FORESCOUT
Active Defense for the Enterprise of Things.

Sicurezza IoT

Scegliere un modello Zero Trust flessibile per proteggere i dispositivi non tradizionali nell' Enterprise of Things

I dispositivi IoT spesso rimangono invisibili all'interno delle reti aziendali perché, a differenza dei sistemi tradizionali, non sono facili da monitorare e raramente supportano agent software. Di conseguenza, ampliano la superficie di attacco dell'azienda e rappresentano un grave rischio poiché sono suscettibili a compromissioni e sfruttabili come comodi punti di intrusione in reti vulnerabili. Le aziende devono dotarsi di una soluzione di sicurezza che, su base continua, sia in grado di identificare, segmentare e imporre la conformità di ogni dispositivo IoT, anche su reti eterogenee.

Dispositivi IoT: il gioco vale la candela?

I dispositivi IoT sono risorse aziendali valide, in alcuni casi addirittura indispensabili. Incrementano la produttività, migliorano la qualità di prodotti e servizi offerti, generano profitti. Il 63% delle aziende si aspetta di ottenere un ritorno finanziario dai progetti IoT nell'arco di tre anni[2]. Aggressori sofisticati e ben finanziati studiano sempre con attenzione le aziende alla ricerca di punti deboli da sfruttare, come lacune in materia di visibilità e sicurezza dei dispositivi IoT, vulnerabilità che causano interruzioni dell'attività, violazioni dei dati, furti di proprietà intellettuale e danni reputazionali. Due considerazioni importanti:

- In una recente indagine condotta dal Ponemon Institute è emerso che quasi 9 intervistati su 10 si aspettano di subire un attacco informatico o una violazione dei dati, diretta ad applicazioni o dispositivi IoT non sufficientemente protetti, nel giro dei prossimi due anni[3].
- Entro il 2023 il CIO medio sarà responsabile di oltre il triplo degli endpoint che gestiva nel 2018.[4]

DEFINIZIONE DI ZERO TRUST

Il modello di gestione della sicurezza aziendale Zero Trust, ossia fiducia zero, di Forrester è una metodologia concettuale e architetturale. Nella sua forma più semplice, l'approccio Zero Trust consiste nel creare interazioni in cui sia l'utente, sia il dispositivo e sia l'accesso siano considerati affidabili. Ogni utente può accedere esclusivamente alle risorse aziendali di cui ha bisogno per svolgere le proprie mansioni. Secondo Forrester[1], per implementare una strategia Zero Trust efficace, è necessario:

- Riprogettare le reti creando microperimetri protetti
- Rafforzare la sicurezza dei dati usando tecniche di offuscamento
- Limitare i rischi causati da un eccesso di privilegi e accessi utente
- Impiegare l'analisi e l'automazione per migliorare drasticamente il rilevamento e la risposta alle minacce

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

Nei moderni ambienti EoT (Enterprise of Things), a cui si collegano un numero infinito di oggetti IT, IoT e OT (tecnologie operative) che interagiscono tra loro, le aziende devono poter contare su una soluzione di sicurezza che renda tutti i dispositivi IoT e con connessione IP visibili e controllabili secondo un approccio alla sicurezza basato sul modello Zero Trust. In caso contrario, qualsiasi dispositivo sarà suscettibile di essere violato e sfruttato per scopi malevoli.

L'approccio Zero Trust di Forescout

Forescout ritiene che la strategia di sicurezza IoT debba basarsi su un approccio Zero Trust che combini visibilità completa sui dispositivi, segmentazione proattiva della rete e controllo degli accessi basato sul principio del privilegio minimo per tutte le risorse digitali, ovvero dispositivi, utenti, applicazioni e carichi di lavoro. La piattaforma Forescout consente di gestire in modo efficace i rischi informatici, operativi e di conformità dell'intero ambiente EoT perché garantisce:

- Visibilità completa sui dispositivi IoT, IoMT (Internet of Medical Things) e OT non gestiti nonché su tutti i sistemi con connessione IP
- Individuazione e valutazione dei dispositivi IoT che hanno credenziali deboli o predefinite e automazione delle azioni basate sulle policy per l'imposizione di password complesse
- Informazioni in tempo reale su comunicazioni e comportamenti sospetti dei dispositivi IoT nell'intero ambiente esteso
- Segmentazione dei dispositivi in zone di sicurezza affidabili tramite l'applicazione di una policy di controllo degli accessi basata sul principio del privilegio minimo di Zero Trust
- Automazione del coordinamento di policy Zero Trust condivise in ambienti in cui sono presenti sistemi di più vendor e in domini di rete diversi
- Eliminazione delle gestioni di sicurezza separate per accelerare la risposta e ottimizzare il valore degli investimenti fatti in altre soluzioni di sicurezza
- Per le aziende che operano nel settore sanitario, rileva proattivamente e riduce vulnerabilità e minacce, applica policy di accesso e regole di segmentazione della rete granulari, neutralizza immediatamente le minacce rivolte ai dispositivi medicali e facilita la remediation grazie a una stretta integrazione con Medigate

"Forescout è il fornitore del modello di sicurezza per IoT/OT basato sul modello Zero Trust da considerare. La messa in sicurezza dei dispositivi IoT/OT è uno dei problemi più spinosi per le aziende. Questo è il punto forte di Forescout. Le funzionalità della sua piattaforma per la sicurezza IoT/OT fanno impallidire quelle dei concorrenti."

THE FORRESTER WAVE: ZERO TRUST EXTENDED ECOSYSTEM PLATFORM PROVIDERS, FORRESTER RESEARCH, OTTOBRE 2019

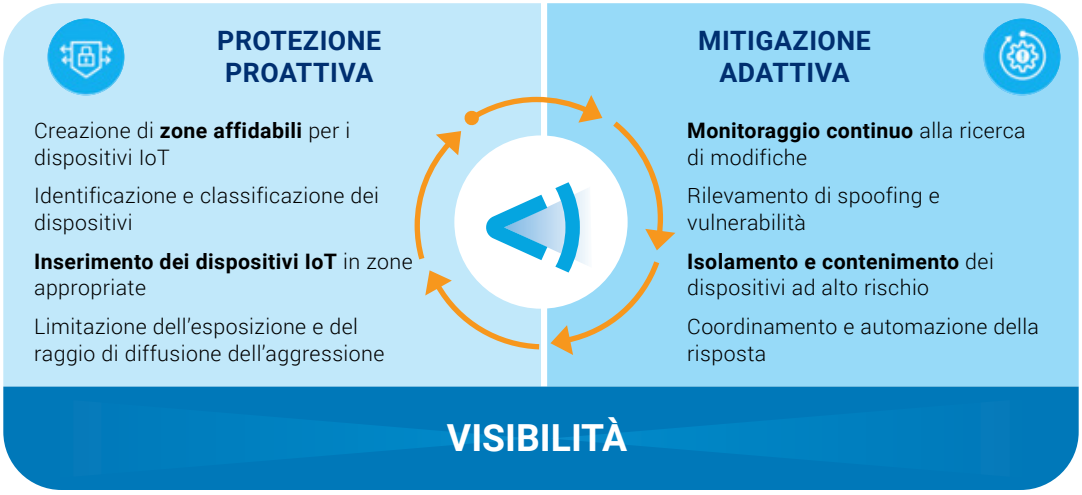

Figura 1: Forescout difende attivamente tutti i dispositivi del tuo ambiente EoT identificando, segmentando e imponendo la conformità di ogni dispositivo

Individuazione e classificazione del 100% dei dispositivi con connessione IP

È indispensabile ottenere visibilità completa e dati contestuali su tutti i dispositivi IoT, OT e sugli endpoint dell'infrastruttura critica di un ambiente eterogeneo. La piattaforma Forescout:

- Senza ricorrere ad agent software, individua immediatamente qualsiasi dispositivo con connessione IP, fisico o virtuale, che si connette alla rete.
- Fornisce una visibilità estesa su tutti i dispositivi usando una combinazione di oltre 20 tecniche di ricerca attive e passive, di profilazione e classificazione.
- Utilizza Forescout Device Cloud, il più ampio data lake in crowdsourcing di dati di intelligence sui dispositivi al mondo che contiene profili di dispositivi, comportamenti e profili di rischio di oltre 12 milioni di dispositivi e che rappresenta il punto di riferimento per più settori.

Segmentazione dinamica della rete e automazione dei controlli

Nei moderni ambienti EoT eterogenei, un'azienda che adotta il modello Zero Trust deve possedere funzionalità di segmentazione della rete e di coordinamento della risposta agli eventi in tutti i domini EoT. Con Forescout, è possibile:

- Combinare le procedure di accesso alle identità utente, per scoprire chi fa che cosa, quando, dove e perché
- Spostare i dispositivi in segmenti di rete dinamici in base a policy e dati contestuali aggiornati in tempo reale
- Mappare i flussi di dati per progettare e simulare policy di segmentazione da implementare in modalità non intrusiva
- Automatizzare la segmentazione per ridurre i rischi informatici e operativi

Coordinamento della sicurezza e imposizione della conformità

Moltissime aziende sono sommerse da una montagna di costose soluzioni di sicurezza che servono a un solo scopo e che non sono in grado di condividere i dati che acquisiscono né di elaborare una risposta agli incidenti coordinata. Forescout è l'antidoto a questa inefficienza. Con i prodotti Forescout eyeExtend è possibile condividere i dati contestuali sui dispositivi tra la piattaforma Forescout e gli altri strumenti di sicurezza e IT con cui automatizzare i flussi di lavoro e l'applicazione di policy su soluzioni eterogenee. Queste funzionalità di coordinamento aiutano a:

- Migliorare la protezione dei dispositivi IoT e la conformità di tutti i dispositivi
- Ridurre il tempo medio di rilevamento e risposta
- Ottenere un ROI maggiore sui software di sicurezza esistenti
- Automatizzare l'aggiornamento del database di gestione delle configurazioni ed eliminare la compilazione manuale degli inventari, operazione dispendiosa in termini di tempo e suscettibile di errori

"Ora finalmente abbiamo visibilità sulla nostra rete, vediamo anche i dispositivi IoT come stampanti, telefoni VoIP e telecamere di sorveglianza. Forescout classifica ogni dispositivo e lo inserisce nel segmento VLAN appropriato."

– KEN COMPRES, SENIOR NETWORK SECURITY AND INTEGRATION ENGINEER/CSO, HILLSBOROUGH COMMUNITY COLLEGE COLLEGE

1 Five Steps to a Zero Trust Network (I cinque fondamenti di una rete Zero Trust), Roadmap Report, Forrester Research, ottobre 2018

2 A New Roadmap for Third Party IoT Risk Management, Benchmark Study (Nuova roadmap per la gestione del rischio IoT, Analisi comparativa), Ponemon Institute, Sabine Zimmer, 3 giugno 2020

3 Internet of Things: Unlocking True Business Potential (IoT: come valorizzarne il potenziale per il business), Gartner

4 Gartner Top Strategic IoT Trends and Technologies Through 2023 (Principali trend e tecnologie per l'IoT individuate da Gartner fino al 2023), settembre 2018

Vedere non basta. Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

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

FORESCOUT
Active Defense for the Enterprise of Things.

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

info-italia@forescout.com
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Maggiori informazioni su forescout.it