2024 API SECURITY IMPACT STUDY

Healthcare Industry

API incidents are on the rise. Learn how the healthcare industry is addressing API security challenges — and what you can do to defend against evolving threats.

In an industry where patient and member trust is paramount, healthcare organizations face a growing security challenge: API vulnerabilities.

Electronic health records, telemedicine, and connected medical devices have become prime targets for cybercriminals — and protected health information (PHI) accessed through unsecured APIs can lead to HIPAA violations, compromised patient privacy, and damaged trust that takes years to rebuild.

The scale of this challenge is significant. In Akamai's comprehensive survey, an alarming 84.7% of healthcare professionals reported API security incidents within the past year — slightly higher than the 84% cross-industry average.

But perhaps most concerning is the impact on trust: Healthcare respondents report "loss of trust and reputation" (28.7%) as one of their top concerns following API incidents. In a world where patients can easily switch providers, this reputational damage can have lasting effects beyond immediate costs.

Read on to gain industry insights from the 2024 API Security Impact Study.

While attacks rise, visibility is a growing concern

The financial toll of API attacks is substantial, with healthcare organizations spending an average of $510,600 to address these incidents.

Despite these risks, the data reveals a concerning gap in priorities. When asked about their main cybersecurity priorities in the next 12 months, healthcare organizations ranked "securing APIs from threat actors" in 11th place (16.7%) out of 12 options. Instead, they're focusing on securing authentication for staff accessing systems (24.7%) and managing developer secrets (22.7%).

Distinguishing between legitimate and malicious API activity remains challenging for healthcare providers. While 65% of your peers report having full API inventories, only 24% of that subset knows which APIs handle sensitive data — a concerning drop from 40% in 2023. For healthcare, where data privacy isn't just good practice but law, this visibility gap creates significant risk.

Consider what can happen to an API deployed by a clinical department without proper oversight from central IT or security teams. That API might have been:

- Built to share patient records without proper HIPAA-compliant controls
- Left active after system upgrades, creating unknown access points
- Missed by traditional security tools not designed to detect unmanaged APIs
- Exploited by attackers to access protected health information
- Abused by an authentic partner, using the endpoint for unintended use cases

84.7% of healthcare organizations experienced API incidents in the past 12 months

65% of healthcare organizations have full API inventories — but of those, only 24% know which APIs return sensitive data

$510,600 = financial impact of API security incidents for healthcare organizations in the past 12 months

Top 3 impacts

1. **Loss of trust and reputation** (28.7%)
2. **Loss of productivity** (28.7%)
3. **Increased internal scrutiny** (27.3%)

Source:
Akamai, "API Security Impact Study," 2024

Akamai

This isn't just hypothetical. With healthcare data breaches reaching record highs and data breach costs averaging $4.88M,[1] API vulnerabilities represent a growing compliance and security risk. Moreover, this scenario reflects what your peers cite as top causes of their API incidents.

How API incidents impact compliance, cost to business, and team stress

According to the May 2024 Gartner® Market Guide for API Protection,[2] "Current data indicates that the average API breach leads to at least 10 times more leaked data than the average security breach."

It's no wonder that HIPAA compliance demands increasingly focus on API security. While HIPAA doesn't explicitly mention APIs, it requires restricting PHI access based on workforce roles. This requires authentication and access controls in APIs that transmit patient data. Healthcare providers and payers — and their regulators — need to know what types of data are traveling through not only their own APIs, but also their partners' and suppliers' APIs, adding yet another challenge to managing third-party risk for the healthcare sector.

Losing the trust of regulators can result in increased scrutiny and more work for teams that are stretched thin struggling to meet compliance demands. It can also lead to costly fines. With that in mind, it's clear that healthcare companies are keenly aware of the financial consequences of API threats. For the first time, we asked respondents in the three countries we surveyed to share the estimated costs of API security incidents they experienced in the past 12 months.

	Healthcare industry	Average of all industries
U.S.	$510,600	$591,404
U.K.	£363,885	£420,103
Germany	€643,884	€403,453

Q3. If you have experienced an API security incident, what has been the estimated total financial impact of these incidents combined? Please include all related costs such as system repairs, downtime, legal fees, fines, and any other associated expenses.

While the financial impacts are significant, we heard loud and clear from study participants that the costs go far beyond the bottom line. When asked to list the top impact of an API security incident, it wasn't cost. As mentioned earlier, our respondents emphasized "loss of trust and reputation" (28.7%) and "loss of productivity" (28.7%). These consequences have long-lasting effects — damaged patient trust can harm future years' revenue, while productivity losses in already strained healthcare workforces can accelerate burnout and staff disengagement.

[1] IBM Cost of a Data Breach Report, 2024

[2] Gartner, Market Guide for API Protection, 29 May 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Reduce risk and stress through proactive API security

API attacks against healthcare companies are growing in scope, scale, sophistication, and cost. This includes GenAI-fueled bot attacks that quickly adapt to bypass traditional API security tools and other perimeter defenses. Many security teams in your industry are experiencing these threats firsthand and feeling the impacts, both financial and human. But even when organizations understand the significance of API threats, they're left with the question: *What can we do about it?*

Taking measures now to better secure your APIs — and the data they exchange — can empower your organization to protect its revenue and alleviate the burden from security teams, all while preserving the hard-earned trust of boards of directors and customers. These steps include building your team's knowledge about advanced API threats and the capabilities you need to defend against them.

To read the full report and learn about best practices for API visibility and protection, download the **2024 API Security Impact Study**.

Ready for a conversation about your challenges and how Akamai can help?

Request a customized Akamai API Security demo

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 about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X and LinkedIn. Published 03/25.