

eyeSight

Visibilità completa dei dispositivi

SENZA AGENT

Acquisisci un inventario unificato e in tempo reale dei dispositivi connessi alla rete.

ACCURATO

Profila tutti i dispositivi per ottenere il contesto necessario alla realizzazione di sicurezza e conformità proattive.

EFFICACE

Identifica i dispositivi ostili, vulnerabili o non conformi e crea criteri per limitare i rischi.

AFFIDABILE

Ottieni l'assicurazione in tempo reale sul funzionamento di strumenti di sicurezza e controlli di conformità.

EFFICIENTE

Misura e segnala automaticamente il comportamento di conformità e l'esposizione al rischio informatico, riducendo al minimo l'errore umano e aumentando l'efficienza.

Scopri, classifica e valuta continuamente ogni dispositivo connesso in tutta l'impresa.

Forescout eyeSight offre approfondimenti senza pari sull'intero panorama EoT senza interrompere i processi aziendali critici.

- Individua tutti i dispositivi con connessione IP.
- Classifica automaticamente i dispositivi e acquisisci il contesto completo
- Valuta la conformità ai criteri e il comportamento di sicurezza del dispositivo.



SCOPRI

Visualizza i dispositivi dall'istante in cui si connettono alla rete.

Monitora continuamente seguendo l'andamento dei dispositivi.

Assicurati l'inventario in tempo reale delle risorse senza interrompere le attività.



CLASSIFICA

Identifica i diversi tipi di dispositivi IT, IoT e OT.

Sfrutta la potenza di Forescout Device Cloud.

Migliora efficacia, copertura e velocità della classificazione automatica.



VALUTA

Individua le aree scoperte dalla sicurezza e le lacune nella conformità.

Valuta l'adesione ai mandati interni ed esterni.

Ottieni un quadro completo della situazione sul rischio informatico e operativo.



SCOPRI

Scoperta continua senza agent

Elimina i punti ciechi e riduci il rischio operativo con la visibilità completa su tutto l'EoT:

- Laptop, tablet, smartphone, sistemi BYOD/ospiti e dispositivi per lavoro in remoto.
- Dispositivi IoT nelle reti dei campus, nei data center, nelle filiali, nei siti remoti e nelle reti edge.
- Istanze di cloud pubblico e privato in ambienti AWS, Azure e VMware.
- Sistemi di tecnologia operativa (OT) compresa l'automazione medica, industriale ed edile.
- Infrastrutture di rete fisiche e SDN, compresi switch, router, punti di accesso wireless e centraline.

Sfrutta la flessibilità di oltre 20 tecniche di monitoraggio attivo e passivo attraverso reti cablate, wireless, VPN, virtuali e definite da software. Evita di interrompere l'attività dei dispositivi sensibili alle tecniche di scansione attive.

DA PASSIVO A INFRASTRUTTURA

Trap SNMP

Analisi del flusso del traffico SPAN

- NetFlow
- NetFlow flessibile
- IPFIX
- sFlow

Richieste DHCP

Traffico agente-utente HTTP

Fingerprinting TCP

Analisi dei protocolli

Richieste RADIUS

DA PASSIVO A DISPOSITIVO FINALE

Polling dell'infrastruttura di rete

Integrazione SDN

- Meraki
- Cisco ACI

Integrazione cloud pubblico/privato

- VMware
- AWS
- Azure

Interrogazione dei servizi di directory (LDAP)

Interrogazione di applicazioni web (REST)

Database di query (SQL)

Coordinamenti eyeExtend

DA ATTIVO A DISPOSITIVO FINALE

Ispezione di Windows senza agent

- WMI
- RPC
- SMB

Ispezione di Mac e Linux senza agent

- SSH

NMAP

Query SNMP

Query HTTP

SecureConnector®

CLASSIFICA

Classificazione automatica e intelligente

I criteri zero trust possono essere applicati solo se radicate nel contesto completo del dispositivo. Raccogliere manualmente questo contesto è quasi impossibile, e i criteri zero trust implementati senza un contesto completo del dispositivo possono mettere a rischio le operazioni. L'ispezione approfondita dei pacchetti di oltre 150 protocolli IT e OT consente ad eyeSight di profilare in modo tutti i dispositivi IT, IoT e OT. La tassonomia di classificazione multidimensionale identifica la funzione e il tipo di dispositivo, il sistema operativo e la versione, il fornitore e il modello, tra cui:

- Oltre 600 differenti versioni dei sistemi operativi.
- Oltre 5.700 differenti marche e modelli.
- I dispositivi sanitari di oltre 400 importanti fornitori di tecnologia medica.
- Migliaia di sistemi di controllo e di dispositivi di automazione industriale utilizzati nei settori manifatturiero, energetico, petrolio e gas, servizi pubblici, minerario e altri settori delle infrastrutture strategiche.

EYESIGHT RISOLVE:

Lacune di visibilità causate da team isolati e strumenti di sicurezza diversi.

Rischi operativi e aziendali dovuti ai processi manuali inclini all'errore.

Informazioni incomplete sulle minacce che ostacolano l'esecuzione dei criteri di difesa zero trust.

Lacune della sicurezza quando gli strumenti basati su agenti non sono aggiornati o non funzionano correttamente.

Dispositivi inaffidabili non rilevati o spoofing.

Non conformità che può emergere rapidamente tra scansioni sporadiche.

Classificazione automatica con tecnologia Forescout Device Cloud

Device Cloud, il più grande data lake al mondo di informazioni sui dispositivi raccolte in crowdsourcing, assicura la comprensione più completa e accurata di tutti i rischi dei dispositivi nel contesto di qualsiasi.



EFFICACIA COPERTURA VELOCITÀ

Approfondimenti in crowdsourcing sui dispositivi



Aggiornamenti libreria classificazioni

CLASSIFICA IL TUO DISPOSITIVO

Funzione	+	Sistema operativo	+	Fornitore e modello	
• Tablet	• Punto vendita (POS)	• Windows 7	• iOS	• Apple iPad	• GE Water Processor
• Punto di accesso wireless	• Raggi X	• Windows Server 2016	• CentOS	• Apple iPhone	• Hitachi Power System
• Stampante	• Climatizzazione ambienti	• OS X 10.7 Lion	• Android	• Apple Airport	• Hoana Medical
• Server VoIP		• OS X 10.10 Yosemite		• 3M Control System	

VALUTA

Valutazione dello stato del dispositivo

Un altro elemento essenziale dei criteri zero trust è incorporare l'integrità della sicurezza e il profilo di rischio dei dispositivi connessi. eyeSight monitora continuamente la rete per valutare la configurazione, lo stato della sicurezza e gli indicatori di rischio dei dispositivi connessi e stabilire se essi aderiscano o meno agli obblighi di conformità e agli standard di sicurezza. I criteri zero trust possono basarsi su condizioni di rischio e conformità, quali:

- 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, specie i sistemi IoT e OT, utilizzano password predefinite o elementari?
- Sono stati rilevati dispositivi inaffidabili, compresi quelli che si spacciano per dispositivi legittimi?
- Quali dei dispositivi connessi sono più vulnerabili alle ultime minacce?

Vedere non basta.
Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

forescout.com/platform/eyeSight

info-italia@forescout.com

Tel. (internazionale) +1-408-213-3191



Active Defense for the Enterprise of Things™

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

MONITORA

Visibilità e conformità EoT

Ottieni approfondimenti fruibili dalle dashboard pronte all'uso e personalizzabili per individuare rapidamente, assegnare la priorità e mitigare proattivamente i rischi su tutto quanto è connesso. Le viste dinamiche consentono ad analisti della sicurezza e team SOC di eseguire le azioni seguenti:

- Valutare l'avanzamento di rischio e conformità su tutti o su qualsiasi sottoinsieme di criteri.
- Identificare dispositivi vulnerabili e compromessi per accelerare la risposta agli incidenti.
- Rilevare le tendenze della conformità nel corso del tempo.
- Personalizzare e condividere viste predisposte per dirigenti e revisori di rischio e conformità.
- Cercare e filtrare rapidamente le risorse EoT per criteri o attributi dei dispositivi

Segmentazione, coordinamento e applicazione

Estendere il valore di eyeSight con una suite di prodotti Forescout per progettare e implementare i criteri zero trust per il controllo accessi alla rete, la sicurezza IoT, la segmentazione della rete e la sicurezza OT.

Per ulteriori informazioni sui prodotti Forescout eyeSegment, eyeControl, eyeInspect e eyeExtend, visita www.forescout.com/platform/.

[Maggiori informazioni su Forescout.it](https://www.forescout.com/platform/)

© 2020 Forescout Technologies, Inc. Tutti i diritti riservati. Forescout Technologies, Inc. è una società del Delaware. Un elenco dei nostri marchi e brevetti è reperibile alla pagina <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Altri marchi, prodotti o nomi di servizi possono essere marchi o marchi di servizio dei rispettivi titolari. Versione 08_20