FORESCOUT
Active Defense for the Enterprise of Things™

il moderno controllo degli accessi alla rete

Perché la visibilità e il controllo dei dispositivi senza agent sono fondamentali per un'efficace sicurezza informatica

Visibilità e controllo dei dispositivi: Perché non puoi farne a meno

La capacità di individuare, classificare, valutare e controllare ogni dispositivo connesso alla propria rete è un presupposto essenziale per conseguire sicurezza Zero Trust. Solo chi possiede una conoscenza in tempo reale gli endpoint fisici e virtuali presenti in ogni segmento, informazioni dettagliate sul livello e sullo stato della sicurezza e di funzionalità automatizzate di remediation e controllo accessi basate policy, può essere certo che i sistemi e i dati siano protetti, reagendo rapidamente e con precisione agli eventi di sicurezza.

100%

VISIBILITÀ IN TEMPO REALE

I criminali informatici sono costantemente alla ricerca di dispositivi non gestiti e non protetti e non tarderanno a individuare i punti ciechi della tua rete e ad approfittarne. La visibilità e il controllo senza agent sono i pilastri su cui si basano la sicurezza e la conformità. Giocano inoltre un ruolo essenziale nell'affrontare numerose problematiche dell'azienda. Per esempio, la visibilità continua e approfondita sui dispositivi si traduce in un accurato **inventario delle risorse in tempo reale** che permette al personale informatico e della sicurezza di ridurre i costi operativi, assicurando al contempo la conformità normativa ed evitando il mancato superamento delle revisioni.

forescout.com/solutions/network-access-control info-italia@forescout.com Tel. (internazionale) +1-408-213-3191

Perché la visibilità e il controllo sono così difficili da ottenere

Il metodo tradizionale a cui si ricorreva per gestire gli endpoint della rete consisteva nell'installare un software su ogni dispositivo. Questo metodo funzionava quando la maggior parte degli endpoint era statica, costituita da PC o server di proprietà dell'azienda. La mobilità, la diversità dei tipi di dispositivo e la virtualizzazione hanno reso la visibilità contestuale e il controllo molto più complicati.

L'esplosione nel numero e diversità dei dispositivi ha radicalmente alterato il panorama dei dispositivi. I sistemi informatici-fisici come i dispositivi Internet of Things (IoT) e i sistemi OT (Tecnologie Operative) ora si connettono alla rete aziendale. Molti dipendenti lavorano da casa e alcuni si connettono al cloud. L'impresa moderna si è rapidamente evoluta nell'**Enterprise of Things** e molti di questi oggetti non sono in grado di supportare gli agent di gestione. Ma anche per quelli che li supportano, l'approccio basato sugli agent è problematico:

- i sistemi basati su agent non funzionano se l'agent manca, non funziona o è disattivato.
- I metodi basati su agent e su 802.1X causano dei punti ciechi nella tua rete e creano complessità operativa, con il risultato spesso di distribuzioni incomplete.
- Se isolati, gli strumenti per conformità dei dispositivi non godono di una visuale unificata, perpetuando così i punti ciechi.
- 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.
- I dipendenti mobili, che utilizzano dispositivi BYOD, ospiti e in telelavoro rendono la sicurezza dipendente dagli agent molto dispendiosa in termini di tempo, oltre che inefficace.
- Le reti in cui sono presenti sistemi di più vendor sono molto diffuse e richiedono alternative all'autenticazione 802.1X che non richiedono upgrade di hardware o software.

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 le entità sconosciute e verosimilmente non protette.[1]

DOTT. CHASE CUNNINGHAM
ANALISTA PRINCIPALE, FORRESTER RESEARCH

La soluzione Forescout per una soluzne NAC moderna

Per affrontare le problematiche prevalenti negli odierni ambienti dinamici e diversificati, Forescout Technologies ha introdotto la metodologia di controllo dell'accesso alla rete (NAC) senza agent.

La piattaforma Forescout offre una visione continua e unificata su tutti i dispositivi di ambienti fisici, data center, cloud e reti OT. Fornisce visibilità continua e granulare su:

- Dispositivi di rete degli ambienti fisici: laptop, tablet, smartphone, sistemi BYOD/ospiti e dispositivi IoT
- Infrastrutture dei data center: macchine virtuali, hypervisor, server fisici e altri componenti virtuali e fisici per le reti.
- Infrastrutture di cloud pubblici e privati: macchine virtuali AWS®, Microsoft® Azure® e VMware®.
- Sistemi OT e di controllo industriale (ICS): dispositivi medicali, industriali e di automazione degli edifici
- Infrastrutture di reti fisiche e software: switch, router, firewall, VPN, access point wireless e controller

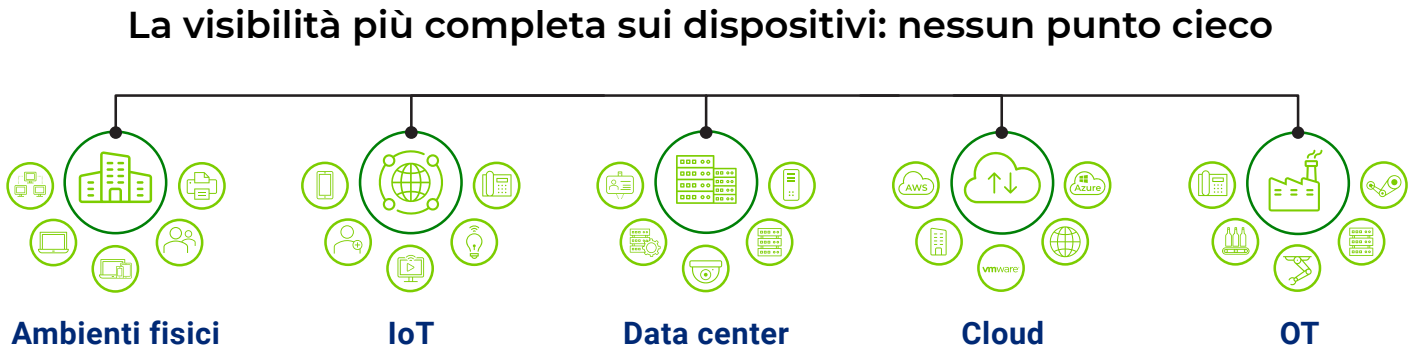


Figura 1: la visibilità di Forescout sui dispositivi è scalabile in tutta l'azienda estesa per fornire un inventario, dettagliato e in tempo reale, di tutto ciò che si connette alla tua rete.

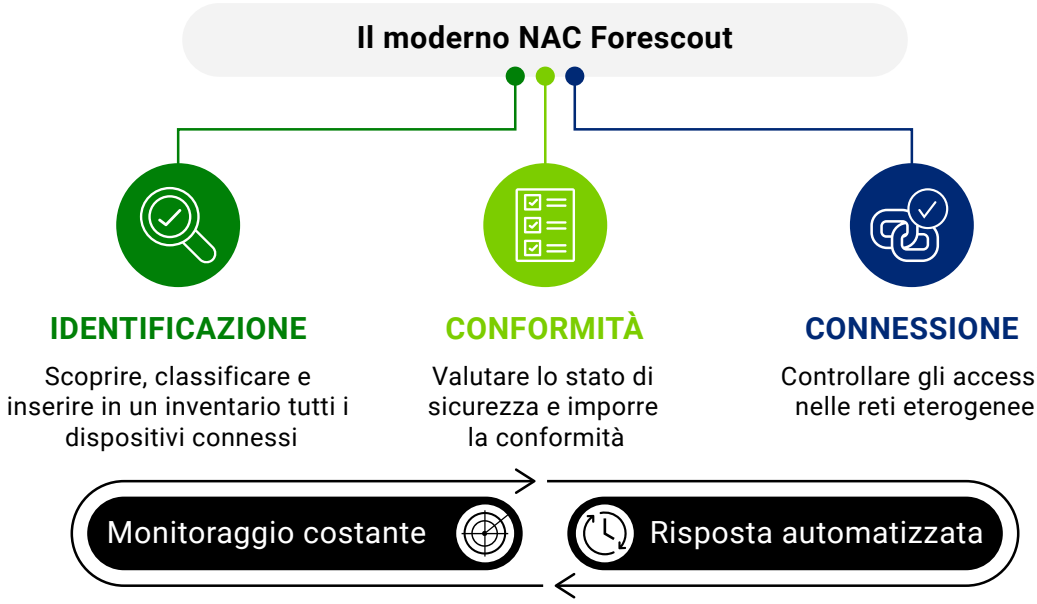


Figura 2: la moderna soluzione NAC di Forescout offre funzioni essenziali a qualsiasi rete eterogenea senza richiedere agent software o l'autenticazione 802.1X.

Come funziona

La moderna soluzione NAC di Forescout consente ai dipartimenti IT di:

- Scegliere fra oltre 20 tecniche attive e passive per il rilevamento dei dispositivi senza agent più completo in tutte le ubicazioni, le reti e i tipi di dispositivo, senza punti ciechi.
- Classificare automaticamente e accuratamente i dispositivi in base a funzione, sistema operativo e versione, marca e modello.
- Creare e mantenere automaticamente un inventario delle risorse in tempo reale di ogni dispositivo con connessione IP alla tua rete estesa.
- Valutare e monitorare continuamente lo stato di sicurezza di tutti i dispositivi, senza gli agent.
- Conformarsi alle policy di sicurezza e alle normative di settore grazie all'automazione del ripristino degli endpoint.
- Imporre controlli flessibili della rete in base ad autenticazione, ruolo degli utenti, tipo dei dispositivi e stato di sicurezza, in qualsiasi rete eterogenea cablata, wireless o VPN.
- Imporre il controllo degli accessi con privilegi minimi per la protezione Zero Trust.

Identificazione di ogni dispositivo su tutte le reti

La piattaforma Forescout utilizza oltre 20 tecniche di raccolta dei dati configurabili che sfruttano l'integrazione profonda con i migliori switch per reti IT e OT, router, access point wireless, firewall, concentratori VPN, fornitori di soluzioni per data center e cloud. La piattaforma ascolta in modalità passiva il traffico della rete analizzando i flussi di molteplici protocolli diversi ed è in grado di interagire con l'infrastruttura di rete e con gli endpoint.

Le tecniche di visibilità di Forescout includono:

- Metodi **passivi per la rete e per i dispositivi finali**. Rientrano in questa categoria la ricezione di trap SNMP da switch e controller wireless, il monitoraggio di porte SPAN e l'analisi di flussi di dati codificati con protocolli diversi (Forescout consente un esame approfondito dei pacchetti creati con più di 150 protocolli IT e OT), la raccolta e l'analisi di dati di flusso, la valutazione di richieste DHCP e l'analisi del traffico agente-utente HTTP. Se viene implementato lo standard 802.1X, Forescout monitora anche le richieste RADIUS utilizzando un server integrato oppure esterno.
- Metodi **attivi nell'infrastruttura di rete**. Rientrano in questa categoria gli switch di polling, i concentratori VPN, i controller wireless e i controller per cloud privati e pubblici per compilare l'elenco dei dispositivi connessi e delle macchine virtuali. Per ottenere dati su utenti e dispositivi, la piattaforma Forescout interroga servizi di directory, applicazioni web e database esterni.
- Metodi **attivi nei dispositivi finali**. Ad esempio: la scansione di segmenti di rete alla ricerca di dispositivi connessi con Nmap, l'ispezione remota di dispositivi Windows con WMI o di dispositivi Mac e Linux con SSH, la profilazione degli endpoint tramite query SNMP.

Tecniche di individuazione dei dispositivi

TECNICHE PASSIVE	ATTIVE PER L'INFRASTRUTTURA	DA ATTIVO A DISPOSITIVO FINALE
Trap SNMP	Polling dell'infrastruttura di rete fisica	Ispezioni senza agent Windows (WMI, RPC, SMB)
Traffico SPAN • Richieste DHCP • Traffico agente-utente HTTP • Fingerprinting TCP • Analisi dei protocolli medici (20 protocolli) • Analisi dei protocolli ICS per l'OT (olre 70 protocolli)	Integrazione dell'infrastruttura di rete basata su controller • Juniper Mist • Cisco ACI, Cisco Meraki	Ispezioni senza agent macOS, Linux (SSH)
Analisi dei flussi • NetFlow • NetFlow flessibile • IPFIX • sFlow	Integrazione di cloud privati (infrastruttura virtuale) • VMware	Nmap
Richieste DHCP (tramite ip-helper)	Integrazione di cloud pubblici • AWS • Azure	Query SNMP su endpoint
Agent utente HTTP (tramite reindirizzamento dell'URL)	Interrogazione dei servizi di directory (LDAP)	Ispezione basata su agent (SecureConnector)
Richieste RADIUS	Interrogazione delle applicazioni web (REST)	
MAC OUI	Interrogazione dei database esterni (SQL)	
	Coordinamenti (ITSM, UEM, EPP, EDR, VA)	

Figura 3: metodi di Forescout per la visibilità dei dispositivi

Il vantaggio di disporre di più metodi di individuazione

La piattaforma Forescout presenta un livello di efficienza, flessibilità ed efficacia unico perché mette a disposizione diversi metodi di individuazione che sono facilmente configurabili all'inizio e altrettanto facilmente modificabili in seguito.

Distribuzione semplificata e a costi contenuti in ambienti di grandi dimensioni: La capacità di scegliere fra oltre 20 tecniche attive e passive offre la flessibilità necessaria per ottenere una visibilità completa sui dispositivi in qualsiasi rete eterogenea, a prescindere dalla sua complessità e dalle dimensioni o numero delle ubicazioni remote. Il tutto, senza dover effettuare l'upgrade dell'infrastruttura (software/hardware) né impiegare un'appliance locale in ogni sito/ufficio remoto.

Nessun punto cieco: non è insolito che i clienti aziendali possiedano delle sedi remote che non possono impiegare appliance aggiuntive né fornire il traffico SPAN. La nostra capacità di sfruttare multiple tecniche, attive e passive, risolve qualsiasi limitazione della rete e fornisce il 100% di copertura dei dispositivi senza punti ciechi.

Tecniche di individuazione, classificazione e valutazione passive per le reti critiche della sanità e OT/ICS. In molti casi le reti critiche sono ambienti che non si prestano ad attività di sondaggio e scansione attive perché il rischio potenziale di interrompere sistemi medici e di controllo dei processi è troppo elevato. La piattaforma Forescout fornisce visibilità sulle reti sanitarie critiche e OT tramite una combinazione di tecniche interamente passive, fra le quali il monitoraggio del traffico SPAN per l'ispezione approfondita dei pacchetti di oltre 150 protocolli specifici in ambito IT, sanità e OT. Ciò che distingue la soluzione Forescout è che, una volta identificati accuratamente i dispositivi, può selettivamente applicare i metodi attivi su dispositivi specifici per la valutazione aggiuntiva senza rischiare l'interruzione delle attività.

Non solo ricerca, ma classificazione e valutazione: grazie alla sua capacità intrinseca di combinare tecniche di profilazione attive e passive, la piattaforma Forescout non si limiterà semplicemente a identificare un dispositivo connesso in base all'indirizzo MAC o IP. Per classificazione si intende il processo di acquisizione e messa in relazione di diversi strati di dati contestuali con l'obiettivo di creare un profilo altamente dettagliato di ogni dispositivo. La valutazione è il processo che consiste nel raffrontare le proprietà del dispositivo rilevato con le policy di sicurezza per esercitare il controllo degli accessi e formulare le decisioni di ripristino. Entrambi i metodi meritano un'analisi più approfondita.

Classificazione automatica e intelligente

Per creare policy granulari è fondamentale conoscere il contesto completo in cui opera ogni dispositivo. Per decidere come proteggere e gestire al meglio ciascun dispositivo, è necessario conoscerne la finalità operativa. L'aumento del numero e della varietà di dispositivi rende pressoché impossibile acquisire manualmente dati sul contesto e, d'altro canto, la creazione di policy senza un contesto adeguato è alquanto rischiosa. Forescout classifica automaticamente i dispositivi tradizionali, IoT e OT con una tassonomia multidimensionale che identifica la funzione, il tipo, la marca e il modello di ogni dispositivo, oltre al sistema operativo e alla versione.

La piattaforma classifica automaticamente:

- Oltre 575 differenti versioni dei sistemi operativi.
- Oltre 5700 diverse marche e modelli di prodotti.
- I dispositivi sanitari di oltre 400 importanti produttori di tecnologia medicale.
- Migliaia di dispositivi di controllo e automazione industriale utilizzati nei settori manifatturiero, energetico, petrolio e gas, servizi pubblici, minerario e altri settori delle infrastrutture strategiche.

Forescout Device Cloud è il motore che alimenta la classificazione automatica della piattaforma e assicura che questa ricca fonte di informazioni rimanga all'altezza di gestire l'aumento e la diversificazione dei dispositivi. Grazie all'analisi di oltre 12 milioni di dispositivi dei clienti aziendali, Device Cloud è il più grande data lake al mondo di informazioni provenienti dai dispositivi, un'unica fonte attendibile e intersettoriale di impronte digitali, comportamenti e profili di rischio di tutte le singole risorse presenti nella tua rete. Forescout Research pubblica frequentemente nuovi profili al fine di migliorare efficacia, copertura e velocità della classificazione nell'intero panorama dei dispositivi.

Valutazione dello stato senza agent e remediation automatica

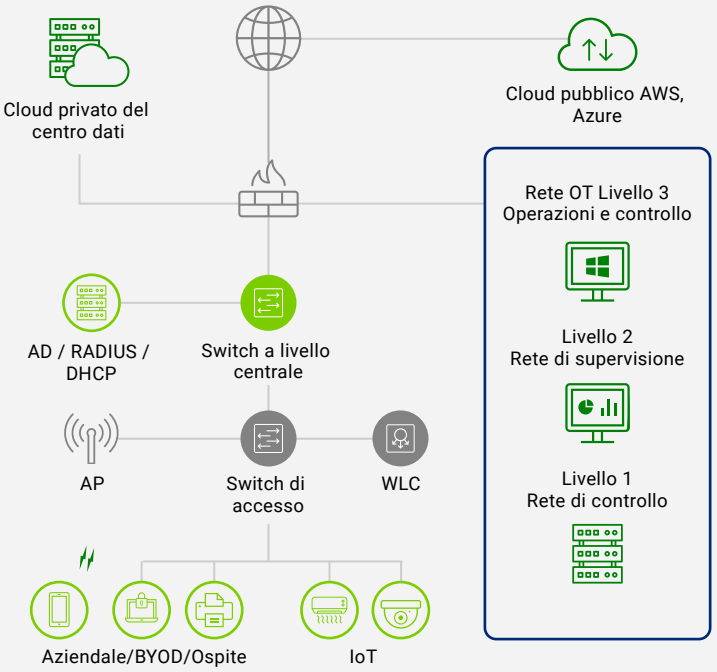
La classificazione comunica il contesto operativo e la finalità di un dispositivo: in pratica indica di che tipo di dispositivo si tratta. Per ottenere una visione completa, tuttavia, è necessario disporre di un altro strumento che determini l'integrità di ciascun dispositivo. Forescout monitora continuamente la rete e valuta la configurazione, la condizione e lo stato di sicurezza dei dispositivi connessi per determinarne i profili di rischio, la conformità alle normative e la loro adesione alle policy di sicurezza. Forescout risponde a domande importanti, ad esempio:

- I dispositivi utilizzano sistemi operativi approvati e aggiornati con le ultime patch?
- 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 utilizzano password predefinite o elementari (particolarmente rischioso per i dispositivi IoT)?
- Sono stati rilevati dispositivi inaffidabili, compresi quelli che si spacciano per legittimi tramite tecniche di spoofing?
- Quali dei dispositivi connessi sono più vulnerabili alle ultime minacce?

Dopo aver risposto a queste domande fondamentali, la **piattaforma Forescout impone la conformità ai dispositivi automatizzandone il processo di remediation** per mezzo di comandi nativi o di terze parti. Importanti nuove funzionalità:

- Garantire la corretta configurazione degli endpoint e avviare il processo di remediation per le violazioni critiche alla configurazione, incluse password predefinite o non sicure.
- Assicurare costantemente che gli agent di sicurezza stiano funzionando correttamente (che siano installati, in esecuzione e aggiornati).
- Disabilitare o bloccare applicazioni non autorizzate che potrebbero introdurre rischi o gravare inutilmente sulla larghezza di banda della rete o sulla produttività delle risorse.
- Identificare vulnerabilità ad alto rischio e patch critiche mancanti e avviare le azioni correttive.
- Avviare azioni di correzione preventive come l'installazione del software di sicurezza necessario, l'aggiornamento degli agent o l'applicazione delle patch di sicurezza.
- Implementare policy e automatizzare i controlli per la conformità della configurazione nelle distribuzioni cloud, tra cui AWS, Azure e VMware.

Classificazione e valutazione dei dispositivi



CHI
- Utente
- Nome
- Email
- Titolo
- Gruppo
- Abbonamento/Account
- Titolare/Ruolo IAM

COSA
- Funzione
- Sistema operativo
- Marca/Modello
- Indirizzo IP
- Agent browser
- Porte
- Dispositivo virtuale/fisico
- Indirizzo Mac

STATO?
- App
- Servizi
- Processi
- Versioni
- Registro
- Patch
- Crittografia
- Antivirus

DOVE?
- Switch
- Controller
- Porta switch/SSID/VLAN
- AWS/Azure
- Regione
- VNet/VPC
- Livello Purdue

Figura 4: la piattaforma Forescout classifica rapidamente ogni dispositivo in base al tipo, rileva se è gestito a livello aziendale o non gestito, se è IoT o OT, di tipo fisico o virtuale e ne verifica lo stato di conformità.

"L'IoT e le tecnologie dei dispositivi abilitati dalla rete hanno introdotto una potenziale compromissione delle reti. Ciascun dispositivo introduce nuove forme di codice e risorse che il personale della sicurezza deve rintracciare e trattare come infrastruttura non affidabile. È necessario isolare, proteggere e controllare ogni dispositivo nella rete, continuamente". [2]

FORRESTER

8 GIUGNO 2020

La visibilità è la chiave per il controllo

Ogni cliente ha una rete differente, è per questo che le rispettive esigenze variano e le policy di sicurezza sono univoche. È quindi fondamentale distribuire una soluzione flessibile, che metta in sicurezza tutte le reti: cablate, wireless e VPN. Per esempio, nelle proprie reti cablate le grandi imprese impiegano solitamente la soluzione Forescout **senza 802.1X**. Scelgono questa opzione perché è facile da distribuire, non richiede di effettuare l'upgrade dell'infrastruttura hardware/software, né complesse configurazioni di switch o endpoint, come la 802.1X, e funziona nelle infrastrutture di rete ove sono presenti uno o più fornitori. Questa prassi è coerente con le raccomandazioni di Gartner di non utilizzare la 802.1X nelle reti cablate, se si desidera una distribuzione più semplice e minori costi operativi. Tuttavia, nelle reti wireless, la prassi normale è quella di impiegare l'autenticazione 802.1X per i dispositivi informatici degli utenti aziendali. Le opzioni di distribuzione ibride e flessibili di Forescout supportano facilmente entrambe queste prassi.

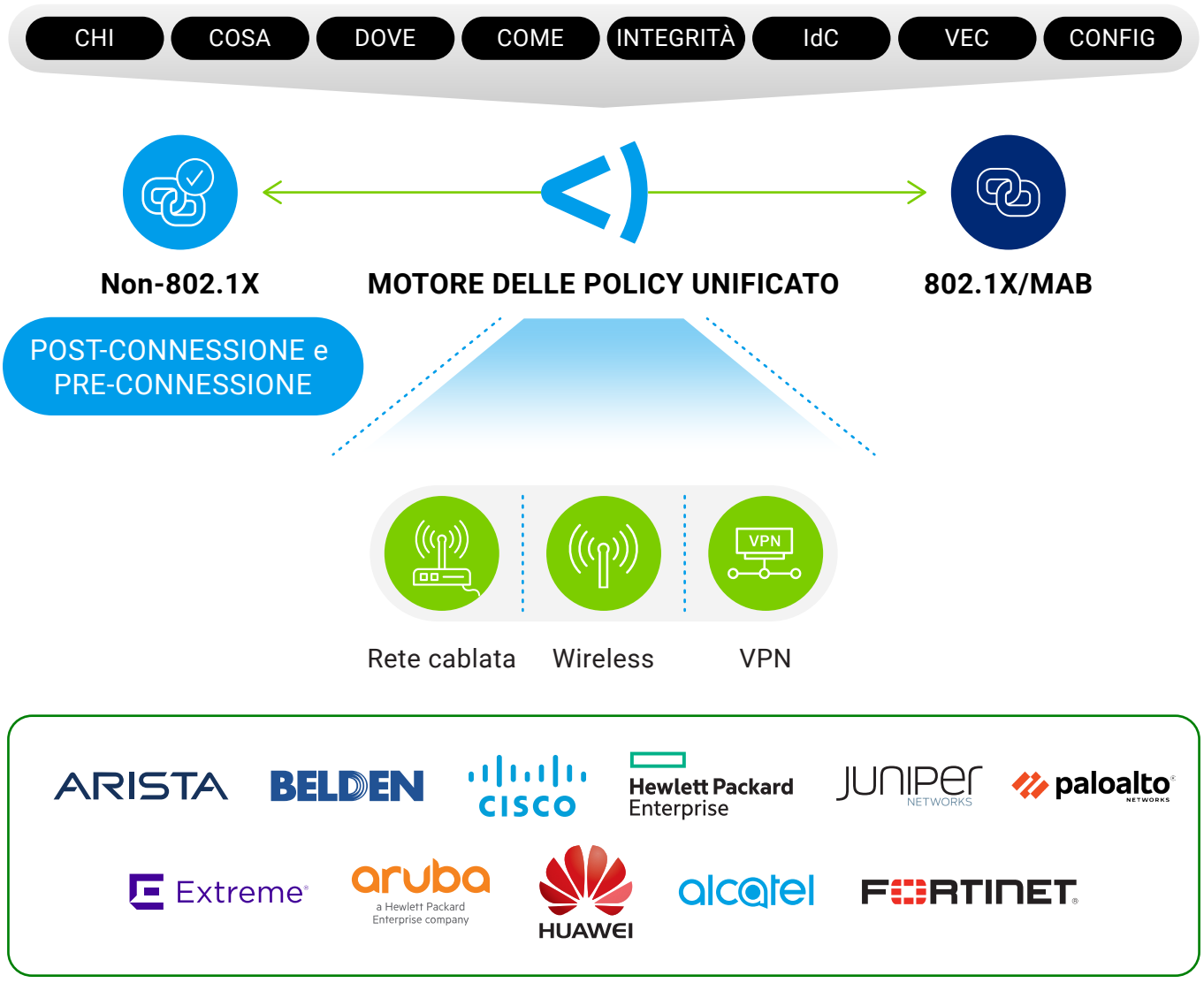


Figura 5: Forescout offre le opzioni senza 802.1X e con 802.1X per la protezione degli endpoint nelle reti multifornitore cablate, wireless e VPN.

Ecco alcuni dei principali vantaggi derivanti dall'utilizzo della piattaforma Forescout per la protezione dell'accesso alla rete:

Maggiore flessibilità

- Ampia gamma di metodi per il controllo degli accessi, con o senza 802.1X.
- Robusta architettura cablata, senza 802.1X: non intrusiva, facile da impiegare, con minima configurazione, nessun upgrade dell'infrastruttura, opzioni pre-connessione e post-connessione, immediata redditività e rapido ritorno sull'investimento.
- Motore delle policy unificato per implementare un accesso differenziato (ospite, BYOD, aziendale, IoT) e sicuro con Zero Trust.

Nessun upgrade

- Funziona con l'infrastruttura esistente senza dover effettuare l'upgrade di software/hardware.
- Funziona con il fornitore scelto per l'infrastruttura della rete (per esempio, switch, controller wireless, IaaS), riducendo la dipendenza dal produttore.
- Redditività e ritorno sull'investimento più rapidi.

Eterogeneità

- Integrazione diretta (tramite SNMP, SSH, Telnet, RADIUS) con centinaia di switch e controller wireless di oltre 30 fornitori di infrastruttura di rete, con sistemi operativi di differenti versioni. Ciò consente di controllare gli accessi in qualsiasi rete multifornitore.
- Soluzione flessibile e non intrusiva che abbassa i costi di distribuzione, manutenzione e operativi.
- Il supporto eterogeneo permette a un'azienda acquirente di ottenere rapidamente visibilità e controllo sulle risorse, dopo una fusione o acquisizione.

Segmentazione su scala aziendale

- Sfrutta la visibilità offerta dalla piattaforma Forescout per comprendere lo stato della segmentazione in tempo reale e su qualsiasi dispositivo, ovunque.
- Progetta e simula le policy di segmentazione logica in modo da valutarne l'impatto prima di applicarle.
- Monitora in tempo reale l'integrità della segmentazione e reagisci alle violazioni delle policy in tutta l'azienda estesa.

Puoi avere maggiori informazioni sulla soluzione Forescout per la segmentazione su scala aziendale qui.

LE MIGLIORI PRATICHE PER LA DISTRIBUZIONE DEL NAC

Per la distribuzione della soluzione NAC, Forescout consiglia le seguenti procedure:

Reti wireless: 802.1X è l'autenticazione standard per i dispositivi informatici degli utenti aziendali nelle reti wireless. Dopo l'autenticazione, Forescout identifica e valuta senza agent la conformità dei computer Windows, macOS e Linux.

Con il motore delle policy di Forescout, i clienti possono scegliere di correggere automaticamente e di imporre gli appropriati controlli di rete per il rispetto delle policy di sicurezza (per esempio, avvisa l'utente, risolve il problema, blocca e/o condivide il contesto con gli strumenti di terze parti).

Reti cablate: Forescout consiglia le architetture senza 802.1X. Data la complessità legata alla distribuzione e gestione delle autenticazioni 802.1X e MAB nelle reti cablate, la maggior parte dei clienti sceglie l'opzione senza 802.1X. I clienti iniziano con il rilevamento dei dispositivi, l'identificazione e valutazione dello stato/conformità e poi impongono gli appropriati livelli di accesso alla rete usando dei controlli non basati su 802.1X in qualsiasi rete eterogenea. Nota: Forescout supporta completamente 802.1X anche nelle reti cablate.

Coordinamento con i prodotti informatici e di sicurezza
Durante l'interno processo di controllo degli accessi alla rete, Forescout può funzionare insieme ai tuoi strumenti esistenti scambiando in tempo reale il contesto dei dispositivi e automatizzando i flussi di lavoro delle risposte. Ciò non solo accelera la mitigazione del rischio, ma ti consente anche di massimizzare il ritorno sull'investimento nei prodotti esistenti per la sicurezza e la gestione informatica. Grazie alle integrazioni pronte all'uso di eyeExtend e all'app eyeExtend Connect, aiutiamo i clienti a trasformare rapidamente la gestione della sicurezza: da silos isolati a un sistema di risposta automatizzato e su scala aziendale che difende attivamente la tua Enterprise of Things.

I seguenti sono alcuni dei benefici derivanti dal coordinamento con gli strumenti di sicurezza esistenti durante la procedura NAC:

Condivisione del contesto dei dispositivi
- Condividi il contesto dei dispositivi con i tuoi strumenti esistenti di gestione delle risorse per assicurarti di avere sempre l'inventario più aggiornato e più accurato (CMDB).
- Fornisci in tempo reale il contesto dei dispositivi agli addetti alla sicurezza e alle applicazioni per la correlazione e l'assegnazione delle priorità agli eventi.

Avviamento dei flussi di lavoro alla connessione
- Gli strumenti esistenti potrebbero non valutare la vulnerabilità dei dispositivi transitori a causa di scansioni sporadiche. Forescout opera con gli strumenti di sicurezza per attivare le scansioni delle vulnerabilità in tempo reale al momento delle connessioni.
- Avvia l'applicazione delle patch e gli aggiornamenti della protezione immediatamente al momento della connessione per ridurre la superficie di attacco.

Valutazione dello stato di sicurezza
- Verifica che gli agent di sicurezza esistenti siano funzionali e identifica i dispositivi che presentano rischi e IdC.
- Rileva gli account con privilegi, ma illegittimi od obsoleti, nei dispositivi che si connettono.

Azioni di risposta automatizzate
- Argina, metti in quarantena o blocca i dispositivi vulnerabili, compromessi e ad alto rischio.
- Avvia le azioni di mitigazione e correzione basate sulle policy per la risposta agli incidenti.

Forescout domina attualmente il sottoinsieme senza agent del mercato NAC, con il 64,7% della quota di mercato. Si stima che ciò includa anche la maggiore percentuale delle distribuzioni NAC ibride nel settore. Questa crescita è largamente dovuta alla robusta serie di funzioni di Forescout, finalizzate a soddisfare le esigenze della parte maggiormente crescente di questo mercato: i dispositivi che, non supportando gli agent, richiedono un approccio senza agent.

IDC
MAGGIO 2020[3]

Vedere non basta. Bisogna proteggere.

La moderna soluzione NAC di Forescout offre una via senza agent, flessibile e non intrusiva alla protezione Zero Trust. Consulta queste risorse per saperne di più sul modo in cui Forescout difende in maniera attiva l'Enterprise of Things:

Leggi la Guida Gartner al Mercato per il NAC: scopri perché Gartner definisce Forescout "Una delle più diffuse soluzioni NAC sul mercato".

Visita il sito web di Forescout: avrai maggiori informazioni sulla moderna soluzione NAC di Forescout, compresi i casi di utilizzo che affronta, il modo in cui assicura la conformità dei dispositivi e cosa dicono i clienti di Forescout.

Mettici alla prova: scopri la differenza tra prima e dopo l'utilizzo della piattaforma Forescout con una prova pratica che ti guiderà attraverso sei potenti esperienze di utilizzo.

Richiedi una demo: visita la pagina della demo sul sito web di Forescout per richiedere una dimostrazione personalizzata e avere accesso a un ricco campionario di demo e video su richiesta.

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook (L'ecosistema Zero Trust eXtended: Piano strategico per le reti: il manuale dell'architettura e delle operazioni di sicurezza), Forrester Research, 2 gennaio 2019
2. Forrester Research, Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles And Techniques (Mitigare il ransomware con un approccio Zero Trust: rafforzare le difese con principi e tecniche Zero Trust), 8 giugno 2020
3. IDC, Worldwide NAC Market Shares, 2019: Diverse Market Demands Expand NAC's Addressable Market (Richieste di mercato diversificate ampliano il mercato per le soluzione NAC), maggio 2020

Vedere non basta. Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

forescout.com/solutions/network-access-control 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