Ebook

API Security Risks in Healthcare

How leaders are responding in the AI era

Akamai Security

Executive summary

Healthcare organizations are rapidly expanding APIs to power patient portals, telehealth platforms, electronic health records (EHRs), and AI-driven diagnostics and treatment recommendations.

But this expansion doesn't come without risk. In Akamai's recent survey of 305 healthcare and life sciences leaders, 84% of respondents said that their organization had experienced at least one API-related security incident in the past 12 months.

Today, attacks involving APIs linked to AI technologies like apps, agents, and large language models (LLMs) are the most common incident type in healthcare. At the same time, visibility into which APIs return sensitive data remains critically low: Only 20% of healthcare organizations maintain a full inventory *and* know which APIs expose protected health information (PHI) or personal data. These gaps are amplifying risk as AI investments accelerate.

This ebook spotlights what healthcare security leaders are experiencing, the business impacts they're seeing, and the practical steps many organizations are prioritizing to strengthen patient trust and AI resilience.

Key findings

API incidents are widespread in healthcare, with AI-linked attacks now the leading type.

The study found that 84% of healthcare organizations had at least one API security incident in the past year. Of those, nearly 58% faced four or more incidents. Attacks involving APIs linked to AI technologies topped the list at 41%, making them the most commonly reported incident type that healthcare teams are dealing with today.

Even as AI-linked attacks become more prevalent, classic vulnerabilities persist. Leaders cited insufficient protections beyond web application firewalls (WAFs) as the top root cause of API incidents (62%), followed by API misconfigurations (50%) and lack of authentication controls (47%) — all issues highlighted by the Open Worldwide Application Security Project (OWASP) since its first API Security Top 10 in 2019.

A significant visibility gap persists with regard to sensitive patient data.

Although 78% of organizations claim a full API inventory, that visibility often falls short in practice: 51% say they don't know which of those APIs return sensitive data, and 41% still lack dedicated API security staff. In an industry governed by strict rules on data handling, this dual visibility and resourcing gap creates immediate compliance and breach risk as AI systems pull increasing volumes of data through APIs.

Healthcare leaders are increasingly focused on API security, but maturity testing, runtime protection, and priority alignment aren't fully keeping pace.

Securing AI technologies is now the number one cybersecurity priority for 40% of healthcare organizations, and 62% have increased their focus on API security over the past year. However, heavy reliance on WAFs (88%) continues, even though many organizations report that WAFs are insufficient, while adoption of dedicated API security solutions remains low (34%). Only 38% of healthcare organizations perform functional testing with an advanced security focus, and just 26% fully embed security testing across the software development lifecycle (SDLC) and CI/CD pipelines.

Scaling AI in healthcare without sacrificing patient trust

Healthcare teams are embedding APIs into AI applications faster than ever before. These APIs serve as the critical connection point to determine what data AI models can access, what actions they can trigger, and how patient care workflows actually operate. From diagnostic tools and personalized treatment recommendations to telehealth platforms and EHR systems, APIs are the invisible backbone powering healthcare's AI ambitions.

While this adoption is accelerating rapidly, the Akamai study shows that security foundations aren't keeping up. Visibility gaps, testing limitations, and rising incidents are creating real risks around PHI, personal data, regulatory compliance, and patient trust.

Key takeaway 1

Healthcare organizations face frequent API incidents, with AI-linked attacks leading the way

Healthcare stands out for its frequency of API incidents. More than half of the organizations that faced API incidents reported four or more in the past 12 months, one of the highest rates across industries. Prompt injections topped the list of concerns for AI/LLM-linked APIs, followed closely by data exfiltration risks. When asked about root causes, 62% of leaders mentioned that while WAFs — the most commonly used tool for cybersecurity — are useful, further security is needed to prevent future incidents, suggesting that traditional cybersecurity methods lack the sophistication to ward off AI-related attacks. Meanwhile, 50% of the surveyed leaders pointed to API misconfigurations and 47% cited lack of authentication controls as causes of the API security incidents their organizations have experienced.

API incidents hit healthcare organizations hard

84% experienced at least one API-related security incident

Nearly **58%** of those hit faced four or more incidents

41% reported AI-linked API attacks

47% cite prompt injections as top AI/LLM concern

Visibility into sensitive patient data flows remains a critical visibility gap

Although more than three-quarters of healthcare organizations say they have a full API inventory, very few actually know which of those APIs return sensitive data. This visibility gap is especially concerning in healthcare, an industry in which APIs often handle PHI that is governed by strict regulations like the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and other regional data protection laws.

The consequences show up clearly in the impacts reported by the surveyed leaders. Loss of productivity topped the list, revealing that a compromised AI-powered healthcare application causes a ripple effect: As teams race to fix issues, other work goes on standby, and with systems down, essential processes and information become inaccessible, slowing or even halting daily operations.

Loss of productivity was followed by loss of trust and reputation and direct costs to fix security issues. Financial impacts varied widely by country, with some healthcare organizations reporting costs well above US$1 million per incident when including remediation, downtime, and project delays. The average annual financial impact of API security incidents for healthcare organizations was approximately US$720,000.

Visibility into sensitive data is critically low

56% have full inventory but no sensitive data visibility

20% have full inventory and sensitive data visibility

33% said lack of visibility into AI/LLM-linked APIs is their top concern

Healthcare API baseline

Healthcare organizations are facing a challenging combination of high incident rates and low visibility as they scale AI. Here's a quick snapshot of where things stand:

84%

faced at least one API security incident

20%

have full inventory and sensitive data visibility

50%

cited API misconfiguration as a cause of their organization's API security incidents

19%

have little or no integrated security testing in API SDLC and CI/CD pipelines, relying on occasional manual checks (13%) or testing only after deployment (7%)

Key takeaway 3

Healthcare leaders are prioritizing AI security while API testing and runtime maturity continue to evolve

Securing AI technologies against attacks ranks as the top cybersecurity priority for healthcare organizations. At the same time, almost two-thirds of healthcare leaders said their organization increased focus on API security over the past year, driven mainly by rapid API growth from AI initiatives, regulatory and compliance requirements, and security audits that revealed vulnerabilities.

Seventy-three percent of healthcare organizations have dedicated personnel responsible for API security testing, but only 26% fully embed security testing at every stage of the SDLC and CI/CD pipelines. This is a major gap, as embedded security testing helps shift security from reactive to proactive, helps avoid last-minute bottlenecks, and makes the SDLC pipeline more sustainable and cost-effective.

AI security tops the priority list for healthcare organizations

40% rank securing AI technologies as their top priority

62% reported an increased focus on API security

97% factor API security into compliance

Only **38%** perform functional testing with an advanced security focus

88% use WAFs, but **62%** say more protections are needed

Only **34%** use dedicated API security solutions

Guidance for healthcare security leaders

The healthcare organizations that are most successful at closing visibility and testing gaps are better positioned to adopt AI safely. Leaders should follow these practical steps:

01

Start with continuous, accurate discovery

Implement automated tools that maintain a real-time inventory of all APIs — including shadow, zombie, and AI-linked APIs — and automatically flag which ones return sensitive data. Without this baseline, risk prioritization is guesswork.

02

Move beyond basic functional testing

Embed advanced security testing (not just functional checks) at every stage of the SDLC and CI/CD pipelines so vulnerabilities are caught early rather than after deployment. Untested APIs can't be resilient against the inevitable attacks that will target AI apps and agents.

03

Add dedicated runtime protection

Layer purpose-built API security on top of existing WAFs to stop AI-linked attacks, prompt injections, and data exfiltration in real time before they reach patient data or AI models.

04

Align directly with healthcare regulations

Build API governance processes that map explicitly to HIPAA, cyber resilience rules, and emerging AI requirements so compliance becomes part of everyday operations.

05

Connect visibility to business outcomes

Help C-suite and board leaders understand how poor API visibility directly impacts patient trust, HIPAA compliance, potential fines, care disruption, and the safe scaling of AI initiatives.

06

Use automated purpose-built solutions

Use solutions like Akamai API Security and Akamai App & API Protector for automated discovery, behavioral runtime defense, and seamless testing that scales alongside AI-driven API growth.

Looking ahead

Healthcare leaders seem to understand the need for increased security. Many cite API security incidents, data breaches, and rapid API growth from AI and cloud initiatives, along with tightening regulatory requirements, as the main reasons for increasing their focus.

But the data still shows a need to step up API visibility, security controls, and the tools being used to protect sensitive data. Perhaps most important, the high number of security incidents proves most healthcare organizations still have a long way to go.

As more than three-quarters of organizations prioritize securing AI apps and agents without disrupting AI-enabled services or revenue, the next phase must focus on deeper automation, tighter alignment between AppSec and DevSecOps, and broader use of dedicated API security controls that complement existing WAF and gateway investments.

Download the full 2026 API Security Impact Study for an in-depth look at sector benchmarks and broader insights across industries.

Download the report

Ready to take the next step to securing your APIs? Schedule a personalized demo of Akamai API Security to see how you can secure your full API estate, with discovery, runtime protection, testing, and comprehensive visibility into all APIs, including those powering patient portals and AI-driven diagnostic tools.

Schedule your demo

Methodology

This ebook is based on Akamai's 2026 API Security Impact Study, conducted by Phronesis Partners in November 2025. The survey included 1,840 security professionals globally, with 305 respondents from healthcare and life sciences. Participants were evenly divided between C-level, AppSec, and DevSecOps roles. All percentages in this report have been rounded.

Akamai Security

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more at **akamai.com** and **akamai.com/blog**, or follow Akamai Technologies on **X** and **LinkedIn**. Published 05/26.