AKAMAI PARTNER STORY

SIOS Fortified API Security with Akamai

Leader in API platform design and integration reduced security risks and better enabled mission-critical services

Resolved API security issues

Expanded service offerings

Fortified enterprise DX

Specialists in API ecosystem design

SIOS Technology excels in designing comprehensive API ecosystems for Japanese enterprises in finance, information and communications, and manufacturing. As these businesses increasingly rely on APIs, the threat landscape is evolving fast. Web attacks targeting API vulnerabilities are surging, and traditional protections like API gateways and WAFs are no longer enough. By adding Akamai's API Security solution to its portfolio of services, SIOS can better protect its enterprise customers against the risks associated with the fast-expanding API economy.

A decade on the API front lines in Japan

For more than 10 years, SIOS Technology has built large-scale API platforms for some of Japan's most demanding sectors. What started as an open source system integrator evolved into a one-stop provider of API platform design, development, operations, and related services.

"When we launched our API solutions business, APIs were not very well known," recalled Tsukasa Nihei, Corporate Vice President and Head of API Solutions SL at SIOS. "Now, it's common to see systems with thousands of APIs."

This explosive growth reshaped both sides of the market. On the demand side, companies need more connected services to support IoT, AI, and the sharing economy. On the supply side, the rise of XaaS creates pressure to link and monetize services quickly.

With API integration driving new value, ignoring it is a real business risk. In fact, SIOS has seen APIs become essential for rapid experimentation and iterative development.

SIOS

Location

Japan
api-ecosystem.sios.jp

Industry

Software and SaaS

Solution

API Security

Akamai

Security challenges multiplied with API scale

As SIOS scaled API environments for customers, the threat surface grew with it. "When services connect through APIs, yesterday's competitors become today's partners, and the security stakes rise dramatically," said Nihei.

According to him, challenges fall into three emerging areas:

- A surge in API endpoints has produced a growing number of vulnerable entry points.
- With data fragmented across microservices, it's increasingly difficult to visualize the flow of data.
- The flow of complex information across the API economy makes it challenging to manage monetization.

"The moment players with limited understanding enter the ecosystem, they become easy targets and the network becomes highly vulnerable," Nihei explained. "This creates a chink in your armor, leaving the door open for malicious players such as hackers and data extraction."

Traditional, centralized security controls including API gateways and web application firewalls are no longer enough. Regional regulations like GDPR and a growing variety of use cases only add to the complexity. SIOS needed a security partner with deep API intelligence and enterprise-grade support.

Choosing Akamai for comprehensive protection across the API lifecycle

Unlike companies that focus solely on selling a single API management system, SIOS takes a multi-vendor approach, delivering the right solution for each customer's unique needs. In line with this strategy, it added Akamai API Security to its service portfolio.

"We chose Akamai API Security because its permission management features allow us to tailor configurations to each use case," said Nihei. "That level of control is essential for enterprise services."

He also emphasized Akamai's reliability: "Akamai's 24/7 enterprise support is a must for the types of mission-critical systems we design and service."

With API Security, SIOS can ensure APIs are secure, resilient, and ready for safe production use. API Security:

- Discovers and inventories all APIs, including RESTful, SOAP, dormant, and zombie APIs, regardless of configuration
- Automatically runs 200+ tests simulating threats from the OWASP API Security Top 10, to identify vulnerabilities before APIs are deployed in production
- Uses machine learning to profile API behavior, detect anomalies, and block real-time attacks such as data leaks, tampering, and unauthorized access

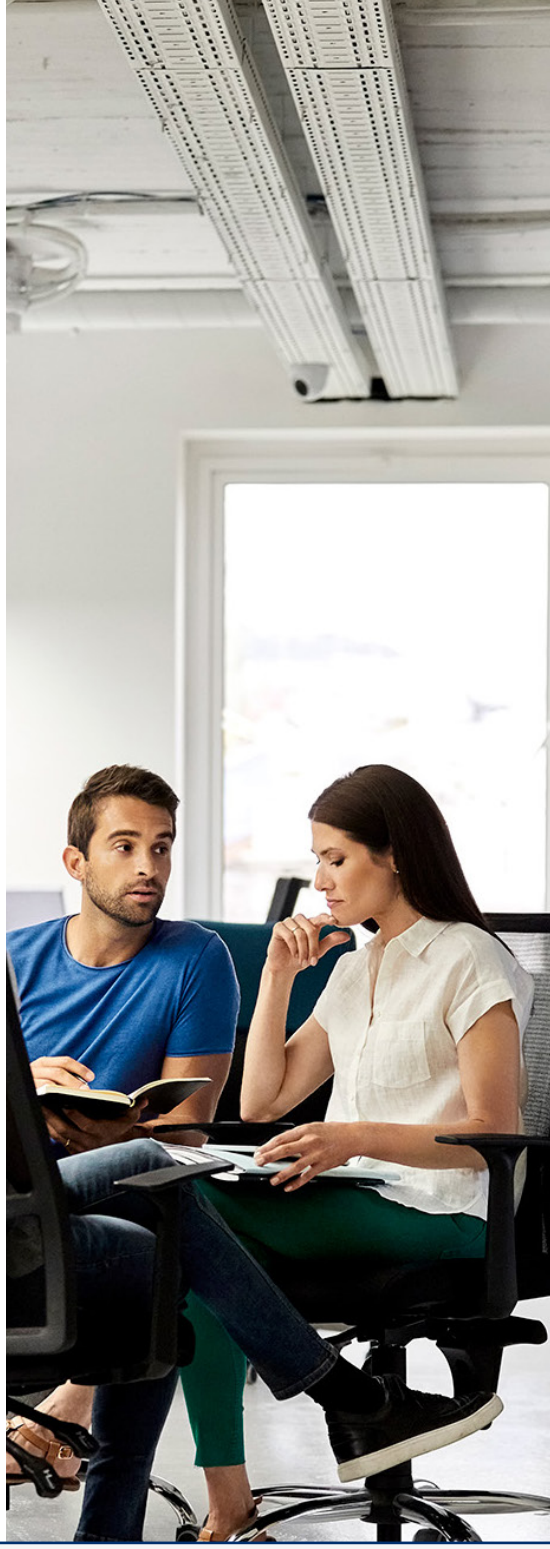
> "Akamai's detailed permission controls and always-on enterprise support made it the right choice for mission-critical API services.
>
> — **Tsukasa Nihei**
> Corporate Vice President, Head of API Solutions SL, SIOS Technology

According to Nihei, this level of protection helps prevent both data loss and business damage. “API attacks can cause reputational harm or block new business initiatives,” he said. “Akamai API Security prevents those risks before they happen.”

Strengthening Japan’s API ecosystem for the long term

As APIs move from technical connectors to strategic business enablers, SIOS sees its partnership with Akamai as essential to supporting Japan’s digital transformation. By combining SIOS’ decade of API expertise with Akamai’s robust, AI-driven protection, enterprise customers gain the confidence to innovate faster, securely, and at scale.

“APIs don’t just connect systems; they enable alliances and partnerships. We will continue working with Akamai to provide the infrastructure that supports this,” concluded Nihei.



SIOS

SIOS Technology, Inc. started out integrating systems that use open source software such as Linux, and now sells and provides services for its own software and SaaS. Recently, it has been focusing on DX technologies such as the cloud, and provides products and services that support the utilization of AI and the next generation. The company will continue to pursue innovative software technology, create value as an influential presence in the global IT industry, and contribute to the development of society. For more information, please visit sios.jp.

| Published 12/25

Akamai