

## Case Study

# Asia-Pacific Telecommunications Giant Boosts API Security Using the Cequence Unified Protection Platform

## A Global Technology Leader

One of the world's largest telecommunications companies is also well known as an award-winning industry technology leader. In addition to serving millions of customers globally, they play a key role in their native country's communications infrastructure. "We are focused on delivering the world's most secure, reliable, and innovative technology solutions for our customers, rather than competing solely on price," says their Regional CISO.

## IT and Business Challenges

With a team of hundreds of IT and security professionals that handle a wide range of cybersecurity functions, including architecture, pen testing, and assurance for global operations, it's crucial that oversight happen across the organization and into its numerous acquired companies. "We currently oversee approximately 100 subsidiaries," noted the Regional CISO. "To ensure cohesive security practices across our entities, we operate a group security model. That's why we need to deploy the best telecommunications and API security solutions, to ensure the most practical and secure outcomes for all of our organizations."

## Managing IT Complexity

The organization's IT environment is highly complex, with tens of thousands of legacy servers and one of the most complex, leading-edge 5G mobile networks in the world. Utilizing cloud services for most of its applications, using Azure, AWS, and Google GCP, the company also depends on a large number of mission-critical SaaS applications. With nearly 40,000 APIs, many of which are customer-facing or support business-to-business applications, "I always tell people that we have one of everything, many of most things," explained the Regional CISO.

## Searching for a Way to Improve API Security

Before using Cequence, the organization managed API security through multiple API gateway providers, offering a basic level of control, but it was recognized that the company's existing API security model was not as

**"Having a purpose-built, dedicated API security solution for all our internet-facing applications is a substantial benefit for us. With Cequence, we have successfully achieved all of our API security goals."**

Regional CISO

### Challenge

- ✓ **Wanted to improve API security** to minimize the risk of data breaches
- ✓ Needed the ability to **identify and fix any API vulnerabilities** before deploying apps
- ✓ Looking for a solution that was **easy to deploy and manage**

advanced as it needed to be. “While good design, assurance, and architecture are all important, APIs are subject to frequent changes, which can lead to data leaks or security issues, despite careful design,” noted the Regional CISO. “Attackers often target APIs due to the valuable data they provide. As our use of APIs expanded, we decided to seek out a dedicated API security solution that we could use across all of our enterprises.”

## Deploying Cequence Security

Cequence’s Unified API Protection solution was selected in 2022 to secure the company’s internet-facing APIs. While Cequence was initially deployed as an on-premises solution, it was later transitioned to Cequence’s SaaS delivery offering. “Cequence has demonstrated a real willingness to understand our challenges and assist in resolving them,” acknowledged the Regional CISO. “Some vendors simply adhere to their published integration patterns and then leave you to manage the environment on your own. Cequence’s willingness to go the extra mile has been commendable. Their focus on ensuring we derive the greatest value from the platform has been evident from the very beginning.”

## Increased Confidence and Speed When Rolling out Applications

“By sharing the visibility and insights we obtain from Cequence API security platform with our development teams, we are enabling them to enhance the security of their designs before launching new applications,” said the Regional CISO. “Although API testing is still necessary, the implementations are now much faster due to up-front validation of our security processes.”

## Recommending Cequence to Others

When asked if he would recommend Cequence to his peers, the Regional CISO replied, “Yes, absolutely. I am a huge fan of Cequence. Their technology is excellent, but it’s the process of working directly with the Cequence team that’s the biggest differentiator for me. They really care about our success. Too often we deal with vendors who don’t have the time, aren’t interested, or aren’t willing to be flexible with our needs. That’s definitely not the case with Cequence.”

## Providing Reassurance to the Board and Executive Team

“Cequence helps us demonstrate to our board and senior executive team that we have a superior security solution in place that enables us to protect all of our APIs,” said the Regional CISO. “Given the sensitivity of protecting confidential information in our country—particularly following a significant API-led security breach that was experienced by one of our competitors—this assurance has been invaluable. Having a purpose-built, dedicated API security solution for all our internet-facing APIs is a substantial benefit for us. With Cequence, we have successfully achieved our API security goals.”

### Solution

#### The Cequence Unified API Protection Platform

### Benefits

#### Wanted to improve and automate bot management

- ✓ Gained the ability to easily discover and protect all internal and external APIs
- ✓ Achieved a fast and seamless deployment
- ✓ Enhanced data security with the ability to identify and fix any API vulnerabilities before launch
- ✓ Obtained excellent on-going support and training from the Cequence team

**“Cequence’s willingness to go the extra mile has been commendable. Their focus on ensuring we derive the greatest value from the platform has been evident from the very beginning.”**

### Regional CISO