Netskope is a global cybersecurity leader 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 for the next-generation tools needed to protect their customers from malicious API attacks.

I think that most organizations haven’t seen the benefit and value of API security yet. For many CISOs, it’s a scenario where they’re kind of a sitting duck. It’s an unfunded or an underfunded area.

James Robinson
Deputy CISO, Netskope
The Problem

Whether deploying smaller applications or larger ones with a myriad of microservices, the reality is they are all utilizing APIs, which means every one of those exposed APIs is part of the attack surface. As evidence, Netskope discovered that there were abuses within a customer’s API estate that hadn’t been detected and that Netskope had no visibility into. 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 issue - which meant they wouldn’t be able to use legacy solutions like a web application firewall or 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.

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 in order to onboard a new tool, the security team was well aware that they would need developers to be partners in the effort.

"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.” Robinson added.

The Solution

Netskope decided to leverage the Noname API Security Platform to protect their APIs in both pre-production and in production. To secure APIs in production, they used the Discovery module in the Noname Platform to get an accurate inventory of their customers internal, external, and 3rd party APIs, as well as classify any sensitive data that traversed those APIs. Once they had an accurate inventory, they then utilized our Runtime Protection module to detect anomalies and block API attacks in real-time.

From a pre-production perspective, Netskope leveraged Noname’s industry-leading Active Testing module, which is an API security testing solution that helps the organization test APIs for vulnerabilities and misconfigurations before they are deployed. It can perform over 100 business logic-based tests against APIs, which not only helps developers secure their code, but also ensures the quality of the API product they’re about to release.
During the evaluation phase, the developers immediately saw features that would make their lives easier. They saw that Noname could assist in scenarios where the developer doesn't have an API spec because of how old it is, but now they're able to quickly build one. They don't have to go look at the code to understand the API – the spec is being created automatically for them. The same experience is true for the logs and transactions. They can conduct queries in different systems and look at log lines.

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

"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. So there was a two kind of a two part or a multiplier of a win that happened there. Not only the highest criteria of being able to detect the most and put us in the best position to discover, but then detect an attack and then respond to that attack," said the Deputy CISO.

Moving forward

In terms of moving forward, Netskope plans to leverage Noname to address API governance, ensuring 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 Noname deployed both in the cloud and on-prem. The on-premise deployment has been a gamechanger for them and their customers in the public sector and other highly regulated industries.

"It was very easy to work with Noname. There were others that were a little bit pushy where I would say, "if this is how the relationship is when we're dating, how's it going to be when we're married?" added Robinson. He went on to say, "the engagement is something that I haven't seen from many other vendors that I've used. In fact, I used [Noname] a couple of times as reference with other other companies and said you should do it more like this."
About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.

nonamesecurity.com  info@nonamesecurity.com  +1 (415) 993-7371