FORESCOUT

Le novità di Forescout 8.1

La trasformazione digitale prosegue senza sosta: le aziende connettono alle loro reti un numero sempre maggiore di dispositivi smart per automatizzare le operazioni aziendali e aumentare l'efficienza. Che si tratti di IoT, IIoT o OT, questi dispositivi portano un'espansione e una diversità senza precedenti alle reti aziendali.

> "Entro il 2021, il reparto CIO, CISO o CSO gestirà direttamente il 70% della sicurezza OT, rispetto al 35% di quanto avviene oggi."[1]
> *– Gartner, maggio 2018*

Per guidare questa trasformazione delle attività, le aziende devono aumentare la connettività e la condivisione delle informazioni fra reti in precedenza separate. Ciò sta accelerando la convergenza di IT e OT e crea nuovi flussi di dati fra i dispositivi IT connessi nella sede fisica, le applicazioni basate sul cloud e i sistemi tecnologici operativi. Nonostante i vantaggi ciò aumenta i rischi per le aziende, dato che gli autori delle minacce possono muoversi lateralmente in reti ora interconnesse, per accedere a informazioni sensibili o provocare interruzioni delle attività.

La convergenza di IT e OT aumenta la pressione su CIO e CISO, che ora hanno il compito di proteggere questo ecosistema aziendale nella sua interezza. Il personale IT non deve più solo gestire dispositivi, applicazioni e dati degli utenti, ma ha la responsabilità di far svolgere le operazioni aziendali in sicurezza e senza intoppi. Per affrontare questa sfida ha bisogno di visibilità e controllo completi sui dispositivi.

Forescout 8.1: visibilità e controllo unificati sui dispositivi per la sicurezza IT and OT

Forescout 8.1 è la prima piattaforma unificata per la visibilità e il controllo dei dispositivi nelle reti IT e OT convergenti. Permette alle aziende di avere una visione d'insieme completa su tutti i dispositivi nell'ambiente interconnesso e di coordinare le azioni che mitigano il rischio sia informatico sia operativo. Nuove funzionalità:

- La visibilità su Cisco ACI, Microsoft Azure e gli ambienti degli switch industriali Belden, che amplia la copertura a centri dati, cloud e reti OT, fornisce alle aziende il campo visivo di cui necessitano nei domini IT e OT
- Gli ampi miglioramenti della classificazione automatica per i dispositivi IoT e OT, la valutazione delle vulnerabilità per i sistemi di controllo industriale (ICS) e il rilevamento dei dispositivi ostili aumentano la resilienza informatica di entrambe le reti IT e OT
- Coordinamento per la segmentazione con i firewall Fortinet e Cisco DNA Center e risposta agli eventi con ServiceNow per estendere la capacità di automatizzare i controlli e aumentare l'efficienza delle operazioni di sicurezza
- Scalabilità senza paralleli di due milioni di dispositivi in una singola distribuzione che abbraccia ambienti fisici, virtuali, cloud e ibridi

Scalabilità enterprise

Gestisci due milioni di dispositivi in una singola distribuzione che abbraccia gli ambienti fisici, virtuali, cloud e ibridi

Scoperta dei dispositivi

Nuova visibilità su Microsoft Azure, Cisco ACI e gli ambienti industriali di switch Belden, oltre alla visibilità sui livelli inferiori dello stack della rete OT.

Classificazione automatica

La nuova ispezione approfondita dei pacchetti di oltre 100 protocolli IT e OT permette la classificazione automatica dei dispositivi medicali, industriali, di automazione degli edifici e IoT.

Valutazione dei rischi

La nuova valutazione delle vulnerabilità OT e ICS e il rilevamento dei dispositivi ostili che identifica e blocca gli impostori aumentano la resilienza informatica.

Automazione dei controlli

Nuovo coordinamento per la segmentazione della rete con i firewall Fortinet e Cisco DNA Center e risposta agli eventi con ServiceNow ITSM e Security Operations.

Rilevamento dispositivi ampliato

La sicurezza comincia sapendo con certezza cosa c'è nella rete. Ciò significa identificare tutti i dispositivi nel momento in cui si connettono alla rete. Per il 2019 si prevede che altri 900 milioni di dispositivi fisici e virtuali saranno presenti nelle reti aziendali. La stragrande maggioranza di questa espansione è dovuta ai dispositivi IoT e OT e alle istanze dei cloud pubblici e privati.

> "Entro il 2023 il CIO medio sarà responsabile di oltre il triplo degli endpoint che gestiva nel 2018."[2]
> *– Gartner, settembre 2018*

- Forescout 8.1 continua ad ampliare la visibilità in queste aree per fornire una vista unificata di tutti i dispositivi nelle reti di sede, centro dati, cloud e OT
- La visibilità multicloud include ora Microsoft Azure, in aggiunta alle funzionalità esistenti per AWS e VMware
- L'integrazione con Cisco ACI offre visibilità sugli ambienti SDN per i data center
- L'integrazione con il portafoglio di switch industriali Belden offre una più ampia visibilità sulle reti OT
- Il monitoraggio passivo nei livelli inferiori dello stack di rete OT fornisce visibilità nei dispositivi di supervisione, controllo dei processi e strumentali

Classificazione automatica superiore

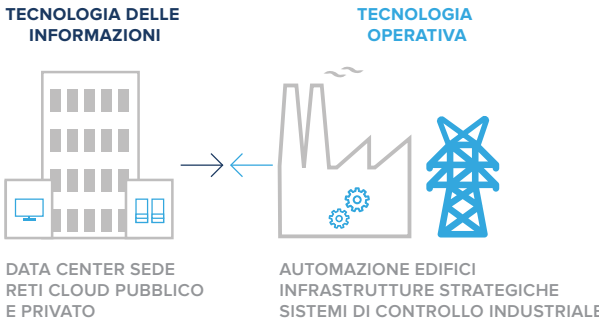
La diversità dei dispositivi IoT e OT rende difficile per le aziende identificarli e catalogarli accuratamente e senza una classificazione granulare non è facile creare e imporre policy mirate per proteggerli. Forescout 8.1 include degli ampi potenziamenti che ti consentono di classificare automaticamente un maggior numero di dispositivi e sfruttare tale contesto per l'imposizione delle policy:

- Ampia copertura per identificare oltre 500 versioni di sistemi operativi e più di 5000 fra marche e modelli di dispositivi
- La classificazione dei dispositivi sanitari di oltre 350 fabbricanti di tecnologia medicale, compresi i Global Top 20
- Nuova ispezione approfondita dei pacchetti di oltre 100 protocolli IT e OT per classificare automaticamente migliaia di dispositivi di automazione industriale nei settori manifatturiero, energia, petrolio e gas, servizi pubblici, minerario e infrastrutture strategiche
- Maggiore efficacia, velocità e copertura della classificazione grazie a Forescout Device Cloud, con oltre otto milioni di dispositivi IT, IoT e OT.

Valutazione dei rischi multidominio

Valutazione delle vulnerabilità nelle tecnologie operative

Con la crescente connettività fra le reti IT e OT, è importante capire il profilo di rischio dei dispositivi in entrambi i domini. Dato che possono essere compromessi i dispositivi vulnerabili di uno qualsiasi dei due, le minacce possono passare da un dominio all'altro, causando interruzioni alle attività e perdite finanziarie.



- Forescout 8.1 aggiunge la valutazione delle vulnerabilità OT e ICS alle funzioni di valutazione esistenti per Windows, segnalandoti i dispositivi ad alto rischio presenti nella rete
- I frequenti aggiornamenti provenienti da Forescout offrono informazioni puntuali sulle vulnerabilità ed esposizioni comuni (CVE) degli ICS per identificare i dispositivi vulnerabili e coordinare le azioni di remediation
- Per i dispositivi industriali e operativi vulnerabili che possono essere coperti da patch o risanati solo durante le finestre della manutenzione pianificata, Forescout impone i controlli di mitigazione come la segmentazione di tali dispositivi in zone "sicure" della rete fino al momento in cui potranno essere risanati

Individuazione dei dispositivi inaffidabili

Un'altra problematica dovuta all'esplosione di IoT e OT è il furto dell'identità dei dispositivi e lo spoofing degli indirizzi MAC. Gli autori delle minacce che cercano di accedere alle reti possono prendere di mira un maggior numero di indirizzi MAC, dato che i dispositivi IoT e OT sono spesso inclusi in lunghe whitelist per farli accedere alla rete. Sovente i dispositivi presentano schermate non protette, che possono rivelare l'indirizzo MAC a chiunque si trovi a passare. Gli impostori possono facilmente nascondersi dietro dispositivi legittimi al fine di accedere alla rete e causare problemi o acquisire informazioni sensibili.

Forescout 8.1 include un nuovo rilevamento dei dispositivi inaffidabili (in attesa di brevetto) che identifica e blocca gli impostori che usano le tecniche di spoofing degli indirizzi MAC.

- Il monitoraggio continuo della rete rileva molteplici scenari di spoofing in reti cablate e wireless, comprese le connessioni simultanee e i tentativi di sostituzione nello stesso luogo e in luoghi diversi
- Forescout identifica i dispositivi di vittime e impostori e, in base alle policy, blocca i tentativi di spoofing per impedire gli accessi non autorizzati
- Forescout ti permette di dimostrare ai verificatori la resilienza allo spoofing MAC e migliorare la conformità alle verifiche

Coordinamento e automazione dei controlli

Gli addetti alla sicurezza informatica sono inondati dal crescente numero di problemi di sicurezza e conformità segnalati dai relativi strumenti, che però non hanno un sufficiente contesto del dispositivo perché le funzioni di ordinamento per priorità e di automazione possano imporre i controlli. Di conseguenza gli addetti alla sicurezza, benché altamente qualificati, perdono tempo nella risoluzione manuale di problemi a basso impatto perché non possono concentrarsi su una riduzione proattiva del rischio o sul rispondere rapidamente alle minacce. Forescout 8.1 ti offre sia il contesto dei dispositivi sia la capacità di coordinare le azioni e automatizzare i controlli.

> "Entro il 2021 il 70% delle grandi imprese includerà funzioni di automazione, coordinamento e risposta di sicurezza, tramite SIEM o una piattaforma dedicata: un enorme crescita rispetto a meno del 5% nel 2018."[3]
> *– Gartner, dicembre 2018*

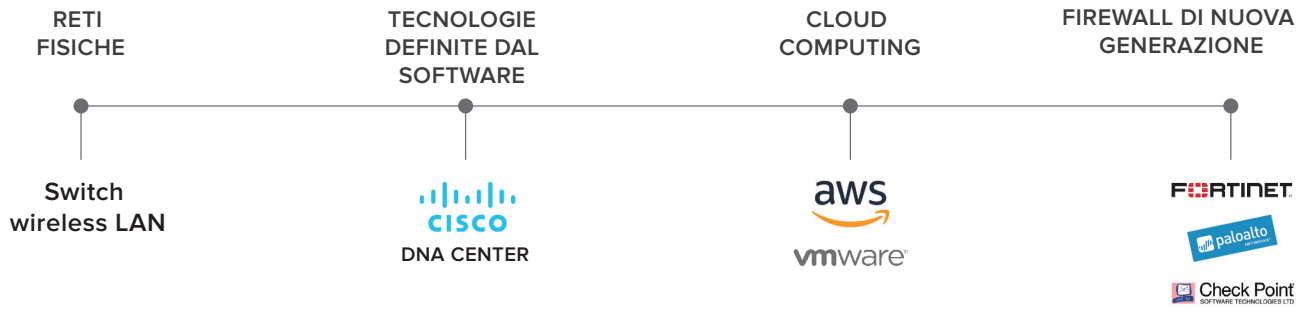
Segmentazione della rete

Mentre le aziende definiscono le proprie architetture di sicurezza di nuova generazione per IoT e OT, la segmentazione gioca un ruolo importante. A differenza di quelli tradizionali, i dispositivi IoT and OT non possono essere regolarmente coperti dalle patch o protetti tramite agent. Quindi la segmentazione di tali dispositivi in zone di sicurezza logiche è una strategia essenziale per la mitigazione dei rischi.

Forescout 8.1 consente di coordinare la segmentazione in svariate tecnologie di imposizione, comprese alcune nuove integrazioni:

- Automazione dei controlli di segmentazione con i firewall Fortinet, in aggiunta al coordinamento esistente con Palo Alto Networks e Check Point, il che dà un supporto eterogeneo dei firewall di nuova generazione
- Coordinamento dei controlli di segmentazione con Cisco DNA Center, in aggiunta alle integrazioni esistenti con le tecnologie definite dal software e di networking nel cloud come VMware NSX e AWS

Segmentazione della rete interdominio



Automazione della risposta agli eventi

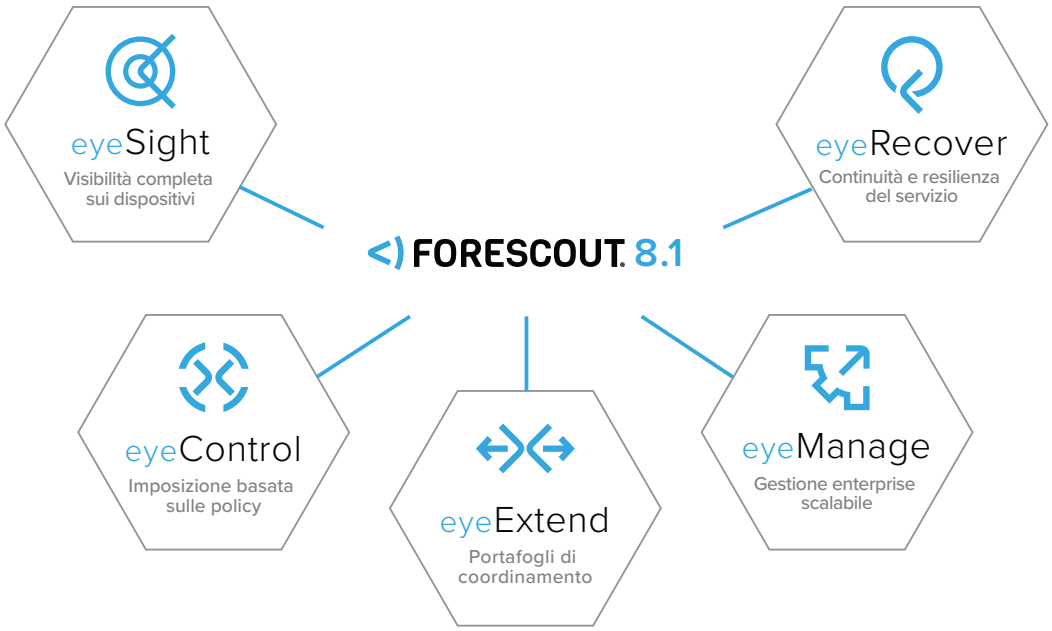
I reparti IT e della sicurezza guardano sempre di più all'automazione della risposta per affrontare i problemi a basso rischio, in modo che le risorse qualificate possano concentrarsi sulla mitigazione dei rischi e su altri fattori dall'impatto elevato sulle attività. Forescout 8.1 ora si integra con i prodotti ServiceNow ITSM e Security Operations, automatizzando e accelerando la risposta agli eventi.

- Il nuovo coordinamento con ServiceNow ITSM automatizza la creazione degli interventi di servizio e la risposta basata sulle policy per la conformità della configurazione
- Il nuovo coordinamento con ServiceNow Security Operations automatizza la creazione degli interventi di sicurezza e la risposta alle minacce per i dispositivi compromessi o ad alto rischio
- Il coordinamento potenziato con ServiceNow CMDB aggiorna gli elementi di configurazione dopo il completamento dell'intervento, al fine di facilitare i flussi di lavoro ad anello chiuso per la gestione di servizio e sicurezza

Una piattaforma scalabile e flessibile

Forescout 8.1 offre scalabilità e flessibilità di distribuzione senza pari per soddisfare i severi requisiti degli ambienti delle grandi imprese:

- Con una singola installazione puoi gestire fino a due milioni di dispositivi fisici o virtuali che abbracciano le reti di sede, centro dati, cloud e OT
- Una suite modulare di prodotti offre flessibilità in base all'evoluzione dei requisiti aziendali. Partendo da Forescout eyeSight per la visibilità dei dispositivi, ogni prodotto aggiuntivo apporta potenti funzionalità per l'automazione dei controlli, il coordinamento della sicurezza, la resilienza operativa e la sicurezza OT
- Per la flessibilità dell'acquisto, tutti i prodotti software Forescout sono ora disponibili come licenza perpetua o abbonamento a scadenza



1 2018 Strategic Roadmap for Integrated IT Security – Gartner, maggio 2018
2 Gartner Top Strategic IoT Trends and Technologies Through 2023, settembre 2018
3 Gartner, Emerging Technology Analysis: SOAR Solutions 7 dicembre 2018, Eric Ahlm

FORESCOUT

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

Numero verde (USA) 1-866-377-8771
Tel. (Internazionale) +1-408-213-3191
Assistenza 1-708-237-6591

Maggiori informazioni su Forescout.com