Akamai-Kundenreferenz

Schutz von Kunden mit Akamai API Security

Leader in Sachen Sicherheit hilft Tausenden von Kunden bei der Gewährleistung der Compliance und dem Schutz Zehntausender von APIs

Netskope ist ein weltweit führender Anbieter von Cybersicherheit und definiert Cloud-, Daten- und Netzwerksicherheit neu. Tausende von Kunden, darunter mehr als 25 der Fortune 100, vertrauen auf Netskope, um sich neuen Bedrohungen zu stellen, Technologiewechsel zu erleichtern und sie bei der Einhaltung gesetzlicher Vorschriften zu unterstützen.

Unter den vielen geschäftskritischen Technologiebereichen, die es zu schützen gilt, sind Zehntausende von APIs weltweit, für deren Sicherheit Netskope verantwortlich ist – eine Leistung, die das Unternehmen nur durch einen neuen Ansatz jenseits der traditionellen Anwendungssicherheit realisieren konnte. Nachdem Netskope Lücken in der API-Sicherheitslage eines seiner Kunden entdeckt hatte, wandte sich das Unternehmen an Noname Security (jetzt ein Akamai-Unternehmen), das die Tools der nächsten Generation bereitstellte, die zum Schutz der Kunden vor böswilligen API-Angriffen benötigt wurden.

Blick über die Firewall hinaus

Unabhängig davon, ob die Kunden kleinere Anwendungen oder größere mit unzähligen Microservices einsetzen, verwenden sie letztendlich alle APIs, was bedeutet, dass jede dieser exponierten APIs Teil der Angriffsfläche ist. Netskope hat beispielsweise festgestellt, dass es innerhalb des API-Bestands eines Kunden zu Missbräuchen gekommen war, die nicht erkannt worden waren und die Netskope nicht sehen konnte. Aus diesem Grund begann das AppSec-Team von Netskope mit der Suche nach einer Lösung, die sowohl die eigenen APIs als auch die APIs der Kunden sowie andere öffentlich zugängliche digitale Ressourcen schützen würde.

netskope

Standort

Santa Clara, Kalifornien
netskope.com

Branche

Hightech

Lösung

Akamai API Security

Die wichtigsten Vorteile

- API-Lebenszyklus vollständig gesichert
- API-Angriffe werden in Echtzeit blockiert
- API-Spezifikationen werden automatisch erstellt

Akamai

Netskope erkannte, dass es sich nicht um ein herkömmliches Problem handelte, was bedeutete, dass sie keine herkömmlichen Lösungen wie eine Web Application Firewall verwenden oder herkömmliche Anwendungssicherheitstests durchführen konnten. Die Menge der Protokolle, die Arten der Angriffe, die beobachtet wurden, und die Arten des API-Missbrauchs erforderten einen anderen Ansatz.

James Robinson, stellvertretender CISO von Netskope, war sich auch darüber im Klaren, dass sein Team bei dem Versuch, auf Unternehmensebene zu skalieren, maschinelles Lernen und fortschrittliche Tools nutzen müsste, um einen vollständigen Überblick über den API-Bestand zu erhalten. Dem Sicherheitsteam war jedoch klar, dass es für die Einführung eines neuen Tools Entwickler als Partner benötigen würde.

Ein Gewinn für das Sicherheitsteam

Netskope entschied sich für die Noname API Security Platform (jetzt Teil von Akamai API Security), um APIs sowohl in der Vorproduktions- als auch in der Produktionsphase zu schützen. Zur Sicherung von APIs in der Produktion kam das Discovery-Modul von Akamai API Security zum Einsatz, um eine genaue Bestandsaufnahme der internen, externen und Drittanbieter-APIs der Kunden zu erstellen und alle sensiblen Daten zu klassifizieren, die diese APIs durchliefen. Sobald eine genaue Bestandsaufnahme vorlag, wurde das Runtime Protection-Modul eingesetzt, um Anomalien zu erkennen und API-Angriffe in Echtzeit zu blockieren.

Im Rahmen der Vorproduktion nutzte Netskope die API-Sicherheitstestlösung von Akamai, mit der Unternehmen APIs vor der Bereitstellung auf Schwachstellen und Fehlkonfigurationen testen können. Die Lösung kann automatisch mehr als 100 dynamische Tests ausführen, die bösartigen Traffic simulieren. Dies hilft nicht nur den Entwicklern eines Unternehmens, ihren Code zu sichern, sondern gewährleistet auch die Sicherheit des API-Produkts, das für Kunden freigegeben werden soll.

Während der Evaluierungsphase fielen den Entwicklern sofort Funktionen ins Auge, die ihnen das Leben erleichtern würden. Sie erkannten, dass Akamai ihnen helfen kann, wenn der Entwickler aufgrund des Alters der API keine API-Spezifikation hat – jetzt ist es möglich, schnell eine zu erstellen. Sie müssen sich den Code nicht ansehen, um die API zu verstehen, da die Spezifikation automatisch für sie erstellt wird. Dasselbe Erlebnis gilt für die Protokolle und Transaktionen. Die Entwickler können Anfragen in verschiedenen Systemen durchführen und sich die Protokollzeilen ansehen.

> Als wir intern begannen, uns mit der Lösung zu befassen, brauchten wir definitiv Entwickler, die uns als Partner zur Seite standen. Ohne ihre Unterstützung werden Sie nicht in der Lage sein, auf ihre kritischen Systeme zuzugreifen – im Grunde das Herzstück ihrer Anwendungen.
>
> **– James Robinson**
> **Deputy CISO, Netskope**

Es überrascht nicht, dass die Plattform auch ein großer Gewinn für das Sicherheitsteam war. Das Team konnte nicht nur herkömmliche Angriffe erkennen, sondern auch ausgefeiltere Bedrohungen aufdecken.

Ausblick Wahrung der Compliance bei Kunden

Für die Zukunft plant Netskope, Akamai für die API-Governance einzusetzen, um sicherzustellen, dass das Unternehmen und seine Kunden die weltweit immer strengeren Datenschutzgesetze und -vorschriften einhalten. Das Unternehmen plant außerdem, weiterhin verschiedene Anwendungsfälle zu untersuchen, da Akamai API Security sowohl in der Cloud als auch vor Ort eingesetzt wird. Die On-Prem-Bereitstellung hat für das Unternehmen und seine Kunden im öffentlichen Sektor und in anderen stark regulierten Branchen alles verändert.

> Noname war nicht nur der Gewinner, sondern unterstützte uns auch dabei, eine bessere und schnellere Bereitstellung zu erreichen, damit wir schneller auf den Markt kommen.
>
> **– James Robinson**
> **Deputy CISO, Netskope**

netskope

Unternehmen setzen zunehmend auf eine SASE-Architektur (Secure Access Service Edge), um Daten bei jeder Übertragung zu schützen, die digitale Transformation zu unterstützen und die Effizienz und Rendite ihrer Technologie zu steigern. Netskope ist bereits ein weithin anerkannter Experte und Innovator in den Bereichen CASB, SWG, Zero Trust Network Access, Firewall as a Service und anderen Komponenten des Security Service Edge (SSE), der die für eine erfolgreiche SASE-Architektur erforderlichen Sicherheitsdienste beschreibt.

Trotz der Beliebtheit von SASE werden jedoch oft verwirrende Anbieterinformationen mit Produktsets geliefert, die nur aus Einzelteilen bestehen und in zweifelhafter Weise als „SASE“ vermarktet werden. Die meisten dieser Produkte sind weder nativ integriert noch in der Lage, Technologieumgebungen zu vereinfachen, und es fehlen ihnen entscheidende Netzwerk- und Infrastruktur-Transformationsfunktionen – all dies birgt das Risiko höherer Sicherheitsvorfälle, Netzwerkausfälle und einem schlechten ROI.

Netskope Borderless SD-WAN in Kombination mit Netskope Intelligent SSE in einer vollständig konvergierten SASE-Plattform, die diese Herausforderungen auf einzigartige Weise bewältigt.

Akamai