Ebook

API Security Risks in Commerce

How leaders are responding in the AI era

Akamai Security

Executive summary

In Akamai's 2026 survey of 310 global commerce leaders, more than 80% of respondents said that their organization had experienced at least one API-related security incident in the past 12 months, with many seeing repeated incidents rather than one-off events. This widespread exposure comes as commerce organizations have poured billions into becoming AI leaders — embedding shopping assistants, dynamic pricing engines, personalized recommendations, and autonomous agents into every customer journey.

Yet the APIs that serve as the critical infrastructure for these innovations were never built to be resilient against attacks that can jeopardize ROI.

A single cleverly crafted prompt from an attacker can manipulate an AI shopping assistant into passing down requests to an underlying API that lacks adequate protections and is designed to simply execute programmed tasks. The outcome: With no questions asked, AI-linked APIs will expose sensitive customer data, share payment details, or trigger unauthorized actions. Even more concerning, attacks involving APIs linked to AI technologies have surged to become the second-most-common incident type, just behind classic access-control exploits.

At the same time, visibility remains dangerously incomplete. Only about 20% of commerce teams maintain a full API inventory *and* know which APIs return sensitive data. If personal customer information or payment details are stolen, that can quickly erode customer trust and trigger regulatory action under rules like the Payment Card Industry Data Security Standard (PCI DSS). As AI initiatives accelerate, this gap is widening, turning what should be competitive advantages into potential liabilities for customer trust, revenue, and brand reputation.

This ebook spotlights what commerce security leaders are seeing on the front lines, the tangible business impacts they're facing, and the practical steps many organizations are already prioritizing to protect customer loyalty while safely scaling AI.

Key findings

API incidents are widespread in commerce, with access-control exploits and AI-linked attacks now the leading types.

The study found that 85% of commerce organizations experienced at least one API-related security incident in the past year, with 47% of those affected reporting four or more incidents. Exploitation of missing or insufficient access controls ranked as the most common incident type, followed closely by attacks involving APIs linked to AI technologies.

A significant visibility gap persists with regard to sensitive customer and payment data.

While many organizations report having a full API inventory, very few actually know which APIs return sensitive data, like personal customer information or payment details. This low level of visibility is consistent with the cross-industry average. As AI applications become increasingly dependent on these connections, the risk grows.

Commerce leaders are increasingly focused on API security, but testing maturity and readiness for AI-linked threats lag behind adoption.

Securing AI technologies is now the top cybersecurity priority for 41% of commerce organizations, and 62% reported increasing their focus on API security over the past year. However, only 47% of commerce security leaders say their organization is prepared to detect and mitigate AI-linked API attacks. These attacks are now among the most frequent incidents they face — yet most leaders don't currently know where their AI-linked APIs live.

Scaling AI in commerce without sacrificing customer trust

Commerce teams are embedding APIs into AI applications faster than ever. These APIs act as the critical control layer for what data AI models can access, what actions they can trigger, and how customer journeys unfold. From personalized product recommendations and dynamic pricing to seamless checkout, real-time inventory updates, and fraud detection, APIs are the invisible backbone powering commerce's AI ambitions.

While this adoption is accelerating rapidly, the Akamai study shows that security foundations aren't keeping pace. Visibility gaps, testing limitations, and rising incidents are creating real risks around customer personal data, payment information, regulatory compliance, and long-term brand trust.

Commerce organizations face frequent API incidents, with access controls and AI-linked attacks leading the way

Commerce leaders report that exploitation of missing or insufficient access controls was the most common incident type they faced last year, followed very closely by attacks involving APIs linked to AI technologies.

Incident frequency is also notable: A significant share of commerce organizations that experienced API incidents reported multiple occurrences over the past 12 months. When it comes to APIs linked to AI technologies, rapid AI development serves as a risk multiplier, making older, long-standing API security gaps more problematic. Leaders are most concerned about insecure large language model (LLM)–connected endpoints, data exfiltration risks, and prompt injection attacks. As for root causes of API incidents, leaders most frequently pointed to API misconfigurations, gaps in inventory and oversight of shadow APIs, and the fact that web application firewalls (WAFs) help but are not sufficient on their own.

API incidents hit commerce organizations hard

85% experienced at least one API security incident

41% reported attacks involving AI-linked APIs

47% of those affected faced four or more API incidents

Key takeaway 2

Lack of visibility into sensitive customer and payment data flows remains a critical gap

While many commerce organizations say they have a full API inventory, very few know which of those APIs return sensitive data. This visibility gap is especially concerning in commerce, an industry in which APIs often handle personal customer information and payment details that fall under strict PCI DSS and data-protection rules.

These gaps are reflected in the impacts reported by the surveyed leaders. When APIs are compromised, organizations experience churn, less customer goodwill, loss of trust and reputation, and decreased productivity. Financial impacts varied widely by country, with some commerce organizations reporting substantial costs per incident when including remediation, downtime, and project delays.

Visibility into sensitive data is critically low

47% feel prepared for AI-linked API attacks at a time when these attacks, along with access-control exploits, rank as the most frequent incidents in commerce

35% cited loss of customer goodwill and churn

Commerce API baseline

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

22%

can track sensitive data in inventoried APIs

14%

lack integrated security testing in API software development lifecycle (SDLC) and CI/CD pipelines

74%

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

Commerce leaders are prioritizing AI security, yet testing maturity and runtime protection lag behind

Securing AI technologies against attacks is the top cybersecurity priority for 41% of commerce organizations. More than 60% report increasing their focus on API security over the past year, but looking at the organizations' priorities tells a different story. Only 19% rank improving API security as their top priority. For these organizations, this heightened attention is driven by rapid API growth from AI initiatives, regulatory and compliance requirements, and vulnerabilities uncovered through security audits.

But many organizations aren't focused on API security, and API security maturity itself hasn't kept pace. While many teams have moved beyond basic functional testing, too few are conducting rigorous security testing against real-world attack methods such as those in the the Open Worldwide Application Security Project (OWASP) API Security Top 10. As such, it's not surprising that fewer than half feel prepared for the AI-linked API attacks that now rank among the most frequent incidents.

There's also a notable perception gap between leadership and frontline teams. The study revealed that while C-suite security executives often overestimate readiness, the DevSecOps and AppSec professionals who work with APIs every day report lower confidence in testing and protection capabilities. When asked about the maturity and integration of their API security testing, C-suite executives reported 2%–3% more readiness than AppSec and 6%–12% more than DevSecOps professionals in the same organizations.

Compounding the issue, WAF adoption remains high, even as 49% of organizations acknowledge that WAFs alone are insufficient against modern API and AI-linked threats like prompt injection, data exfiltration, and insecure LLM-connected endpoints.

Dedicated API security tools with advanced testing and behavioral runtime protection are far less common, leaving critical gaps in both pre-deployment testing and real-time defense.

On the compliance front, while a strong majority say they factor API security into regulatory efforts, fewer organizations are translating this into consistent action through detailed risk assessments, ongoing reporting, or proven security controls.

Priority is rising, but testing and protection maturity still lag

97% of commerce enterprises say they factor API security into regulatory compliance, but only **59%** actually factor APIs into risk assessments, only **50%** factor them into required security plans, and only **36%** factor them into compliance reporting

85% use WAFs for API security, while **49%** acknowledge that WAFs don't provide enough protection to prevent API incidents

Guidance for commerce security leaders

The organizations that most effectively close visibility and testing gaps are best positioned for safe AI adoption.

The study highlights a few practical steps:

01

Start with continuous, accurate discovery.

Implement automated tools that maintain a real-time inventory of all APIs — including zombie and shadow APIs, and those linked to AI applications — and automatically flag which ones return sensitive customer or payment 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.

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 customer data or AI models.

04

Align directly with commerce regulations

Build API governance processes that map explicitly to PCI DSS, the General Data Protection Regulation (GDPR), cyber resilience rules, and emerging AI requirements, so compliance becomes part of everyday operations.

05

Shut down the perception gap

Give frontline AppSec and DevSecOps teams the visibility and tools they need so C-suite confidence matches actual day-to-day reality.

06

Use automated purpose-built solutions

Use products like Akamai API Security and Akamai App & API Protector for automated discovery, behavioral runtime defense, and integrated testing that scale with AI-driven API growth.

Looking ahead

In the coming year, commerce organizations must move beyond awareness of AI-related API risks and start closing the significant gaps that are holding them back. With repeated incidents continuing, visibility still critically low, and many teams relying on traditional WAFs that struggle against prompt injection and other AI-linked attacks, the priority must shift to foundational improvements.

The most successful teams will focus on three critical areas:

1. Implementing continuous, automated discovery to uncover zombie, shadow, and AI-connected APIs
2. Shifting from basic functional testing to rigorous, OWASP-style security testing throughout the development lifecycle
3. Adding dedicated API security and behavioral runtime protection on top of existing WAFs to stop attacks in real time

Only by addressing these long-standing weaknesses can commerce leaders safely accelerate AI initiatives without exposing customer data, triggering regulatory issues, or damaging brand trust.

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 your AI shopping assistants and recommendation engines.

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 310 respondents from commerce organizations. 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.