FORESCOUT

Panoramica della soluzione

Com'è una soluzione NAC moderna?

Identifica tutti i dispositivi, valuta lo stato di sicurezza e applica il controllo degli accessi su reti eterogenee

> "I moderni strumenti NAC sono più adatti per isolare i dispositivi e le entità prive di autorizzazione (utenti, segmenti, dispositivi, ecc.) e impedire che entrino in contatto con la rete. Utilizzate queste nuove tecnologie NAC, come quella proposta da Forescout, per tenere lontane dalle vostre reti Zero Trust entità sconosciute verosimilmente non protette."[1]
>
> — Chase Cunningham, Analista principale, Forrester Research

Le reti moderne hanno bisogno di una soluzione di controllo degli accessi, o NAC (Network Access Control) avanzata, in grado di svolgere operazioni più complesse della semplice autenticazione dei dispositivi. Una soluzione NAC moderna deve avere la capacità di identificare i dispositivi, valutarne lo stato di sicurezza e conformità, applicare il controllo degli accessi su reti eterogenee, monitorare su base continua tutti i dispositivi connessi e automatizzare la risposta quando rileva comportamenti non conformi o insoliti.

Problematiche

Poiché il mondo del lavoro e i rischi informatici sono in continua evoluzione, le aziende devono poter fare affidamento su una soluzione NAC in grado di affrontare queste problematiche:

- In molte reti, il numero di dispositivi non gestiti supera abbondantemente il numero di quelli gestiti, e si tratta di sistemi che non possono essere autenticati con metodi tradizionali
- L'incremento del volume di dispositivi non gestiti comporta l'introduzione di rischi aggiuntivi e di punti ciechi
- Le reti in cui sono presenti sistemi di più vendor sono molto diffuse e richiedono alternative all'autenticazione 802.1X
- I sistemi aziendali o personali remoti che si collegano alla rete fanno emergere nuove problematiche di gestione della sicurezza
- L'incapacità di automatizzare le policy di sicurezza, conformità e accesso ha come effetto l'aumento dei costi operativi e dei processi manuali

La soluzione

Se queste problematiche ti suonano familiari, è arrivato il momento di valutare una soluzione di controllo degli accessi alla rete. La piattaforma Forescout sta ridefinendo il concetto di controllo degli accessi alla rete e la maniera per risolvere le sfide organizzative e i rischi informatici della tua azienda. Tra l'altro, con Forescout, l'implementazione di una soluzione NAC moderna non comporta complessità né interruzioni dell'attività. Entro qualche giorno dall'attivazione,

> "Ci hanno detto che avremmo potuto implementare la piattaforma Forescout in un pomeriggio. Io e il mio collega ci siamo scambiati uno sguardo incredulo. E invece l'implementazione è durata poche ore!"
>
> — Mike Roling, CISO, Stato del Missouri

godrai di una visibilità completa su tutti i dispositivi che si collegano alla rete, e nel giro di qualche settimana tutti i controlli basati su policy saranno attivi.

La nostra moderna piattaforma NAC mette a disposizione funzionalità di sicurezza della rete fondamentali che vanno ben oltre la semplice autenticazione. Si tratta di identificazione granulare di dispositivi e utenti, valutazione dello stato di sicurezza e conformità, monitoraggio costante dei dispositivi, opzioni di controllo flessibili e risposte automatizzate.

Le tecnologie NAC tradizionali non sono in grado di effettuare in modo sicuro l'autenticazione dei sistemi non tradizionali, come i dispositivi IoT, che si connettono alle nuove reti CAN. Inoltre, valutano lo stato di sicurezza e conformità dei computer ricorrendo ad agent. Le capacità di rilevamento e profilazione di Forescout, invece, identificano, classificano e valutano accuratamente qualsiasi dispositivo, permettendoti di elaborare policy di accesso sensibili al contesto. La piattaforma Forescout lavora in presenza o in assenza di agent, con o senza il protocollo 802.1X e monitora su base continua tutti i dispositivi della rete.

Identificare: scoprire, classificare e inserire in un inventario tutti i dispositivi connessi

Grazie alla piattaforma Forescout, i responsabili della sicurezza e dell'IT ottengono una visibilità totale in tempo reale su tutti i dispositivi connessi tramite IP nel momento stesso in cui si agganciano alla rete. In questo modo possono disporre di un inventario aggiornato e accurato di tutte le risorse.

- Scegli tra un ventaglio di oltre 20 tecniche di ricerca attive e passive e di metodi di profilazione per individuare quelli più adatti al tuo ambiente aziendale e assicurare una disponibilità della rete senza interruzioni
- Gli oltre 12 milioni di profili di dispositivi presenti nel Forescout Device Cloud sono gli strumenti di classificazione altamente affidabili e tridimensionali che Forescout usa per determinare funzione, sistema operativo, marca, modello e altre caratteristiche di ogni sistema
- Ottieni una copertura completa per tutte le sedi, le reti e i tipi di dispositivi senza punti ciechi, con o senza l'autenticazione 802.1X

Rendere conforme: valutare lo stato di sicurezza e conformità

> "La quantità di informazioni che raccoglie la piattaforma Forescout è incredibile. È senza dubbio la migliore soluzione che abbia mai usato per individuare, identificare e controllare i sistemi. Per noi è diventata indispensabile."
>
> — Joseph Cardamone, Senior Information Security Analyst, Haworth International

Gli strumenti di sicurezza basati su agent non rilevano i dispositivi gestiti senza agent o in cui l'agent è guasto o non funzionante. Di conseguenza, non rilevano neanche i dispositivi IoT, dal momento che non possono ospitare agent di sicurezza, il che amplia ulteriormente la superficie di attacco. La piattaforma Forescout però, consente di automatizzare la valutazione dello stato di sicurezza e il ripristino di tutti i dispositivi IP dal momento in cui si connettono e in seguito su base continua.

- Trova e ripara i dispositivi gestiti dai software di sicurezza esistenti che presentano agent guasti o mancanti
- Rileva i dispositivi non conformi, i cambiamenti di stato, le vulnerabilità, le credenziali deboli, gli indicatori di compromissione, i tentativi di spoofing e gli altri indicatori di rischio, il tutto senza ricorrere ad agent
- Valuta e monitora su base continua i dispositivi non gestiti, inclusi quelli che non possono ospitare agent, per imporre la conformità alle policy di sicurezza

Aumenta il valore degli investimenti in tecnologie informatiche e di sicurezza

La maggior parte delle soluzioni di sicurezza si limitano a segnalare le violazioni e ad avvisare l'operatore.

La piattaforma Forescout include moduli plug-and-play che estendono le capacità di visibilità e controllo per:

- Condividere con gli strumenti di sicurezza e gestione IT i dati contestuali sui dispositivi in tempo reale
- Coordinare i flussi di lavoro e automatizzare le azioni di risposta
- Valutare su base continua lo stato di sicurezza e imporre la conformità sui dispositivi sottoposti a correzione automatica

Scopri come su forescout.it.

"Le funzionalità della piattaforma [Forescout] per la sicurezza IoT/OT fanno impallidire quelle dei concorrenti. Massima visibilità, massimo controllo operativo e massima sicurezza. Sono questi i capisaldi della strategia Zero Trust di Forescout."[2]

— Forrester Research

Connettere: imporre la conformità alle policy di accesso in reti eterogenee

La piattaforma Forescout implementa la strategia di sicurezza Zero Trust basata sull'identità di dispositivi e utenti, sull'integrità dei dispositivi e lo stato di conformità in tempo reale senza richiedere aggiornamenti hardware e software dell'infrastruttura.

- Applica alle risorse aziendali il controllo degli accessi basato sul principio del privilegio minimo definito in funzione del ruolo, del tipo di dispositivo e dello stato di sicurezza
- Impedisci l'accesso a dispositivi non autorizzati, inaffidabili e che si spacciano per legittimi
- Affronta con fiducia le verifiche interne e le normative esterne, con la consapevolezza che le misure di sicurezza attive garantiscono la conformità senza intralciare la produttività

Perché Forescout:

1. Implementazione veloce, flessibile e non intrusiva.
2. Valutazione della stato di sicurezza e dei rischi senza ricorrere ad agent.
3. Immediata redditività e rapido ritorno sull'investimento.
4. Può essere utilizzata con l'infrastruttura esistente.
5. Non richiede aggiornamenti software o hardware.
6. Si integra con i principali prodotti di sicurezza e IT.
7. Elimina i costi operativi e la complessità di 802.1X sulle reti cablate.
8. Scalabilità di classe enterprise: arriva a coprire 2 milioni di endpoint.
9. Il solido motore di gestione delle policy automatizza la risposta agli incidenti e riduce il tempo medio di risposta.
10. Piattaforma Forrester Zero Trust.

Fai il passo successivo:

- Richiedi una demo di Forescout
- Visita il nostro sito Web www.forescout.it

***Note**

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook, Forrester Research, 2 gennaio 2019
2. Forrester Wave™: Zero Trust eXtended Platform Providers, Q4 2019

FORESCOUT

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