

2024 API SECURITY IMPACT STUDY

Retail and Ecommerce Industry

How your peers view and experience the growing threat to APIs

The APIs powering retail and ecommerce companies' digital initiatives are under attack. Using increasingly innovative methods, threat actors can access data in unprotected APIs to steal credit card data, siphon funds from loyalty programs, launch credential stuffing attacks, and more. 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 CISOs to AppSec staff — to learn about their experiences with API-related threats.

This brief filters those findings for your industry, where 68% of respondents reported experiencing API security incidents in the past 12 months. What were the impacts? Your peers' top answers included rising stress levels for their teams and damaged credibility among senior executives and boards. This response is understandable, given the reported costs, with retail and ecommerce professionals citing a US\$526,531 price tag for addressing API incidents they've experienced.

Read on to gain industry insights from the [2024 API Security Impact Study](#).

While attacks rise, visibility declines

While a notable majority of retail and ecommerce respondents experienced API security incidents, their 68% average was lower than the 84% reported across all eight industries surveyed. Meanwhile, your industry peers' top security priorities for the next 12 months are "defending against GenAI-fueled attacks" and "securing APIs from threat actors."

Is there a link between prioritizing APIs and preventing attacks? It's possible that retail and ecommerce companies' security teams have recognized the importance of API protection and their efforts are reducing incidents. However, our findings also suggest these teams are not seeing every instance of API abuse.

Distinguishing between genuine and malicious or fraudulent API activity remains challenging for retail and ecommerce companies. Visibility into risk is also a challenge. While 67% of your industry peers report having full API inventories, *only 29%* of this subset know which of their myriad APIs return sensitive data. This includes personally identifiable information (PII) or credit card details.

Consider what can happen to an API deployed by a business unit without collaboration or oversight of the retailer's central IT or security teams. That API may have been:

- Built to return customers' 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 fraudsters who access real customers' loyalty accounts and redeem cash

68% of retail/ecommerce companies experienced an API security incident in the past 12 months¹

Only 29% of retail/ecommerce companies with full API inventories know which APIs return sensitive data¹

\$526,531 = financial impact of API security incidents for retail/ecommerce companies experiencing them in the past 12 months¹

Top 3 impacts¹

1. **Increased stress** and/or pressure for my team
2. **Costs incurred** to fix the issue
3. **Hurt our department's reputation** with senior leaders and/or board of directors

44% of web attacks against commerce organizations targeted APIs²

Sources:

1. Akamai, "API Security Impact Study," 2024
2. Akamai State of the Internet (SOTI), "Lurking in the Shadows: Attack Trends Shine Light on API Threats," 2024



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.

Top causes of API incidents cited by retail/ecommerce security teams

1. APIs in generative AI tools, e.g., LLMs – 24.7%

2. API had unintended internet exposure – 24.0%

3. API misconfiguration – 22.0%

4. Web application firewall didn't catch it – 21.3%

5. API gateway didn't catch it – 20.7%

6. Vulnerability due to API coding errors – 20.0%

7. A well-known technology tool/service – 20.0%
8. Network firewall didn't catch it – 18.7%

9. Authorization vulnerabilities – 17.3%

10. Software solution downloaded from the internet – 16.7%

11. Lack of API authentication controls – 16.0%

12. Mid-tier software solution – 14.7%

13. Unmanaged APIs (e.g., zombie) – 13.3%




Q. What do you believe are the causes of API security incidents your organization has experienced? (Select up to 3.) n=1,207

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.”³ It’s no wonder why the widely followed PCI DSS v4.0 regulation has added requirements around API security. Companies — 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 ecommerce.

Losing the trust of regulators can result in increased scrutiny and more work for stretched teams struggling to meet compliance demands. It can also lead to costly fines. And with costs in mind, it’s clear that retail and ecommerce 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 financial impact of API security incidents they experienced in the past 12 months.

³ 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.

	Retail/ecommerce	All industry average
 US	\$526,531	\$591,404
 UK	£258,815	£420,103
 Germany	€348,467	€403,453

Q. 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. n=1,207

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. Our retail and ecommerce respondents emphasized the human toll: stress and pressure on their teams.

Top 5 impacts of API security incidents for retail and ecommerce companies

1. It led to increased stress and/or pressure for my team/department – **28.7%**
2. Costs incurred to help fix the issue – **28.0%**
3. It hurt our department's reputation with our senior leaders and/or board of directors – **25.3%**
4. It led to increased internal scrutiny of our team/department among the business – **23.3%**
5. Fines from regulators – **25.3%**

Q. What costs and/or impacts, if any, have API security incidents had on your business? (Select up to 3.) n=1,207

Next steps: Reduce risk and stress through proactive API security

API attacks against retail and ecommerce companies are growing in scope, scale, and sophistication. 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 hard-earned trust of boards of directors and customers alike. 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](#), formerly known as Twitter, and [LinkedIn](#).
Published 11/24.