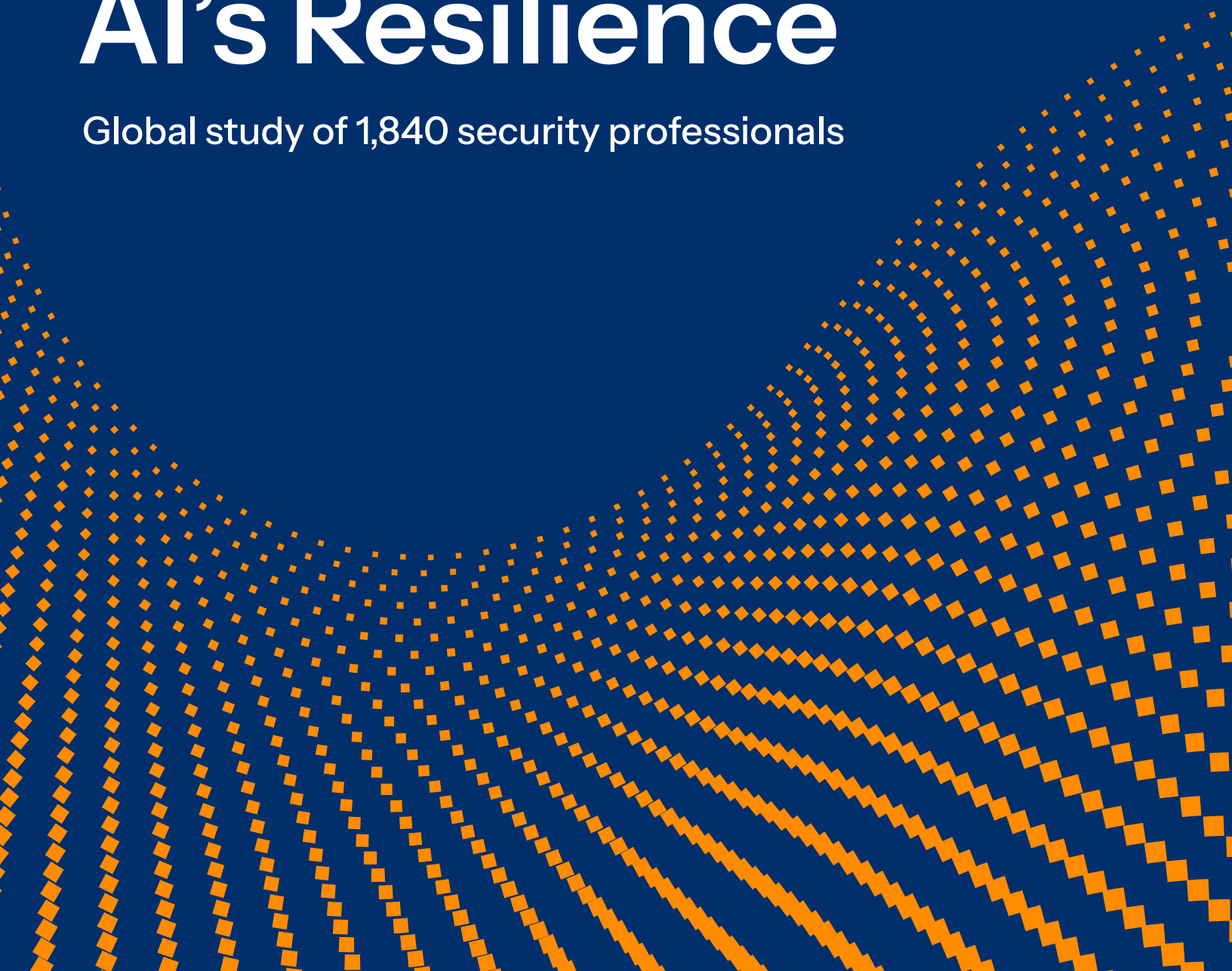
Akamai Security

API Security Impact Study

# How API Risks Threaten Your AI's Resilience

Global study of 1,840 security professionals



# Introduction

For four consecutive years, Akamai has tracked the state of API security across successive waves of enterprise innovation — digitization, cloud growth, and now AI adoption — each accompanied by rapid API growth. Across these phases, proliferating APIs have expanded the attack surface faster than organizations have strengthened API testing, visibility, and resilience against threats.

This year's findings confirm a clear pattern: API growth is outpacing API resilience, and AI adoption is amplifying the risk exposure.

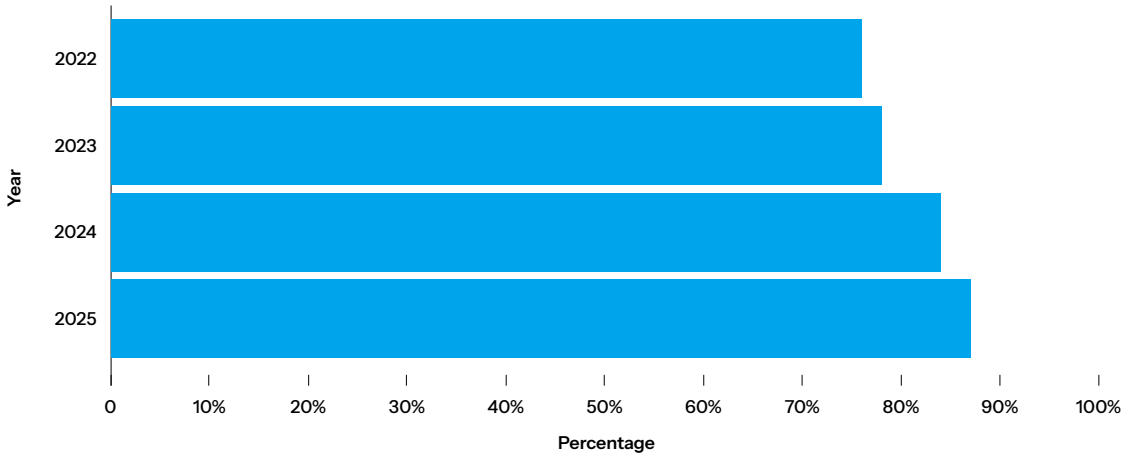
Global enterprises now manage sprawling API estates. The global median inventory per enterprise exceeds 5,900 APIs while the top quartile exceeds 29,400. As estates expand, the sightline into API risk and security coverage has not kept pace, and reported API security incidents have risen steadily over the four years of our research.

In our 2026 study, 87% of respondents reported experiencing at least one API-related security incident in the past 12 months, up from 76% in 2022.

Our 2026 study is based on a global survey reflecting insights from 1,840 security professionals across six industries and 10 countries in Asia-Pacific, the Americas, and EMEA. Respondents were evenly distributed between C-suite executives with a security focus and DevSecOps and AppSec professionals, allowing us to compare leadership and technical perspectives.

## More organizations are impacted by API security incidents

The percentage of organizations experiencing API-related incidents has risen steadily for four consecutive years.




*Author's note: Each of the annual API Security Impact Study editions that we reference reflect the prior 12 months of data (for example, our 2026 report covers findings from 2025).*

APIs underpin core business operations, making product capabilities available to customers, connecting partners and revenue channels, and automating back-office workflows. Yet many APIs remain outside centralized oversight because they are not consistently detected, inventoried, or governed by IT and security teams.

This year's findings reveal how rapid AI development is making these problems worse.

Across industries, global enterprises invested US$37 billion in generative AI (GenAI) in 2025, more than three times the amount in 2024, with US$19 billion of this total invested in the application layer.[1] These applications rely on APIs to determine what data they can access, what systems they can trigger, and what actions they can perform.

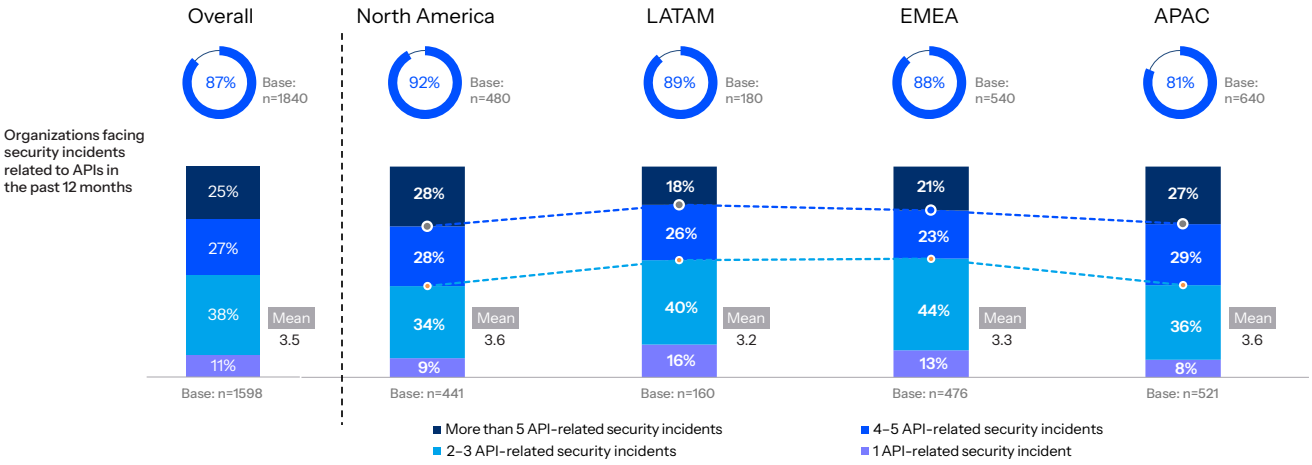
While APIs are only programmed to carry out tasks (rather than making autonomous decisions), they are created with an inherent power to govern AI's reach and authority. The problem is that APIs are not built to be resilient, so their power comes without the right level of visibility or controls. Each new AI deployment deepens dependence on the API layer that supports enterprise systems.

As API estates expand and governance falls behind, the impact is visible in our survey findings. Four data points stand out:

- **Poor visibility puts data at risk.** Only 27% of enterprises with full API inventories know which of their APIs return sensitive data, down from an already-low 40% in 2022.
- **AI-linked APIs are a significant source of security events.** Forty-two percentage of respondents attribute incidents to APIs powering AI applications, agents, and LLMs.
- **Misconfigurations are the leading cause of incidents.** This aligns with proprietary research from our solutions — and comes at a time when nearly half of enterprises report being only slightly-to-moderately prepared to address misconfigurations.
- **Financial impact is material.** API-related incidents cost an average of US$700,000 per organization — with the top quartile exceeding $1.8 million — driven by remediation, downtime, and legal exposure.

*1 Tim Tully, Joff Redfer, Deey Das, and Derek Xiao, 2025: The state of generative AI in the enterprise, Menlo Ventures, December 9, 2025.*

## Tracking API security incidents and volume by region




Akamai's fourth annual study continues to show persistent gaps in API testing and visibility. These challenges extend beyond human development error. Whether coded by developers or automated AI coding assistants, APIs typically undergo functional testing, but security testing is not uniformly integrated across the development lifecycle or aligned to modern attack techniques.

Our research indicates signs of hope: a growing awareness of API risks among leadership and their security teams. For example, for nearly 80% of enterprises, API security is among their top three cybersecurity priorities. Two-thirds of respondents report increased focus on API security over the past 12 months. And more than half (52%) cited API security incidents as among the top five threats that are most important to their organization for achieving cyber resilience.

However, as you'll see in this year's report, we've identified four structural leadership challenges:

- **Unfinished business securing existing APIs:** Year-on-year data shows organizations continue to struggle with visibility and protection across APIs.
- **A perception gap between leadership and technical teams:** C-suite leaders report higher confidence in their enterprises' API security testing processes — a key measure of an API's resilience — than the teams responsible for implementing them.
- **Overreliance on traditional security approaches:** Manual inventory processes and legacy tools fail to keep pace with API sprawl, particularly as AI accelerates development and integration.
- **Limited preparedness for emerging API threats:** Without robust discovery and inventory capabilities, organizations lack visibility into AI-linked APIs and other unmanaged assets, leaving expanding sources of risk.

The above structural gaps place enterprises on a path to higher attack frequency, broader business impact, and greater exposure to evolving threats to APIs and the applications they power. Let's explore the research findings, starting with the connection between API risk and AI risk.

Akamai Security

*Chapter 1*

# The state of play in 2026

## Fast AI and API growth opens the door to growing attacks

Enterprise investment in AI is accelerating as organizations deploy applications to automate workflows, enhance productivity, and drive revenue. More than half (51%) of AI adopters classify themselves as fast innovators, deploying predictive and generative AI across three or more business functions.[2] Yet API security maturity has not kept pace as AI-driven and cloud native applications rapidly expand API estates.

### As API estates grow, API visibility declines

For years, organizations have focused time, money, and staff on API functionality, with security applied inconsistently — or worse, not at all. Many APIs are deployed with misconfigurations, weak authentication controls, and other vulnerabilities that attackers readily exploit. Many organizations still lack a complete and accurate runtime inventory. Shadow endpoints, third-party services, and legacy APIs also frequently operate outside centralized oversight.

These weaknesses are now being amplified by AI adoption. Our research shows that 42% of those who reported API-linked security incidents over the past year experienced attacks involving APIs linked to AI technologies, such as apps, agents, and LLMs.

While approximately three-quarters of our surveyed respondents report having a full inventory of their APIs, less than one in four know which APIs access sensitive data. This distinction is critical. Without visibility into sensitive data flows, organizations cannot reliably prioritize risk or remediate issues early in the software development lifecycle.

Inventories are also often static and incomplete — for years, they have failed to capture shadow, rogue, zombie, or deprecated APIs. Now, a new class of APIs is widening the visibility gap: One-third (33%) of organizations cite "lack of visibility into AI/LLM-linked APIs and their risks" as one of the top three risks of APIs that interact with LLMs and related AI technologies. Traditional inventories frequently lack ownership clarity and do not record whether traffic is passing through approved controls.

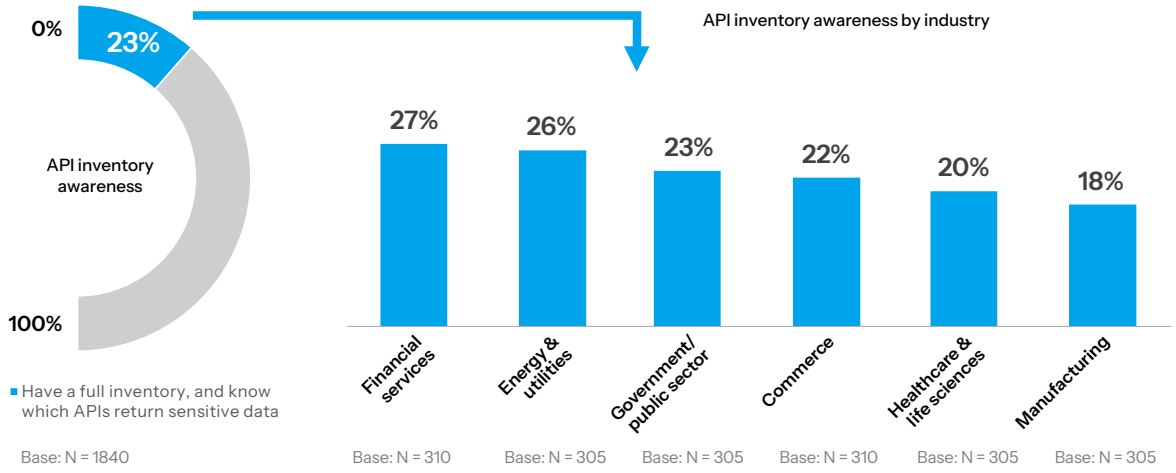
*2 The State of AI in 2025, McKinsey, ibid.*

Two global industries stand out as having the lowest visibility into which of their APIs return sensitive data: healthcare (20%) and manufacturing (18%). Limited awareness of sensitive data flows — think HIPAA-regulated patient data — increases the likelihood that high-risk APIs operate without clear governance.

In manufacturing, visibility is declining as organizations integrate IT and operational technology (OT) and expose data through stakeholder-facing applications, potentially increasing the sector's appeal to attackers.

## API inventory and awareness – organizations with full inventory and knowledge of APIs

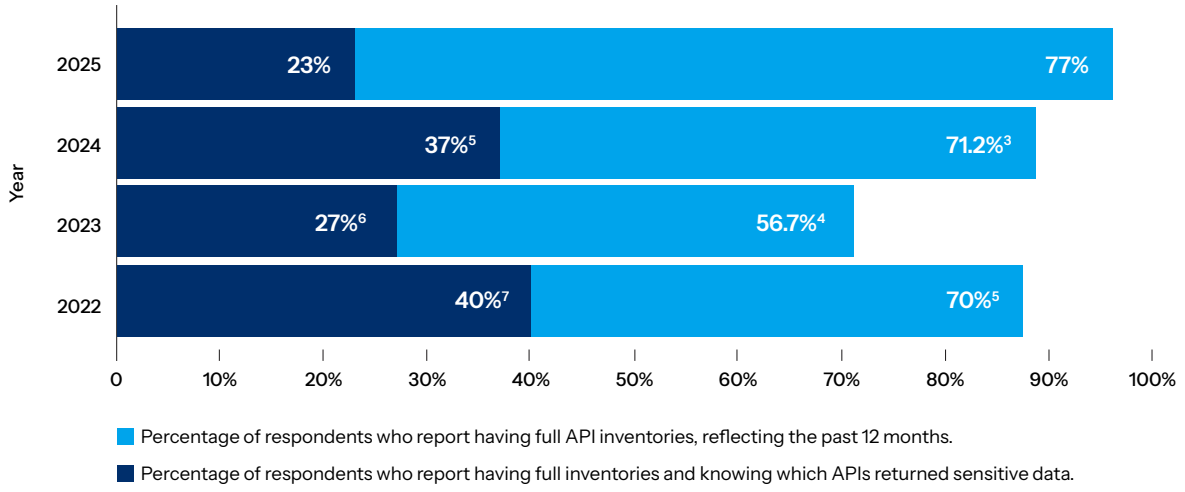
### Q: Do you have a full inventory of your APIs, and do you know which return sensitive data?



## API security is a long-term issue

Inventory completeness has fluctuated over the past four years while knowledge of sensitive data flows has declined, indicating persistent gaps in API visibility.

### Visibility into which APIs return sensitive data has reached an all-time low




As long-standing risks like poor API visibility remain unaddressed, new threats compete for security teams' attention. We asked respondents to rank their cybersecurity priorities for the next 12 months. Their top two priorities both center on emerging AI risks:

- Securing enterprise AI technologies such as AI-infused applications from attacks, which include LLM-linked APIs.
- Defending against threat actors who use AI-powered attack methods, such as supercharged DDoS attacks and malicious bots targeting the application layer.

Imagine a scenario in which an attacker successfully performs a prompt injection that tricks an AI app into doing the wrong thing. When the prompt asks for customer records or PII, it is the API that finds the data and brings it to the requestor, no questions asked.

*3 Findings limited to China, Japan, India and Australia.*

*4 Findings limited to UK, US, and Germany.*

*5 Findings limited to UK, US, and Germany.*

## Unmanaged APIs that create security blind spots

Many APIs operate outside formal inventory and governance processes, creating persistent visibility gaps. AI adds a new player to the existing roster of hidden APIs.

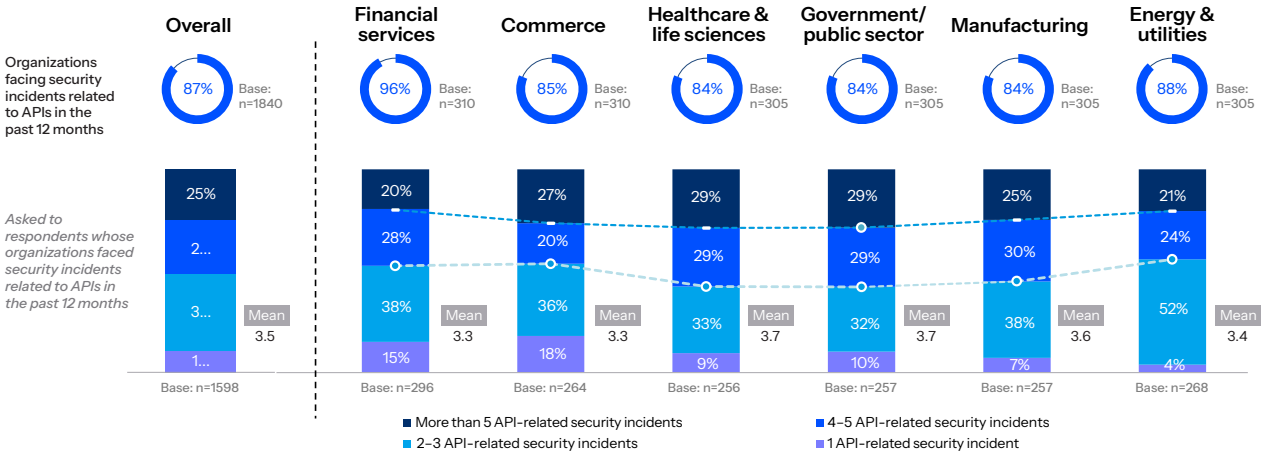
- **AI-linked APIs:** APIs that provide or retrieve sensitive data, connect to agents or LLMs, or enable automated actions without comprehensive visibility or governance.
- **Shadow APIs:** Undocumented APIs that operate outside officially monitored and inventoried channels.
- **Rogue APIs:** Unauthorized or malicious APIs introduced without approval or oversight.
- **Zombie APIs:** APIs that remain active despite being replaced or superseded.

## Where API risks have an outsized impact

API-related security incidents are not evenly distributed across industries. Financial services stands out: Nearly all respondents in this sector (96%) reported an API-related attack in the past 12 months. The industry's concentration of customer, account, and transaction data makes it an attractive target. Unaddressed vulnerabilities, including those identified in the OWASP API Security Top 10, are also widely known and exploited by attackers, contributing to the high incidence of attacks.

## API security incidents: A cross-industry view

### Q: Did your organization experience any security incidents related to APIs in the past 12 months? If so, approximately how many?



Akamai Security

*Chapter 2*

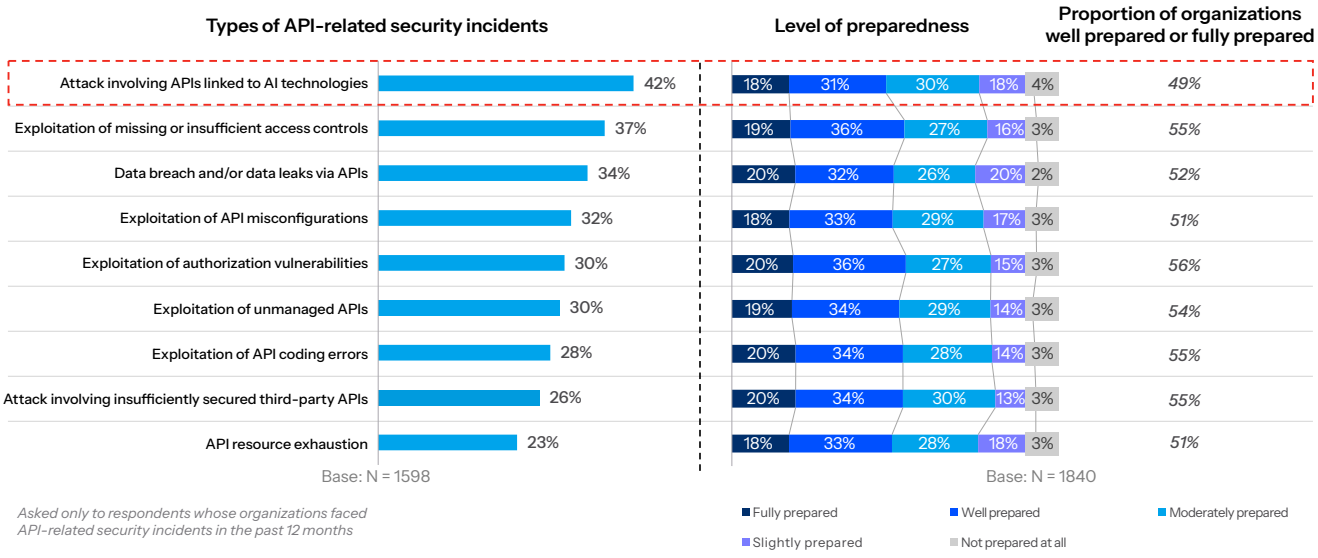
# The cost and confidence gap

## Rising API incidents and uneven resilience in the AI era

According to the leaders and practitioners we surveyed, the most common category of API security incidents they faced in 2025 was attacks on APIs linked to their enterprises' AI technologies, such as AI-enabled applications. This finding is interesting because in AI adoption's still-early stages, it's difficult for enterprises to know which of their APIs are connected to AI apps and their corresponding LLMs. But at a time when organizations are under pressure to embed AI into *all* of their existing tools, apps, and services, the fact that security teams are mindful that this connection exists is important.

### AI-linked API attacks are the most frequently reported incident type, yet organizations rate themselves *least prepared* to address them

**Q: Which of the following types of API-related security incidents has your organization experienced in the last 12 months?**

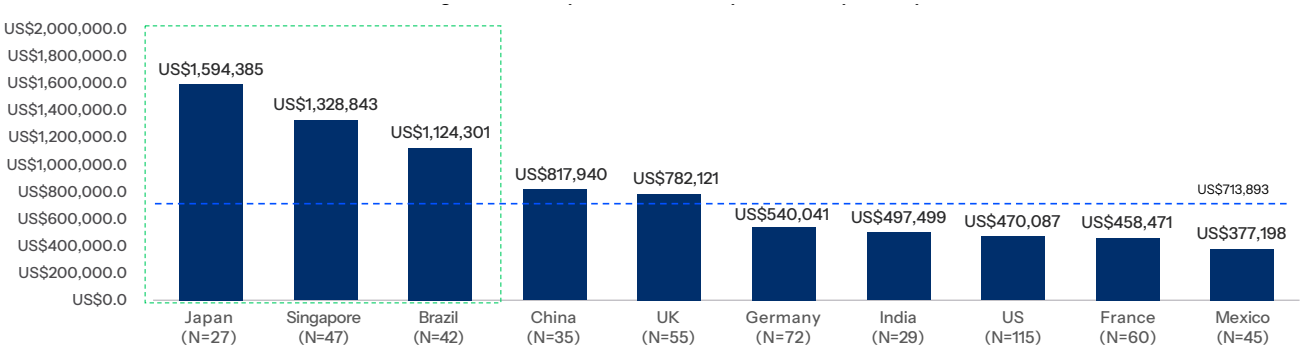


## API security incidents cause real business harm

According to Akamai's 2025 State of the Internet report, State of Apps and AI Security, API security issues are expected to cost organizations US$100 billion in 2026, up from $87 billion in 2025[6]. In our 2026 API Security Impact Study's findings, we see that organizations experienced an average of 3.5 API-related security incidents over the past 12 months, with a combined average cost of $700,000.

### Average annual API security incident costs across countries

**Q: If you have experienced one or more API security incidents in the past 12 months, what has been the estimated total financial impact of these incidents?** (Please include all related costs such as system repairs, downtime, legal fees, fines, and any other associated expenses.)




*Asked to respondents whose organizations faced security incidents related to APIs in the past 12 months and is either at CISO/CTO/CIO job level*

The highest costs for API incidents were reported in Japan, Singapore and Brazil. Respondents in these countries also reported lower security maturity across several indices.

- For example, the percentage reporting a full API inventory and visibility into sensitive data flows was below a global average of 23% in Japan (at 11%) and Brazil (15%).
- Respondents in Japan, Singapore and Brazil also reported lower use of dedicated API security tools and weaker integration of security testing across the API development lifecycle.
- In Brazil, only 10% had fully integrated security testing, compared to 16% overall.

*6 State of Apps and API Security, Akamai, 2025.*

## Impacts extend beyond remediation

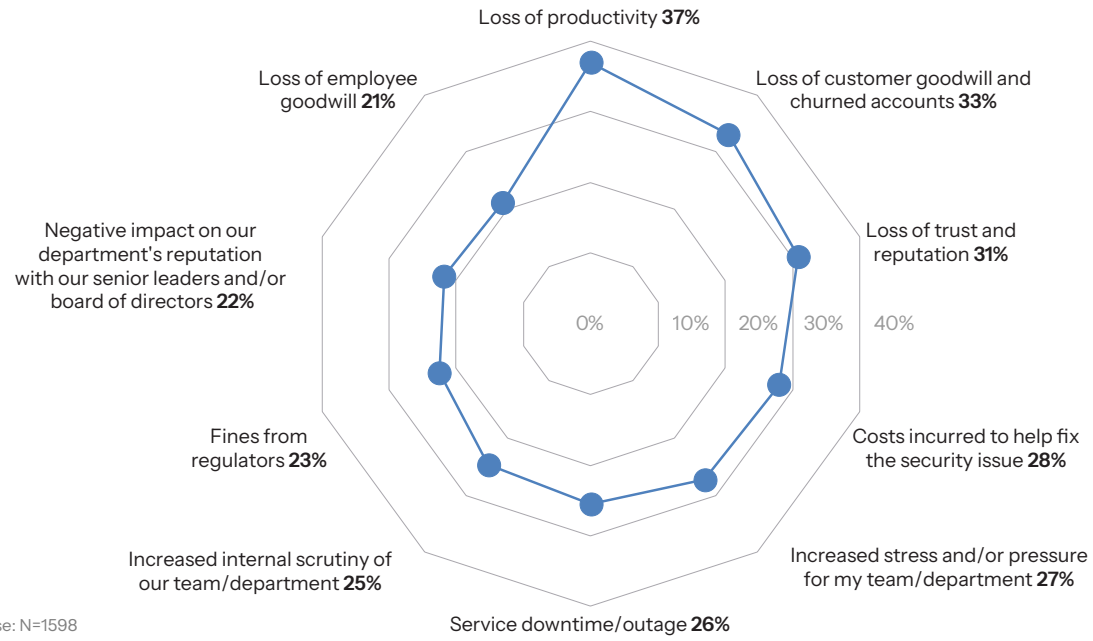
The top three impacts cited by respondents who experienced API security incidents all focus on what an organization loses when the APIs underpinning its business are compromised:

1. **Loss of productivity** (37%)
2. **Loss of customer goodwill and churned accounts** (33%)
3. **Loss of trust and reputation** (31%)

When considering that our respondents' most frequently cited incident type was an attack on their AI-linked APIs, the financial stakes of lax API security become clear. As mentioned, enterprises have now invested billions in Gen AI-enabled applications. If the APIs behind those applications aren't seen, secured, and tested, the overarching AI investment is at risk.

### How API security incidents are impacting enterprises

**Q: What costs and/or impacts, if any, have API security incidents had or are likely to have on your business?** (Please select up to three options)




Base: N=1598

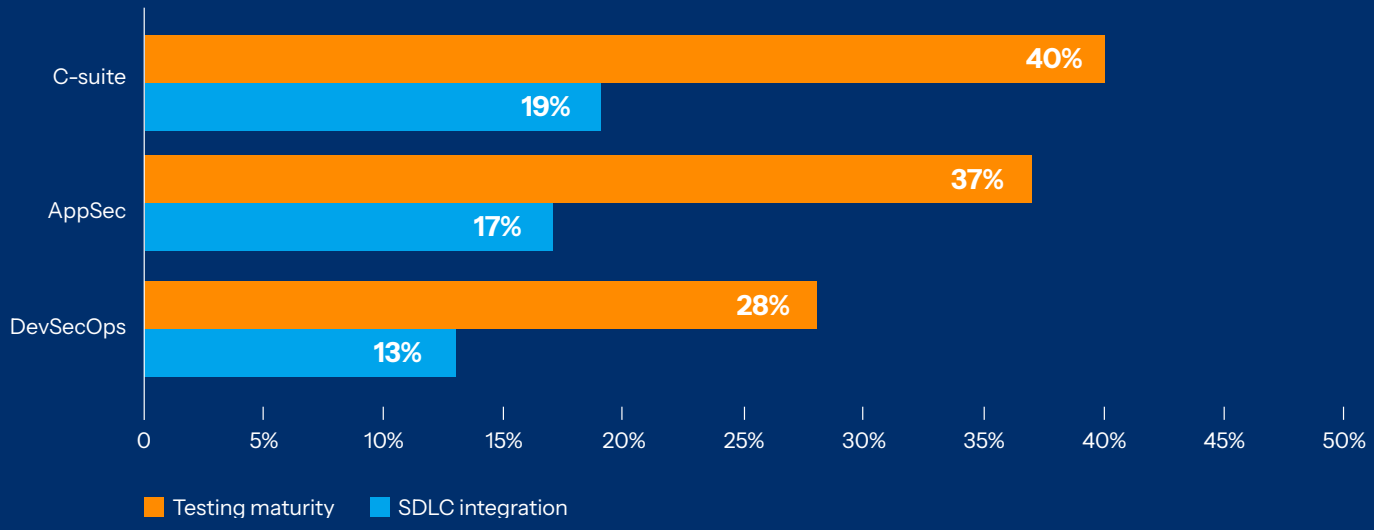
## C-suite leaders' assessment of API security testing consistently exceeds their frontline teams' confidence

By testing APIs for vulnerabilities in development, enterprises can ensure their APIs will be resilient against attacks once in production. However, our research shows an alarming lack of security-focused testing throughout the software development lifecycle (SDLC) and practitioners on whether APIs are being adequately tested.

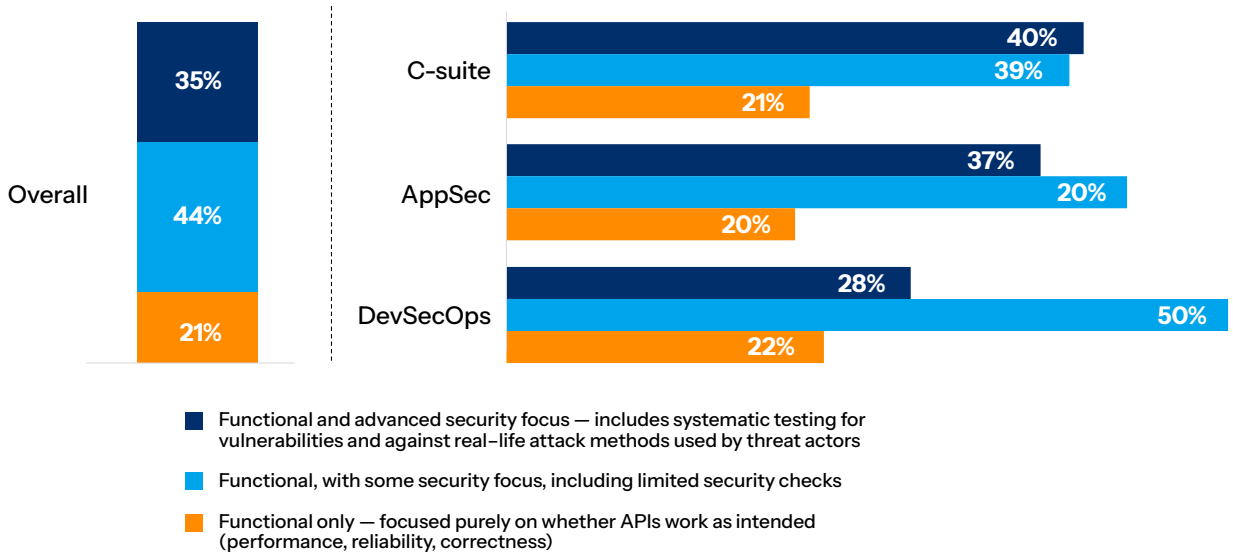
Respondents were asked to evaluate the maturity of API testing within their organization. Our scale ranged across three levels:

- Functional testing that verifies whether APIs work as intended.
- Testing with *some* security focus that includes limited security checks.
- Advanced testing that systematically evaluates APIs for vulnerabilities and real-world attack methods.

They were also asked to what extent security testing was integrated into their organization's API software development cycle and CI/CD pipelines. Forty percent of C-suite leaders report advanced API testing maturity, compared with 28% of DevSecOps teams. Leadership confidence exceeds what implementation teams report on the ground.



## Nature of API testing in organizations




Based on the findings, we see a very real risk: The gap between what leaders believe and what is occurring on the ground may lead to underinvestment in dedicated resources, API testing, runtime controls, and remediation capabilities.

Leadership overconfidence may therefore contribute to under-governance of API risk, even as cybersecurity budgets are projected to rise. While 99% of executives anticipate budget increases, more than half (54%) expect growth of only 6% to 10%, potentially limiting the resources a security team can direct toward closing API maturity gaps.[7]

Strengthening API visibility and embedding security testing across the development lifecycle are foundational steps toward improving resilience as API estates expand. We'll further explore the topic of testing later in this report. In the next section, we'll take a closer look at the connection between securing APIs and protecting the AI applications they power.

### Cybersecurity budgets are spread thin

Many organizations (70%) are already dedicating more than 10% of their cybersecurity budgets to AI-related priorities. However, this funding is spread across multiple priorities — fraud protection (57%), predictive analytics, and enhanced detection (53%) — indicating that API security may be under-resourced.[8] There is a critical link between securing AI and securing the APIs that power it.

*7 "Is a Cybersecurity Boom on the Horizon? KPMG Survey Shows Surge in Cybersecurity Investment as AI Threats Redefine Risk," KPMG, December 15, 2025.*

*8 Cam Sivesind, "The Great Cyber Budget Boom: 99% of Leaders Are Increasing Spend," SecureWorld, December 18, 2025.*

*Chapter 3*

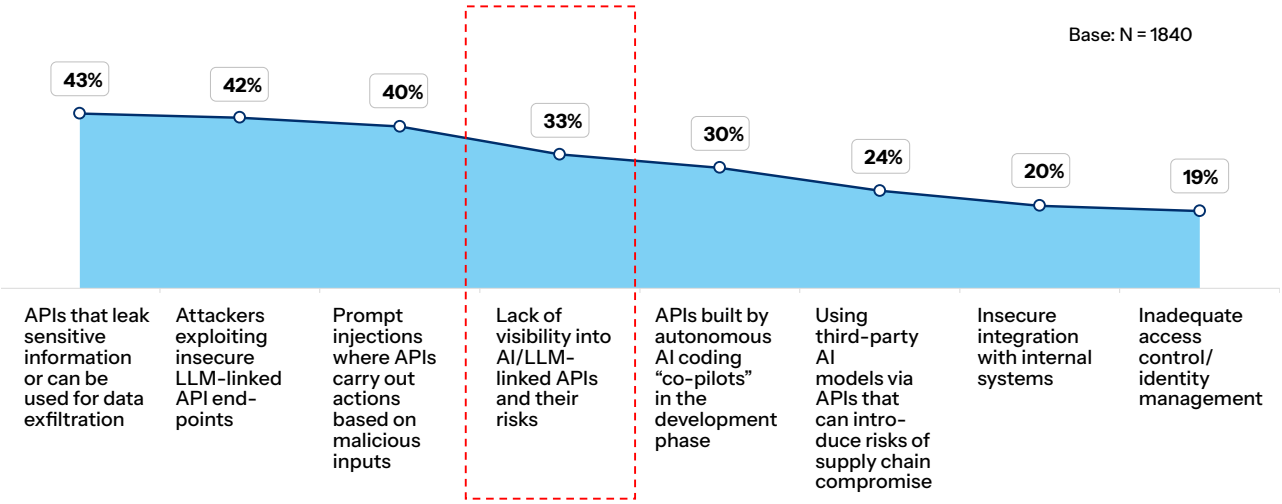
# The API security response gap

## Why API security maturity is not keeping pace with innovation

APIs control how AI applications access data, trigger workflows, and exchange information across systems. In our study, respondents cite data leakage, insecure LLM-linked endpoints, and prompt injection as the top risks associated with AI-linked APIs. Over a third (33%) also cited a lack of visibility. When organizations cannot see where AI-linked APIs operate within their environments, they cannot reliably test, govern, or secure them. As AI deployments scale, this expanding layer of interconnected APIs increases operational exposure. Without clear oversight, the system directing AI activity risks resembles a busy airport without a functioning control tower.

### Among top risks of AI-linked APIs, poor visibility ranks low

**Q: When it comes to your organization's APIs that interact with LLMs and related AI technologies, what are the risks that concern you the most?**



Although securing AI is a stated priority, our respondents are largely unprepared for what's coming, as are their APIs. Fewer than half of respondents rank their ability to secure AI-enabled systems against attack as a top-three cyber resilience competency.

## How organizations rate their cyber resilience for securing AI technology

**Q: Please rate your enterprise's current level of cyber resilience for top business priorities using a 10-point rating scale, where 1 is the lowest level of resilience and 10 is the highest.**

| Top business priorities for achieving cyber resilience | Proportion ranking in top 5 | Level of cyber resilience (top 3 box) | Net level of cyber resilience (top 3 box – bottom 5 box) | Mean level of cyber resilience |
|---|---|---|---|---|
| Secure against attacks targeting our AI apps, agents, etc. | 77% | 42% | 24% | 7.1 |
| Ensure AI-enabled digital services continue uninterrupted | 70% | 44% | 23% | 7.1 |
| Protect our ability to generate revenue | 69% | 36% | 17% | 7.0 |
| Prevent direct losses | 63% | 37% | 18% | 7.0 |
| Gain better visibility into our AI technologies' risks | 59% | 50% | 41% | 7.4 |
| Address vulnerabilities in our agentic AI technologies | 58% | 36% | 18% | 7.0 |
| Ensure our AI developers' productivity isn't disrupted | 52% | 38% | 18% | 7.1 |
| Avoid regulatory penalties and/or compliance failures | 52% | 45% | 29% | 7.2 |

*Despite AI's strategic importance, mean resilience scores across AI-related priorities cluster between 7.0 and 7.4 out of 10. These self-assessment scores suggest organizations feel moderately confident in their ability to secure AI applications, agents, and systems, even as other findings in the study point to gaps in API visibility and testing maturity that underpin those systems.*

## Moving beyond traditional controls

As API estates expand and AI-driven traffic becomes more autonomous, long-held assumptions about predictable application behavior and controllable entry points are breaking down, shifting risk from the network edge to the governance of the API layer itself.

Despite this shift, most organizations continue to rely heavily on perimeter-based controls. Four in five respondents (80%) report using a web application firewall (WAF). Adoption of purpose-built API security platforms is lower, with 40% using a web application and API protection (WAAP) platform and 35% using a dedicated API security tool.

These findings reflect the limitations of relying on any single control as APIs increasingly govern AI-driven workflows. For example, WAFs can be a layer of application security, but resilience now depends on integrating perimeter defenses with API-aware visibility, runtime protection, and governance across the AI stack, complemented by rigorous API testing.

**Four in five respondents (80%) report using a web application firewall (WAF). Adoption of purpose-built API security platforms is lower, with 40% using a web application and API protection (WAAP) platform and 35% using a dedicated API security tool.**

Enterprise leaders should consider a layered application security model that combines:

- **Dedicated API security capabilities** to provide continuous discovery, sensitive data awareness, runtime protection, and integrated security testing across the API lifecycle.
- **WAAP** platforms that extend traditional WAF functions with API-aware inspection and application-layer defenses in a unified control plane.
- **Protection against automated threats**, including bot mitigation and behavioral analysis to manage both human and AI-driven interactions.
- **Monitoring and governance of AI interactions**, including visibility into prompts, responses, and model-initiated API calls, with security controls for inbound and outbound activity — aligned with enterprise compliance frameworks and centralized policy controls.

*Chapter 4*

# How organizations are addressing API risk

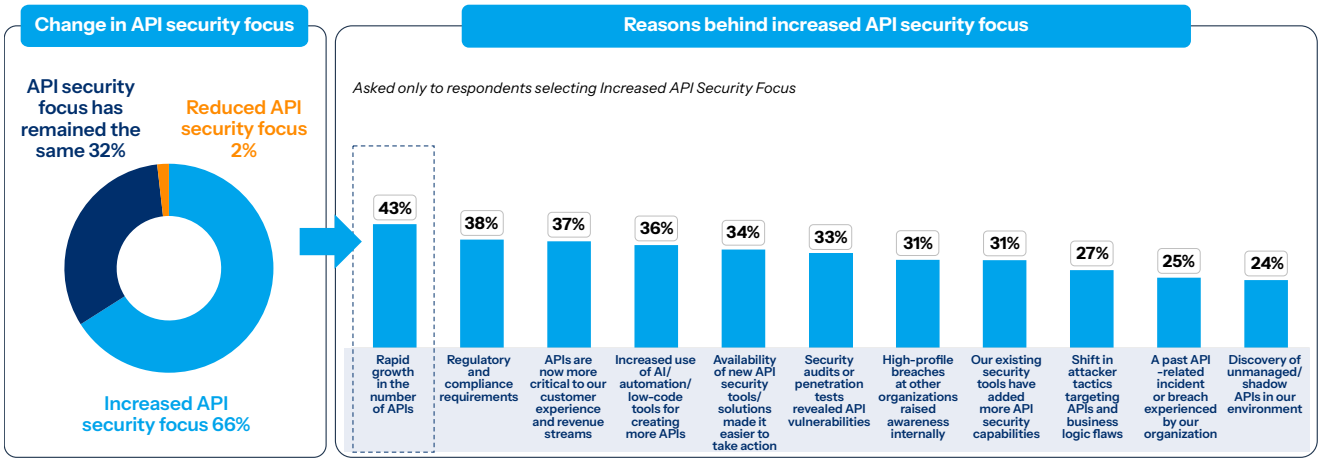
## Enterprise focus on API security is increasing, yet structural gaps in resourcing, maturity, and lifecycle integration persist

When asked how their organization's focus on API security has changed over the past year, two-thirds reported an increase. The top three drivers were:

- Rapid growth in API estates driven by AI initiatives, cloud migration, microservices, and broader digital transformation
- Regulatory and compliance requirements
- APIs linked to customer experience and revenue-generating services

### Rapid API growth and regulatory pressure are the primary drivers behind organizations' growing emphasis on API security

**Q: What are the reasons for your organization's increased focus on API security over the past year?**



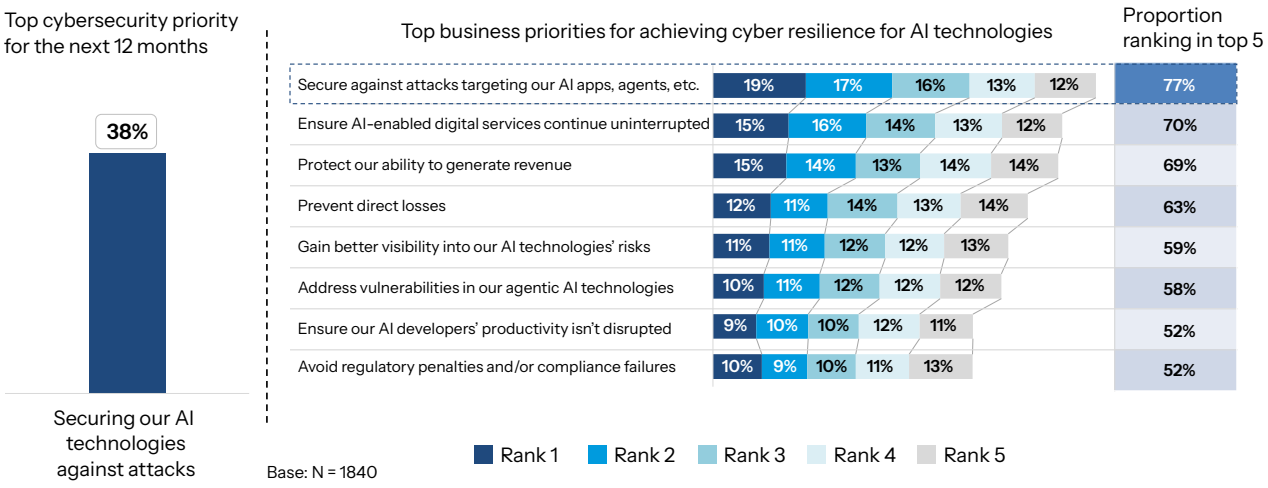

Base: N=1840

Base: N =1214

These rankings align with our finding that shows respondents view protecting AI technologies as the number-one cybersecurity priority for the next 12 months. Enterprises aim to protect substantial AI investments, secure sensitive data, and maintain application performance. Some of this investment is in AI-native applications — many of which are existing apps and services built upon or linked to AI tech, such as LLMs.

## Securing AI technologies against attacks ranks as the leading business priority for achieving AI cyber resilience.

**Q: When it comes to cyber resilience for your enterprise's AI technology (i.e., having controls and capabilities to ensure ensure AI apps and agents can withstand and recover from attacks), what business priorities are most important to you?**




Base: N = 1840

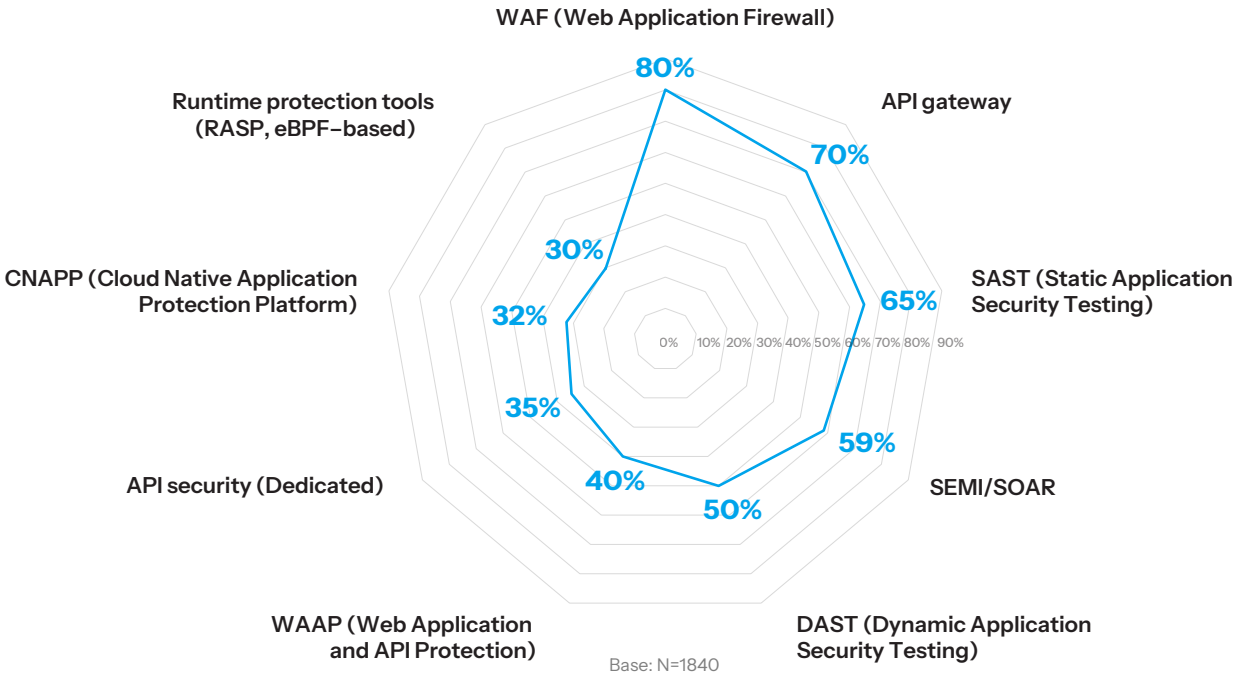
## Finding the right people, processes, and tools

We know that the right combination of people, processes, and tools is vital for strong cyber resilience in the face of jeopardized business continuity — an AI app's ability to operate, function safely, and generate revenue as intended. When it comes to securing APIs, here's what we discovered about the combination that organizations are investing into one of the most significant ways to ensure API resiliency: testing.

Approximately one in two organizations (53%) report having dedicated personnel responsible for API security. These teams focus on testing (82%), threat intelligence (81%), remediation (75%) and compliance integration (69%). Enterprises continue to rely primarily on legacy perimeter and application security tools, with adoption of dedicated API security platforms lagging significantly behind.

## Security teams use both legacy and specialized tools for API security

### Q: Which of the following types of API security tools or platforms does your organization currently use?




Base: N=1840

## API testing across enterprises varies considerably in scope

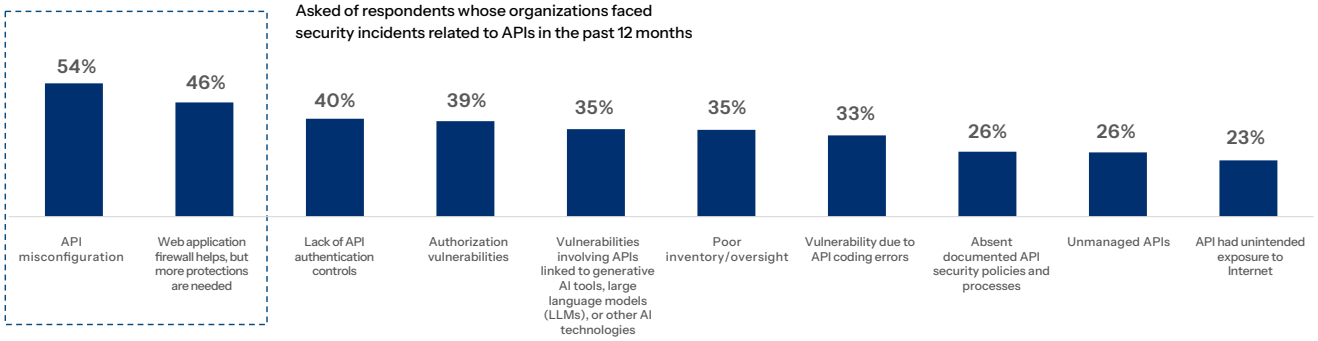
According to our findings, security-focused testing across the SDLC can mitigate four of the top five common API issues associated with security incidents. Testing involves continually evaluating the API landscape, driving targeted remediations, and automating security workflows.

## Functional testing may miss common API issues

Many of the leading causes of API incidents relate to misconfigurations, access control weaknesses, and visibility gaps — issues that are well understood yet continue to persist.

### Exploring the root causes of API security incidents

**Q: What do you believe are the causes of the API security incidents your organization has experienced?**




Base: N=1598

## The overemphasis on API functional testing

Testing addresses many of the most common API issues linked to incidents. However, maturity varies significantly across organizations.

API testing at many enterprises is functional in nature, with limited security depth. While 44% report functional testing with some security focus, only 35% report fully mature testing that combines functional evaluation with advanced security focus. Overreliance on functional testing leaves organizations exposed as AI accelerates API development and integration. While AI coding assistants are incredibly helpful for busy developers, they are not governed or secured — and their presence exacerbates an already-dangerous trend of untested vulnerable APIs.

Indeed, increased use of AI coding assistants is a top-three-ranked reason for enterprises that increased their focus on API security over the past 12 months — a view shared by our C-level and AppSec respondents.

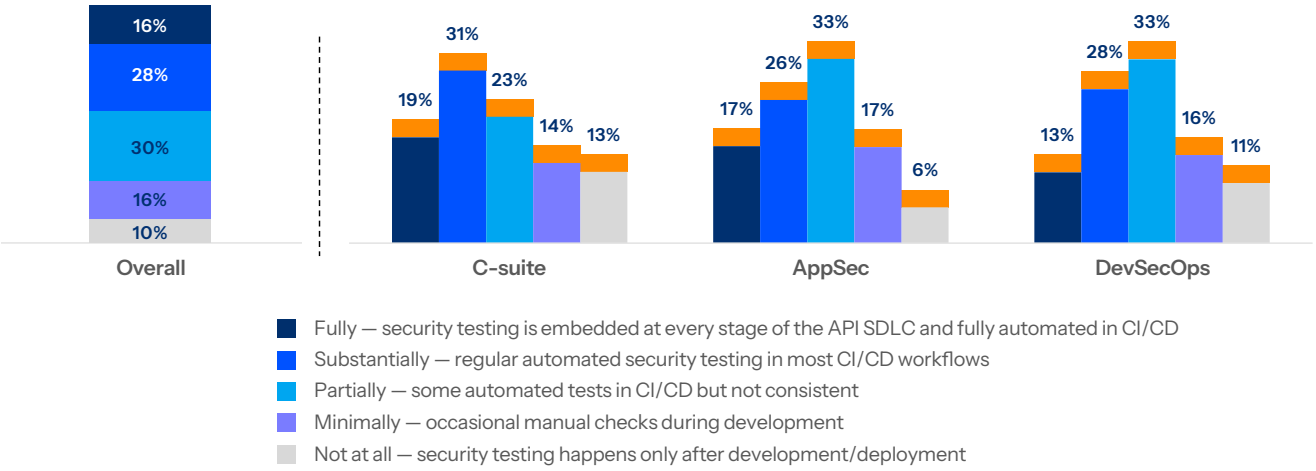
Security testing integration into the API software development lifecycle (SDLC) also remains inconsistent:

- Approximately 30% report that testing is only partially integrated into SDLC and CI/CD processes
- A further 16% report that testing is embedded across every stage of development

Earlier integration reduces remediation cost and limits the introduction of vulnerabilities into production environments.

## API testing needs a stronger security focus

### Q: To what extent is security testing integrated into your organization's API software development lifecycle (SDLC) and CI/CD pipelines?



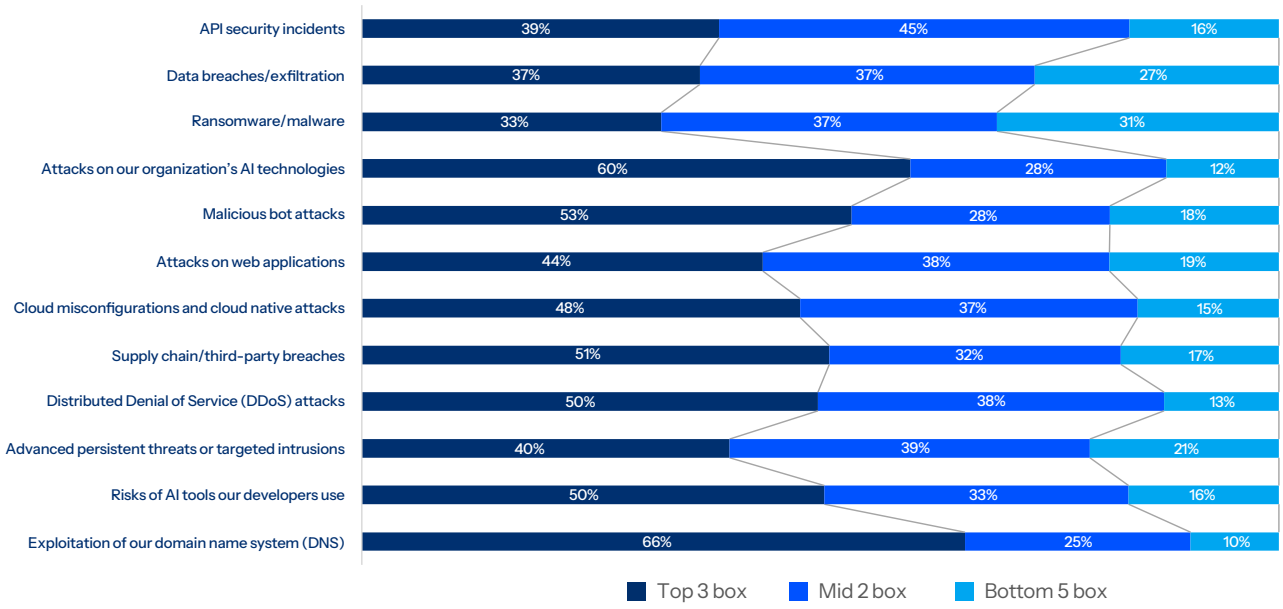

Base: N=1840

Base: C-suite, n=611; Appsec, n=597; DevSecOps, n=632

But despite an increase in comprehensive and consistently integrated testing, our study reveals that just 39% are satisfied with their resilience against API security incidents.

## API security resilience ranks among the three weakest areas of overall cyber resilience

**Q: What are the top five cyberthreats that are most important to your organization from the perspective of achieving cyber resilience? Rate your level of satisfaction with your organization's resilience against that threat.**




Scale: 1 - Not at all Satisfied, 2, 3, 4, 5, 6, 7, 8, 9, 10 - Extremely Satisfied
Base: N ranges from 187 to 952

The gap between innovation speed and testing maturity is not just operational. As APIs increasingly govern AI-enabled workflows, weaknesses at the testing layer scale across business-critical systems. API security resilience already ranks among the weakest areas of overall cyber resilience. Without stronger lifecycle integration, exposure is likely to compound as API estates expand.

That said, for an AI application or agent to be truly resilient, organizations need to secure the many APIs powering those apps and serving as their connection to LLMs. So by taking care of the top threat, organizations can improve their resilience against many of the threats listed in the chart shown here, including data breaches and attacks that threaten business continuity. **The AI race is underway, but it's not too late to shore up API security.**

## API security is core to compliance

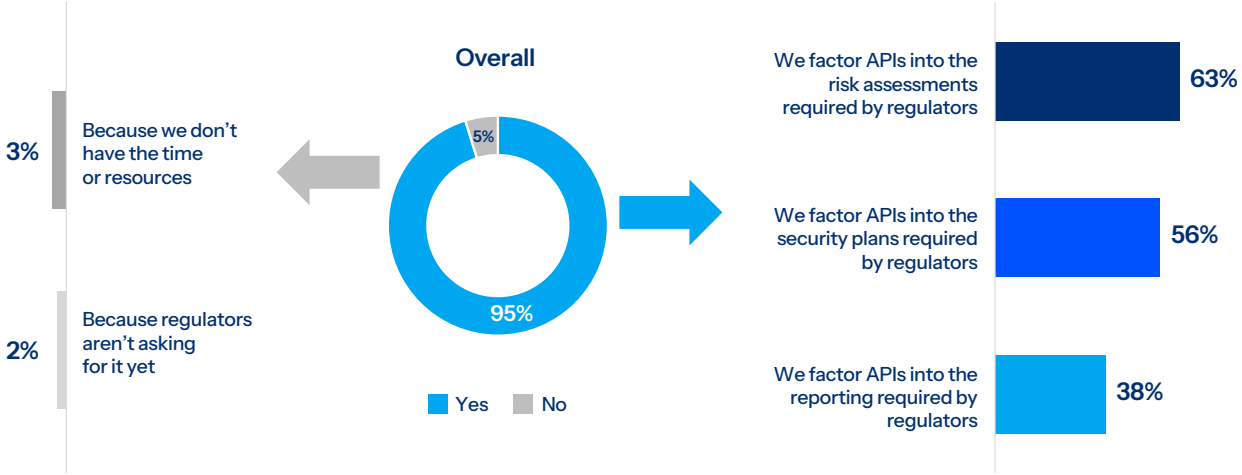
Regulatory scrutiny is intensifying as digital, cloud, and AI initiatives expand enterprise data exposure.

Although 95% of our respondents report that they're factoring API security into regulators' data protection requirements, far fewer translate that intention into the necessary actions for compliance, from documented security processes to formal reporting. This execution gap exposes organizations to governance risk, particularly as API estates grow and AI-linked APIs increase data interdependence.

Given the prevalence and financial impact of API-related incidents, integrating compliance controls directly into API security processes is not administrative hygiene — it is a governance necessity.

### Inclusion of API security in compliance requirements

**Q: Do you factor API security into meeting your regulators' compliance requirements for data protection?**

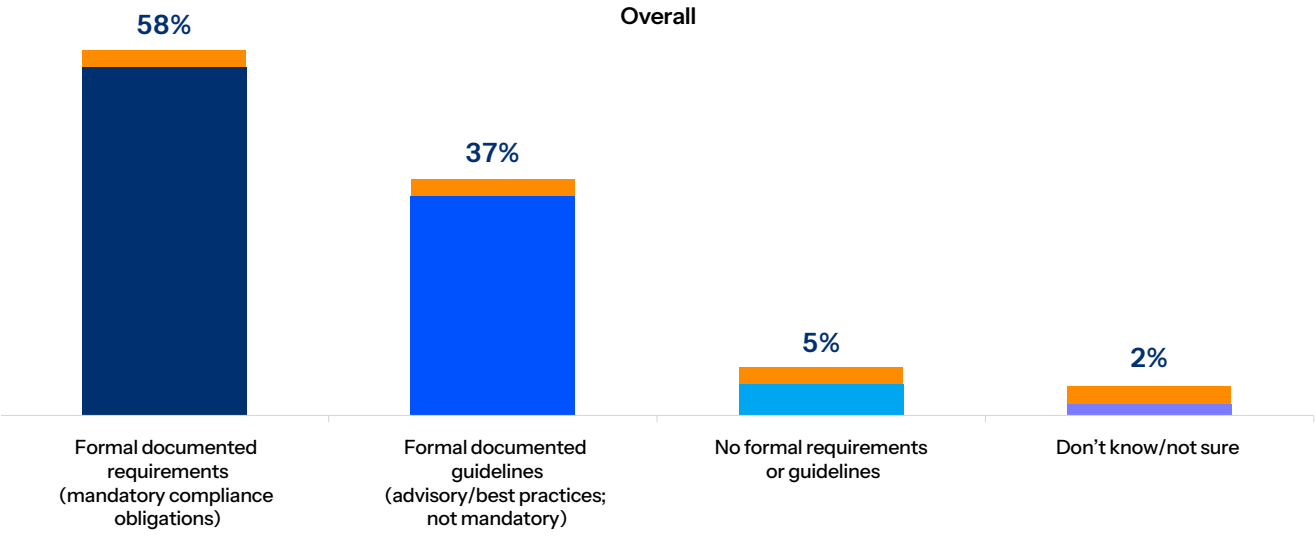



Base: N=1840

While mandatory API security requirements are common, more than one-third of organizations operate under non-mandatory guidance, rather than enforceable compliance obligations. This reflects the current state of APIs in regulatory rules and requirements. In many cases, APIs are not explicitly mentioned in a regulator's documentation. But with APIs emerging as a leading cause of breaches, organizations should proactively view API security compliance as essential.

## Regulators' expectations vary when it comes to API security

### Q: To what extent do regulators in your industry/jurisdiction include API security requirements in the following areas?




Base: N=1840

API estates are expanding rapidly, AI deepens operational dependence on interconnected APIs, and testing and governance maturity are not advancing at the same pace. Closing this gap requires more than incremental improvements. It requires a deliberate shift in how API security is prioritized, governed, and integrated into enterprise resilience strategy. Organizations should be aware of the specific, documented rules for APIs, rather than having to guess and risk fines.

Akamai Security

*Chapter 5*

# Transforming API security in 2026

## Securing AI innovation at scale in 2026 depends on securing the APIs that power it

As digital transformation accelerates, API expansion is outpacing the maturity of visibility, testing, and governance controls, exposing organizations to higher incident rates and escalating financial impact.

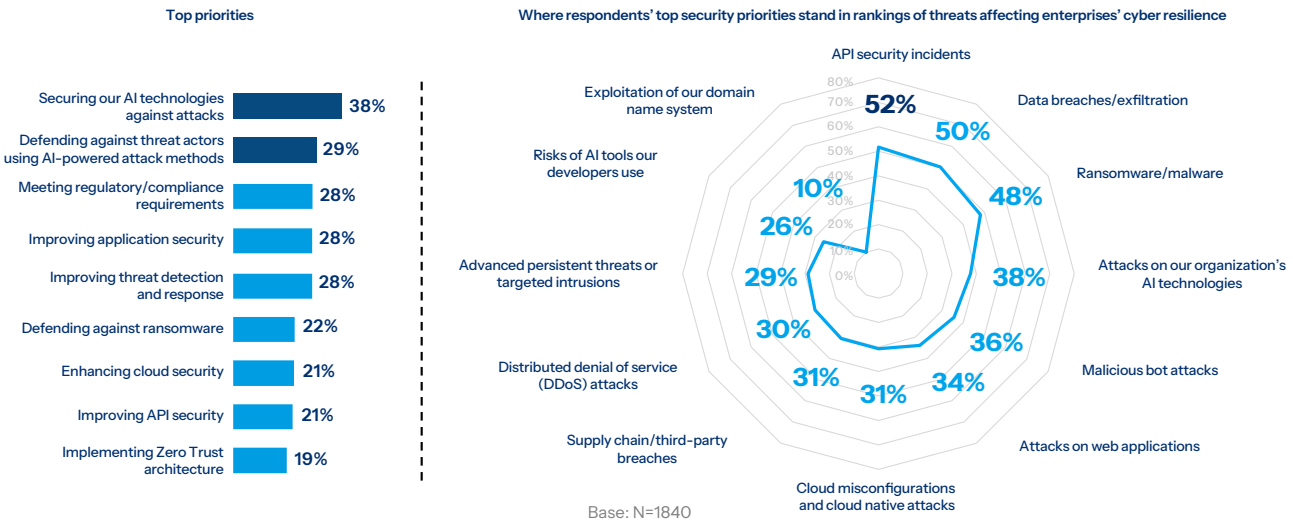
The imbalance extends beyond breach probability. It introduces operational fragility across the customer, revenue, and automated workflows that APIs increasingly orchestrate. Put plainly, if an AI attack grinds a widely used AI application's operations to a halt, or if an API gives out customer data to an attacker who writes a compelling prompt, the fallout will be widespread and significant.

Enterprise focus on API security is rising. However, our research shows that increased attention has not consistently translated into stronger lifecycle integration, deeper testing maturity, or clearer ownership. In some cases, executive confidence in API resilience exceeds the assessments of the teams responsible for securing it.

When we asked our 1,840 respondents to rank their top security priorities for the next 12 months, securing APIs ranked second-to-last (21%), significantly lower than their number-one priority, securing AI technologies (38%). This suggests that enterprises aren't yet fully grasping the connection between vulnerable APIs and the AI innovations they power. However, our respondents also believe that API security is the top threat to their organizations' cyber resilience, which is a step in the right direction.

AI security now sits at the top of the cybersecurity agenda, but the threat landscape remains dominated by API and application-layer exposures.

## Q: What are your organization's top cybersecurity priorities for the next 12 months?




Now it's time for enterprise security teams to make the connection between securing APIs, protecting their AI innovations, and ensuring cyber resilience at both a micro scale (keeping AI apps running) and macro scale (ensuring business continuity). Advancing API security maturity in parallel with innovation will strengthen resilience across digital services, customer platforms, and automated workflows, reinforcing not only AI initiatives but also the broader enterprise technology foundation.

Akamai Security

*Chapter 6*

# Six strategic opportunities to strengthen API testing, extend visibility, and build resilience in the AI era

We know that AI is amplifying the already-present risks of unseen and unsecured APIs. But it's not too late to strengthen organizational resilience. By implementing tools, controls, and processes like those outlined below, organizations can close security gaps and ensure resilience for APIs and the AI innovations they power.

1. **Close foundational visibility gaps**
   Accurate, continuously updated visibility into API estates remains the starting point. Organizations must understand not only how many APIs exist but also which expose sensitive data, integrate third parties, or support AI-enabled workflows. Without this baseline, prioritization and governance decisions are impaired.

2. **Embed security across the API lifecycle**
   Functional testing alone is insufficient. Security must be consistently integrated into design, development, and deployment workflows, with accountability for remediation. As AI accelerates API development and integration, lifecycle discipline becomes critical to prevent vulnerabilities from scaling rapidly.

3. **Strengthen runtime resilience**
   APIs operate dynamically across distributed systems. Perimeter-based defenses do not address behavioral abuse, business logic exploitation, or data leakage patterns in production environments. As APIs increasingly orchestrate AI-driven processes, runtime oversight becomes essential to maintaining operational trust.

4. **Align investment to measurable exposure**
   Incident frequency and cost data demonstrate that API weaknesses create direct financial and operational impact. Budgeting and resource allocation should reflect this exposure, particularly in sectors managing sensitive data, business-critical services, and AI-enabled decision-making.

5. **Formalize governance and accountability**
   API security must be incorporated into documented processes, reporting structures, and compliance controls. Clear ownership and executive oversight reduce the disconnect between perceived and actual maturity and ensure that AI-linked APIs are governed with the same rigor as other critical assets.

6. **Treat API security as a prerequisite for AI trust**
   As AI systems increasingly orchestrate enterprise processes, APIs determine what data models access, what workflows they trigger, and what actions they execute. Weaknesses at the API layer therefore become weaknesses in AI execution. Strengthening API maturity is not separate from AI security; it is foundational to sustaining trust in AI at scale.

## About the study

In November 2025, Akamai commissioned Phronesis Partners to conduct a global study of 1,840 key decision-makers across 10 countries and six industries. The goal was to understand the current state of API security and be able to:

- Provide insights into the latest leader and team thinking about API security.
- Identify gaps that could indicate the need for new processes and solutions; discuss regional and industry nuances.
- Quantify the cost of maintaining the status quo: limited visibility, growing risks, cost of remediating incidents.
- Point toward a new way forward: evolving API-aware security to proactively manage risks and what capabilities are needed.

About survey respondents

- Respondents spanned 10 countries and six industries.
- More than three-fourths were the final decision-makers on cybersecurity priorities.
- They were divided between C-level, AppSec, and DevSecOps.

**Learn how Akamai can help you secure your enterprise against common API attack methods highlighted in the OWASP Top 10 API Security Risks.**

**Read white paper**

# Credits

## Editorial and writing

John Natale — Phronesis Partners

## Review and subject matter contribution

Barney Beal
Stas Neyman
Yariv Shivek

## Promotional materials

Ellen O'Brien

## Marketing and publishing

Georgina Morales Hampe

## State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports. akamai.com/soti

## Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/security-research

## Akamai security research

Read the Akamai security research blog for a rapid response perspective on today's most important research. akamai.com/blog/security-research

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 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 04/26.