FORESCOUT
Active Defense for the Enterprise of Things™

Segmentazione zero trust semplice e senza alcuna interruzione di servizio per l'OT

Proteggi in sicurezza le reti OT estese con un'avanzata gestione dei rischi e la segmentazione dinamica

Gli approcci tradizionali alla protezione dei dispositivi OT (tecnologie operative) nelle reti OT e dei sistemi di controllo industriale (ICS), hanno dipeso a lungo dal mantenimento della separazione fra applicazioni industriali, reti informatiche e utenti ad accesso remoto. Ora però, mentre le aziende OT modernizzano le proprie infrastrutture con nuove tecnologie, quali Cloud SCADA, DCS e sistemi avanzati di esecuzione della produzione (Manufacturing Execution Systems, MES), le tradizionali strategie a zona non sono più sufficienti per mantenere sicuri gli ambienti OT.

Le sfide degli ambienti OT includono:

- Rischio di spostamento laterale del malware e degli hacker, minacce interzonali provenienti dal reparto informatico e l'impatto degli utenti remoti sull'infrastruttura informatica-fisica e OT.
- Rilevamento e mitigazione della diffusione del malware e delle minacce interzonali che influiscono sull'infrastruttura informatica-fisica e OT.
- Complessità operativa generata dalla presenza di fornitori diversi e dall'applicazione discontinua dei controlli di segmentazione negli ambienti OT estesi.

La soluzione Forescout: il meglio per l'OT

Se le problematiche citate sopra ti suonano familiari, è arrivato il momento di valutare la soluzione Forescout. Ti aiuta a semplificare la segmentazione Zero Trust e a ottimizzare la gestione dei rischi relativi a dispositivi IT, OT e di controllo industriale nella tua eterogenea Enterprise of Things (EoT).

Con la piattaforma Forescout puoi:

- **Accelerare la segmentazione Zero Trust** nei gruppi IT e OT.

"Entro il 2021 l'80% dei progetti di IoT industriale [IIoT] avrà dei requisiti di sicurezza specifici dell'OT, rispetto al 40% di oggi".[1]

GARTNER

"Le tecnologie IoT e dei dispositivi di rete hanno introdotto una potenziale violazione di reti e aziende. [...] I team preposti alla sicurezza devono isolare, proteggere e controllare ogni dispositivo nella rete, continuamente".

FORRESTER RESEARCH

forescout.com/platform/eyeSegment info-italia@forescout.com Tel. (internazionale) +1-408-213-3191

- **Comprendere istantaneamente lo stato di segmentazione IT-OT**, in tempo reale e su qualsiasi dispositivo, ovunque si trovi nell'ambiente esteso.
- **Visualizzare i flussi del traffico** in base alla tassonomia logica di utenti, applicazioni, servizi, funzioni, ubicazioni, dispositivi e livello di rischio.
- **Ridurre la superficie di attacco e mantenere la conformità** tramite la segmentazione dinamica fra gli ambienti IT, IoT e OT.
- **Ottimizzare i flussi di lavoro IT-OT** e sfruttare gli investimenti esistenti con una policy di segmentazione uniforme in tutta l'azienda.
- **Ridurre costi e rischi della conformità tramite l'efficiente gestione dell'accesso tra reti**, con la necessità di un minor numero di persone.

"Negli ultimi tre anni quasi il 20% delle aziende ha subito almeno un attacco basato sull'Internet of Things (IoT)".[3]

GARTNER

Gestione ottimizzata del rischio e segmentazione Zero Trust per le reti IT-OT

La soluzione Forescout assicura visibilità estesa sui dispositivi per le reti OT e abilita la gestione efficace e in tempo reale di una vasta gamma di rischi operativi e informatici. La soluzione affronta i problemi delle aziende negli ambienti OT estesi, legati alla segmentazione multi-dominio con molteplici casi d'uso e alla mitigazione dei rischi, per accelerare il rilevamento e la risposta non intrusivi contro le minacce.

Forescout eyeSegment ti aiuta a progettare e distribuire la segmentazione Zero Trust associando automaticamente i flussi del traffico a una tassonomia logica di utenti, applicazioni, servizi, funzioni, ubicazioni, dispositivi e livelli di rischio nell'intera rete aziendale. Ciò rende possibile determinare in tempo reale i valori di riferimento del traffico OT senza distribuire gli agent né riprogettare l'infrastruttura. Ti permette inoltre di modellare l'impatto delle policy di segmentazione prima di imporle.

AUMENTA IL VALORE DEGLI INVESTIMENTI IN TECNOLOGIE INFORMATICHE E DI SICUREZZA

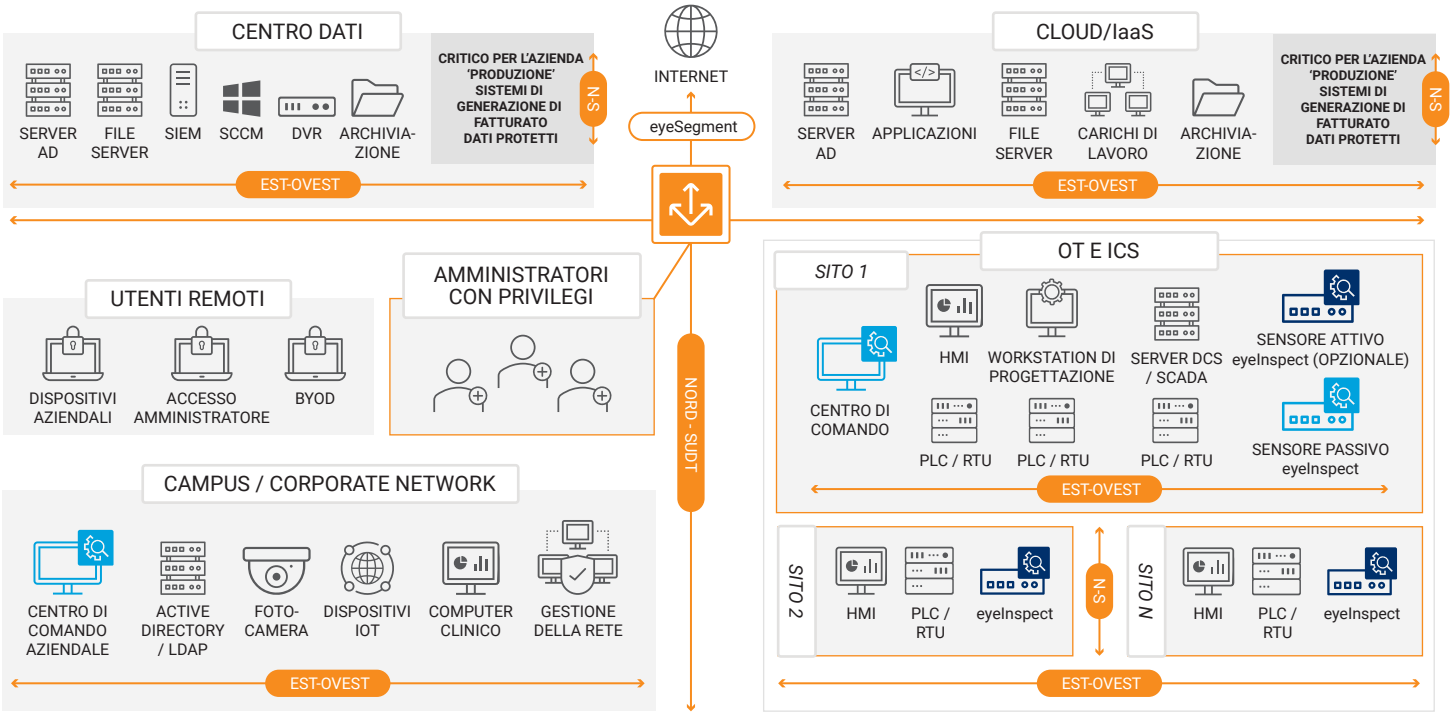
- Affronta il rischio della convergenza IT-OT (spostamento laterale) con un approccio unificato alla policy di segmentazione.
- Affronta il rischio legato ai dispositivi OT con la pianificazione granulare della policy di segmentazione, il monitoraggio e la risposta.
- Abilita una segmentazione non intrusiva e dinamica per gli ambienti OT sensibili sfruttando l'investimento esistente (infrastruttura).

Forescout eyeInspect (ex SilentDefense) protegge l'infrastruttura essenziale con un'ispezione approfondita dei pacchetti (DPI) brevettata e una vasta libreria di indicatori di minaccia specifici per i sistemi di controllo industriale. eyeInspect monitora in tempo reale le comunicazioni nella rete e fornisce dettagliate informazioni contestuali su risorse della rete, protocolli e contenuti delle comunicazioni. Con funzioni potenti, quali l'Aggregazione Avanzata degli Avvisi e i Valori di Riferimento delle Risorse, puoi automatizzare le attività di rilevamento delle minacce e di conformità che riducono il rischio e supportano l'imposizione della segmentazione OT.

Figura 1. La matrice di eyeSegment ti permette di concentrarti sulle cose più importanti, così puoi analizzare e indagare un particolare andamento del traffico nel tuo ambiente. A prescindere da dove ti trovi nella gerarchia della tabella, puoi creare le policy di eyeSegment che desideri per segmentare uno specifico modello di traffico e proteggere la tua impresa, garantendo al contempo la continuità operativa e produttiva.

La soluzione Forescout per la segmentazione della rete trova un'ampia gamma di utilizzi per l'OT. Grazie alla sua flessibilità, in ogni scenario la piattaforma Forescout è in grado di abbassare il rischio di interruzione dell'attività e di ridurre al minimo i costi operativi legati ai progetti di segmentazione. Ecco alcuni dei principali casi d'uso:

- Mitigazione dei rischi, mantenimento della conformità e riduzione dei costi operativi nelle reti OT.
- Visibilità istantanea e in tempo reale sugli ambienti OT per modellare policy di segmentazione non intrusive.
- Accelerazione della segmentazione Zero Trust IT-OT.



Fgura 2. La soluzione Forescout ti aiuta a mitigare le minacce e a comprendere istantaneamente, in tempo reale, lo stato della tua segmentazione. Nell'esempio di cui sopra, eyeSegment impedisce ai dispositivi connessi di attraversare i domini della sanità e IT-OT.

1. Invest Implications: 'Cool Vendors in Industrial IoT and OT Security (Fornitori interessanti per la sicurezza IIoT e OT), Gartner Research, aprile 2018
2. Mitigating Ransomware With Zero Trust (Mitigare il ransomware con il modello Zero Trust), Forrester Research, Inc., 8 giugno 2020
3. IoT Security Primer: Challenges and Emerging Practices (Manuale di base per la sicurezza IoT: sfide e pratiche emergenti), Gartner, gennaio 2020

Vedere non basta. Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

forescout.com/platform/eyeSegment info-italia@forescout.com Tel. (internazionale) +1-408-213-3191

FORESCOUT
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

Maggiori informazioni su Forescout.it