FORESCOUT

Visibilità totale: la chiave per una strategia Zero Trust

Forescout propone una piattaforma di visibilità dei dispositivi per una strategia Zero Trust

> "La visibilità è una condizione essenziale per difendere qualsiasi risorsa preziosa. Non si può proteggere quello che non si vede. Maggiore è la visibilità sulla rete da qualsiasi punto dell'ecosistema aziendale, più facile sarà individuare prontamente gli indizi di una violazione e intervenire.[3]"

Zero fiducia

Non c'è da stupirsi che il modello di sicurezza Zero Trust sia diventato una colonna portante delle strategie di sicurezza aziendale e dei piani di sviluppo delle soluzioni di sicurezza. Le architetture di sicurezza di tipo perimetrale che applicano automaticamente dei livelli di affidabilità elevati nella rete interna portano sistematicamente a risultati disastrosi e costosi da rimediare. Da un recente studio condotto dalla Online Trust Alliance è emerso che il numero di incidenti informatici segnalati dalle aziende nel 2017 è quasi raddoppiato. In realtà, nei primi tre trimestri del 2017, le violazioni hanno esposto oltre 7 miliardi di dati, un incremento di quattro volte rispetto al 2016.[1] Il Ponemon Institute ha quantificato questa emorragia finanziaria, stimando che il costo di remediation per ogni dato rubato sia di 141 dollari e che il costo medio complessivo di una violazione dei dati arrivi a 3,62 milioni di dollari.[2]

I numerosi difetti della sicurezza perimetrale

I moderni ambienti aziendali fanno un uso massiccio di servizi e infrastrutture cloud, una pratica che sostanzialmente dissolve il perimetro aziendale. I carichi di lavoro, i dati e la forza lavoro stessa sono ormai entità mobili, e come tali devono essere protette con un modello di sicurezza agile. Contemporaneamente, gli utenti richiedono di accedere a più account, dati e risorse, mentre il volume e l'eterogeneità dei dispositivi che si connettono alle risorse di rete mettono fuori gioco le tradizionali modalità di gestione degli endpoint. Dal momento che molti di questi dispositivi non sono dotati o non supportano gli agent di gestione aziendale (è il caso dei dispositivi degli ospiti, dei sistemi BYOD, dei dispositivi IoT e OT), accade che i responsabili della sicurezza siano inconsapevoli dei dispositivi connessi alla rete aziendale, che non riescano a identificare gli utenti che li usano, a valutarne lo stato di sicurezza né a controllare le attività che svolgono.

I difetti sistemici che caratterizzano il modello di sicurezza perimetrale hanno spinto gli analisti di Forrester Research a sviluppare un'alternativa denominata Zero Trust. Zero Trust è un modello concettuale e architettonico introdotto nel 2010. Stabilisce che i responsabili della sicurezza devono 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.

Zero Trust: da modello concettuale a framework completo

Le prime versioni del modello Zero Trust si limitavano a esporre i concetti della microsegmentazione e dell'accesso basato sul principio del privilegio minimo, senza offrire istruzioni specifiche su come utilizzare i controlli di sicurezza esistenti nelle implementazioni. Con il tempo, il modello base si è evoluto diventando quello che Forrester ha battezzato l'ecosistema Zero Trust eXtended (ZTX). Si tratta di un framework completo che associa specifiche tecnologie di sicurezza alle sette dimensioni chiave di un tipico ambiente aziendale a cui applicare i principi Zero Trust: reti, dati, utenti, carichi di lavoro, dispositivi, visibilità e analisi, automazione e coordinamento.

Il framework ZTX aiuta i responsabili della sicurezza a capire in che modo usare la tecnologia per:

- Applicare i principi di isolamento, segmentazione e protezione della rete
- Applicare i principi di classificazione, isolamento, cifratura e controllo dei dati
- Proteggere gli utenti della rete e le risorse dell'infrastruttura proteggendo contemporaneamente le risorse dagli utenti
- Proteggere l'intero stack di applicazioni nei cloud pubblici e privati
- Automatizzare e coordinare controlli e processi Zero Trust in ambienti eterogenei
- Garantire visibilità e analisi per scoprire e mettere in sicurezza ogni angolo dell'ambiente aziendale esteso

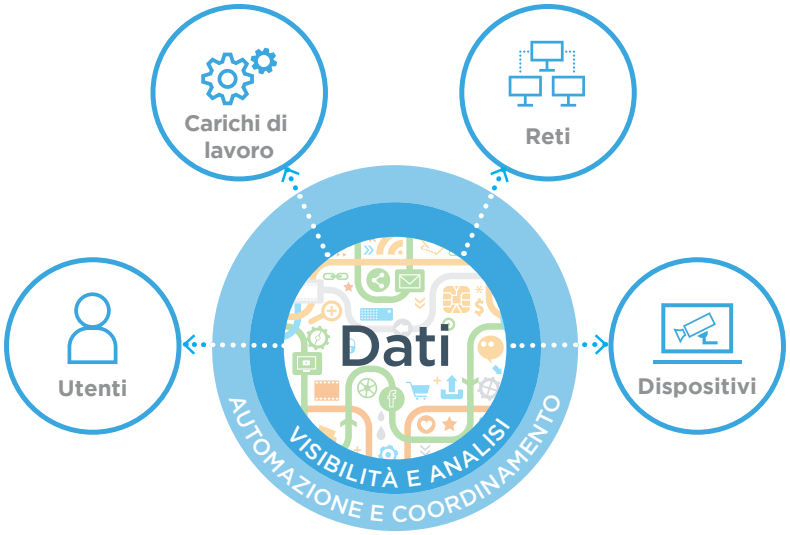

Figura 1: Le sette dimensioni dell'ecosistema ZTX di Forrester Research

Se la visibilità è la domanda, Forescout è la risposta

Esempio di strategia Zero Trust: individuare e classificare il 100% dei dispositivi connessi alla rete (e non solo quelli dotati di agent endpoint installati e operativi) e applicare una policy di controllo degli accessi basata sul principio del privilegio minimo, con analisi granulare dei dispositivi, dell'identità e delle autorizzazioni dell'utente, dei software, della conformità, della configurazione e dello stato di sicurezza. Per poter applicare una policy degli accessi restrittiva, è necessario vedere, valutare e controllare tutto ciò che accade nella rete.

Forrester dà molto peso all'argomento visibilità nella sua strategia Zero Trust. Secondo l'analista di Forrester Chase Cunningham:

Per mettere in atto una strategia di questo tipo, è necessario disporre di una soluzione per la visibilità e il controllo dei dispositivi in grado di rilevare e monitorare gli host che sfuggono ai tradizionali sistemi di gestione degli endpoint: dispositivi di ospiti e BYOD, endpoint aziendali con agent disabilitati, dispositivi inaffidabili, dispositivi IoT, switch e router di rete, sistemi di automazione e controllo industriale, macchine virtuali in cloud pubblici.

Visibilità e controllo con la piattaforma Forescout

Forescout esemplifica la trasformazione che hanno subito le principali tecnologie di rete che si sono evolute in piattaforme Zero Trust. La piattaforma Forescout è una soluzione di sicurezza senza agent che individua e valuta in modo dinamico gli endpoint nel preciso istante in cui si connettono a una qualsiasi rete estesa, eterogenea e multicloud. Determina rapidamente utente, proprietario, sistema operativo e configurazione dei dispositivi, software, servizi, stato delle patch e presenza di agent di sicurezza. Quindi, esegue operazioni di correzione, controllo e monitoraggio continuo di tali dispositivi.

Forescout esegue queste operazioni su dispositivi aziendali gestiti, dispositivi di ospiti non gestiti, server fisici e virtuali, infrastrutture di rete, sistemi di controllo e automazione industriale e dispositivi IoT. Non sono necessari agent software né una conoscenza precedente dei dispositivi. La piattaforma viene distribuita rapidamente nell'ambiente esistente e raramente richiede modifiche all'infrastruttura, upgrade o riconfigurazione degli endpoint. Funziona perfettamente in ambienti cloud fisici, virtuali e ibridi.

La piattaforma Forescout individua e classifica il 100% dei dispositivi con connessione IP, ed esegue una valutazione continuativa senza agent dei rischi e dello stato di sicurezza per ricavare in tempo reale la situazione complessiva di ogni dispositivo connesso. Quindi, usa questi dati di intelligence per attivare automaticamente controlli basati su policy e coordinare interventi sui dispositivi. Queste funzionalità costituiscono la base dell'efficace modello di sicurezza Zero Trust.

Tra i fornitori Zero Trust eXtended Ecosystem, Forrester ha dato il riconoscimento Zero Trust alla piattaforma Forescout. Secondo Forrester, Forescout offre funzionalità leader del mercato in cinque categorie del modello Zero Trust.[4]

Visibilità, analisi e controllo dei dispositivi Zero Trust

Individuazione senza agent di qualsiasi dispositivo - La piattaforma Forescout combina metodi attivi e passivi senza agent per cercare tutti i dispositivi presenti nella rete estesa ed eterogenea dell'azienda includendo ambiente fisico, data center, cloud e reti OT. Rileva PC e notebook, server fisici e virtuali, dispositivi mobili e IoT, istanze cloud e sistemi OT senza richiedere apparecchiature di rete di uno specifico fornitore, aggiornamenti dell'infrastruttura esistente né riconfigurazioni di switch e porte degli switch, con o senza autenticazione 802.1X.

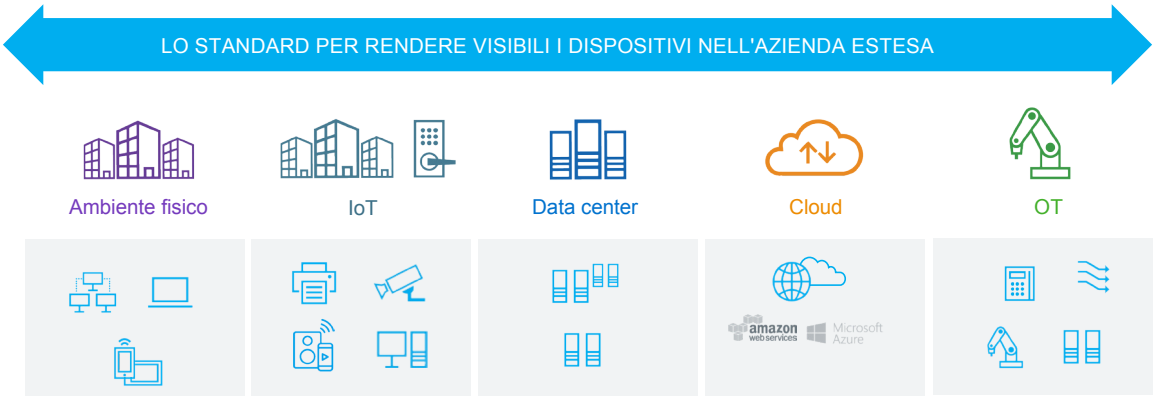

Figura 2: Visibilità e controllo dei dispositivi nell'azienda estesa con la piattaforma Forescout.

Dall'individuazione alla profilazione dei dispositivi – I vari metodi di individuazione e profilazione presenti nella piattaforma Forescout generano e mantengono aggiornato un elevato volume di informazioni sull'identità, lo stato e il comportamento dei dispositivi. Il livello di astrazione adattiva analizza miliardi di pacchetti di dati non elaborati che transitano nei diversi sistemi della rete, mette in correlazione i dati tra loro e li consolida creando un inventario completo della popolazione di dispositivi con funzionalità di analisi dettagliata di ciascun elemento. Il livello di astrazione si adatta e si evolve insieme all'ambiente IT e inserisce sistematicamente nell'inventario i nuovi dati non appena diventano disponibili. I dati di questo inventario dettagliato possono guidare e informare decisioni e azioni, oltre che costituire la base delle misure per la mitigazione dei rischi.

Inoltre, la piattaforma Forescout consente di monitorare e visualizzare le comunicazioni tra i dispositivi, le origini dati e gli altri elementi interdipendenti del sistema. Questo aspetto si rivela particolarmente importante per la segmentazione, la pianificazione e la definizione delle policy.

La piattaforma Forescout consente di monitorare e visualizzare le comunicazioni tra i dispositivi, le origini dati e gli altri elementi interdipendenti del sistema. Questo aspetto si rivela particolarmente importante per la segmentazione, la pianificazione e la definizione delle policy.

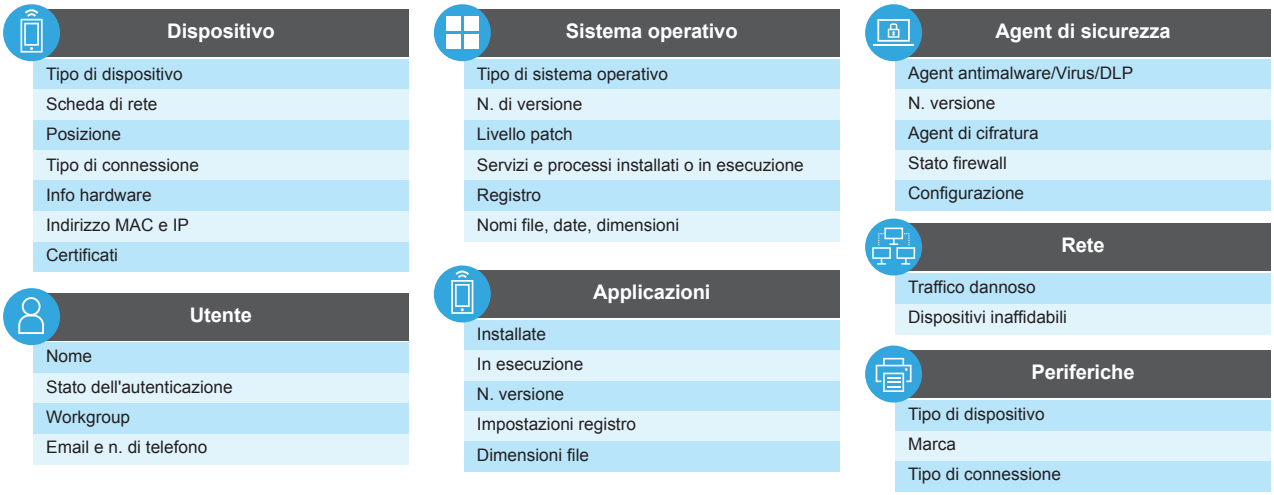

Figura 3: Il processo di classificazione di Forescout estrae dati dettagliati su tutti i dispositivi con connessione IP.

Visibilità continua e controllo dei dispositivi basato su policy - Il motore delle policy in tempo reale di Forescout utilizza i dati di intelligence raccolti per raffrontare continuamente i dispositivi con una serie di policy che impongono il comportamento previsto. Attiva istantaneamente le policy sulla base di vari attributi, anche personalizzabili, come ingresso nella rete e autenticazione. Ad esempio, Forescout può identificare un nuovo dispositivo IoT con connessione a Internet in uscita e assegnarlo automaticamente a un segmento di rete ad accesso limitato. Può rilevare cambiamenti dello stato di sicurezza di un dispositivo, se, ad esempio, il software antivirus o di cifratura è stato disattivato o non funziona correttamente. La piattaforma procede a una nuova valutazione dei dispositivi mentre sono connessi alla rete e ogni volta che vi entrano o escono, condivide dati in tempo reale sui dispositivi e, in collaborazione con sistemi terzi, avvia valutazioni dello stato di sicurezza, come la scansione dei dispositivi, per rilevare vulnerabilità o indicatori di compromissione.

Forescout è in grado di eseguire azioni di controllo direttamente su un dispositivo o sull'intera infrastruttura di rete, come spiegato più avanti. Le azioni eseguite sugli host includono l'avvio e l'arresto di applicazioni, l'aggiornamento di software antivirus e di protezione, la disattivazione di periferiche e la richiesta di conferme agli utenti finali. Queste policy vengono applicate automaticamente, indipendentemente da dove risiedono i dispositivi. Ove necessario e coordinandosi con strumenti esterni, la piattaforma Forescout può avviare automaticamente azioni di remediation, come l'applicazione di patch sui dispositivi, e di reinstallazione di software di protezione generici o specifici per la ricerca di vulnerabilità, la protezione degli endpoint e la cifratura.

Dati di intelligence sui dispositivi personalizzabili per le operazioni di sicurezza e la risposta agli incidenti - Ai responsabili della sicurezza manca una visuale completa sui dispositivi connessi e sul relativo contesto di classificazione, connessione e conformità. Ciò ostacola la risposta agli incidenti e la creazione di report sulla conformità. In aggiunta alla console, la piattaforma Forescout include ora un pannello di controllo Web personalizzabile che fornisce una visuale unificata sul panorama dei dispositivi e lo stato di conformità in tutta l'azienda estesa. Questo strumento si interfaccia con Forescout eyeManage per fornire informazioni sui diversi tipi di dispositivi connessi alla rete estesa.

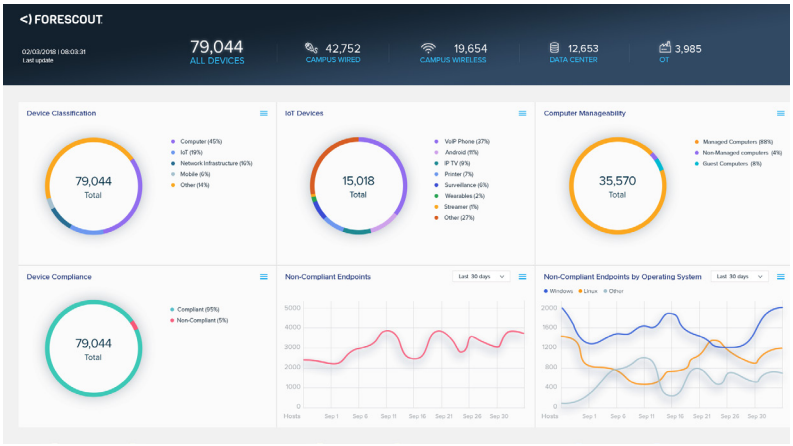

Figura 4: Visuale completa dei dispositivi per i centri operativi di sicurezza.

Funzionalità Zero Trust per la rete

Gestore accessi Zero Trust - La piattaforma Forescout esercita azioni di controllo degli accessi sull'intera infrastruttura di rete, fungendo da servizio centralizzato per l'intermediazione e la risoluzione degli accessi utilizzando i dati integrati di cui dispone su identità degli utenti, ruolo, autenticazione e stato del dispositivo. Si integra in modalità nativa con i prodotti di oltre 30 produttori di switch e controller wireless e si connette direttamente a router che eseguono Linux usando vari metodi, da soli o combinati, che includono SNMP, CLI e NETCONF. Quando interviene su uno switch della rete, questa tecnologia può cambiare la VLAN assegnata, aggiungere una lista di controllo degli accessi o disattivare una porta switch, mentre su un controller wireless può rifiutare la connessione a un indirizzo MAC o cambiare il ruolo di un utente. Può anche limitare l'accesso a utenti remoti che si connettono tramite VPN.

Un tratto distintivo della piattaforma senza agent Forescout per l'implementazione del modello Zero Trust nel mondo reale è che può individuare, valutare e concedere l'accesso a qualsiasi dispositivo legacy con connessione IP. Forescout vede e controlla ogni dispositivo con connessione IP e si integra con qualsiasi elemento dell'infrastruttura IT e OT senza eccezioni.

Un tratto distintivo della piattaforma senza agent Forescout per l'implementazione del modello Zero Trust nel mondo reale è che può individuare, valutare e concedere l'accesso a qualsiasi dispositivo legacy con connessione IP.

Con l'acquisizione di SecurityMatters, Forescout ha esteso la portata della sua visione oltre la rete IT arrivando ad abbracciare le reti OT e gli ambienti dei sistemi di controllo industriale. Le funzionalità combinate ora includono l'acquisizione e l'ispezione dei pacchetti di dati di oltre 100 protocolli IT/OT, la mappatura della rete, l'analisi dei flussi, il monitoraggio delle policy e dei comportamenti, l'analisi della rete, la valutazione delle minacce e il calcolo del rischio.

Segmentazione dinamica della rete - Forescout interagisce anche con i firewall di nuova generazione per creare punti di scelta e controllo che servono per la segmentazione dinamica basata sulle policy. I firewall di nuova generazione sorvegliano la rete usando la classificazione di utenti, dispositivi, applicazioni e traffico. Si appoggiano a dati contestuali su utenti e dispositivi estrapolati da varie fonti, come la piattaforma Forescout, per applicare policy di accesso granulari per un controllo preciso e flessibile sulle risorse. In questo modo i reparti IT riescono a implementare la segmentazione dinamica della rete e a creare policy di sicurezza sensibili al contesto all'interno dei firewall di nuova generazione usando il contesto degli endpoint fornito da Forescout.

Funzioni di automazione e coordinamento Zero Trust

Per far funzionare prodotti fino a quel momento separati come se fossero uno solo, la piattaforma Forescout coordina le attività di gestione della sicurezza a livello di infrastruttura. Il suo speciale mix di tecnologie di interoperabilità per rete, sicurezza e gestione può essere esteso a più di 70 prodotti di sicurezza e gestione IT esterni* tramite l'integrazione API e i prodotti Forescout eyeExtend. Il risultato è un sistema coordinato che accelera la risposta agli incidenti, migliora notevolmente l'efficienza operativa e garantisce un livello di protezione eccellente.

Forescout abilita l'automazione e il coordinamento della sicurezza in tre modi:

- **Condivisione in tempo reale dei dati contestuali** - Forescout monitora costantemente e condivide in modo dinamico i dati sull'identità dei dispositivi che risiedono negli endpoint, i dati di configurazione e le informazioni di sicurezza con gli altri sistemi di gestione della sicurezza utilizzati nel sistema. Questo scambio di dati bidirezionale completa le proprietà globali che possono essere applicate ai motori di regole di altri strumenti per perfezionare policy e azioni.
- **Automazione dei flussi di lavoro** - Forescout consente di condividere decisioni basate sulle policy che prima richiedevano di essere analizzate e applicate manualmente sui vari sistemi. L'automazione di questi processi e flussi di lavoro genera una risposta coordinata e istantanea.
- **Automazione delle azioni di risposta** - Non sono rari i prodotti di sicurezza che segnalano al personale IT la presenza di problemi, come i sistemi avanzati per il rilevamento delle minacce, i sistemi di gestione degli eventi e delle informazioni di sicurezza o ancora gli strumenti di valutazione delle vulnerabilità. Forescout, però, usa istantaneamente questi dati per attivare una risposta automatica e svolgere un'ampia gamma di azioni basate su policy, come isolare un dispositivo oppure correggere un endpoint per eliminare le minacce.

Funzionalità Zero Trust per i carichi di lavoro

Facendo leva sui diversi componenti dell'infrastruttura e sui carichi di lavoro, la piattaforma Forescout scopre, classifica e profila i server fisici e virtuali degli ambienti ibridi data center/cloud. Inoltre, segue e monitora i carichi di lavoro che si spostano all'interno degli ambienti ibridi data center/cloud per prevenire qualsiasi lacuna di visibilità. Forescout acquisisce le proprietà del cloud o dell'hypervisor dal livello più basso fino a quelle delle applicazioni installate o eseguite nei carichi di lavoro. Quindi, usa questi dati contestuali per assicurarsi che solo utenti e dispositivi autorizzati accedano a carichi di lavoro specifici, nel contesto del modello Zero Trust.

Funzionalità Zero Trust per gli utenti

Integrandosi ai principali sistemi di directory e identità, la piattaforma Forescout raccoglie informazioni sugli utenti, come il ruolo e le autorizzazioni di accesso. Quindi, combina queste informazioni con i dati sulla configurazione dei dispositivi, lo stato di sicurezza e la conformità che ha raccolto affinché tutti questi aspetti vengano considerati nel processo decisionale. Il monitoraggio continuo del comportamento degli utenti e l'integrazione con sistemi di gestione dei privilegi di accesso consente di scoprire gli account con autorizzazioni non conformi.

Funzionalità Zero Trust per i dati

Forescout gestisce la sicurezza dei dati di tutti i dispositivi con connessione IP mostrando la presenza e lo stato dei software di cifratura, offuscamento o di altro tipo previsti dalle policy. Se tali applicazioni non sono presenti o sono inattive, Forescout può svolgere azioni basate su policy come avvisare l'utente, avvisare un amministratore o mettere in quarantena il dispositivo finché la situazione non viene corretta.

Per entrare nel mondo Zero Trust, parti dalla visibilità totale sui dispositivi

Esistono 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 cinque potenti esperienze di utilizzo.
- **Richiedi una Demo:** visita la pagina della demo 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.
- **Contatta i servizi di consulenza Forescout:** stai pensando di strutturare il tuo ambiente secondo il modello Zero Trust? I consulenti Forescout sono esperti certificati per l'implementazione del prodotto, lo sviluppo dei processi e l'integrazione dei sistemi, oltre che profondi conoscitori delle migliori pratiche per l'accesso alla rete e la conformità degli endpoint.

Dati aggiornati al 31 dicembre 2018

***Note**

1 Online Trust Alliance, Cyber Incident and Breach Trends Report (Studio sulle tendenze delle violazioni e degli incidenti informatici), gennaio 2018
2 Ponemon Institute, 2017 Cost of Data Breach Study (Studio sul costo delle violazioni dei dati nel 2017), giugno 2017
3 Forrester Research, The Zero Trust eXtended (ZTX) Ecosystem (L'ecosistema Zero Trust eXtended), gennaio 2018
4 Forrester Research, The Zero Trust eXtended Ecosystem Road Map: The Zero Trust Security Playbook (Roadmap per l'ecosistema Zero Trust eXtended: strategia per la sicurezza Zero Trust), 11 luglio 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