Akamai Customer Story

# Leading Telecom in Asia Secured APIs from Threats

The company gained visibility into — and protections for — every API in its estate

Discovered unmanaged APIs | Improved API protection | Secured sensitive data

The telecommunications industry across Asia is investing heavily in developing new technologies and expanding networks to meet customers' demand for better digital services, as mobile devices proliferate. Behind the scenes, APIs provide:

- The necessary connectivity for the telco industry's transformation, while expediting DevOps teams' processes
- The foundation to provide mobile phone services, internet access, and other telecommunication products to customers around the continent
- The ability to offer more personalized solutions and ultimately improve the customer experience

One of the region's leading telcos also sees the great opportunity that APIs enable — specifically for offering new digital voice and data solutions. And as the 5G era approaches, the company has set its sights beyond telephony and onward to big data, AI, IoT, and other emerging digital applications. However, it also understands that APIs are proliferating not only in number, but in risk. Having witnessed other major telecom providers suffer the effects of API attacks in 2022 and 2023, the company engaged with Noname Security (now an Akamai company).

Telecommunications Company

**Location**

Asia

**Industry**

Network Operator

**Solution**

Akamai API Security

Akamai

## A need for visibility into all APIs and their risks

As with many organizations, lack of visibility into APIs and their risks is a prevalent challenge for security teams. According to our research, only 4 in 10 organizations with full API inventories know which of their APIs return sensitive data. By using our API security solution's Discovery module, we determined that our telecom customer had been experiencing a similar challenge.

Prior to working with Akamai, the customer's API security controls consisted mainly of a legacy API management platform and web application firewall (WAF). From an application security and API delivery perspective, this arrangement made sense. However, neither solution provided the high degree of security controls and observability required to comprehensively protect APIs from today's attack methods. One key reason: Not all APIs are routed through a proxy like a WAF or API gateway, and these unmanaged APIs are appealing targets for malicious actors.

But even with an accurate audit of its API inventory, the company still needed capabilities to secure APIs during their normal functioning as they operate and manage requests. Quite simply, it would be unworkable for an organization's security team to manually identify malicious behavior in its environment.

There are hundreds, if not thousands, of API endpoints that need to be protected in real time. Commonly used AppSec solutions typically cannot keep up with every API call in a customer's environment — this can leave a company's IT environment vulnerable to cyberattacks without the proper API runtime protection capabilities.

## Solutions for seeing every API and securing against API threats

The first phase of the engagement entailed a pilot deployment to locate the company's internal APIs, assess configurations, and understand the types of data traversing the APIs. The customer was immediately impressed with the speed in which the discovery was executed, the accurate inventory findings, and the sensitive data exposure the tool identified.

Due to the pilot's positive outcomes, the customer then expanded the coverage area of the Noname API Security Platform (now part of Akamai API Security) to its entire internal and external API estate. This exercise also revealed more hidden production APIs, and uncovered the most imminent threats facing the environment.

We found that the customer needed a stronger defense against major security vulnerabilities to protect their APIs from future attacks. With Akamai API Security deployed, the customer can now detect suspicious behavioral anomalies and trigger incident response protocols — in real time. This helps an organization to avoid having to rely on delayed reporting and access logs to inform its remediation process. Once suspicious behaviors are detected with Akamai API Security, they are reported to the customer's API gateway, SIEM system, and other information security engines to inform the entire security team. The customer can choose to have its staff remediate the issue(s) manually, semiautomatically, or fully automatically, depending on the use case and severity of the vulnerability.


 | Published 09/24