

Ebook

# API Security Risks in Financial Services

How leaders are responding in the AI era



# Executive summary

Financial services organizations operate in one of the world's most API-intensive environments. Every instant payment, open-banking connection, robo-advisor recommendation, fraud-detection model, and AI-powered wealth-management assistant runs on APIs. These interfaces move money, verify identities, assess risk, and deliver personalized experiences at scale.

But that same connectivity is also creating outsized exposure. For Akamai's 2026 API Security Impact Study, we surveyed 310 security leaders from financial services enterprises, including banks, brokerages, insurance providers, and fintech organizations, across 10 countries.

The survey revealed that nearly all financial services organizations faced at least one API-related security incident in the past 12 months, with nearly half reporting four or more incidents. And these attacks can be costly: The average annual financial impact of API security

incidents for financial services organizations was approximately US\$620,000. The highest costs for API incidents were reported in China, Singapore, and Japan, and costs were above average in Brazil and the U.K.

Data breaches and leaks via APIs emerged as the most frequent incident type, followed immediately by attacks involving APIs linked to AI technologies, including customer-facing AI applications.

Visibility into these APIs is still surprisingly limited. Just over a quarter of financial services teams maintain a complete inventory and know exactly which APIs expose sensitive data. At the same time, most leaders are still reporting a mix of functional and security-focused testing rather than fully advanced security testing — which suggests the gap isn't just about visibility, but also about the maturity and strength of their defenses.

As AI adoption accelerates across lending engines, chatbots, and fraud models, this gap is turning high-value customer and transactional data into an attractive target. But the study also shows that traditional API weaknesses remain central — especially misconfiguration, missing access controls, and authorization vulnerabilities.

This spotlight highlights what financial services security leaders are confronting day-to-day, the real financial and reputational costs they're facing, and the concrete actions many are taking to safeguard trust while responsibly scaling AI.



# Key findings



**API incidents are pervasive in financial services, with data leaks and AI-linked attacks topping the list.**

Nearly all (96%) financial services organizations reported an API-related security incident in 2025, and almost half (48%) of those affected experienced four or more incidents within a 12-month span. Data breaches or leaks via APIs ranked as the most common incident type (40%), with attacks on AI-linked APIs a very close second (39%).

The number one underlying cause of these incidents? API misconfiguration, cited by 65% of leaders — pointing to ongoing operational and governance gaps alongside emerging AI exposure. It goes to show that even as AI risks dominate attention, most breaches still stem from unresolved foundational issues.



**A persistent visibility shortfall leaves sensitive financial data exposed.**

Although 78% of organizations claim a full API inventory, that visibility often falls short in practice: 51% say they don't know which of those APIs return sensitive data, and 41% still lack dedicated API security staff. In an industry governed by strict rules on data handling, this dual visibility and resourcing gap creates immediate compliance and breach risk as AI systems pull increasing volumes of data through APIs.



**Leaders are elevating API security, but preparedness for AI-specific threats lags.**

Securing AI technologies now ranks as the top cybersecurity priority for 41% of financial services organizations, and 74% have increased their focus on API security over the past year. However, while many teams report moderate overall readiness, they feel least prepared for the types of AI-linked attacks most commonly encountered across their sector over the past year, highlighting a gap between rapid AI adoption and security maturity.

# Scaling AI in financial services without eroding customer trust

Financial institutions are rapidly integrating AI into core operations: real-time fraud scoring, personalized lending decisions, intelligent chatbots, predictive cash-flow tools, and next-generation robo-advisors. In every case, APIs act as the bridge between models, customer data, core banking systems, and third-party services.

The Akamai study reveals that security maturity isn't advancing at the same speed. High incident volumes, incomplete visibility, and uneven testing practices are creating real exposure across customer data, regulatory obligations, and brand reputation.

The good news? API risk is on the radar, with 97% of leaders factoring it into compliance requirements. Yet gaps remain in execution. For example, while 70% factor APIs into required risk assessments, only 34% factor APIs into required reporting, limiting visibility for both organizations and their regulators.

# Financial services organizations face frequent API incidents, led by data leaks and AI-linked attacks

AI applications, agents, and large language models (LLMs) depend on APIs to reach sensitive systems and customer records. In financial services, these same APIs have become high-value targets. Financial services also stands out for incident frequency: Nearly half of organizations that were hit reported four or more separate events.

When asked which AI-related risks worry them most, respondents pointed first to attackers exploiting insecure LLM-linked endpoints, followed by APIs that could leak sensitive data or enable exfiltration, and finally, lack of visibility into AI/LLM-linked APIs. These concerns are well founded: AI-linked API attacks ranked among the most commonly reported incident types over the past 12 months.

Root-cause analysis most often pointed to API misconfigurations, web application firewalls that help but don't go far enough, and vulnerabilities tied to generative AI tools and LLMs.

In other words, while AI is amplifying risk, most incidents still come back to familiar API security failures.

## API incidents hit financial services hard

**96%** experienced at least one API security incident

**48%** of those hit faced four or more incidents

**39%** reported data breaches via APIs

**39%** reported attacks on AI-linked APIs

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

Most financial services organizations maintain a full API inventory, yet only 27% also know which APIs return sensitive data. Since these APIs handle personal financial information, account details, and payment data governed by PCI DSS, DORA, and GDPR, the visibility gap is especially concerning.

Business impacts highlight the issue. Our respondents ranked loss of customer goodwill and churn as the top consequences their organizations faced, followed by loss of trust and reputation, and loss of productivity. When incidents occur, the combined costs of remediation, downtime, project delays, and potential fines add up quickly.

To move forward, organizations should continue to deepen their understanding of how API visibility plays a part in real business risks, including operational disruption, customer impact, and regulatory exposure.

## Visibility into sensitive data is critically low

**27%** have full inventory plus sensitive data visibility

**55%** feel prepared for AI-linked API attacks

**58%** have dedicated API security personnel

**38%** cited loss of customer goodwill and churn as top consequences

# Financial services API baseline

Financial services organizations face an unusually high incident rate paired with limited visibility as AI development expands. Here's the current snapshot:



**96%**

were hit by API incidents last year



**64%**

cite misconfiguration as root cause



**74%**

are increasing focus on API security



**41%**

rank securing AI as top priority



**27%**

have full sensitive-data visibility

# Financial services leaders claim to prioritize API security, but gaps remain in practice

Protecting AI technologies against attack is now the leading cybersecurity priority across the sector. At the same time, 74% of financial services leaders reported a sharper focus on API security in the past year, driven by rapid API growth from AI and digital initiatives, along with regulatory pressure and audit findings.

Testing practices are advancing, with more teams moving past purely functional checks — but many teams still feel ill-equipped to detect and stop the AI-linked threats they encounter most frequently.

This gap is reflected in cybersecurity solution choices. More than 80% of organizations report using web application firewalls (WAFs), which were designed before the AI boom and lack capabilities such as deep API visibility, data-driven risk analysis, and advanced threat detection. Meanwhile, only 34% have adopted dedicated API security platforms that provide these capabilities.

## Reported priorities aren't fully aligning with actions

**97%** factor API security into regulatory compliance, but only **34%** factor APIs into required reporting

**74%** increased focus on API security last year, but **81%** still rely primarily on traditional WAFs

**41%** rank securing AI technologies as top priority, but only **22%** are prioritizing API security

# Guidance for financial services security leaders

Financial institutions that close visibility and testing gaps fastest will be best positioned to adopt AI securely. The study highlights several immediate, high-impact actions:

01

## Establish continuous, accurate discovery

Deploy automated tools that surface hidden and unmanaged APIs, including shadow and zombie APIs, as well as AI-linked endpoints. Keep a live inventory of every API, instantly classifying those returning sensitive financial or customer data. Without this foundation, risk decisions are guesswork.

02

## Advance testing beyond functional checks

Only 17% of enterprises embed security-focused API testing into every stage of the API SDLC and CI/CD pipeline. And most organizations that are testing APIs focus on functionality. Just one-third (34%) say they employ both functional and advanced security testing. This leaves the majority of APIs insufficiently validated against risks before reaching production. Enterprises need rigorous testing to ensure APIs are resilient.

03

## Layer dedicated runtime protection

Add purpose-built API security on top of existing WAFs to block prompt injections, data exfiltration, and AI-specific attacks in real time.

04

## Map controls directly to financial regulations

Embed API governance processes that explicitly address PCI DSS, DORA, GDPR, cyber resilience mandates, and emerging AI rules so compliance becomes part of daily operations, not just a periodic exercise.

05

## Align leadership and technical teams

Ensure AppSec and DevSecOps practitioners have the visibility and tools needed, so that executive confidence reflects frontline reality.

06

## Adopt purpose-built platforms.

Use solutions like [Akamai API Security](#) and [Akamai App & API Protector](#) for automated discovery, behavioral runtime defense, and seamless testing that scales alongside AI-driven API growth.

# Looking ahead

Financial services leaders are recognizing that API attacks targeting AI applications are becoming increasingly inevitable. As a result, they're moving beyond incident response toward resilience by design, focusing on proactively testing APIs, identifying vulnerabilities, and fixing them before they can be exploited.

The top drivers for heightened API security focus include the surge in API volume from AI and cloud programs, stricter regulatory expectations, and the growing recognition that APIs now sit at the center of both revenue and risk.

With a clear majority prioritizing the protection of AI apps and agents, alongside uninterrupted customer services and revenue continuity, the coming year will focus on tighter automation, stronger AppSec and DevSecOps collaboration, and broader deployment of dedicated API security controls that complement existing WAF and gateway investments.

Critically, the data shows that the organizations best positioned to improve are those that first close foundational gaps in discovery, inventory accuracy, and misconfiguration management.

**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 applications.**

**Schedule your demo**

## Methodology

This spotlight 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 Financial Services. Participants were evenly divided between C-level, AppSec, and DevSecOps roles. All percentages in this report have been rounded.



---

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](https://akamai.com) and [akamai.com/blog](https://akamai.com/blog), or follow Akamai Technologies on [X](#) and [LinkedIn](#). Published 05/26.