FORTINET

Quali miglioramenti della sicurezza degli endpoint di prossima generazione sono necessari?

Come i responsabili dell'infrastruttura IT possono proteggere gli endpoint e migliorare l'efficienza operativa

Sommario

FORTINET

Panoramica preliminare

Gli endpoint continuano a essere uno dei bersagli preferiti degli attacchi informatici. Un laptop, uno smartphone o un dispositivo Internet-of-Things (IoT) compromesso può consentire alle minacce di spostarsi lateralmente infettando altri endpoint all'interno dell'organizzazione e permettere agli aggressori di accedere ad altre risorse critiche. Oltre a indebolire la sicurezza, le intrusioni distolgono il personale dalle attività che migliorano le prestazioni della rete e semplificano le operazioni.

Per affrontare queste sfide, i responsabili dell'infrastruttura IT hanno bisogno di soluzioni integrate di rete e sicurezza che proteggano gli endpoint, riducano al minimo l'impatto operativo associato alla superficie di attacco in espansione e consentano ai loro team di ampliarle. Una profonda connessione tra la sicurezza degli endpoint e la sicurezza della rete offre miglioramenti fondamentali per una protezione olistica dell'azienda, garantendo una visibilità basata sul rischio di tutti i dispositivi endpoint, controlli di accesso basati su policy, condivisione della threat intelligence in tempo reale, nonché risposte e flussi di lavoro per la sicurezza automatizzati.

Solo il 26% dei responsabili delle tecnologie afferma di essere “pronto” agli attacchi informatici.[1]

Introduzione: il responsabile dell'infrastruttura IT e la sicurezza degli endpoint

La superficie di attacco degli endpoint si sta espandendo rapidamente, spinta da una crescita esponenziale dei dispositivi degli utenti finali. Il fenomeno è accentuato da una proliferazione di dispositivi connessi come sensori IoT, tecnologie indossabili, sistemi di controllo industriale (ICS) e veicoli a guida automatica. Di conseguenza, gli attacchi informatici sono ormai diffusi e continuano ad aumentare, se consideriamo che la metà delle organizzazioni ha subito almeno una violazione a livello di endpoint negli ultimi 12 mesi.[2] La maggior parte delle organizzazioni si rivolge ai responsabili dell'infrastruttura IT per affrontare il problema, e quasi tre quarti (73%) di loro sono direttamente responsabili della sicurezza degli endpoint.[3]

Al di là delle minacce in sé, esistono gravi problemi di sicurezza della rete e degli endpoint, che generalmente si situano in compartimenti distinti e non comunicanti. Gli approcci tradizionali alla sicurezza della rete e degli endpoint non riescono a integrare i molteplici componenti di sicurezza coinvolti. In risposta, i responsabili dell'infrastruttura IT devono abbattere queste compartimentazioni scegliendo un'architettura di sicurezza che integri gli elementi di rete e sicurezza, compresi gli endpoint, in una piattaforma di sicurezza intelligente. Questa trasformazione richiede quattro miglioramenti essenziali: una migliore visibilità del rischio, controlli dinamici degli accessi, condivisione della threat intelligence e flussi di lavoro per la sicurezza automatizzati.

56%

percentuale dei responsabili dell'infrastruttura IT che passa più della metà del tempo a occuparsi di sicurezza informatica.[4]

Requisito 1: migliorare la visibilità del rischio

La visibilità è un prerequisito fondamentale per una sicurezza efficace degli endpoint: non è possibile garantire ciò che non si può vedere. Il personale che gestisce le infrastrutture IT deve essere perfettamente a conoscenza dello stato degli endpoint sia all'interno che all'esterno della rete aziendale, tra cui vulnerabilità senza patch, software obsoleti, applicazioni potenzialmente indesiderate, comportamenti a rischio e violazioni delle policy. La visibilità basata sul rischio dipende da una chiara comprensione delle esposizioni al rischio degli endpoint, tra cui identità degli utenti, stato di protezione ed eventi legati alla sicurezza.

Il compito del responsabile dell'infrastruttura IT è quello di selezionare soluzioni per la sicurezza degli endpoint che possano condividere la telemetria in tempo reale con altri strumenti di sicurezza come, ad esempio, firewall, sandbox e filtri web. Ciò significa anche che i flussi di lavoro per la sicurezza e l'attenuazione delle minacce devono interagire senza soluzione di continuità tra i vari elementi. Tutto questo può far perdere tempo prezioso al personale se non sono presenti i giusti punti di integrazione. Pertanto, una soluzione per la sicurezza degli endpoint di prossima generazione deve consentire di valutare immediatamente lo stato della sicurezza attraverso strumenti di gestione riuniti in un'unica interfaccia.

$8,19M

Costo totale medio di una violazione dei dati negli Stati Uniti.[5]

Requisito 2: migliorare i controlli degli accessi

Una volta ottenuta la visibilità del rischio, i responsabili dell'infrastruttura IT hanno bisogno di un controllo degli accessi alla rete più capillare e dinamico. In questo caso, la sicurezza degli endpoint deve applicare le policy e i controlli a tutti i dispositivi e difendersi dagli attacchi sferrati tramite dispositivi endpoint. A tal fine, la sicurezza degli endpoint deve garantire che gli endpoint soddisfino tutti gli standard di compliance e sicurezza prima di concedere l'accesso alla rete, oltre a fornire capacità di analisi e mettere in quarantena endpoint compromessi e non autorizzati.

Il raggruppamento dei dispositivi endpoint in segmenti basati sull'intento che consentono il controllo dinamico degli accessi è una parte importante del processo. Ciò richiede capacità di distribuzione e gestione semplificate, tra cui attività di compliance e reporting, per il personale che si occupa dell'infrastruttura IT, sovraccarico e non in grado di gestire queste attività manualmente.

67%

percentuale dei responsabili delle tecnologie secondo cui la carenza di competenze impedisce all'organizzazione di stare al passo con il cambiamento.[6]

Requisito 3: condividere la threat intelligence

Gli attacchi diventano sempre più mirati e virulenti, per cui la finestra temporale per una risposta efficace agli incidenti continua a ridursi. L'accelerazione dei tempi di risoluzione richiede una condivisione istantanea e bidirezionale della threat intelligence attraverso una profonda integrazione tra gli endpoint e gli strumenti di sicurezza della rete. Quando un componente di rete intercetta una nuova minaccia, invia automaticamente l'intelligence agli altri endpoint e alle soluzioni di sicurezza distribuite in tutta l'organizzazione, in modo istantaneo.

La condivisione delle informazioni in tempo reale consente al personale che gestisce l'infrastruttura IT di ottenere un quadro completo e preciso della strategia di sicurezza immediata della rete. La sicurezza degli endpoint incrocia gli eventi con il traffico di lavoro e i feed di threat intelligence per verificare le segnalazioni, rilevare le minacce e identificare le potenziali compromissioni. L'integrazione profonda aiuta a migliorare il rapporto segnale-rumore, riducendo al minimo i falsi positivi e il numero eccessivo di segnalazioni, oltre a fornire un quadro più accurato della strategia di sicurezza immediata della rete.

Per massimizzare la produttività del personale, i responsabili dell'infrastruttura IT devono considerare la possibilità di aumentare la sicurezza degli endpoint con un abbonamento a un servizio di valutazione della sicurezza. Possono infatti utilizzare gli strumenti di tale servizio per comprendere meglio la strategia di sicurezza della loro organizzazione rispetto a organizzazioni omologhe e agli standard riconosciuti. Possono inoltre ottenere indicazioni dettagliate ed elenchi di azioni da intraprendere per migliorare sistematicamente la loro strategia di sicurezza e riferire tali miglioramenti ai dirigenti.

206 giorni

Tempo medio per identificare una violazione dei dati, in aumento del 5% rispetto all’anno scorso.[7]

Requisito 4: automatizzare i flussi di lavoro per la sicurezza

L'automazione dei flussi di lavoro fondamentali per la sicurezza è un miglioramento essenziale che consente ai responsabili dell'infrastruttura IT di raggiungere un'efficace sicurezza degli endpoint riducendo al contempo la pressione sui loro team, i quali sono sovraccarichi e spesso con risorse insufficienti. L'automazione della sicurezza degli endpoint offre vantaggi alla strategia di sicurezza dell'organizzazione attraverso la gestione delle vulnerabilità, la risposta e il contenimento automatizzati degli incidenti e la compliance degli endpoint. Di seguito sono riportate alcune delle capacità fondamentali di cui i responsabili dell'infrastruttura IT hanno bisogno per ottenere tali vantaggi in una soluzione di sicurezza degli endpoint:

Gestione delle vulnerabilità. La gestione delle vulnerabilità include la capacità di automatizzare le patch per il software e i sistemi operativi degli endpoint e fornire una soluzione flessibile e automatizzata a piccoli problemi di sicurezza senza l'intervento umano. Queste capacità aiutano a eliminare le lacune difensive di base nella strategia di sicurezza degli endpoint, riducendo al contempo le attività manuali e ripetitive per il personale che gestisce l'infrastruttura IT.

Automazione della risposta agli incidenti. L'automazione della risposta e del contenimento degli incidenti accelera i tempi di contenimento e risoluzione eliminando il tempo di risposta umana dai flussi di lavoro per la sicurezza. La sicurezza degli endpoint deve mettere in quarantena automaticamente gli endpoint sospetti o compromessi per prevenire la diffusione dell'infezione ad altri dispositivi e il movimento laterale delle minacce all'interno dell'organizzazione. Così facendo, inoltre, si contribuisce a ridurre al minimo gli errori umani e si facilita il rispetto da parte degli endpoint di standard di riservatezza dei dati e normative di settore sempre più rigorosi.

Architettura API aperta. Per consentire la più ampia interoperabilità possibile delle capacità di automazione della soluzione di sicurezza degli endpoint in tutta l'architettura di sicurezza della rete, i responsabili dell'infrastruttura IT hanno bisogno di una soluzione di sicurezza degli endpoint che si basi su un'architettura API aperta e compatibile con altri prodotti di sicurezza di terzi. Tale capacità estende l'integrazione della sicurezza, contribuendo al tempo stesso a massimizzare gli investimenti esistenti in altre soluzioni antivirus e prodotti di sicurezza.

“Visto l’esercito globale di dispositivi connessi e una superficie di attacco che tutti i partner e i fornitori dell’ecosistema dell’azienda, gli autori delle minacce hanno un chiaro vantaggio.”[8]

Sintesi: cosa cercare

La rapida espansione della superficie di attacco, strettamente legata alla crescita del numero di endpoint che si collegano alla rete e vi risiedono, rende più difficile la protezione dagli attacchi informatici. Aumenta inoltre il tempo che i team responsabili dell'infrastruttura IT dedicano alla gestione degli endpoint.

Incapaci di vedere attraverso gli endpoint e gestire in modo centralizzato e proattivo le vulnerabilità, i responsabili dell'infrastruttura IT hanno bisogno di un approccio di prossima generazione alla sicurezza degli endpoint che non aumenti i costi o il tempo impiegato per gestire la sicurezza degli endpoint. La sicurezza degli endpoint deve invece superare la compartimentazione tra un endpoint e l'altro, e tra questi e la rete. In tal modo, si possono condividere la threat intelligence e la telemetria in tempo reale, ottenendo un controllo centralizzato degli accessi e automatizzando le verifiche di compliance, il reporting e i flussi di lavoro per patch e risposta agli incidenti.

[1] Anna Frazzetto, et al., "A Changing Perspective: CIO Survey 2019," Harvey Nash/KPMG, 2019.

[2] Lee Neely, "Endpoint Protection and Response: A SANS Survey," SANS Institute, 12 giugno 2018.

[3] "The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, 18 agosto 2019.

[4] Ibid.

[5] "Cost of a Data Breach Report 2019," IBM Security and Ponemon Institute, aprile 2019.

[6] Anna Frazzetto, et al., "A Changing Perspective: CIO Survey 2019," Harvey Nash/KPMG, 2019.

[7] "Cost of a Data Breach Report 2019," IBM Security and Ponemon Institute, aprile 2019.

[8] "The Post-Digital Era is Upon Us: Are You Ready for What's Next?," Accenture, 2019.

www.fortinet.com

446935-A-0-IT

febbraio 16, 2021 12:33 PM

eb-next-generation-endpoint-security_IT