Storie di clienti Akamai

La protezione dei clienti con Akamai API Security

Un'azienda leader nel settore della sicurezza aiuta a garantire la conformità a migliaia di clienti e a proteggere decine di migliaia di API

Netskope è un'azienda leader a livello globale nel settore della cybersicurezza, che sta ridefinendo la sicurezza di cloud, dati e reti. Migliaia di clienti, tra cui più di 25 aziende Fortune 100, si affidano a Netskope per affrontare le minacce in continua evoluzione, facilitare le svolte tecnologiche e aiutare le organizzazioni a conformarsi agli obblighi normativi.

Tra le varie aree tecnologiche mission-critical che protegge, Netskope è responsabile della sicurezza di decine di migliaia di API a livello globale, un compito che l'azienda ha realizzato adottando un approccio innovativo rispetto al tradizionale sistema di sicurezza delle applicazioni. Dopo aver rilevato delle falle nel sistema di sicurezza delle API di uno dei suoi clienti, Netskope si è rivolta a Noname Security (ora acquisita da Akamai) perché aveva bisogno di strumenti di nuova generazione per proteggere i suoi clienti dai devastanti attacchi alle API.

Oltre i confini del firewall

Indipendentemente dal fatto che le applicazioni implementate dai clienti siano più piccole o più grandi con una miriade di microservizi, la realtà è che usano tutte le API, pertanto ognuna delle API esposte diventa parte della superficie di attacco. Ad esempio, Netskope ha rilevato che si erano verificati abusi nel patrimonio delle API di un cliente che erano passati inosservati e che Netskope non era riuscita ad individuare. Pertanto, il team AppSec di Netskope ha iniziato a cercare una soluzione in grado di proteggere sia le proprie API che quelle dei suoi clienti, insieme ad altre risorse digitali pubbliche.

Netskope sapeva che il problema non era di tipo tradizionale, pertanto non avrebbe potuto usare soluzioni già esistenti come un WAF (Web Application Firewall) o eseguire test convenzionali sulla sicurezza delle applicazioni. La quantità dei registri, le forme di abuso delle API e i tipi di attacchi osservati richiedevano un approccio diverso.

Sede

Santa Clara, California
netskope.com

Settore

High-tech

Soluzione

Akamai API Security

Risultati principali

- Ciclo di vita delle API totalmente protetto
- Attacchi alle API bloccati in tempo reale
- Specifiche delle API create automaticamente

James Robinson, Deputy CISO di Netskope, aveva capito anche che, nell'intento di passare ad un livello aziendale, il suo team doveva utilizzare l'apprendimento automatico e strumenti avanzati per ottenere una visibilità completa sul patrimonio delle sue API. Tuttavia, per implementare un nuovo strumento, il team addetto alla sicurezza sapeva bene di aver bisogno dell'aiuto degli sviluppatori in questo processo.

Una vittoria per il team addetto alla sicurezza

Netskope ha deciso di utilizzare la piattaforma Noname API Security (ora parte di Akamai API Security) per proteggere le sue API sia in fase di preproduzione che durante la produzione. Per proteggere le API in fase di produzione, l'azienda ha utilizzato il modulo di individuazione disponibile nella soluzione Akamai API Security per stilare un inventario accurato delle API interne, esterne e di terze parti, nonché per classificare i dati sensibili trasmessi tramite le API. Una volta stilato un inventario accurato, l'azienda ha usato il modulo di protezione del runtime per rilevare le anomalie e bloccare gli attacchi alle API in tempo reale.

Durante la preproduzione, Netskope ha utilizzato il modulo per l'esecuzione dei test di Akamai API Security per eseguire i test delle API in modo da individuare vulnerabilità ed errori di configurazione prima dell'implementazione delle API. La soluzione può eseguire automaticamente più di 100 test dinamici che simulano il traffico dannoso in modo non solo da aiutare gli sviluppatori a proteggere il proprio codice, ma anche a garantire la sicurezza del prodotto per la protezione delle API che stanno rilasciando per i clienti.

Durante la fase di valutazione, gli sviluppatori hanno visto immediatamente ciò che avrebbe semplificato il loro compito: Akamai poteva aiutarli a creare rapidamente una specifica API se quella esistente era obsoleta. Gli sviluppatori ora non devono guardare il codice per capire di quale API si tratta perché la specifica viene creata automaticamente. Lo stesso approccio vale per i registri e le transazioni. Ora, gli sviluppatori possono condurre query in vari sistemi ed esaminare le righe dei registri.

Non sorprende, quindi, che la piattaforma si sia rivelata anche un importante successo per il team addetto alla sicurezza, che non solo ha iniziato a rilevare gli attacchi tradizionali, ma anche ad individuare minacce più sofisticate.

> A livello interno, quando abbiamo iniziato ad esaminare la soluzione, avevamo sicuramente bisogno del supporto degli sviluppatori, senza il quale non potremmo riuscire ad accedere ai nostri sistemi critici, praticamente al cuore delle loro applicazioni.
>
> **- James Robinson**
> **Deputy CISO, Netskope**

Uno sguardo al futuro: garantire la conformità dei clienti

Guardando al futuro, Netskope intende utilizzare Akamai per gestire la governance delle API, garantendo che la sua azienda e i suoi clienti rimangano conformi agli obblighi e alle leggi sulla privacy dei dati sempre più numerose a livello globale. Inoltre, l'azienda intende continuare ad esaminare vari casi di utilizzo dopo aver implementato la soluzione Akamai API Security sia nel cloud che on-premise. L'implementazione on-premise è stata una vera e propria svolta per l'azienda e per i suoi clienti che operano nel settore pubblico e in altri settori altamente regolamentati.

> Noname non solo si è rivelata un'azienda vincente, ma, soprattutto, ci ha supportato migliorando e velocizzando il nostro processo di implementazione per consentirci una più rapida immissione dei prodotti sul mercato.
>
> **- James Robinson**
> **Deputy CISO, Netskope**

Le organizzazioni stanno rapidamente adottando un'architettura SASE (Secure Access Service Edge) per salvaguardare i dati ovunque vengano spostati, supportare la trasformazione digitale e migliorare l'efficienza e il ritorno sugli investimenti (ROI) derivante dai propri strumenti tecnologici. Netskope è già un'azienda ampiamente riconosciuta per le sue competenze e il suo livello di innovazione nelle soluzioni CASB, SWG, ZTNA, FWaaS (Firewall-as-a-Service) e in altri componenti del sistema SSE (Security Service Edge), che descrive i servizi di sicurezza necessari per la riuscita di un'architettura SASE.

Nonostante la popolarità dell'architettura SASE, tuttavia, spesso i vendor utilizzano messaggi confusi per accompagnare gruppi frammentari di prodotti, che vengono commercializzati in modo discutibile con la dicitura "SASE". La maggior parte di questi prodotti non sono integrati in modo nativo né riescono a semplificare gli ambienti tecnologici, mancando anche delle funzionalità critiche di trasformazione delle infrastrutture e delle reti, tutte componenti che incrementano i rischi di subire incidenti di sicurezza, riscontrare problemi di downtime delle reti e mantenere basso il ROI.

Le soluzioni Netskope Borderless SD-WAN e Netskope Intelligent SSE combinate in una piattaforma SASE totalmente convergente possono risolvere questi problemi in modo esclusivo.

Akamai