Forescout eyeExtend Connect

Integrazione agevole con la piattaforma Forescout per ottenere approfondimenti contestuali sui dispositivi e velocizzare la risposta alle minacce su scala aziendale

Per aumentare il valore derivante dagli investimenti in tecnologie IT e di sicurezza, i clienti Forescout sfruttano le integrazioni pronte all'uso con i prodotti di nove tecnologie di sicurezza tra le più diffuse. Queste integrazioni favoriscono un sensibile aumento delle efficienze grazie al coordinamento dei flussi di lavoro di sicurezza. Oltre a questi prodotti preconfigurati, Forescout propone ora ai clienti un metodo più rapido e semplice per integrare un maggior numero delle loro attuali tecnologie con la piattaforma Forescout. eyeExtend Connect, un nuovo prodotto Forescout, consente infatti alla nostra comunità di clienti e di partner di sviluppare, utilizzare e condividere velocemente app eyeExtend, che collegano la piattaforma Forescout ad altre tecnologie. Questo permette di sfruttare il valore dei prodotti di sicurezza esistenti con i dati contestuali approfonditi sui dispositivi forniti da Forescout, di automatizzare i flussi di lavoro di sicurezza e l'applicazione delle policy tra soluzioni eterogenee e di accelerare la risposta a livello di sistema per mitigare i rischi.

La soluzione

Forescout eyeExtend Connect semplifica la creazione di app facili da utilizzare e da distribuire. Tramite le app Forescout eyeExtend è ora possibile integrare facilmente la piattaforma Forescout con le tecnologie IT e di sicurezza esistenti e coordinare i flussi di lavoro di sicurezza tra tecnologie di protezione informatica eterogenee.

Con eyeExtend Connect, le tecnologie di sicurezza esistenti possono sfruttare i dati contestuali approfonditi sui dispositivi di Forescout eyeSight, comprese le proprietà dei dispositivi, il loro stato di sicurezza, la loro conformità alle policy aziendali, la loro posizione in rete, i dati contestuali sugli utenti, e altro ancora. Questi dati sui dispositivi possono essere estratti automaticamente da altri prodotti IT o di sicurezza, oppure trasmessi alla piattaforma Forescout dai dispositivi stessi. eyeExtend Connect aiuta anche a velocizzare la risposta alle minacce consentendo di automatizzare azioni basate su policy a livello di sistema per mitigare le minacce, gli incidenti e le lacune nella conformità.

eyeExtend Connect mette a disposizione i seguenti strumenti per coordinare i flussi di lavoro e condividere il contesto dei dispositivi.

eyeExtend connect

Problematiche

- Affidarsi alle integrazioni preconfigurate offerte da Forescout o dai suoi partner tecnologici elimina la necessità di coordinare i flussi di lavoro con altre tecnologie di sicurezza interne all'azienda
- I lunghi cicli di sviluppo delle integrazioni personalizzate dilatano i tempi in cui si realizza il valore degli attuali investimenti in sicurezza
- Gli strumenti di sicurezza che funzionano in modo indipendente senza condividere dati contestuali su utenti e dispositivi richiedono un notevole impegno manuale in caso di risposta agli eventi di sicurezza, con aumento del rischio informatico e perdita di produttività

Vantaggi

- Ottimizzazione del ritorno sugli investimenti in tecnologia attuali grazie all'integrazione con tutti i tipi di strumenti di altre marche
- Time-to-value più breve grazie all'integrazione semplice e rapida con la piattaforma Forescout tramite le app eyeExtend
- Consolidamento dello stato di sicurezza grazie a una migliore sinergia tra strumenti informatici e di sicurezza, con approfondimenti fruibili sui dispositivi ottenuti più velocemente e automazione della risoluzione dei rischi e delle minacce

In breve

- Sviluppate e distribuite facilmente le app eyeExtend per l'integrazione con la piattaforma aperta Forescout
- Condividete le app con la comunità per contribuire e ottenere riscontri
- Sviluppate app portabili con script Python e configurazione JSON
- Integratele con un'ampia gamma di servizi web di terzi
- Ampliate le funzioni di visibilità e controllo di Forescout con dati contestuali sui dispositivi e controlli di altre marche
- Abilitate le interazioni bidirezionali con API REST aperte, basate su standard
- Ricevete e inviate informazioni a un SQL (Structured Query Language) standard
- Generate query personalizzate per ricevere e inviare informazioni a un server LDAP standard
- Ricevete e inviate informazioni tramite syslog a un server designato

App eyeExtend

Sviluppate applicazioni che sfruttano le funzioni chiave della piattaforma Forescout per conoscere e condividere il contesto degli endpoint, eseguire azioni di controllo sulla rete e applicare le policy a livello di sistema. eyeExtend Connect è dotato di uno schema JSON di facile utilizzo per definire parametri, tag e configurazioni controllate dall'utente per rendere portabili le vostre app eyeExtend (migrazione dall'ambiente di prova a quello di produzione, da un'area geografica all'altra, da ambienti IT a OT, ecc.). Inoltre, le interazioni con API di terzi sono definite con script Python molto diffusi che garantiscono notevole flessibilità in quanto aumentano la varietà dei tipi di integrazioni che si possono creare. I casi d'uso e le applicazioni essenziali, come la mitigazione delle minacce, la risposta agli eventi e la gestione della conformità si possono automatizzare con modelli di policy integrabili nelle app.

Caratteristiche principali delle app eyeExtend:

- Plug-and-play
- Rilevamento di nuovi dispositivi e proprietà
- Azioni di controllo esterne di terzi
- Modelli di policy personalizzati
- Interazioni API gestite tramite script
- Icone di terzi personalizzabili

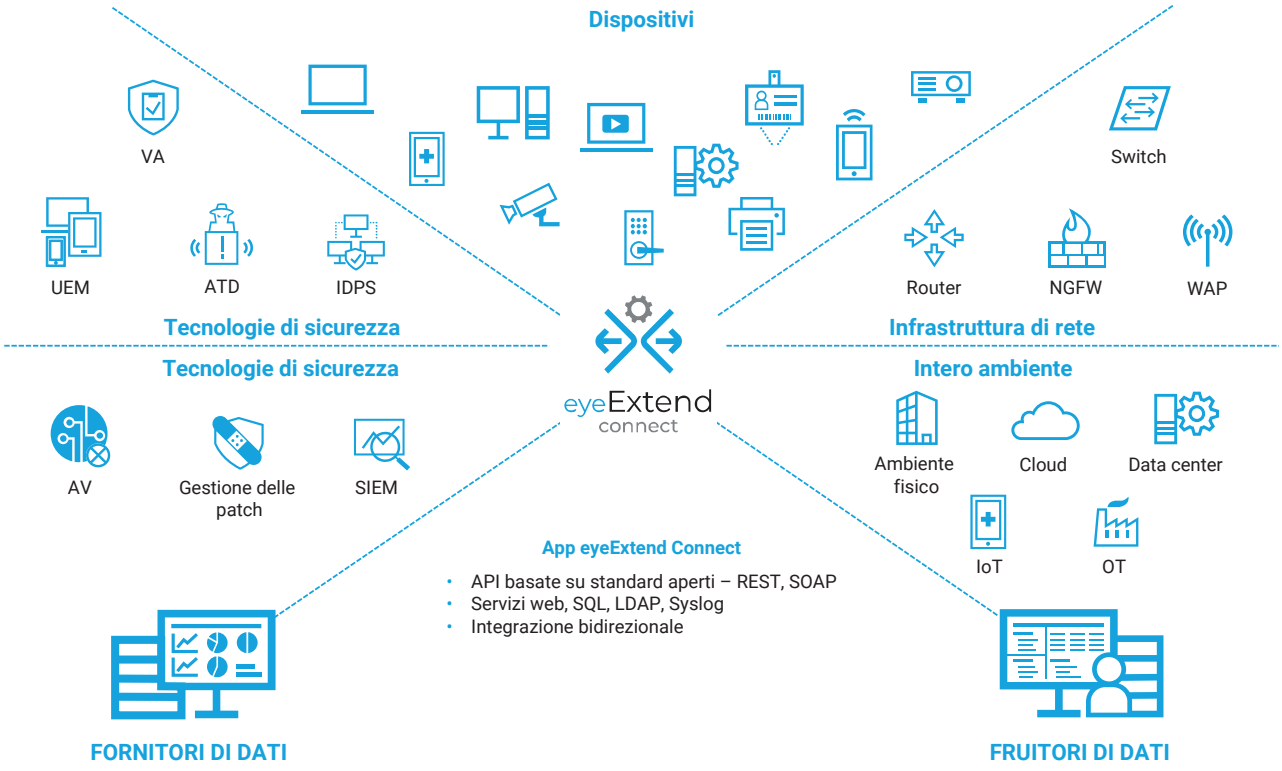
WebAPI e DataExchange (DEX)
La piattaforma Forescout è dotata di una serie di API RESTful che consentono alle applicazioni esterne di recuperare i dati delle policy e le proprietà dei dispositivi Forescout. Il plugin DEX (Data Exchange) consente la comunicazione bidirezionale tra la piattaforma Forescout e le API RESTful esterne per la condivisione in tempo reale dei dati contestuali sui dispositivi.

SQL
Il plugin DEX è in grado di ricevere e inviare informazioni a un database SQL standard. Questo tipo di integrazione consente alle applicazioni sviluppate internamente di condividere le informazioni con prodotti di altre marche in grado di interfacciarsi tramite un database interno o esterno. È possibile interrogare database esterni e creare proprietà Host per archiviare i dati recuperati dalla piattaforma Forescout. Queste proprietà Host possono essere utilizzate nelle policy Forescout e visualizzate nelle viste del NOS (NAC) e di inventario. È possibile anche aggiornare i database esterni in base alle informazioni raccolte dalla piattaforma Forescout, generalmente per consentire l'intervento di un prodotto esterno.

LDAP
Con il plugin DEX si possono generare query personalizzate per il trasferimento bidirezionale delle informazioni a un server LDAP standard. È possibile ad esempio interrogare il server LDAP e creare proprietà Host Forescout per archiviare i dati così recuperati. Queste proprietà Host si possono utilizzare nelle policy della piattaforma Forescout e visualizzare nelle viste NAC e di inventario.

Syslog
Il plugin DEX si può configurare per ricevere e inviare informazioni tramite syslog a un server designato. Questo tipo di interfaccia si usa per molti tipi di integrazioni con prodotti che aggregano i registri e ne consentono l'analisi, ad esempio i prodotti di gestione degli eventi e delle informazioni di sicurezza (SIEM), oppure con altre soluzioni che possono inviare e ricevere avvisi in questo modo. Il formato dei messaggi è personalizzabile.

Figura 1: coordinamento dei flussi di lavoro tra dispositivi, ambienti e tecnologie di sicurezza eterogenee



VA: valutazione delle vulnerabilità, **ATD:** protezione avanzata dalle minacce, **IDPS:** prevenzione delle intrusioni in rete, **UEM:** gestione degli endpoint unificata, **AV:** antivirus, **SIEM:** gestione degli eventi e delle informazioni di sicurezza, **WAP:** access point wireless, **NGFW:** firewall di nuova generazione

Casi d'uso generali

Sebbene Forescout offra 25 soluzioni pronte all'uso per casi d'uso specifici, per i casi d'uso personalizzati dei clienti si possono utilizzare le app eyeExtend. Ecco alcuni esempi:

Rilevamento, classificazione e valutazione di ogni dispositivo collegato in rete nel momento in cui si collega
Forescout eyeExtend Connect, basato su Forescout eyeSight, consente a un prodotto IT o di sicurezza integrato di fornire il contesto che permette di identificare meglio i dispositivi su scala aziendale: nell'ambiente fisico, nei data center, negli ambienti OT e cloud. Ad esempio, l'app eyeExtend per Ubiquiti agevola una maggiore visibilità dei dispositivi collegati tramite Wi-Fi e utilizza gli attributi dei dispositivi rilevati per migliorare le decisioni delle policy nella piattaforma Forescout. L'app eyeExtend per Ubiquiti ora può trasmettere le informazioni sul dispositivo Ubiquiti collegato tramite Wi-Fi a un altro prodotto di gestione dei servizi IT (ITSM) o di gestione delle risorse per rettificarne il database di gestione delle configurazioni. Un'altra app importante, l'app eyeExtend per Google Cloud, offre ai clienti la visibilità in tempo reale delle istanze di cloud computing in evoluzione integrandosi con Google Cloud ed estraendo il contesto dell'inventario di Google Cloud.

Miglioramento della visibilità e del controllo dei dispositivi collegati tramite VPN che accedono alla rete
eyeExtend Connect identifica tutti i dispositivi che si collegano alla rete aziendale tramite VPN. Sfruttando l'integrazione con la piattaforma Forescout, gli addetti alla sicurezza possono stabilire se la risorsa che si collega tramite VPN è una risorsa aziendale e controllare gli accessi dei dispositivi che si collegano da posizioni non autorizzate.

Coordinamento del flusso di lavoro delle informazioni sulle violazioni delle policy IT o di sicurezza
È possibile inviare avvisi di violazione delle policy in tempo reale tramite svariate piattaforme di collaborazione e messaggistica. Si può definire una policy per ottenere i dati sugli eventi dei dispositivi dalla piattaforma Forescout tramite email, piattaforme di messaggistica o di collaborazione quando si prendono decisioni in materia di policy per automatizzare le azioni di controllo della rete. Ad esempio, l'app eyeExtend per Slack si integra con la piattaforma di collaborazione per inviare avvisi di violazione delle policy in tempo reale a un canale utilizzato dal reparto IT o di sicurezza su Slack.

Automazione della registrazione dei dispositivi mobili, miglioramento della gestione della sicurezza e imposizione della conformità costante
eyeExtend Connect coordina le azioni di condivisione e di controllo dei dati dei dispositivi con i sistemi UEM per garantire la gestione unificata delle policy di sicurezza per i dispositivi della rete indipendentemente dal tipo (PC, Mac, Linux®, tablet, smartphone), dalla connessione (cablata, wireless, VPN) o dal proprietario del dispositivo (aziendale o personale). Questa gestione completa dei dispositivi consente l'automazione della registrazione dei dispositivi, l'imposizione della conformità dei dispositivi tramite azioni regolate dalle policy, l'applicazione di controlli personalizzati per gli accessi alla rete e l'accelerazione delle azioni di risposta e di remediation. Ad esempio, con l'app eyeExtend per Google Mobile Management i clienti visualizzano il contesto dei dispositivi Chromebook. Questi dati facilitano il perfezionamento delle policy di accesso e di sicurezza dei dispositivi BYOD aziendali.

Automazione delle azioni e dei flussi di lavoro nell'ecosistema dei prodotti IT e di sicurezza per migliorare i processi e rafforzare la sicurezza su scala aziendale
eyeExtend Connect può inviare o ricevere attivatori di azione che indicano alla piattaforma Forescout o a un altro prodotto integrato di eseguire un'azione specifica. Questi attivatori si basano su automazioni regolate dalle policy anziché su processi decisionali basati su playbook che richiedono l'intervento di un operatore umano. Questo determina tempi di risposta più rapidi e reti complessivamente più sicure.

Uso di dati contestuali approfonditi sui dispositivi per l'analisi delle correlazioni per velocizzare la risposta agli eventi
eyeExtend Connect consente alla piattaforma Forescout di trasmettere dati approfonditi sui dispositivi a un sistema SIEM per l'analisi delle correlazioni. Questo fornisce un quadro completo della superficie di attacco dell'azienda, aiuta a ridurre i tempi di recupero degli approfondimenti e facilita le indagini. La piattaforma Forescout inoltre contribuisce a semplificare le attività di sicurezza automatizzando le azioni basate su policy, limitando l'accesso del dispositivo alla rete a seconda della gravità dell'evento comunicata dal SIEM in tempo reale.

In sintesi, eyeExtend Connect vi aiuta ad aumentare rapidamente il ritorno sugli investimenti in materia di sicurezza eliminando la gestione separata degli strumenti di protezione e collegandoli a una piattaforma estremamente intelligente come Forescout con cui potrete automatizzare notevolmente la mitigazione delle minacce e la conformità alle policy.

Nota: alcune funzioni di eyeExtend Connect erano già incluse nel prodotto OIM. Tutte le precedenti funzioni OIM sono ora incluse in eyeExtend Connect.

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