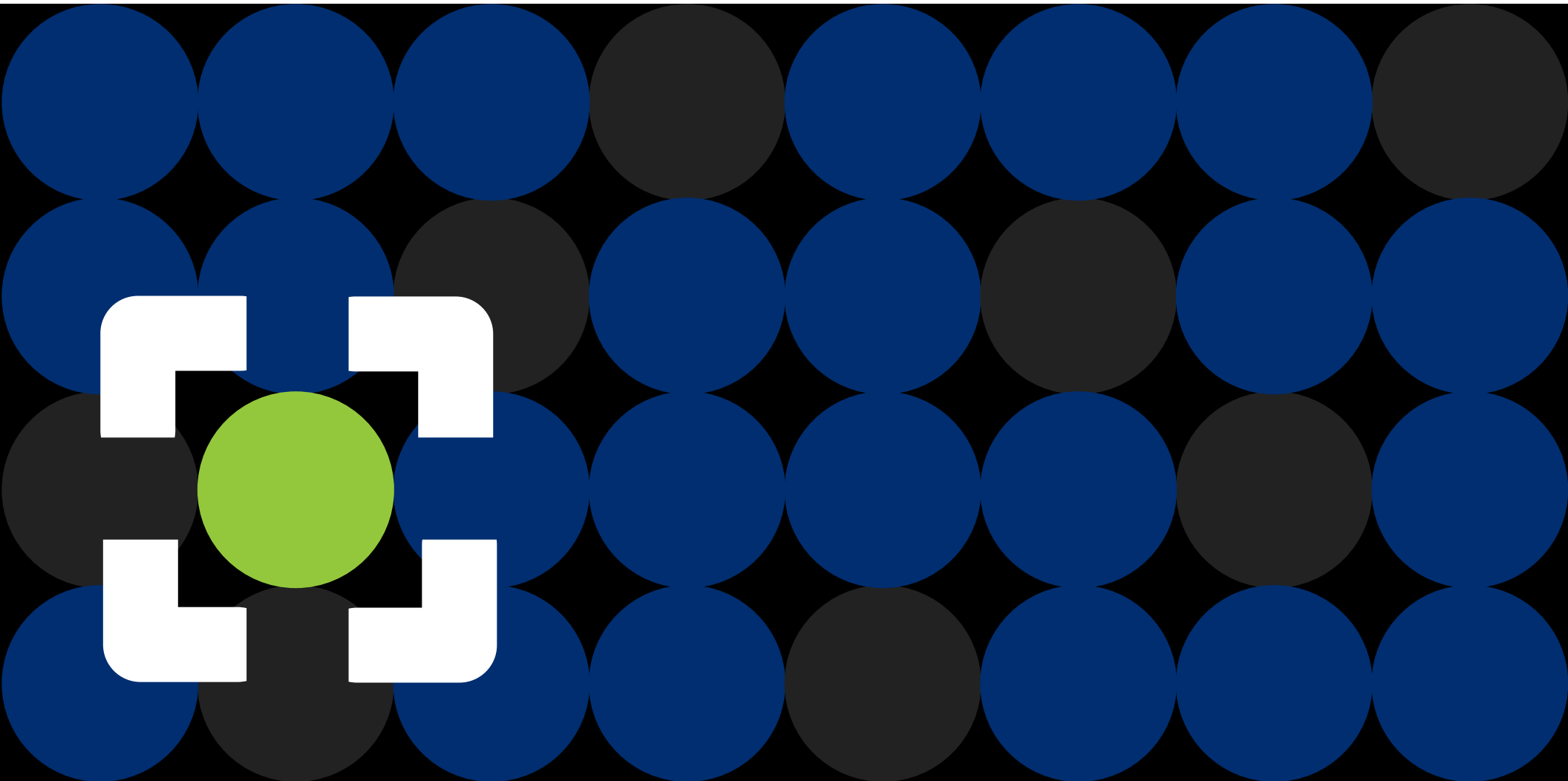
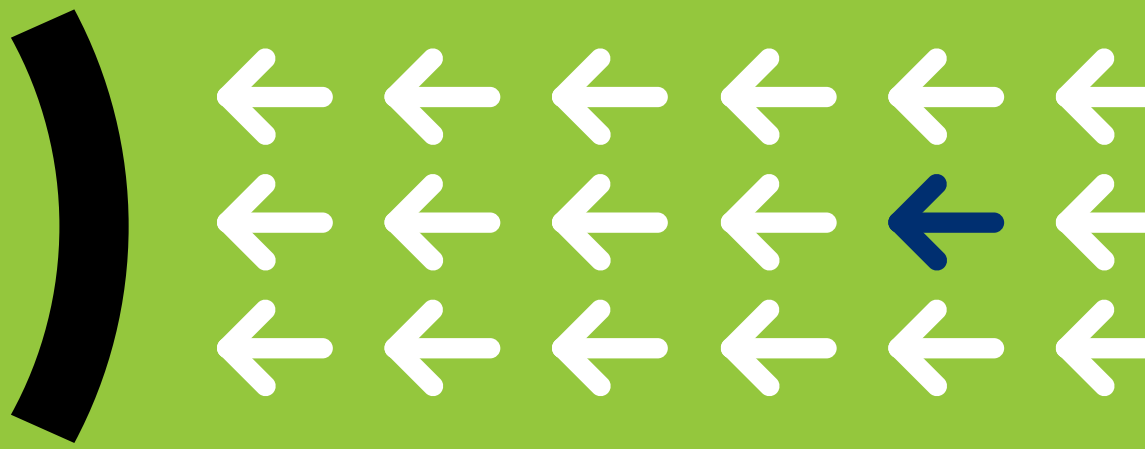
FORESCOUT
Active Defense for the Enterprise of Things™

Come proteggere l'Enterprise of Things
Cinque sfide per la sicurezza



SOMMARIO



INTRODUZIONE

Nelle reti aziendali odierne i dispositivi proliferano in maniera incontrollata. Si tratta di una vera e propria esplosione, sia in termini di numeri (miliardi) che di tipologie (IT, OT, IoT, BYOD). Alcuni di essi sono noti e gestiti, mentre altri passano inosservati e sfuggono al rilevamento. Per quanto riguarda i rispettivi utenti, sono letteralmente sparsi dappertutto. Dipendenti, collaboratori esterni, partner e clienti si connettono al data center o al cloud da qualsiasi luogo, in modo sicura ma anche non sicuro.

Tutto questo rende ciascun ambiente di rete *complicato*: una vera **Enterprise of Things** (EoT) che richiede una pianificazione attenta e azioni risolute quando si tratta di proteggere i dispositivi e l'azienda stessa.

Di seguito esaminiamo le cinque principali sfide poste oggi dall'EoT ai responsabili della sicurezza informatica e delle operazioni, oltre ai consigli pratici per risolverle.

SFIDA 1

Come inventariare i dispositivi non gestiti e regolarne la proliferazione?

> **Per il solo 2020, gli esperti stimano in 31 miliardi le installazioni di dis positivi IoT in tutto il mondo.**
>
> ***SECURITY TODAY, 13 GENNAIO 2020***[1]

> **“Secondo il 62% degli interpellati, la capacità della propria azienda di raggiungere uno stato di sicurezza più maturo dipenderà sempre di più dalla convergenza dei sistemi di controllo IT e OT”.**
>
> **PONEMON INSTITUTE, FEBBRAIO 2019**[2]

I dispositivi gestiti che incorporano un agent di sicurezza, come PC, computer portatili e smartphone aziendali, stanno diventando una rarità rispetto ai miliardi di dispositivi IoT e delle tecnologie operative (OT), privi di agent, che si collegano alle reti. Allo stesso tempo, si sta verificando una convergenza delle reti IT-OT che aumenta la produttività e semplifica la gestione, ma aggiunge anche dei rischi. Nelle odierne reti eterogenee, comprendere quali sono le superfici d’attacco è difficile come mai prima d’ora.

Consigli:

- Stabilisci quali sono gli strumenti che ti forniscono visibilità al 100% sui dispositivi, senza punti ciechi.
- Limita la tua procedura di selezione includendo solamente quelle soluzioni che possono svolgere una valutazione dello stato di sicurezza in tempo reale, senza agent.
- Aiuta le operazioni di sicurezza e il personale informatico con funzioni di inventario delle risorse in tempo reale.

SFIDA 2

Negli ambienti aziendali odierni, dove si annida il rischio?

> **“Edifici intelligenti, dispositivi medici, apparecchiature di rete e telefoni VoIP rappresentano i gruppi di dispositivi IoT più rischiosi”.**
>
> **FORESCOUT RESEARCH, MAGGIO 2020[3]**

> **“Le tecnologie IoT e dei dispositivi di rete hanno introdotto una po tenziale violazione di reti e aziende. [...] I team preposti alla sicurezza devono isolare, proteggere e controllare ogni dispositivo nella rete, continuamente”.**
>
> **FORRESTER RESEARCH, GIUGNO 2020[4]**

Il concetto di analisi dei rischi sta mutando e si sta ampliando, insieme alla tua superficie di attacco. Una recente analisi di Forescout sull’Enterprise of Things ha determinato che sono i dispositivi IoT a costituire il rischio maggiore. “Non solo sono difficili da monitorare e controllare, ma creano anche delle vulnerabilità poiché fanno da ponte tra il mondo fisico e quello cibernetico, che prima erano separati. I dispositivi IoT possono fungere da porte d’ingresso illecite nelle reti oppure essere i bersagli principali del malware specializzato”.[3]

Consigli:

- Per comprendere la tua superficie di attacco utilizza un’analisi dei rischi a più fattori.
- Passa a una strategia di difesa attiva che incorpori un approccio Zero Trust.
- Accelera la risposta alle minacce ordinando gli avvisi per priorità, in base al livello di rischio.
- Infine, ribadiamo che una visibilità totale sui dispositivi è essenziale.

SFIDA 3

Il perimetro della rete è svanito. E adesso?

> **“Per mettere in sicurezza i confini della rete aziendale è necessario adottare delle nuove procedure consigliate”.**
>
> **GARTNER, MAGGIO 2020[5]**

Apertura e sicurezza? Come è possibile, nel caso di reti che abbracciano ambienti fisici, centri dati, cloud e ambienti OT? Ora che le reti aziendali si estendono a qualunque luogo del mondo ove esistano lavoratori e carichi di lavoro, intorno a un’azienda non esiste più un perimetro difendibile. Siamo arrivati a un punto in cui i perimetri devono circondare ogni dispositivo connesso e ogni carico di lavoro. La sicurezza inizia al margine di una risorsa.

Consigli:

- Limita l’accesso alle risorse aziendali usando un modello a privilegi minimi come lo Zero Trust
- Esegui in continuazione il rilevamento di tutti i dispositivi che accedono alla rete e la valutazione del loro stato di sicurezza, a prescindere dalla loro ubicazione.
- Imponi una conformità rigorosa, basata sulle policy, a tutte le risorse: in sede, BYOD e remote.

SFIDA 4

La segmentazione è indispensabile, ma come eseguirla in maniera corretta, senza interrompere le attività aziendali?

> **“Secondo le nostre stime, il 90% delle aziende con cui abbiamo parla to ha in cantiere progetti di segmentazione per quest’anno. Benché si tratti di qualcosa desiderato da tutti, non è sempre chiaro da dove iniziare, quali sono i rischi, né se ne vale i costi e la fatica necessari”.**
>
> **FORESCOUT RESEARCH, GENNAIO 2019[6]**

Per anni la segmentazione della rete ha goduto di una cattiva reputazione. Fino a poco tempo fa, gli strumenti di segmentazione disponibili erano difficili da distribuire e non potevano attraversare i domini della rete, con il risultato di interruzioni delle attività e frammentazione dell’ambiente. I problemi sono solo peggiorati quando le aziende hanno aggiunto dei nuovi dispositivi e hanno ulteriormente ampliato le proprie reti. Oggi però esistono soluzioni di segmentazione solide, per cui non ha più senso rimanere con reti non segmentate e vulnerabili.

Consigli:

- Visualizza la segmentazione e simula le policy prima della distribuzione, in modo da prevenire inutili interruzioni dell’attività.
- Accertati che la tua soluzione principale possa semplificare la segmentazione Zero Trust di qualsiasi dispositivo, ovunque (compresi i dispositivi IT, IoT e OT).
- Accelera l’implementazione del modello Zero Trust in tutto l’ambiente aziendale.
- Scegli una moderna piattaforma NAC, concepita per facilitare la segmentazione della rete.

SFIDA 5

Come risolvere il paradosso del “fare di più con meno”?

> **“Le aziende stanno facendo progressi nella riduzione degli strumenti per la gestione di reti frammentate. Tuttavia, il 64% di esse utilizza ancora da quattro a dieci strumenti per monitorare e risolvere i prob lemi delle proprie reti”.**
>
> **NETWORK MANAGEMENT MEGATRENDS 2020, APRILE 2020[7]**

> **“L’interesse nella sicurezza e gestione dei rischi a livello del consiglio di amministrazione ha raggiunto un picco record”.**
>
> **GARTNER RESEARCH, LUGLIO 2019[8]**

È difficile argomentare che il dipartimento di sicurezza sia un baluardo protettivo efficiente e consenta di risparmiare, quando per gestire sicurezza e rete si utilizza un assortimento di strumenti legacy, frammentati e dalla funzione specifica. Detto questo però, anche i migliori piani di trasformazione possono causare problemi: per esempio, distribuzioni a passo di lumaca, ritorno lento sull’investimento, curve di apprendimento ripide e scarsa soddisfazione per le soluzioni scelte. Per fortuna, selezionando la piattaforma giusta puoi soddisfare tutte le parti interessate, incluso il Direttore Finanziario.

Consigli:

Scegli una piattaforma che possa coordinare gli strumenti esistenti e che soddisfi i criteri seguenti:

- Implementazione veloce, flessibile e non intrusiva.
- Immediata redditività e rapido ritorno sull’investimento.
- Utilizzabile con l’infrastruttura esistente.
- Senza aggiornamenti software o hardware forzati.
- Integrabile con i principali prodotti di sicurezza e IT.
- Rilevamento dei dispositivi, valutandone stato di sicurezza e rischi senza agent.
- Nessuna complessità 802.1X, niente ritardi e costi della distribuzione.
- Possibilità di crescita con elevata scalabilità.
- Miglioramento della produttività delle attività di sicurezza.
- Visibilità, controllo, segmentazione e Zero Trust senza agent.

Che cosa si nasconde dietro queste cinque sfide

Ciascuna delle cinque sfide che abbiamo sopra descritto può sembrare insormontabile. Ma ciascuna di esse, se non risolta, può lasciare aperta la strada al rischio più grave: un attacco informatico che provoca problemi operativi, furto di dati, danni alla reputazione del marchio, multe salate, problemi di pubblica sicurezza e così via.

La chiave è la prevenzione, che implica la disponibilità di una soluzione efficace, in grado di offrire il 100% di visibilità senza agent, il monitoraggio continuo e la risposta automatizzata alle minacce.

*Notes

1. *The IoT Rundown for 2020: Stats, Risks, and Solutions* (Il bilancio dell'IoT per il 2020: statistiche, rischi e soluzioni), Security Today, 13 gennaio 2020
2. *Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT* (Sicurezza, protezione e privacy nel mondo interconnesso di IT, OT e IIoT), Report del Ponemon Institute, febbraio 2019.
3. *The Enterprise of Things Security Report, The State of IoT Security in 2020* (Report sulla sicurezza dell'Enterprise of Things, lo stato della sicurezza IoT nel 2020), Forescout Research Labs, maggio 2020
4. *Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles and Techniques* (Mitigare il ransomware con il modello Zero Trust: migliora le tue difese con i principi e le tecniche Zero Trust), 8 giugno 2020, Forrester Research
5. *Securing the Enterprise's New Perimeters* (Protezione dei nuovi perimetri aziendali), Gartner, 27 marzo 2020
6. *Network Segmentation* (Segmentazione della rete), blog Forescout, gennaio 2019
7. *Network Management Megatrends 2020* (Gestione della rete: i megatrend per il 2020), report Enterprise Management Associates, aprile 2020
8. *Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer* (Cinque domande del consiglio di amministrazione cui i leader della sicurezza e del rischio devono essere preparati a rispondere), Gartner Research, luglio 2019

Vedere non basta. Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

INFORMAZIONI SU FORESCOUT

Forescout è leader nella sicurezza dell'Enterprise of Things e offre una piattaforma completa che identifica, segmenta e applica la conformità costantemente ad ogni oggetto connesso in qualsiasi rete eterogenea. La piattaforma Forescout è la soluzione più distribuita nel mondo, più scalabile e adatta per le grandi aziende, fornendo visibilità e controllo dei dispositivi senza agent. Si distribuisce rapidamente nella tua infrastruttura esistente senza richiedere un agent, un upgrade o l'autenticazione 802.1X. Le aziende Fortune 1000 e gli enti statali si affidano a Forescout per ridurre il rischio di interruzioni dell'attività causate da incidenti o violazioni della sicurezza, garantire e dimostrare la conformità di sicurezza e migliorare la produttività delle procedure di protezione.

forescout.com/platform/eyeSight

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