Forescout eyeSight

Scopri, classifica e valuta continuamente i dispositivi per avere un quadro completo della situazione e ridurre il rischio

I CIO si stanno assumendo la responsabilità della protezione di un crescente numero di sistemi connessi alla rete, soprattutto dispositivi IoT e OT. Dato che non puoi proteggere quello che non riesci a vedere "you can't secure what you can't see™", questo aumento nel numero (e nei tipi) dei dispositivi sta creando un senso collettivo di urgenza per la visibilità su tutti i dispositivi connessi, fisici e virtuali. Questi includono i dispositivi gestiti, non gestiti e sconosciuti connessi da dipendenti, appaltatori e clienti o anche dal personale operativo con le migliori intenzioni. A prescindere dalla loro posizione nella rete (in sede, nel centro dati, nel cloud privato e pubblico e anche negli ambienti OT/ICS), tali dispositivi devono essere adeguatamente rilevati, profilati e monitorati.

Figura 1: visibilità dettagliata su sede, IoT, centro dati, cloud e tecnologie operative

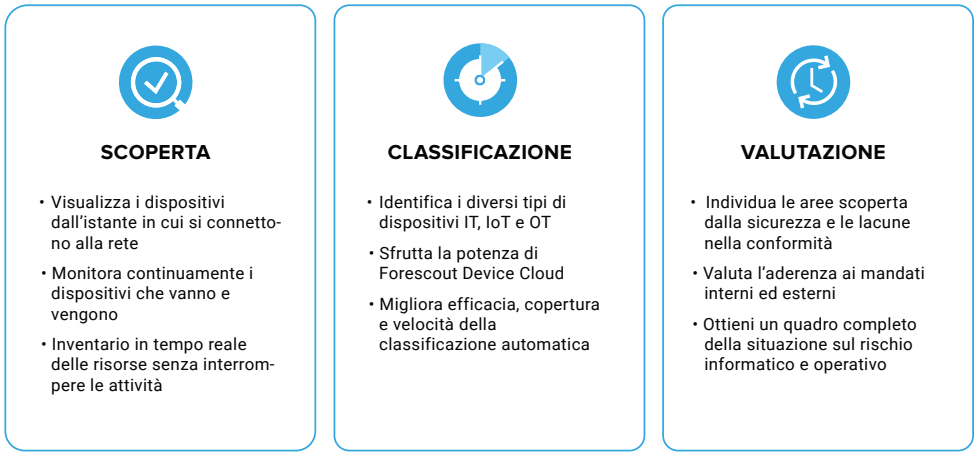
Forescout eyeSight offre approfondimenti senza pari sull'intero panorama delle minacce senza interrompere i processi aziendali critici. Innanzitutto scopre ogni dispositivo con connessione IP nella rete della tua azienda estesa, ma la scoperta è solo il primo passo verso la visibilità completa. Per prendere le giuste decisioni in materia di policy e controllo, un contesto esaustivo è essenziale. Dopo aver scoperto i dispositivi connessi, eyeSight li classifica automaticamente e li valuta rispetto alle policy aziendali. La potente combinazione di queste tre funzioni (scoperta, classificazione e valutazione) offre la visibilità sui dispositivi che è necessaria per decidere le policy e le azioni più appropriate.

eyeSight

In breve

- Inventario unificato e in tempo reale dei dispositivi connessi alla rete, senza agent
- Profilo accurato dei dispositivi per ottenere il contesto necessario alla realizzazione di policy di sicurezza e conformità proattive
- Identificazione dei dispositivi ostili, vulnerabili o non conformi e creazione di policy per limitare i rischi
- Assicurazione in tempo reale sul funzionamento di strumenti di sicurezza e controlli di conformità
- Misurazione e reportistica efficienti della condizione di conformità e dell'esposizione al rischio informatico
- Automazione delle attività comuni per minimizzare l'errore umano e aumentare l'efficienza

Figura 2: le funzioni essenziali di visibilità offerte da eyeSight.



Scoperta continua, senza agent

I dispositivi IoT e OT pongono delle specifiche problematiche di visibilità. L'elevato volume di tali dispositivi crea un problema di vasta scala perché la scoperta manuale non è più fattibile. Inoltre, molti di questi dispositivi non supportano gli agent e sono sensibili alle tecniche attive di sondaggio e scansione che potrebbero causare interruzioni ai sistemi e alle attività. Utilizzando oltre 20 tecniche di monitoraggio attivo e passivo (v. la Figura 3), eyeSight evita le potenziali lacune di visibilità tramite la scoperta automatica di:

- computer portatili, tablet, smartphone, sistemi BYOD/ospiti e dispositivi IoT nelle reti delle sedi;
- computer virtuali, hypervisor e server fisici nei centri dati;
- istanze di AWS, Azure e VMware nei cloud pubblici e privati;
- dispositivi medicali, industriali e di automazione degli edifici nelle reti della tecnologie operative;
- infrastrutture di rete fisiche e definite dal software, compresi switch, router, VPN, punti di accesso wireless e controllori.

Queste capacità di scoperta si combinano per minimizzare il rischio operativo, eliminare i punti ciechi della visibilità e ottenere un inventario continuo dei dispositivi nell'azienda estesa.

Figura 3: tecniche di scoperta attive e passive.

DA PASSIVO A INFRASTRUTTURA	DA PASSIVO A DISPOSITIVO FINALE	DA ATTIVO A DISPOSITIVO FINALE
Trap SNMP	Polling dell'infrastruttura di rete	Ispezione di Windows senza agent • WMI • RPC • SMB
Traffico SPAN	Integrazione SDN • Meraki • Cisco ACI	Ispezione di Mac e Linux senza agent • SSH
Analisi dei flussi • NetFlow • NetFlow flessibile • IPFIX • sFlow	Integrazione cloud pubblico/privato • VMware • AWS • Azure	NMAP
Richieste DHCP	Servizi delle directory di query (LDAP)	Query SNMP
Agente utente HTTP	Applicazioni web di query (REST)	Query HTTP
Fingerprinting TCP	Database di query (SQL)	SecureConnector®
Analisi dei protocolli	Coordinamenti di eyeExtend	
Richieste RADIUS		

Le problematiche

- L'isolamento reciproco di gruppi, strumenti di sicurezza e processi introduce lacune nella visibilità
- I processi manuali soggetti a errori introducono rischi operativi e commerciali
- Le informazioni incomplete sui dispositivi danno poco contesto informatico per costruire delle policy di difesa
- Incapacità di verificare che gli strumenti di sicurezza siano installati, configurati e correttamente funzionanti
- I dispositivi ostili non rilevati causano rischi non necessari per la sicurezza e la conformità
- Le scansioni obsolete, eseguite in momenti particolari, fanno mancare la fiducia nella condizione di conformità

Classificazione automatica e intelligente

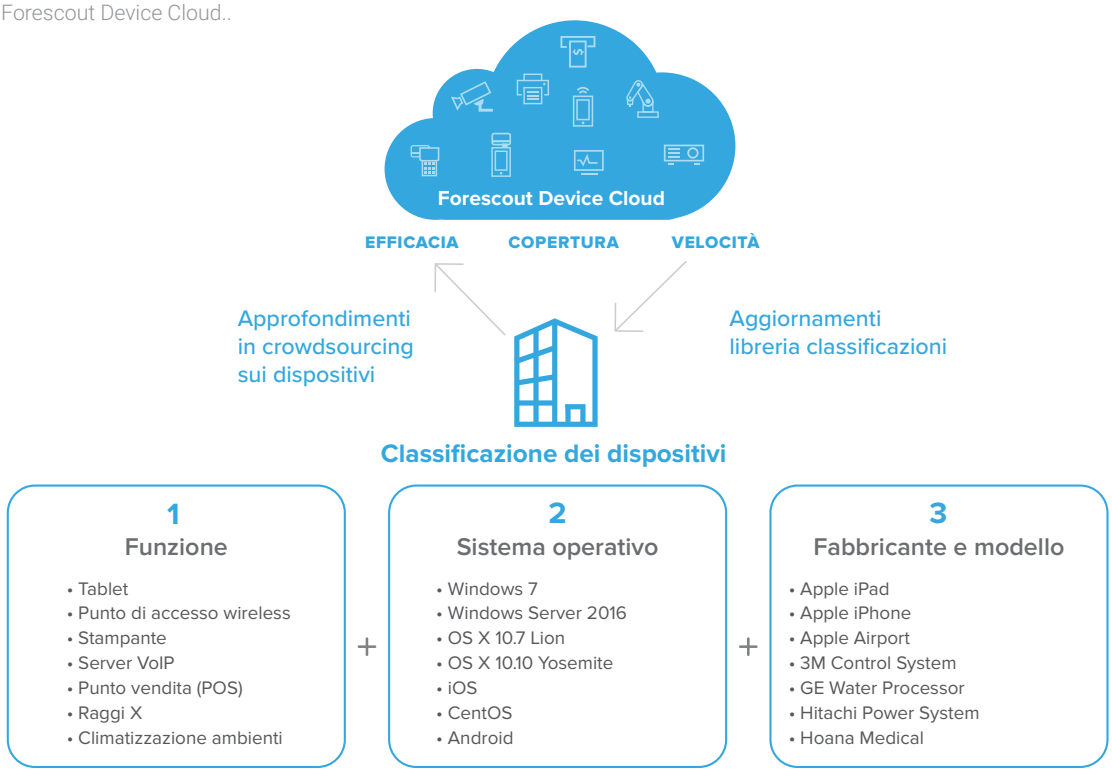
Per creare policy granulari è fondamentale avere il contesto completo di ogni dispositivo. È necessario conoscere il contesto operativo o la finalità di ciascun dispositivo per decidere come proteggerlo e gestirlo al meglio. L'aumento dei dispositivi e la loro diversità rendono pressoché impossibile acquisire manualmente il contesto; la creazione delle policy senza avere il contesto adeguato mette le operazioni a rischio. eyeSight classifica automaticamente i dispositivi tradizionali, IoT e OT con una tassonomia multidimensionale che identifica la funzione, il tipo, il produttore e il modello di ogni dispositivo, oltre al sistema operativo e relativa versione. L'ispezione approfondita dei pacchetti di oltre 100 protocolli IT e OT consente ad eyeSight di rivelare in modo esaustivo l'identità dei dispositivi IoT e OT.

eyeSight classifica automaticamente:

- oltre 500 differenti versioni dei sistemi operativi;
- oltre 5000 differenti marche e modelli;
- i dispositivi sanitari di oltre 350 importanti fornitori di tecnologia medicale;
- migliaia di dispositivi di controllo e automazione industriale utilizzati nei settori manifatturiero, energetico, petrolio e gas, servizi pubblici, minerario e altri settori delle infrastrutture strategiche

Forescout Device Cloud è il motore della classificazione automatica in eyeSight e assicura che questa ricca fonte di contesto continui a tenere il passo con l'aumento e la diversità dei dispositivi. Forescout Research si avvale delle informazioni di intelligence fornite al nostro cloud* da oltre 8 milioni di dispositivi reali e pubblica i nuovi profili di frequente per migliorare l'efficacia, la copertura e la velocità della classificazione nell'intero panorama dei dispositivi.

Figura 4: Forescout Device Cloud..



*Al 31 dicembre 2018.

Valutazione della condizione del dispositivo

La classificazione offre il contesto operativo e la finalità di un dispositivo, in pratica segnala di cosa si tratta. Per il contesto completo è comunque necessario un altro strumento, che determini l'integrità e pulizia di ciascun dispositivo.

eyeSight monitora continuamente la rete e valuta la configurazione, lo stato e la condizione di sicurezza dei dispositivi connessi per determinarne i profili di rischio e la loro adesione alle policy di sicurezza e di conformità alle normative. eyeSight risponde alle domande importanti, fra cui:

- Il software di sicurezza è installato, operativo e aggiornato con le ultime patch?
- Ci sono dei dispositivi che eseguono applicazioni non autorizzate o che violano gli standard di configurazione?
- I dispositivi utilizzano password predefinite o elementari (particolarmente rischioso per i dispositivi IoT)?
- Sono stati rilevati dei dispositivi ostili, compresi quelli che si spacciano per dispositivi legittimi tramite le tecniche di spoofing (e tali dispositivi sono connessi alla rete)?
- Quali dei dispositivi connessi sono più vulnerabili alle ultime minacce?

La potenza delle informazioni di intelligence sui dispositivi

La visibilità dei dispositivi fornita da eyeSight tramite scoperta, profilazione, classificazione automatica e valutazione compare subito nella console Forescout. Consente di acquisire dati di alto livello nelle dashboard personalizzabili e di condividere delle istantanee sui progressi compiuti verso gli obiettivi di rischio e conformità. Queste viste dinamiche aiutano gli addetti a:

- valutare il successo di una particolare policy attuata;
- identificare i dispositivi vulnerabili nel caso di una violazione per accelerare la risposta agli eventi;
- monitorare l'adesione nel corso del tempo a specifici requisiti di conformità;
- costruire viste idonee per dirigenti esecutivi e revisori in merito a rischi e conformità, oltre che sulle potenziali vulnerabilità;
- approfondire le aree di un problema relative a specifiche policy, tipi di dispositivi, sedi, ecc. per la risoluzione.

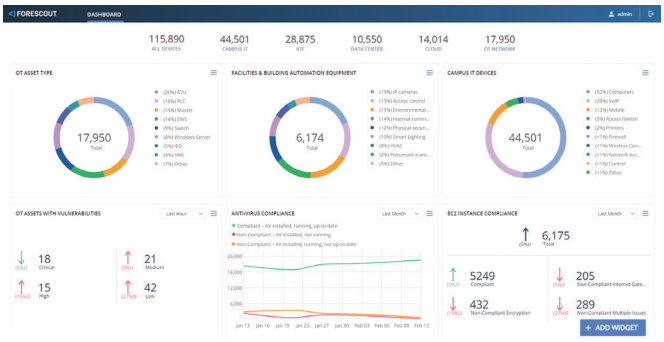


Figura 5. personalizzazione della dashboard per dare a diverse parti interessate il contesto di cui hanno bisogno.

La visibilità sui dispositivi offerta da eyeSight può essere condivisa anche con parti interessate di diverse aree funzionali informatiche tramite le azioni di notifica e le API. Il portafoglio di prodotti eyeExtend condivide il contesto dei dispositivi con altri prodotti leader, informatici e di sicurezza, per automatizzare i flussi di lavoro e coordinare una risposta a livello di sistema.

Senza il fondamentale contesto dei dispositivi di eyeSight, le aziende non possono implementare in tranquillità le policy di controllo, dato che le azioni basate su informazioni insufficienti possono mettere le operazioni aziendali a rischio. eyeSight fornisce gli approfondimenti necessari per progettare e mettere in atto policy granulari e per automatizzare le azioni delle iniziative di gestione delle risorse, conformità dei dispositivi, accesso alla rete, segmentazione della rete e risposta agli eventi. Con i prodotti Forescout eyeControl e Forescout eyeExtend puoi quindi stabilire con tranquillità efficaci controlli basati sulle policy e coordinare le azioni.

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