FORESCOUT

Visibilità sui dispositivi: La soluzione per ridurre i rischi e migliorare lo stato di sicurezza

Sei modi per migliorare la sicurezza con il 100% di visibilità

La messa in sicurezza dell'infrastruttura di rete è un compito che diventa ogni giorno più complesso a causa della crescita esponenziale del volume di dispositivi IoT, della diversificazione delle piattaforme, dell'adozione del cloud e della convergenza IT e OT. La maggior parte dei nuovi dispositivi connessi alle reti provoca seri problemi di visibilità e sicurezza perché non è progettata per supportare gli agent di gestione e questi punti ciechi si ampliano man mano che il cloud computing si estende agli angoli più remoti delle reti distribuite.

Quello che non riusciamo a vedere ci può distruggere. È indispensabile trovare il modo di individuare tutti i dispositivi della rete, a prescindere dalla loro ubicazione, dalla presenza di agent e dalla loro natura fisica o virtuale, di implementare un processo di monitoraggio continuo in tempo reale e di elaborare una strategia per analizzare e classificare i dispositivi non appena si connettono alla rete.

L'eliminazione delle lacune nella visibilità è il modo più efficace per esercitare un impatto positivo sulla sicurezza della rete e le attività di mitigazione dei rischi. Ecco sei opportunità per sfruttare la visibilità totale:

1 Ottenere visibilità senza agent su tutti i dispositivi, BYOD, IoT e OT compresi

Dato che non si può proteggere quello che non si riesce a vedere, è indubbio che per essere attuabile, una soluzione deve offrire una visione precisa e immediata su tutti gli endpoint della rete.

Le tradizionali soluzioni di controllo degli accessi alla rete sono in grado di rilevare solo i dispositivi dotati di agent. Ma non è pensabile installare agent su tutti i dispositivi BYOD e di tipo non tradizionale che entrano in contatto con una rete, come gli smartphone degli utenti, i tablet, i dispositivi indossabili, i dispositivi IoT e OT, i laptop dei collaboratori esterni fino ai dispositivi non autorizzati che provengono da chissà dove. Tutti questi elementi costituiscono un rischio.

È necessario poter contare su una visibilità senza agent per rilevare immediatamente qualsiasi dispositivo che si connette alla rete. Non basta scoprire gli indirizzi IP e MAC. Servono informazioni dettagliate su ogni singolo dispositivo per stabilirne lo scopo, il proprietario e lo stato di sicurezza.

2 Unificare la visione e il controllo sugli ambienti fisici, sui data center e sul cloud

Fino a poco tempo fa, era sufficiente proteggere il data center, ma ora tutto si è complicato. In molti casi, data center singoli si sono trasformati in data center multipli distribuiti in ambienti fisici in più parti del mondo. E poi c'è il cloud.

Ormai non basta più pattugliare solo il perimetro della rete, anche perché un perimetro vero e proprio non esiste più. Bisogna disporre di accesso istantaneo in tempo reale a tutti gli endpoint nelle varie ubicazioni: data center, ambiente fisico o cloud. Non è più pensabile tentare di gestire e mettere in sicurezza dispositivi e carichi di lavoro usando interfacce e strumenti eterogenei e isolati. **Una soluzione praticabile deve offrire una visione complessiva su tutti i sistemi tradizionali, sui dispositivi mobili e IoT oltre che sulle macchine virtuali e le istanze cloud, indipendentemente dalla loro ubicazione**. In più, per riuscire a gestire le crescenti esigenze della rete, questa soluzione deve offrire un livello di scalabilità nettamente superiore al passato.

Questo nuovo paradigma slegato dalla tecnologia e dall'ubicazione impone un nuovo modo di concepire l'interoperabilità delle soluzioni e una minore tolleranza verso la dipendenza dal produttore. Oggi, il valore della tecnologia è amplificato perché i sistemi sono visibili in più dashboard e meccanismi di controllo comuni. Il nuovo paradigma richiede flessibilità di implementazione su architetture centralizzate e distribuite in funzione dei diversi requisiti aziendali.

3 Soddisfare gli obblighi di conformità normativi e dei dispositivi

È abbastanza comune al giorno d'oggi che i sistemi non superino i test di penetrazione o le verifiche della conformità normativa a causa della presenza di dispositivi IoT non rilevati o di altre minacce non correttamente segmentate. Una strategia di sicurezza efficace comincia con una visibilità ininterrotta e un inventario completo dei dispositivi che metta al riparo da rischi legali e finanziari.

Dati di gestione delle risorse informatiche non precisi possono inficiare la conformità ai requisiti normativi come RGPD, HIPAA, PCI e FISMA e comportare multe salate per l'azienda.

Indipendentemente dal tipo di dispositivi che si desidera mettere in sicurezza (finanziari, medici, industriali e così via), il punto di partenza di un programma di rischio e conformità deve essere la visibilità assoluta. È indispensabile poter *vedere e classificare i dispositivi, automatizzarne il controllo e limitare l'accesso* alle varie zone della rete in base ai livelli di autorizzazione, alle policy di sicurezza aziendale e ai requisiti normativi.

Poiché molte normative statali, federali o internazionali prevedono la segnalazione della violazione entro qualche ora dall'incidente, è essenziale che le piattaforme di sicurezza cooperino per rispondere e porre rimedio all'attacco in modo rapido ed efficace.

4 Automatizzare la compilazione e la gestione dell'inventario dei dispositivi

Per gestire in modo efficace e sicuro i beni aziendali è necessario poter fare affidamento su un inventario preciso che includa ogni dispositivo della rete. Basta che dall'inventario manchi un solo dispositivo o che ce ne sia uno con dati di configurazione superati o imprecisi per fornire agli hacker un'opportunità di violare la rete. Cercare i dispositivi con i metodi tradizionali può rivelarsi rischioso. Secondo Gartner "Fino al 2020, senza la ricerca attiva, il 30% delle risorse aziendali resterà nascosto."

Con la ricerca manuale delle risorse si rischia di compilare un database di gestione delle configurazioni incompleto e impreciso che potrebbe compromettere la riuscita delle iniziative di gestione della sicurezza. Il tracciamento delle risorse con fogli di Excel o altri metodi manuali è un metodo insidioso, senza contare che i dati dell'inventario diventano obsoleti velocemente. Oltre ad accelerare la risposta dell'help desk, un inventario dei dispositivi aggiornato mette immediatamente a disposizione *degli addetti alla sicurezza incaricati di rispondere agli attacchi diretti a sistemi operativi di endpoint o a tipi di dispositivi IoT specifici dati precisi sui dispositivi*.

Tra l'altro, se l'utilizzo del software non viene tracciato correttamente, si rischia il sovrautilizzo e la violazione degli accordi di licenza, situazioni che possono comportare gravi sanzioni.

Automatizzando l'inventario e la gestione diventa possibile condividere dati contestuali con gli strumenti di IT Asset Management come ServiceNow® con cui aggiornare in tempo reale i database di gestione delle configurazioni. Un inventario aggiornato facilita una gestione efficace del ciclo di vita dei dispositivi e aiuta le decisioni di bilancio per l'acquisto di risorse.

5 Segmentazione della rete sensibile al contesto

Gli esperti di rete e sicurezza concordano, in linea generale, che la segmentazione della rete dovrebbe essere la priorità numero uno di qualsiasi strategia di protezione. Tramite la valutazione e la segmentazione dei dispositivi è possibile automatizzare l'assegnazione e l'applicazione di liste di controllo degli accessi basate sulle policy e le VLAN, assegnare in modalità dinamica i dispositivi ai segmenti, imporre il controllo degli accessi e limitare gli accessi alle sole risorse autorizzate dei segmenti. Questa strategia impedisce efficacemente ai dipendenti di insinuarsi in zone della rete cui non devono accedere e limita la diffusione degli attacchi malware.

L'aggiunta dei dati contestuali in tempo reale all'assegnazione della segmentazione migliora drasticamente la sicurezza in più modi. Ad esempio, una soluzione con questa funzionalità ha la possibilità di verificare lo stato di conformità di un dispositivo prima dell'assegnazione della segmentazione, oltre a monitorare con continuità lo stato di sicurezza e il comportamento del dispositivo e a riassegnare rapidamente un dispositivo non autorizzato o non conforme a un segmento appropriato o a un segmento VLAN con restrizioni. Questo avviene nel caso in cui, ad esempio, una stampante tenti di collegarsi a un database HR o se una telecamera di sorveglianza tenta di accedere a qualcosa che non è un videoregistratore digitale. *Questo nuovo metodo di segmentazione dinamico e intelligente facilita notevolmente anche le modifiche alla rete e introduce una maggiore flessibilità in termini di architettura perché permette una condivisione e orchestrazione dei dati contestuali con i firewall di nuova generazione*.

In questo caso è necessario dotarsi di una soluzione NAC che si integri facilmente con switch, reti private virtuali, sistemi di gestione cloud e firewall di nuova generazione.

6 Ridurre la finestra di esposizione con una risposta agli incidenti coordinata

I team che si occupano della sicurezza della rete gestiscono in media fino a 15 strumenti, il che significa che le aziende investono molto tempo e denaro per acquistare, imparare ad usare e coordinare questi strumenti. Inoltre, la maggior parte di questi strumenti di sicurezza è ottima per l'invio di avvisi, ma è incapace di applicare azioni correttive. Il risultato è che gli addetti alla sicurezza sono sopraffatti dal volume di avvisi che devono valutare e risolvere manualmente.

Per accelerare la risposta agli incidenti, gli strumenti devono reagire sistematicamente agli avvisi, intervenire automaticamente nel caso di situazioni conosciute e fornire agli analisti della sicurezza informazioni ordinate per priorità quando emergono nuove minacce.

Per ottenere il massimo da questi strumenti, si deve poter contare su un'interoperabilità dei flussi di lavoro immediata e sulla capacità di svolgere operazioni di ricerca e classificazione in modalità automatica. Le soluzioni scelte devono integrarsi naturalmente con gli strumenti di rete esistenti e condividere in tempo reale i dati, gli avvisi e le risposte con altri strumenti ITAM e di sicurezza.

I nuovi strumenti devono anche supportare le reti di più vendor, a prescindere dal fatto che le risorse siano fisiche o virtuali e ubicate in ambienti fisici, data center o cloud.

La soluzione Forescout

La piattaforma di visibilità e controllo dei dispositivi di Forescout consente di realizzare tutti e sei questi compiti, e molti altri. Senza ricorrere ad agent, individua immediatamente qualsiasi dispositivo con connessione IP che si connette alla rete. Fornisce una visibilità estesa sui dispositivi usando una combinazione di tecniche di ricerca attive e passive, profilazione e classificazione. Offre una scalabilità ai vertici del settore: supporta fino a due milioni di dispositivi con un'unica appliance CounterACT® Enterprise Manager.

L'esclusivo approccio senza agent di Forescout rende visibile un'intera gamma di dispositivi (gestiti e non gestiti, aziendali e personali, cablati e wireless) che include i sistemi BYOD, i server, gli switch, l'hardware inaffidabile e i dispositivi IoT.

Forescout sta migliorando la visibilità e il controllo sui dispositivi per contenere i rischi, ridurre la superficie di attacco e automatizzare la risposta agli incidenti nell'intera rete aziendale estesa: la ***tua*** rete.

Glossario degli acronimi

BYOD: bring your own device (portare il proprio dispositivo)

FISMA: Federal Information System Management Act (Legge federale sulla gestione dei sistemi di informazione)

HIPAA: Health Insurance Portability and Accountability Act (Legge sulla portabilità e la responsabilità dell'assicurazione malattia)

IoT: Internet of Things (Internet delle cose)

IP: Internet Protocol (Protocollo internet)

IT: information technology (tecnologia dell'informazione)

ITAM: information technology asset management (gestione delle risorse informatiche)

MAC: Media Access Control (Controllo dell'accesso ai media)

NAC: network access control (controllo di accesso alla rete)

OT: operational technology (tecnologia operativa)

PCI: Payment Card Industry (Industria delle carte di pagamento)

RGPD: Regolamento Generale sulla Protezione dei Dati

VLAN: virtual local area network (rete locale virtuale)

VPN: virtual private network (rete privata virtuale)

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

E-mail info-italia@forescout.com
Tel. (internazionale) +1-408-213-3191
Assistenza +1-708-237-6591