API SECURITY IMPACT STUDY

Financial Services Industry

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

Last year, 88.7% of financial services companies experienced an attack on the APIs that handle their data and connect customers and partners to critical services. Using increasingly innovative methods, threat actors can access data in unprotected APIs to steal personal and financial information, including account balances and transaction histories.

Security teams are feeling the impact and seeking ways to improve. But taking on another attack vector can feel daunting — especially one like APIs, whose misconfigurations or business logic flaws can be easily uncovered and exploited.

How do we know this? Akamai surveyed more than 1,200 IT and security professionals — from chief information security officers to application security staff — to learn about their experiences with API-related threats.

Here, we've filtered our findings for financial services industry respondents, who said the top impacts of their API security incidents were "fines from regulators" and "increased stress and/or pressure for my team/department." These intertwined consequences are easy to understand, given that your peers placed the cost of addressing API incidents at $832,800 — 40% higher than the average across all eight industries surveyed, and higher than any other industry.

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

Visibility is declining as attacks rise

While 84% of organizations across industries experienced API security incidents, financial services organizations were targeted more frequently than average, at 88.7%. Your peers identified two key vulnerabilities driving these attacks: network firewalls failing to catch threats (26.5%) and vulnerabilities within APIs in generative AI tools such as large language models (LLMs) (23.2%).

Despite mounting evidence of API threats — from frequent incidents to high remediation costs and regulatory fines — our findings suggest many financial services teams have yet to make API security a top priority. In fact, API security ranks ninth among cybersecurity priorities for the year ahead at 18.5%.

Distinguishing between genuine and malicious or fraudulent API activity remains challenging for the financial sector, particularly when it comes to visibility into APIs' many risks. While 73.5% of your peers say they have a full inventory of their APIs, only 28.5% of that subset know which ones return sensitive data, which includes personally identifiable information (PII) and data ranging from cardholders' credit histories to large commercial banking clients' financial records.

88.7% of financial services companies experienced an API security incident in the past 12 months

Only 28.5% of financial services companies with full API inventories know which APIs return sensitive data

$832,800 = Financial impact of API security incidents for financial services companies experiencing them in the past 12 months

Top 3 impacts

1. **Increased stress and/or pressure** on the security team
2. **Fines** from regulators
3. **Loss of trust** and reputation

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

Akamai

Consider what can happen to a shadow API deployed by a department or subsidiary of a financial services provider without collaboration or oversight of the company's central IT or security teams. That API may have been:

- Built to return customers' transaction data without proper authorization controls and not adequately tested for misconfigurations
- Replaced by a new version but not deactivated, thus lingering with exposure to the internet
- Slipping past the radar of traditional tools that cannot detect unmanaged APIs
- Exploited by cybercriminals who access real customers' accounts to steal their assets

This story isn't just hypothetical. According to LexisNexis® Risk Solutions' 2023 True Cost of Fraud™ Study, 50% of fraud losses can be traced back to new account opening abuse, where fraudsters abuse APIs to open accounts at scale. Moreover, our scenario reflects what real-life IT and security 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*, "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 why the widely followed PCI DSS v4.0 regulation has added requirements around API security. The standard now requires organizations to validate their API code before release, regularly test for vulnerabilities, and confirm the secure usage of API-based components — particularly important in an industry where APIs facilitate millions of financial transactions daily.

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 financial services companies are keenly aware of the consequences of API threats. For the first time, we asked respondents in the three countries we surveyed to share the estimated financial impact of API security incidents they experienced in the past 12 months.

	Financial services industry	Average of all industries
U.S.	$832,800	$591,404
U.K.	£297,189	£420,103
Germany	€604,405	€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.

* 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 financial services 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. These steps, along with building your team's knowledge about advanced API threats and the capabilities you need to defend against them, can help preserve the hard-earned trust of customers and boards of directors.

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, which discovers APIs, understands their risk posture, analyzes their behavior, and stops threats from lurking inside
- Akamai Account Protector, which helps prevent account opening abuse by monitoring user behavior in real time and adapting to changing risk profiles

Akamai

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.