STORIE DI CLIENTI AKAMAI

Un'azienda del settore produttivo quotata in borsa standardizza i controlli di sicurezza e risparmia tempo con Akamai Guardicore Segmentation

L'azienda del settore produttivo aveva necessità di una soluzione globale e sicura

Visibilità completa della rete

Segmentazione nelle infrastrutture IT

Risposta alle minacce ransomware

Il cliente

Questa azienda leader nel settore produttivo è quotata in borsa (NYSE) e opera nei mercati di tutto il mondo.

La sfida

Protezione di un'organizzazione globale

Il gruppo di sicurezza IT è responsabile di più sedi in tutto il mondo, la maggior parte delle quali sono uffici a uso misto e strutture di produzione. Per garantire una solida strategia di sicurezza, il team doveva standardizzare i controlli di sicurezza in tutta l'organizzazione e fornire una protezione coerente nelle aree geografiche distribuite.

"Volevamo passare da una rete semplice e aperta a un'architettura segmentata basata su best-practice", ha spiegato l'Infrastructure Architect che guida il progetto di segmentazione.

Come molte aziende, questa azienda del settore manifatturiero ha adottato i firewall per il progetto.

Tuttavia, la gestione di una moltitudine di regole basate sull'infrastruttura e di modifiche e aggiornamenti a livello di workstation sulla rete è diventata rapidamente dispendiosa in termini di tempo, anche in un unico sito. Inoltre, sebbene la visibilità sia migliorata, è rimasta limitata a zone specifiche, rendendo difficile ottenere una visione completa e centralizzata dell'attività di rete e delle dipendenze tra le risorse.

Blocco del movimento laterale non autorizzato

Pur offrendo alcuni controlli di segmentazione approssimativi, i firewall non erano in grado di risolvere un altro problema chiave per il team di sicurezza: le comunicazioni peer-to-peer non gestite. Pertanto, era essenziale estendere la protezione e la visibilità a quell'area specifica. Non risolvere tale problema avrebbe lasciato l'organizzazione vulnerabile ad attacchi pass-the-hash, ransomware e altre minacce che si basano sul movimento laterale tra gli endpoint per propagarsi.

Azienda manifatturiera

Sede
Stati Uniti

Settore
Manifatturiero

Soluzione
Akamai Guardicore Segmentation

Risultati principali

- Mitiga la diffusione del ransomware tramite il movimento laterale
- Fornisce una visibilità granulare
- Protegge gli endpoint con la segmentazione
- Facilita la risposta agli incidenti

La scelta di una soluzione

Dopo diverse laboriose implementazioni di controllo del firewall, il team è venuto a conoscenza di Akamai Guardicore Segmentation e ha avviato discussioni interne sui vantaggi e le possibilità della segmentazione di nuova generazione.

Tutte le nuove soluzioni implementate dall'azienda richiedono di eseguire una ricerca completa, quindi il team ha valutato anche diverse alternative. Dopo un accurato processo di verifica, il team ha infine optato per la soluzione Akamai Guardicore Segmentation. "Nessuno di loro ci ha fornito una soluzione completa come [Akamai], con monitoraggio del traffico, etichettatura flessibile e ampia visibilità a livello di applicazione tramite il footprint di un singolo agente su un client", ha affermato l'Infrastructure Architect.

Akamai Guardicore Segmentation

Nella prima fase del progetto, l'azienda ha distribuito Akamai Guardicore Segmentation su circa 2.000 workstation. Dopo l'implementazione della soluzione, il team di sicurezza IT ha immediatamente scoperto un nuovo livello di visibilità sulla rete e sui relativi flussi di comunicazione.

Nuove informazioni e segmentazione in azione

"Con le mappe del traffico di [Akamai], la nostra visibilità è ora migliorata del 1000% e include le comunicazioni da PC a PC", ha affermato l'Infrastructure Architect.

La capacità di esaminare in dettaglio l'attività di un singolo computer, comprendendo al contempo l'attività complessiva a livello di applicazione ha consentito all'organizzazione di prendere decisioni di sicurezza più informate. Ad esempio, alcuni utenti hanno installato applicazioni per le stampanti domestiche sui laptop aziendali. È stato scoperto che molte di queste applicazioni eseguivano continuamente la scansione della rete aziendale per la ricerca dei dispositivi supportati. Sulla base di questa nuova intuizione dalla visibilità di Akamai, il team è stato in grado di interrompere le scansioni.

Akamai Hunt: utilizzare Akamai Guardicore Segmentation per il rilevamento delle minacce

Questa nuova comprensione dell'attività di rete ha anche consentito all'azienda di bloccare i criminali esterni. Ad esempio, subito dopo l'implementazione della piattaforma, il servizio Akamai Hunt ha rilevato una risorsa che stava comunicando con un file con le caratteristiche di un noto malware chiamato GoldenSpy. Il team Hunt ha informato il team di sicurezza IT dell'azienda della minaccia rilevata. Al cliente è stata inoltre fornita un'analisi della portata dell'infezione, dei potenziali rischi (corrispondenza dei risultati con le informazioni di MITRE su GoldenSpy), statistiche (sfruttando Insight) e raccomandazioni per l'indagine interna e la mitigazione. L'azienda ha quindi utilizzato i controlli delle policy di Akamai per mettere in quarantena il sistema infetto e impedire al malware di spostarsi lateralmente su nuovi computer.

Standardizzazione e risparmio di tempo

Questa azienda ora può anche creare e gestire le policy a livello centrale, inclusa una policy centrale globale per le workstation e ha la flessibilità per creare eccezioni isolate quando richiesto da un caso di utilizzo. Ciò garantisce un'applicazione coerente ovunque sia presente un agente Akamai e riduce il rischio di errori di configurazione e ritardi.

> Con un singolo agente su un computer, abbiamo risolto definitivamente il problema di un attacco all'endpoint tramite movimento laterale.
>
> Infrastructure Architect, azienda del settore manifatturiero

Inoltre, anche il tempo di conformità alle policy è notevolmente migliorato nell'organizzazione. Ad esempio, apportare una modifica ai controlli del firewall prima della nuova piattaforma era un processo che poteva richiedere giorni. Utilizzando i nuovi modelli di policy di Akamai come guida iniziale, il team di sicurezza IT può creare controlli di sicurezza anche per i casi di utilizzo più complessi in meno di un'ora e applicarli all'intera base installata in pochi secondi.

Il futuro con Akamai

Sebbene l'obiettivo iniziale del progetto fosse la standardizzazione dei controlli di sicurezza per la segmentazione e l'accesso degli endpoint, sono previsti ulteriori casi di utilizzo con Akamai. Le parti interessate stanno discutendo di un'espansione della protezione per includere server e applicazioni critiche, come il sistema ERP dell'organizzazione.

Indipendentemente dai programmi futuri, il progetto originale è considerato di per sé un successo dall'azienda manifatturiera e ha ridotto drasticamente la superficie di attacco e il rischio per le workstation dell'azienda. Il team ora è molto più sicuro della strategia di sicurezza dell'organizzazione contro gli attacchi che si spostano lateralmente da un endpoint all'altro. Come ha spiegato il leader del progetto, "Ora, con un solo agente su una macchina, abbiamo risolto il problema per sempre e possiamo passare da una workstation senza criteri all'implementazione completa dei controlli di sicurezza in 30 secondi".

Per ulteriori informazioni, visitate il sito akamai.com/guardicore.

> Con le mappe del traffico di [Akamai], la nostra visibilità è ora migliorata del 1000% e include le comunicazioni da PC a PC.
>
> Infrastructure Architect,
> azienda del settore manifatturiero