2024 API SECURITY IMPACT STUDY

Insurance Industry

API incidents are on the rise. Learn how the insurance services industry is addressing this top security concern — and what your organization can do to stay safe.

When disaster strikes — from car accidents to damaged business equipment — policyholders rely on digital services to submit claims and receive assistance from their insurance providers. Behind these services, insurance companies' APIs handle sensitive information that represents a policyholder's life story told in data form.

In an industry where customer trust is paramount, insurance organizations face a growing security challenge: API vulnerabilities.

According to Akamai's comprehensive survey, 76.7% of insurance professionals reported API security incidents within the past 12 months — and the financial impact is substantial, with insurance organizations spending an average of $625,634 to address these incidents in the United States alone.

But perhaps most concerning are the business impacts: "Loss of customer goodwill and churned accounts" (28%) ranks as the top concern for insurance companies following API incidents. In a competitive market where customers 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 remains a key challenge

The financial toll of API attacks is substantial for insurance companies, with costs in the United States ($625,634) exceeding the cross-industry average ($591,404). What's driving these incidents?

According to insurance industry security teams, the top causes include:

1. Unmanaged APIs, such as dormant or "zombie" APIs (22%)
2. APIs with unintended exposure to the internet (21.3%)
3. Traditional tools used for securing APIs failing to catch threats (20%)
4. Authorization vulnerabilities (19.3%)
5. API misconfigurations (18.7%)

Many organizations are aware of the causes of their API attacks, but they lack visibility into a crucial indicator of risk: an API's ability to return sensitive data when called. While 56.7% of insurance organizations report having a full inventory of their APIs (below the 69.7% cross-industry average), only 20.7% know which APIs return sensitive data.

This visibility gap poses significant compliance and security implications in an industry that processes highly regulated personal and financial data.

76.7% of insurance organizations experienced API incidents in the past 12 months

Only 20.7% of insurance organizations with full API inventories know which APIs return sensitive data

$625,634 = financial impact of API security incidents for insurance organizations in the U.S. in the past 12 months

Top 3 impacts

1. Loss of customer goodwill and churned accounts (28%)
2. Damaged departmental reputation with leadership (25.3%)
3. Costs incurred to fix issues (24.7%)

Source:
Akamai, API Security Impact Study, 2024

Akamai

We've noticed several trends that make it challenging to protect APIs:

- **Continuous API sprawl**: With every digital initiative, APIs multiply and constantly evolve, making it difficult to maintain an accurate inventory.
- **Inconsistent standards**: Many insurers have multiple development teams operating in silos across business units without using a central playbook for secure design.
- **Unseen risks**: APIs transmit sensitive policyholder data, but most organizations can't identify which specific APIs return sensitive information.

Consider what can happen to an API deployed by a department without proper oversight from a security team. That API might have been built to share records without proper controls or left active after system upgrades, creating potential exposure points for sensitive customer data.

How API incidents impact compliance, customer trust, and team stress

It's no wonder that insurance companies are keenly aware of the financial consequences of API threats. In our survey, we asked respondents to share the estimated costs of API security incidents they experienced in the past 12 months:

	Insurance industry	Average of all industries
🇺🇸 United States	$625,633.70	$591,404.01
🇬🇧 United Kingdom	£493,000.50	£420,103.18
🇩🇪 Germany	€373,918.72	€403,453.26

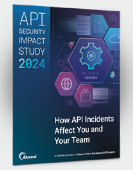
While the financial impacts are significant, we heard loud and clear from study participants that the costs reflect a mix of revenue and reputational concerns. When asked to list the top impact of the API security incident they've experienced:

- 28% listed "loss of customer goodwill and churned accounts"
- 25.3% listed "damaged team reputation among leadership and the board"
- 24.7% listed "costs incurred to fix issues"

Reduce risk and stress through proactive API security

API attacks against insurance 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 offers solutions designed to help organizations reduce risks relevant to the threats discussed in this piece:

- **Akamai API Security**: Discovers APIs, understands their risk posture, analyzes their behavior, and stops threats from lurking inside

- **Akamai Account Protector**: Helps prevent account-opening abuse by monitoring user behavior in real time and adapting to changing risk profiles

Akamai