AKAMAI CUSTOMER STORY

Healthcare Leader Fast-Tracked API Defense

By partnering with Akamai, this top healthcare provider in India protected patient data at scale from threats to vulnerable APIs

Discovered 6,000 APIs

70%
Cut API vulnerabilities by 70%

50%
Sped incident response by 50%

Leading with a secure, patient-first healthcare ecosystem

One of India's leading healthcare providers operates more than two dozen hospitals and is rapidly expanding through acquisitions and new facility launches. To support millions of daily interactions, it relies on custom and third-party apps for everything from patient booking and electronic health records (EHR) to telemedicine and billing. But as its digital footprint grew, so did its attack surface — particularly around APIs. With APIs as the backbone of its interconnected healthcare environment, the organization turned to Akamai to secure its hybrid app environment. The result: real-time protection, full API visibility, and faster threat response — without disruption to patient care.

Digital growth meets mounting cyber risk

Anchored by mobile and web platforms, this healthcare provider's digital services enable patients to book appointments, access lab results, consult doctors, and manage payments. On the back end, clinicians and staff rely on APIs to connect EHR systems, diagnostics, insurance providers, and more. With over 500 million monthly hits across its digital ecosystem, the organization needed a cybersecurity strategy that could scale with it.

But that scale came with challenges. "Some of our APIs were exposed publicly, and we lacked consistent standards," explained its CISO.

The organization was dealing with a legacy web application firewall (WAF) that produced frequent false positives, making rule management painful. Moreover, it had limited visibility into its APIs. "All this was unacceptable in an increasingly hostile cyber landscape," continued the CISO.

Healthcare Leader

Location

India

Industry

Healthcare & Life Sciences

Solutions

App & API Protector

API Security

Professional Services

Akamai

With a third of its web traffic flagged as malicious — including bots, API abuse, and DDoS attacks — the organization needed more than traditional perimeter defense. "We needed an enterprise-grade security partner that could provide both cutting-edge protection and deep industry expertise," the CISO said.

Akamai for scale, strategic fit, and immediate protection

When the clock started ticking on its expiring WAF contract, the healthcare provider evaluated its options. It selected Akamai over a cybersecurity vendor for its cloud native architecture, layered-defense capabilities, and seamless integration across hybrid environments.

Within just 48 hours, Akamai deployed its App & API Protector solution across the organization's most critical applications. According to its CISO, "The deployment demonstrated the strength of Akamai's Professional Services team and the power of its technology."

As it quickly defended against injection attacks, bots, and abuse, the deployment didn't impact the healthcare provider's operations or patient care. "Akamai immediately enhanced our security posture by protecting against web-based threats," said the CISO.

Discovering 6,000 APIs and reducing vulnerabilities by 70%

The organization also deployed Akamai API Security to gain visibility and governance over its API ecosystem. One of the most transformative outcomes was discovering approximately 6,000 previously undocumented APIs, many of which were misconfigured or had security vulnerabilities.

API Security not only revealed shadow APIs, it flagged sensitive data exposure — including personally identifiable information (PII), protected health information (PHI), and authentication tokens — in staging environments. This visibility empowered the healthcare provider to implement strict token- and geo-based access controls, and to remediate misconfigurations quickly.

Immediately upon deploying App & API Protector and API Security, it reduced critical API vulnerabilities by 60%–70%.

> "With Akamai, we went from partial visibility to full control over 6,000 APIs, securing sensitive data and maintaining trust across our digital ecosystem.
>
> — CISO

> With Akamai, we implemented a comprehensive API security strategy combining enterprise-grade solutions with 24/7 threat monitoring and incident response, along with expert consulting services.
>
> — CISO

Integrated protection at the edge

Combining API Security and App & API Protector gave the organization a strategically layered defense strategy. API Security offered deep insight into data flows and potential threats, while App & API Protector provided inline blocking of injection attacks, bot abuse, and DDoS events at the edge. This integrated protection supported threat identification and neutralization efforts before they could impact the organization.

"Akamai's solutions gave us deep visibility into our API ecosystem and real-time protection against attacks. By quickly identifying and remediating vulnerabilities, and blocking malicious traffic at the edge, they minimized the chances of business disruption linked to API threats," the CISO noted.

Professional Services and SOCC: Always-on support

The collaboration with Akamai didn't stop after deployment. Akamai's Professional Services team continued to offer hands-on guidance, threat analysis, and configuration support. Moreover, Akamai's 24/7 Security Operations Command Center (SOCC) provided real-time monitoring and incident response, helping the healthcare provider maintain continuous protection across its vast network.

"In healthcare, uptime, patient data protection, and rapid response are nonnegotiable," said the CISO. "Akamai's SOCC gives us confidence that we're covered, day and night."

40% less triaging, 50% faster incident response

Another benefit of working with Akamai? The healthcare provider streamlined its security. With real-time threat intelligence and centralized rule management, the organization's cybersecurity team spent 40% less time triaging false positives. This freed bandwidth to focus on proactive threat hunting and long-term strategy.

Most importantly, the team cut incident response time in half, an essential improvement for any healthcare provider managing sensitive data under HIPAA and ISO 27001 regulations.

Building a resilient future

As the healthcare provider continues to scale its digital services and footprint across India, Akamai remains a strategic partner in its cybersecurity journey. "We're building a patient-first healthcare ecosystem that leads with security," said its CISO. "Akamai's adaptive, cloud-first solutions help us do that while meeting regulatory expectations and protecting trust."

His advice to other healthcare leaders? "Treat application and API security as part of patient safety. Visibility is your foundation. Then build layered defenses and work with partners who know your industry inside and out," he concluded.

| Published 10/25