FORESCOUT

Le novità di Forescout 8.2

"Nel 2023, il numero complessivo dei dispositivi IoT 'connessi' nel mondo supererà i 35,2 miliardi."

– Worldwide Internet of Things Infrastructure Forecast, 2019-2023, IDC

Gli attacchi del decennio appena trascorso ci hanno insegnato che basta un singolo punto debole in una rete per rendere un'organizzazione vulnerabile alle violazioni. Mentre cresce il numero dei dispositivi IoT e degli altri dispositivi non gestiti collegati alle intranet aziendali sull'onda della trasformazione digitale, urge trovare un equilibrio tra l'innovazione e l'obiettivo, altrettanto essenziale, di rendere sicuri questi dispositivi e salvaguardare le reti.

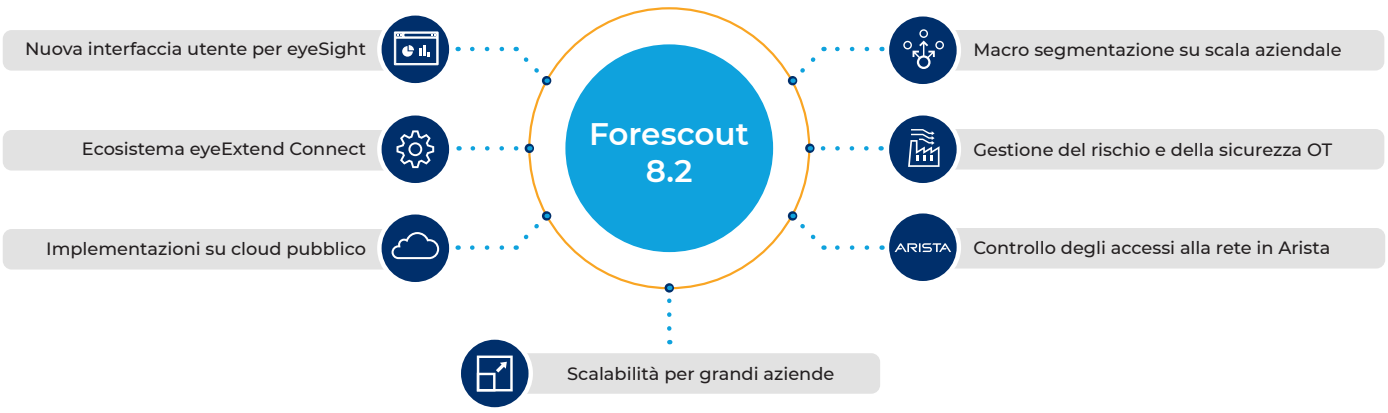
Senza un quadro completo dei dispositivi connessi nei vari domini della rete, la capacità di agire in fretta per mitigare i rischi è praticamente nulla. Dispositivi obsoleti e vulnerabili, endpoint non conformi e non adeguatamente configurati e dispositivi IoT e OT devono essere tutti identificati. I rischi per tutte le reti e le sedi interconnesse devono essere valutati di continuo. Questa visibilità completa determina la capacità di agire in fretta.

Forescout 8.2: maggiore rapidità di rilevamento e intervento

Forescout 8.2 consente di identificare più velocemente tutti i dispositivi connessi, le lacune nella conformità e i rischi sulla vostra rete. Vi permette di intervenire rapidamente e in modo sicuro per mitigare le falle di sicurezza e ridurre il tempo medio di risposta (MTTR) nell'intera rete aziendale estesa.

Le sue caratteristiche principali sono:

- Nuova interfaccia utente su misura a seconda del ruolo per Forescout eyeSight, con dati contestuali fruibili sui dispositivi per individuare, definire le priorità e mitigare in modo proattivo i rischi
- Forescout eyeExtend Connect, un nuovo ecosistema di app basato su community che consente a clienti e partner di sviluppare, utilizzare e condividere più facilmente app per l'integrazione con la piattaforma Forescout
- Nuova flessibilità di implementazione e time to value più breve per le organizzazioni operanti prevalentemente su cloud che desiderano implementare appliance Forescout in ambienti cloud pubblici AWS e Microsoft Azure
- Segmentazione su scala aziendale con Forescout eyeSegment per consentire alle aziende di progettare e implementare policy in completa sicurezza su vari domini di rete e punti di controllo eterogenei
- Integrazione con Forescout SilentDefense™, oltre che con sensori IT/OT integrati sulla stessa appliance per una visibilità unificata dei domini IT e OT, comprese le reti clonate con sovrapposizione degli intervalli IP
- Controllo degli accessi alla rete mediante integrazione diretta con l'infrastruttura Arista senza bisogno di agent o di affidarsi allo standard 802.1X per i dispositivi IT e IoT



Nuova interfaccia utente

Tutti gli utenti possono contare su un contesto e su approfondimenti fruibili su misura a seconda della loro funzione grazie alla nuova interfaccia utente web. Le dashboard visualizzano i dispositivi connessi, segnalano ai team gli aspetti a più alto rischio ed evidenziano i progressi compiuti verso gli obiettivi di conformità. L'inventario dei dispositivi in tempo reale con funzionalità complete di analisi dettagliata permette agli operatori di trovare velocemente i dispositivi e aiuta l'azienda a prevenire le minacce. Opzioni semplici di personalizzazione e condivisione agevolano la comunicazione dei rischi tra le varie funzioni del reparto IT per velocizzare la risposta.

Approfondimenti più rapidi. Le dashboard pronte all'uso sulla visibilità e la conformità dei dispositivi consentono di:

- Identificare la funzione, il sistema operativo, la marca e il modello di tutti i dispositivi connessi
- Stabilire una soglia di conformità e monitorare il rispetto di tutte le policy attive
- Individuare i dispositivi ad alto rischio come:
  - Dispositivi IoT con credenziali deboli, porte aperte o altri errori di configurazione
  - Dispositivi Windows sprovvisti di aggiornamenti di sicurezza o con vulnerabilità
  - Dispositivi con agent di sicurezza non funzionanti o applicazioni non autorizzate
  - Dispositivi OT con vulnerabilità e falle di sicurezza comuni (CVE) critiche
- Identificare le violazioni delle policy come i guasti più frequenti e i dispositivi che risultano non conformi in base a più di una policy (ad esempio che eseguono applicazioni P2P senza firewall o antivirus)

Eliminazione proattiva delle lacune. La nuova vista basata su web delle risorse consente di:

- Cercare in tutto l'inventario dei dispositivi fra ambiente fisico, data center, cloud e OT
- Filtrare in base alla policy, al segmento di rete e a qualsiasi proprietà del dispositivo
- Individuare la posizione dei dispositivi per abbreviare l'MTTR

Ecosistema di app eyeExtend Connect

I clienti sfruttano la piattaforma Forescout per l'integrazione con le altre tecnologie IT e di protezione informatica esistenti per condividere il contesto dei dispositivi, coordinare i flussi di lavoro e automatizzare la risposta. La gamma attuale di moduli eyeExtend di Forescout prevede integrazioni pronte all'uso con oltre 25 dei prodotti più diffusi e permette di aumentare il valore degli investimenti esistenti. Oltre a questi prodotti sviluppati e supportati da Forescout, Forescout 8.2 è dotato di un nuovo ecosistema di app basato su comminity per consentire integrazioni con altre tecnologie.

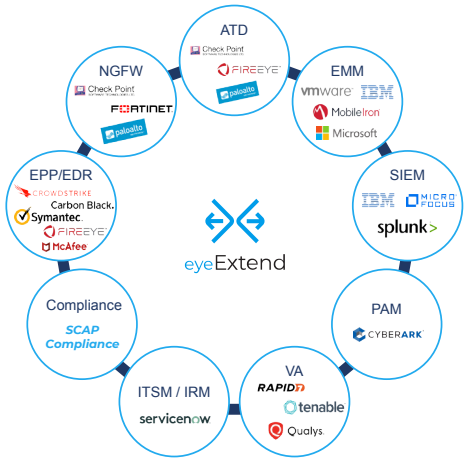
Sfruttando la potenza del crowdsourcing, eyeExtend Connect consente a clienti e partner di sviluppare velocemente, di utilizzare e di condividere app per connettersi alla piattaforma Forescout. Si possono agevolmente condividere i dati contestuali dei dispositivi con altri strumenti, automatizzare i flussi di lavoro e intervenire per velocizzare la risposta a livello di sistema riducendo l'MTTR.

Semplicità di sviluppo. Tutta la flessibilità di poter creare le app in proprio mediante script Python universali e lo standard di scambio dei dati JSON per un time to value più breve.

Semplicità d'uso. Potete scegliere tra le numerose app sviluppate nella community, semplici da distribuire e da personalizzare e portabili da un ambiente di rete all'altro.

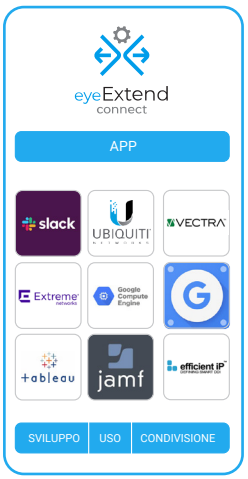
Semplicità di condivisione. Contribuite e imparate dalle procedure consigliate dalla community, condividete le app con i colleghi e sfruttate il crowdsourcing per aumentare il valore dei vostri investimenti in tecnologie informatiche.

Moduli eyeExtend



Sviluppati da Forescout

App eyeExtend



NOVITÀ

Sviluppate dalla community

Macro segmentazione su scala aziendale

Forescout 8.2 integra eyeSegment con le più recenti innovazioni di eyeSight e eyeControl per la segmentazione su scala aziendale su vari domini di rete e punti di controllo eterogenei. Con questa esperienza unificata, potete progettare e implementare in tutta sicurezza la segmentazione della rete e la protezione Zero Trust su scala variabile.

- Mappatura e visualizzazione dei flussi di traffico tra una tassonomia logica di utenti, dispositivi, applicazioni e servizi
- Progettazione, simulazione e perfezionamento dei criteri di segmentazione logici per capirne l'impatto prima dell'applicazione
- Monitoraggio in tempo reale dell'integrità della segmentazione e risposta alle violazioni dei criteri
- Applicazione affidabile delle regole di segmentazione in domini di rete diversi e punti di controllo eterogenei

Gestione della sicurezza e del rischio negli ambienti OT

Sfruttate l'integrazione fra SilentDefense e Forescout 8.2 per vari tipi di casi d'uso di gestione del rischio e della sicurezza in ambienti OT e unificati.

- Condividete la classificazione e le vulnerabilità dei dispositivi OT di SilentDefense con eyeSight e utilizzate la nuova interfaccia utente di eyeSight per avere una visibilità unificata delle reti IT e OT
- Implementate sensori IT e OT integrati sulla stessa appliance per rilevare e classificare i dispositivi negli ambienti unificati
- Identificate in modo univoco i dispositivi e applicate le policy negli ambienti di rete clonati che riutilizzano intervalli di indirizzi IP duplicati su più sedi, linee di produzione o impianti
- Sfruttate le funzioni più avanzate di SilentDefense negli ambienti OT, come la creazione ottimizzata di report sulla conformità NERC CIP, l'ispezione attiva selettiva e non intrusiva per una visibilità più approfondita e un framework di gestione dei rischi delle risorse che aggrega vari fattori di rischio in punteggi basati sull'impatto

Controllo degli accessi alla rete negli ambienti Arista

Forescout 8.2 è dotato di integrazione diretta con l'infrastruttura Arista per applicare il controllo degli accessi alla rete in Arista nonché in ambienti eterogenei. Questo permette di identificare e regolamentare sia dispositivi IT che IoT, senza bisogno di agent o di affidarsi allo standard 802.1X.

- Identificazione e valutazione in tempo reale di tutti i dispositivi IoT e IT quando si collegano alla rete
- Concessione dell'accesso alla rete appropriato in base al contesto di eyeSight e di terzi, che include il tipo di dispositivo, il proprietario, il ruolo dell'utente, lo stato di conformità e di sicurezza del dispositivo
- Mitigazione dei rischi con l'automazione di vari tipi di risposte della rete a seconda della situazione, ad esempio con la limitazione, la segmentazione, la quarantena o il blocco dei dispositivi

Implementazioni su cloud pubblico

In quanto a visibilità e controllo dei dispositivi, le aziende che adottano un approccio 'cloud-first' alla tecnologia finora sono state limitate alle implementazioni fisiche o virtuali nell'ambiente locale. Con Forescout 8.2 potete implementare le appliance sensore e la gestione aziendale Forescout negli ambienti cloud Amazon Web Services o Microsoft Azure senza alcun ingombro nell'ambiente locale. Avete anche la possibilità di associare implementazioni su cloud pubblico ad appliance fisiche e virtuali in infrastrutture cloud private VMware, Hyper-V o KVM.

Fisico | Virtuale | Cloud pubblico | Ibrido
Combina tutti o parte degli elementi di cui sopra

Scalabilità per grandi aziende

Forescout 8.2 consente una scalabilità senza confronti per soddisfare i requisiti severi delle grandi aziende e tenere il passo con la crescita esponenziale dei dispositivi connessi negli ambienti fisici, nei data center, su cloud, negli ambienti IoT e OT.

- Classificazione dei dispositivi tramite una gigantesca knowledge base su cloud con più di 11 milioni di dispositivi aziendali per identificare più velocemente e con maggiore precisione le risorse IoT, OT e IT connesse
- Gestione di due milioni di dispositivi in una singola distribuzione, indipendentemente dal fatto che le implementazioni siano fisiche, virtuali, cloud o ibride

FORESCOUT

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

E-mail info-italia@forescout.com
Tel. (internazionale) +1-408-213-3191
Assistenza +1-708-237-6591

Maggiori informazioni su forescout.it