Akamai Customer Story

Protecting Customers with Akamai API Security

Security leader helps keep thousands of customers compliant and tens of thousands of APIs secure

Netskope is a global cybersecurity leader that is redefining cloud, data, and network security. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope to address evolving threats, facilitate technology shifts, and help them comply with regulatory mandates.

Among the many mission-critical technology areas they protect, Netskope is responsible for securing tens of thousands of APIs globally — a feat the company realized required a new approach beyond traditional application security. After discovering gaps in one of their customer's API security posture, Netskope turned to Noname Security (now an Akamai company) for the next-generation tools needed to protect their customers from malicious API attacks.

Looking beyond the firewall

Whether the customers are deploying smaller applications or larger ones with myriad microservices, the reality is they are all using APIs, which means every one of those exposed APIs is part of the attack surface. For example, Netskope discovered that there were abuses within a customer's API estate that hadn't been detected and that Netskope could not see. For that reason, Netskope's AppSec team began its search for a solution that would secure both their own APIs as well as their customers' APIs, along with other public-facing digital assets.

Netskope knew that the problem wasn't a traditional one — which meant they wouldn't be able to use legacy solutions like a web application firewall or to pursue conventional application security testing. The volume of logs, the types of attacks they were seeing, and the types of API abuses required a different approach.

netskope

Location

Santa Clara, California
netskope.com

Industry

High Tech

Solution

Akamai API Security

Key Impacts

- API lifecycle fully secured
- API attacks blocked in real time
- API specs created automatically

Akamai

James Robinson, Netskope's Deputy CISO, also understood that when trying to scale at an enterprise level, his team would need to leverage machine learning and advanced tooling to get complete visibility into their API estate. But to onboard a new tool, the security team was well aware that they would need developers to be partners in the effort.

A win for the security team

Netskope decided to use the Noname API Security Platform (now part of Akamai API Security) to protect their APIs in both preproduction and during production. To secure APIs in production, they used the Discovery module in Akamai API Security to get an accurate inventory of their customers' internal, external, and third-party APIs, as well as to classify any sensitive data that traversed those APIs. Once they had an accurate inventory, they then used the Runtime Protection module to detect anomalies and block API attacks in real time.

From a preproduction perspective, Netskope used Akamai's API security testing solution that helps organizations test APIs for vulnerabilities and misconfigurations before they are deployed. The solution can automatically run more than 100 dynamic tests that simulate malicious traffic, which not only helps an organization's developers secure their code but also ensures the safety of the API product they're about to release for customers.

During the evaluation phase, the developers immediately saw features that would make their lives easier. They saw that Akamai could assist when the developer doesn't have an API spec because of how old it is — now they're able to quickly build one. They don't have to go look at the code to understand the API because the spec is being created automatically for them. The same experience is true for the logs and transactions. The developers can conduct queries in different systems and look at log lines.

Not surprisingly, the platform was also a major win for the security team. The team not only started to detect traditional attacks but also uncovered more sophisticated threats.

> "Internally, when we started to take a look at the solution, we definitely needed developers to be partners with us. You're not going to be able to get into their critical systems — basically the heart of their applications — without their support."
>
> – **James Robinson**
> Deputy CISO, Netskope

Akamai

Looking forward: Keeping customers compliant

In terms of moving forward, Netskope plans to use Akamai to address API governance, ensuring that they and their customers remain compliant with the globally expanding data privacy laws and mandates. They also plan to continue to explore different use cases as they have Akamai API Security deployed both in the cloud and on-premises. The on-prem deployment has been a game changer for them and their customers in the public sector and other highly regulated industries.

> Not only was Noname the winner, but then on top of that, they also supported a better and faster deployment for us to get to market quicker.
>
> – **James Robinson**
> **Deputy CISO, Netskope**

Organizations are rapidly adopting a secure access service edge (SASE) architecture to safeguard data wherever it moves, support digital transformation efforts, and realize better efficiency and return on investment (ROI) from their technology. Netskope is already a widely acknowledged expert and innovator in CASB, SWG, ZTNA, firewall as a service, and other components of the security service edge (SSE), which describes the security services needed for a successful SASE architecture.

Despite SASE's popularity, however, confusing vendor messaging often accompanies piecemeal product sets that are questionably marketed as "SASE." Most of these products are neither natively integrated nor able to simplify technology environments, and they lack critical network and infrastructure transformation capabilities — all of which risk higher levels of security incidents, network downtime, and poor ROI.

Netskope Borderless SD-WAN combined with Netskope Intelligent SSE in a fully converged SASE platform uniquely addressing these challenges.

| Published 09/24

Akamai