FORESCOUT

Device Visibility and Control senza agent

Capacità fondamentali per una strategia di sicurezza informatica efficace

> "La visibilità è una condizione essenziale per difendere qualsiasi risorsa preziosa. Maggiore è la visibilità sulla rete da qualsiasi punto dell'ecosistema aziendale, più facile sarà individuare prontamente gli indizi di una violazione e intervenire.[1]"
>
> **— Dr. Chase Cunningham, Analista principale, Forrester Research**

Device Visibility and Control: perché non puoi farne a meno

La capacità di individuare, classificare, valutare e monitorare ogni dispositivo connesso alla propria rete è un presupposto essenziale per mettere in sicurezza i sistemi e l'azienda. Solo chi possiede una conoscenza in tempo reale degli endpoint fisici e virtuali presenti in ogni segmento, informazioni dettagliate sulla configurazione e sullo stato di sicurezza e un controllo degli accessi basato su policy può essere certo che il sistema e i dati siano protetti, reagire rapidamente e con precisione agli eventi di sicurezza, soddisfare i requisiti di conformità, gestire i rischi per l'attività e l'infrastruttura e ottimizzare l'efficienza delle operazioni di sicurezza. I criminali informatici sono costantemente alla ricerca di dispositivi non gestiti e non protetti e non tarderanno a scovare i punti ciechi della tua rete e ad approfittarne. La visibilità e il controllo sono i pilastri su cui si basano la sicurezza e la conformità.

Perché la visibilità e il controllo sono così elusivi

Il metodo tradizionale a cui si ricorreva per gestire gli endpoint della rete consisteva nell'installare un software su ogni dispositivo. Questo sistema funzionava fintanto che gli endpoint erano unità statiche come PC o server di proprietà dell'azienda. Ora che la mobilità, la diversificazione dei dispositivi e la virtualizzazione sono situazioni comuni, la gestione della visibilità e del controllo nel contesto è diventata molto più complicata. Nei moderni ambienti aziendali, i segmenti cloud e i data center pullulano di carichi di lavoro dinamici eseguiti su macchine virtuali connesse tramite reti virtualizzate. I segmenti degli ambienti fisici brulicano di laptop, tablet e smartphone BYOD su cui i proprietari non installano agent di sicurezza, oltre che di dispositivi IoT che non li supportano. I segmenti OT, cioè riservati alle tecnologie operative, industriali e di controllo, sono pieni di dispositivi che gestiscono processi mission-critical ma che non supportano agent, non tollerano le intrusioni interne e che comunicano con protocolli proprietari. È evidente che i reparti IT devono dotarsi al più presto di una soluzione senza agent in grado di assicurare una visibilità e un controllo totali su tutti questi ambienti eterogenei.

La soluzione Forescout: Device Visibility and Control senza agent

Per affrontare le problematiche legate alla visibilità e al controllo dei dispositivi dei moderni ambienti dinamici e diversificati, Forescout Technologies ha introdotto la metodologia di protezione della rete senza agent. La piattaforma di visibilità e controllo dei dispositivi ideata da Forescout assicura una visione continua e unificata su tutti i dispositivi di ambienti fisici, data center, cloud e reti OT.

La piattaforma Forescout individua:

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

Figura 1: La soluzione di visibilità di Forescout applicata all'azienda estesa

> "Le valutazioni, la visibilità sugli elementi affidabili o rischiosi e gli scambi di dati contestuali sono diventati il sistema immunitario dei business digitali.[2]"
>
> **— Neil MacDonald, Vice Presidente, Analista, Gartner**

Come funziona

Forescout mette a disposizione dei reparti IT la capacità di:

- Scoprire in qualsiasi rete tutti i dispositivi con connessione IP: dispositivi fisici e virtuali in ambienti fisici, data center, cloud e ambienti industriali
- Classificare varie tipologie di dispositivi IT, IoT e OT/ICS, macchine virtuali e istanze cloud in tempo reale identificando il tipo e la funzione del dispositivo, la marca, il modello, il sistema operativo e la versione
- Valutare e monitorare costantemente lo stato di sicurezza dei dispositivi per garantire la conformità alle policy
- Applicare le policy, le normative del settore e le migliori pratiche come la segmentazione della rete
- Limitare, bloccare o mettere in quarantena i dispositivi non conformi o compromessi
- Automatizzare gli interventi di controllo su endpoint, reti e sistemi terzi

Forescout scopre qualsiasi sistema OT e dispositivo con connessione IP in qualsiasi segmento

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. 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 100 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 lo standard 802.1X è implementato, Forescout può monitorare un server RADIUS sia integrato che esterno.
- **Metodi attivi nell'infrastruttura di rete.** Rientrano in questa categoria le analisi di switch, concentratori VPN, controller wireless e 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.** Rientrano in questa categoria 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
Trap SNMP
Traffico SPAN
Richieste DHCP
Traffico agente-utente HTTP
Fingerprinting TCP
Analisi dei protocolli DICOM (sistemi di imaging medicale)
Analisi dei protocolli ICS per OT (60+ protocolli)
Analisi dei flussi
NetFlow
Flexible Netflow
IPFIX
sFlow
Richieste DHCP (tramite ip-helper)
Traffico agente-utente HTTP (tramite reindirizzamento URL)
Richieste RADIUS
MAC OUI

TECNICHE ATTIVE PER L'INFRASTRUTTURA
Polling dell'infrastruttura di rete fisica
Integrazione dell'infrastruttura di rete basata su controller
Meraki
Cisco ACI
Integrazione di cloud privati (infrastruttura virtuale)
VMware
Integrazione di cloud pubblici
AWS
Azure
Interrogazione dei servizi di directory (LDAP)
Interrogazione di applicazioni web (REST)
Interrogazione di database esterni (SQL)
Orchestrazioni (ITSM, UEM, EPP, EDR, VA)

TECNICHE ATTIVE PER IL DISPOSITIVO FINALE
Ispezioni senza agent Windows (WMI, RPC, SMB)
Ispezioni senza agent macOS, Linux (SSH)
NMAP
Query SNMP su endpoint
Ispezione basata su agent (SecureConnector)

Figura 2: Metodi di individuazione dei dispositivi di Forescout

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.

Tecniche di individuazione, classificazione e valutazione passive per le reti OT. In molti casi le reti OT sono ambienti che non si prestano ad attività di sondaggio e scansione attive perché il rischio di compromettere i sistemi di controllo e i processi aziendali è elevato. Quando si acquisisce una conoscenza più approfondita dei dispositivi, si può scegliere di applicare selettivamente alcuni metodi di ricerca attiva. La piattaforma Forescout offre visibilità sui dispositivi delle reti OT combinando due tecniche totalmente passive: il mirroring del traffico SPAN e l'esame approfondito dei pacchetti di oltre 100 protocolli per reti OT. Forescout supporta i protocolli standard del settore come BACnet, CIP, DNP3, Ethernet/IP, ICCP, IEC 60870-5-104, IEC 60850, IEEE C37.118, Modbus/TCP, OPC, PROFINET e Siemens S7. Il supporto si estende anche ai protocolli proprietari dei principali operatori del settore, ad esempio ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, Schneider Electric e Yokogawa.

Implementazione a costi contenuti in ambienti di grandi dimensioni. La possibilità di ricorrere a tecniche di individuazione remote può contribuire a ridurre il costo complessivo dell'implementazione perché piccole sedi possono essere monitorate senza utilizzare appliance locali.

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 remediation. Entrambi i processi 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 un dispositivo, è necessario conoscerne il contesto operativo o la finalità. 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 500 diverse versioni di sistemi operativi
- Oltre 5.000 diverse marche e modelli di prodotti
- I dispositivi sanitari di oltre 350 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 di 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. Forescout Research and Intelligent Analytics si avvale delle informazioni di intelligence fornite al nostro motore da oltre 8 milioni di dispositivi reali* e pubblica regolarmente i nuovi profili per migliorare l'efficacia, la copertura e la velocità di classificazione nel panorama dei dispositivi dei clienti.

Valutazione dello stato del dispositivo

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 dispositivi che eseguono applicazioni non autorizzate o che violano gli standard di configurazione?
- I dispositivi utilizzano password predefinite o elementari, situazione particolarmente rischiosa per i dispositivi IoT?
- Sono stati rilevati dispositivi inaffidabili, compresi quelli che si spacciano per legittimi tramite tecniche di spoofing?
- Quali dispositivi connessi sono più vulnerabili alle ultime minacce?

Classificazione e valutazione dei dispositivi

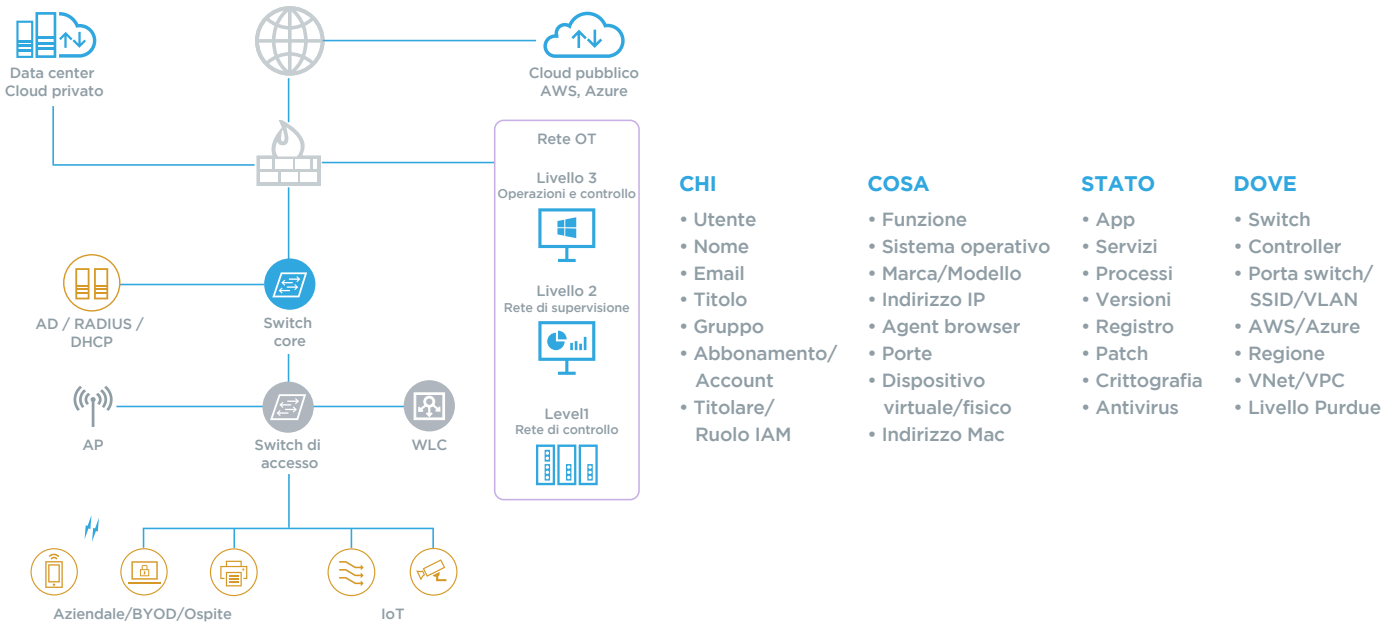

Figura 3: La piattaforma Forescout classifica rapidamente ogni dispositivo in base al tipo, rileva se è gestito a livello aziendale o non gestito, se è IoT o OT, di tipo fisico o virtuale e ne verifica lo stato di conformità.

La visibilità è la chiave per il controllo

La piattaforma Forescout include un motore delle policy che raffronta continuamente i dispositivi con una serie di policy personalizzabili che ne stabiliscono e indirizzano il comportamento in rete svolgendo un processo di monitoraggio continuo in tempo reale su un massimo di due milioni di dispositivi. Le policy sono attivate in tempo reale da eventi che si verificano su uno specifico dispositivo o nella rete. Può trattarsi di eventi di ingresso nella rete, come la connessione alla porta di uno switch o la modifica di un indirizzo IP, di eventi di autenticazione eseguiti, ad esempio, su un server RADIUS oppure di modifiche degli attributi dei dispositivi. La Figura 4 illustra la serie di azioni di controllo che può attuare la piattaforma Forescout quando una policy viene attivata.

Azioni di controllo di Forescout

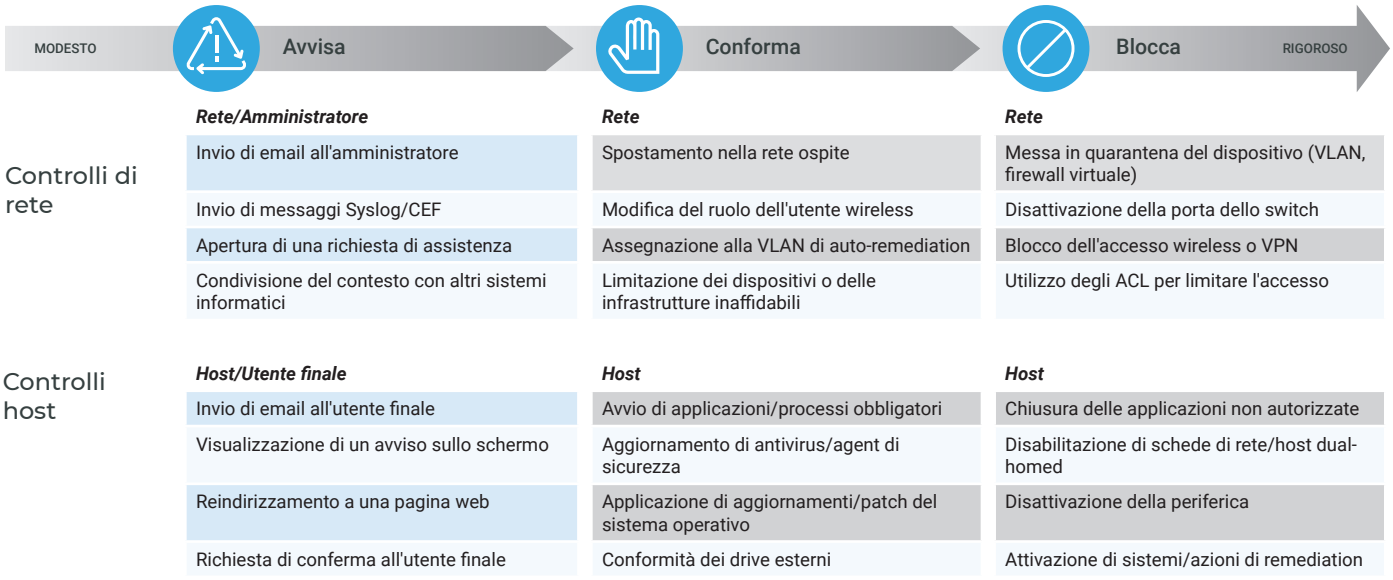

Figura 4: Le azioni di controllo personalizzabili consentono di applicare il livello di controllo appropriato, dal più moderato al più rigoroso, in base alle policy di sicurezza.

Il motore delle policy fa ricorso a due serie di funzioni di controllo. La prima è la serie nativa di Forescout. La seconda è legata a integrazioni per il coordinamento dei controlli e allo scambio di dati con i principali prodotti di sicurezza e gestione IT.

Funzioni di controllo native

Le funzionalità native di Forescout includono controlli sulla rete e gli host. I controlli sulla rete comprendono la segmentazione basata sulle policy, il permesso o il divieto di accesso in base all'identità dell'utente, al ruolo e allo stato del dispositivo. I controlli sugli host assicurano che il sistema sia integro e sicuro per l'avvio e l'arresto delle applicazioni, aggiornano l'antivirus e gli altri agenti di sicurezza basati su host o disattivano i dispositivi periferici.

Il motore delle policy applica le regole automaticamente a prescindere dalla posizione del dispositivo o dal suo spostamento nella rete aziendale, nel data center o nel cloud.

Funzioni di controllo estese

La piattaforma Forescout automatizza l'applicazione delle policy, accelera la risposta a livello di sistema e mitiga i rischi condividendo in tempo reale dati contestuali sul dispositivo e coordinando i flussi di lavoro di svariati prodotti di sicurezza e di gestione IT. Forescout offre integrazioni ai prodotti dei principali leader del settore che operano negli ambiti seguenti:

- Rilevamento avanzato delle minacce
- Strumenti di gestione client
- Gestione della mobilità aziendale (EMM)
- Protezione, rilevamento e risposta degli endpoint
- Gestione dei servizi IT
- Firewall di nuova generazione
- Gestione degli accessi privilegiati
- Gestione degli eventi e delle informazioni di sicurezza (SIEM)
- Valutazione delle vulnerabilità

Grazie a queste integrazioni, Forescout coordina la sicurezza a livello di infrastruttura esercitando controlli basati su policy e diretti alla classificazione di utenti, dispositivi, applicazioni e dati. Applica policy di accesso granulari che esercitano un controllo preciso e flessibile sulle risorse, consentendo ai reparti IT di implementare la segmentazione dinamica della rete e creare policy di sicurezza sensibili al contesto basate su una conoscenza puntuale della situazione.

Azioni di controllo

Una profonda conoscenza delle funzioni di controllo degli accessi è la ragione per cui la piattaforma Forescout dispone di una serie di funzionalità di controllo native ed estese straordinariamente ricca, che costituisce un vero e proprio arsenale di strumenti di sicurezza di rete per i reparti IT.

La piattaforma Forescout controlla l'accesso alle risorse aziendali usando un profilo utente (ospite, dipendente, collaboratore esterno), la classificazione del dispositivo e lo stato di sicurezza per:

- Abilitare l'accesso differenziato per dispositivi ospiti e BYOD
- Applicare policy di accesso alla rete con o senza autenticazione 802.1X
- Agire su dispositivi sospetti, inaffidabili o shadow IT della rete
- Limitare o bloccare l'accesso alla rete dei dispositivi compromessi o dannosi
- Mettere in quarantena o isolare i dispositivi non conformi fino a quando i problemi di conformità non vengono risolti

La piattaforma Forescout automatizza la valutazione della conformità e applica i controlli di remediation per garantire l'allineamento costante con le policy di sicurezza interne, gli standard esterni e normative del settore. 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
- Garantire che le applicazioni e gli agent di sicurezza necessari siano installati, eseguiti 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 di remediation
- Avviare azioni di remediation preventive come l'installazione di software di sicurezza richiesto, l'aggiornamento degli agent o l'applicazione di patch di sicurezza
- Implementare policy e automatizzare i controlli per la conformità della configurazione nelle distribuzioni cloud, tra cui AWS, Azure e VMware

La piattaforma Forescout implementa la segmentazione dinamica della rete applicando policy di segmentazione con diverse tecnologie di controllo nell'azienda estesa tramite una struttura di policy comune. La piattaforma Forescout:

- Assegna dinamicamente i dispositivi ai gruppi di segmentazione sulla base delle proprietà, della classificazione e dello stato di sicurezza
- Applica le regole di segmentazione tramite controlli VLAN, ACL, WLAN e assegna tag negli ambienti fisici e nelle reti OT
- Applica controlli di segmentazione tramite gruppi/tag di sicurezza in ambienti cloud pubblici e privati come AWS e VMware NSX®
- Assegna dispositivi non conformi e vulnerabili a segmenti separati, in particolare quelli cui è possibile applicare patch o azioni di remediation soltanto entro finestre di manutenzione pianificate, per abilitare la business continuity e ridurre la superficie d'attacco
- Impone policy di segmentazione per separare dispositivi specifici e flussi di dati critici dal resto della rete, come richiesto dalle normative HIPAA, RGPD, PCI e SWIFT CSP

La piattaforma Forescout accelera la risposta agli incidenti di sicurezza contenendo in modo rapido ed efficace le minacce e rispondendo rapidamente agli eventi di sicurezza per limitare le interruzioni operative e i danni all'azienda. Questa soluzione per la visibilità e controllo dei dispositivi:

- Identifica i dispositivi ad alto rischio che non sono stati arginati o corretti
- Lavora con le soluzioni ATD per identificare gli indicatori di compromissione sui dispositivi al momento della connessione per ridurre il tempo medio di risposta
- Isola e blocca rapidamente i dispositivi violati o dannosi per evitare la propagazione laterale del malware
- Automatizza la risposta agli incidenti e avvia flussi di lavoro di remediation sui dispositivi violati
- Riduce il tempo medio di risposta fornendo preziose informazioni di contesto relative al dispositivo (connessione, ubicazione, classificazione e stato di sicurezza) ai team di risposta agli incidenti di diverse aree funzionali e alle tecnologie isolate

La sicurezza inizia con la visibilità

Il motivo per cui le operazioni militari sul campo mirano sempre a conquistare le posizioni in quota è che consentono di vedere da lontano i nemici in avvicinamento e di organizzare le difese prima che venga sferrato l'attacco. La piattaforma Forescout offre ai reparti IT una visuale completa sul territorio che devono difendere. Mettendo in atto un'operazione continua di ricerca, classificazione, valutazione e controllo di ogni dispositivo, Forescout rende il campo di battaglia della sicurezza informatica più visibile, comprensibile e gestibile.

Prova Forescout in prima persona

Il modo migliore per comprendere le funzioni di visibilità e controllo dei dispositivi senza agent di Forescout consiste nel vederle all'opera in prima persona. Ci sono vari modi per approfondire la conoscenza della piattaforma Forescout:

Fai un Test Drive. 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.

Crea il tuo report Absolute Visibility and Risk di Forescout. Ottieni una valutazione dettagliata sul livello di visibilità e rischio dei tuoi dispositivi. Contatta il tuo rappresentante Forescout locale per maggiori informazioni.

Richiedi una demo. Visita il sito web di Forescout per richiedere una dimostrazione personalizzata e avere accesso a un ricco campionario di demo e video su richiesta.

Usa lo strumento Business Value ROI di Forescout (in inglese). Calcola il valore che apporta alla tua attività la piattaforma Forescout sulla base del modello di valutazione IDC in soli 10 minuti.

*Dati aggiornati al 31 marzo 2019

1 Forrester Research, "The Zero Trust eXtended (ZTX) Ecosystem" (L'ecosistema Zero Trust eXtended (ZTX)), gennaio 2018

2 Gartner, "Zero Trust Is an Initial Step on the Roadmap to CARTA" (Zero Trust è il primo passo verso CARTA), dicembre 2018

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