.** Anche se le dashboard offrono dei riepiloghi molto utili, spesso sono necessari maggiori dettagli per mantenere pienamente informati amministratori di rete, dirigenti esecutivi, help desk, addetti alla sicurezza informatica e altri gruppi. I report di eyeManage includono le informazioni attuali e tendenziali sulle policy, lo stato di conformità dei dispositivi, le vulnerabilità, i dettagli dei dispositivi e gli ospiti connessi alla rete. I report possono essere visualizzati, pianificati e salvati per automatizzarli e renderli coerenti. Possono inoltre essere generati in qualsiasi lingua supportata dal tuo sistema operativo e salvati nei formati PDF e CSV.

## Gestione della distribuzione su vasta scala

eyeManage combina in un unico sistema la gestione dei dispositivi e la distribuzione Forescout. La scalabilità, le prestazioni, la flessibilità della distribuzione e le capacità di gestione delle licenze in eyeManage soddisfano le rigorose esigenze degli ambienti aziendali più grandi e complessi.

- **Scalabile fino a 2 milioni di dispositivi.** Le organizzazioni necessitano di una piattaforma scalabile, che dia visibilità su tutto il panorama dei dispositivi. eyeManage fornisce un'architettura flessibile di gestione e distribuzione, per le distribuzioni attive dei clienti che superano i due milioni di dispositivi negli ambienti fisici, virtuali, cloud e misti.
- **Distribuzioni delle appliance virtuali.** Semplifica e velocizza il dispiegamento e l'installazione dei prodotti, soprattutto nei siti distribuiti e remoti, impiegando eyeManage come appliance virtuale. eyeManage è installabile nei sistemi VMware®, Hyper-V e KVM. Per ridurre ulteriormente l'impatto nell'ambiente locale, l'appliance virtuale può essere distribuita in AWS o Azure.
- **Configurazione ed espansione con un solo tocco.** Le configurazioni per le appliance Forescout possono essere gestite centralmente al momento dell'impostazione e poi applicate all'intera distribuzione Forescout. Anche gli aggiornamenti possono essere applicati in massa, con la semplice pressione di un tasto, replicando le impostazioni in tutte le appliance Forescout. E quando vengono aggiunte delle nuove appliance, queste ereditano automaticamente le configurazioni esistenti.
- **Scoperta e distribuzione intelligente degli IP.** Automatizza la distribuzione e gestione degli IP in un cluster multi-appliance per ridurre i carichi amministrativi associati all'allocazione degli intervalli IP alle singole appliance.
- **Amministrazione centralizzata delle appliance.** I file di upgrade del software possono essere scaricati in eyeManage e installati secondo la tua pianificazione, che include i backup. Puoi anche avviare i ripristini delle appliance. In eyeManage puoi inoltre allocare e ottimizzare le licenze associate alla tua distribuzione Forescout.
- **Disaster recovery.** Forescout eyeRecover mette a disposizione il failover automatizzato e la resilienza della distribuzione, per assicurare la continuità del servizio nelle distribuzioni di Forescout singole o multisito. eyeRecover offre la scelta fra coppie di appliance dedicate (attiva - in attesa) e cluster di failover delle appliance attive che riallocano in modo intelligente i carichi di lavoro dei nodi, cluster o siti interi colpiti da un guasto. L'amministrazione viene eseguita tramite la console eyeManage.



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

E-mail: [info-italia@forescout.com](mailto:info-italia@forescout.com)  
Tel. (internazionale) +1-408-213-3191  
Supporto tecnico 1-708-237-6591

Maggiori informazioni su [forescout.com](https://forescout.com)

© 2020 Forescout Technologies, Inc. Reservados todos los derechos. Forescout Technologies, Inc. es una empresa de Delaware. Encontrará una lista de marcas comerciales y patentes en <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Los demás nombres de marcas, productos o servicios pueden ser marcas comerciales o marcas de servicios de sus respectivos propietarios. Version 02\_20