Akamai Security

API Security Impact Study

How AI Innovation Amplifies API Risk in APAC

Global study of 640 cybersecurity professionals in China, Japan, India, and Singapore

Akamai Security

Introduction

For four years, Akamai has studied the state of API security across successive eras of business innovation — digitization, cloud adoption, and now AI development — each accompanied by rapid API growth. In 2026, the average global enterprise has nearly 6,000 APIs, with the top quartile exceeding 29,000.

As these environments expand, it becomes even harder to track APIs, identify their risks, and understand whether they've been tested for resiliency against attacks — especially as AI adoption increases the rate of new API connections and dependencies.

Our latest API Security Impact Study survey shows that API security gaps have been increasing year-on-year. This study of 640 cybersecurity decision-makers across four APAC markets points to a clear inflection point: **API growth is outpacing organizations' ability to secure these business-critical connectors, while AI adoption is further increasing risk exposure.**

The findings suggest this API security gap is being shaped by four structural leadership challenges:

- **Unfinished business securing existing APIs, as new risks emerge:** 81% of APAC organizations experienced an API security incident in the past 12 months.
- **A perception gap between leadership and technical teams:** C-suite leaders are more confident about their enterprises' API security testing processes 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 the high-risk actions they can take.

These challenges place enterprises on a path to more attacks and wider business impact. This report examines how those pressures are playing out in the key APAC markets of China, India, Japan, and Singapore, and what they reveal about API security in a fast-moving regional context.

About the study

In November 2025, Akamai commissioned Phronesis Partners to survey 1,840 cybersecurity decision-makers on the current state of API security across 10 countries and six industries globally.

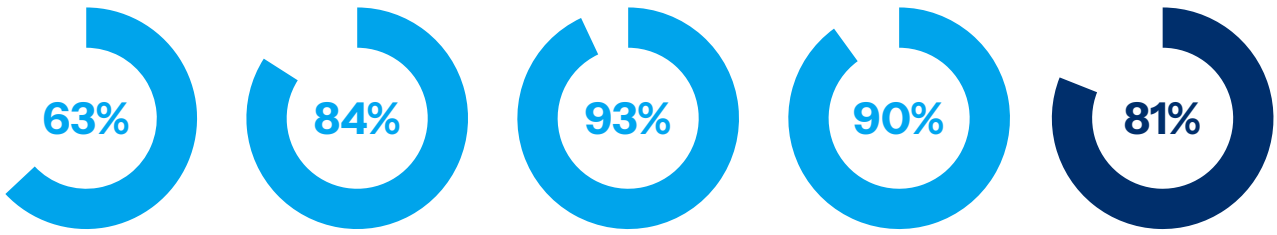
This region-specific report, which accompanies the wider global study, features responses from 640 leaders across C-level, AppSec, and DevSecOps roles based in China, India, Japan, and Singapore.

It reveals the latest leader and team thinking, identifies key region-specific trends, and pinpoints structural API security weaknesses. It also quantifies the cost of maintaining the status quo.

Regional overview: APAC's strengths and weaknesses and the financial impact of weak API security

The four APAC countries featured in our survey may be global leaders in API security, but their ability to track APIs and defend against attacks has failed to keep pace with the growth of large, business-critical, and increasingly AI-connected API estates.

Percentage of organizations that experienced API security incidents in the past 12 months



As shown on the next page, the most common forms of security incidents in China, India, Japan, and Singapore are attacks on APIs linked to enterprise AI applications and LLMs. This is also the type of API security incident that APAC firms say they are least prepared to address.

Top 5 API security incident types in APAC

Q. Which of the following types of API security incidents has your organization experienced in the past 12 months?

Rank	Incident type	APAC average	China	Japan	Singapore	India
1	Attack involving APIs linked to AI technologies (e.g., apps, agents, LLMs)	43%	39%	48%	48%	40%
2	Exploitation of missing or insufficient access controls	37%	36%	32%	43%	39%
3	Data breach and/or data leaks via APIs	36%	43%	31%	40%	35%
4	Exploitation of unmanaged APIs (e.g., shadow or zombie APIs)	34%	22%	36%	36%	40%
5	Exploitation of API misconfigurations	34%	19%	45%	32%	37%

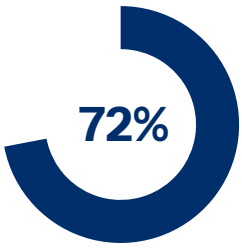
This shortfall in API visibility and security becomes more critical as organizations deploy more AI-enabled applications because APIs connect the models, data, services, and workflows those applications rely on.

Behind the scenes, AI-linked APIs also retrieve data and execute actions, including responding to prompts that may come from an attacker rather than a legitimate user. As those dependencies grow, API weaknesses are more likely to disrupt core business processes rather than remain isolated technical issues.

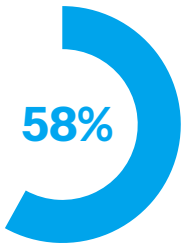
API security strengths in China, Japan, India, and Singapore

APAC organizations in the four markets surveyed are ahead of the global average on API security focus, ownership, and advanced testing. Nearly three-quarters of respondents say their focus on API security has increased, often driven by rapid API proliferation stemming from AI innovation, cloud adoption, and other key business initiatives.

APAC's investment in API security



72% of APAC respondents say their focus on API security has increased over the past year.



58% say their organization has personnel specifically responsible for API security.

40% report advanced, security-focused API testing.

The constant demand for APIs means they are often released hastily, with misconfigurations or missing protections, and without being tested against real-world attack scenarios.

Testing that is security-focused, SDLC-wide, and CI/CD-integrated is critical to ensure resilience against attacks for both APIs and the AI applications that depend on them.

APAC's API visibility and governance gaps

Across the four markets surveyed, many organizations still do not have a complete picture of their API estate as it grows in size and complexity. That gap increases risk because teams cannot assess or protect APIs they have not fully identified.

Many teams still lack a full view of which APIs return sensitive data, even as AI applications make those APIs more exposed and more important to protect.

Most APAC respondents lack visibility into APIs' data-driven risks

Percentage of organizations that have a full API inventory and know which of their APIs return sensitive data

APAC average	22%
China	34%
Japan	11%
India	21%
Singapore	21%

In Japan, for example, just 11% of respondents say they have a full API inventory and know which APIs return sensitive data. That is around half the regional average and makes Japan the lowest-ranked country globally in the study. It is also a significant drop from 2025, when more than three times as many (37%) Japanese respondents said they had full visibility across both measures.

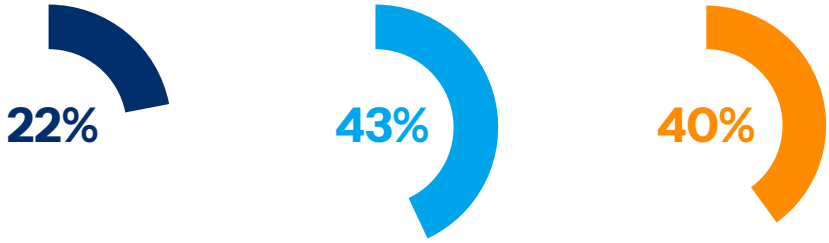
When API security becomes an AI risk

As AI adoption expands, prompting an increase in API estates, the API visibility problem becomes more acute because APIs determine what AI applications can access, return, and trigger.

If teams do not know which AI-linked APIs expose sensitive data, they are less able to spot weak points, test for misuse, or plan for and contain the impact of attacks. At a time when organizations worldwide are expected to spend US$37 billion on generative AI in 2025, including $19 billion at the application layer[1], stronger visibility into AI-linked APIs is becoming a basic requirement for protecting that investment.

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

The API resilience gap in China, Japan, India, and Singapore



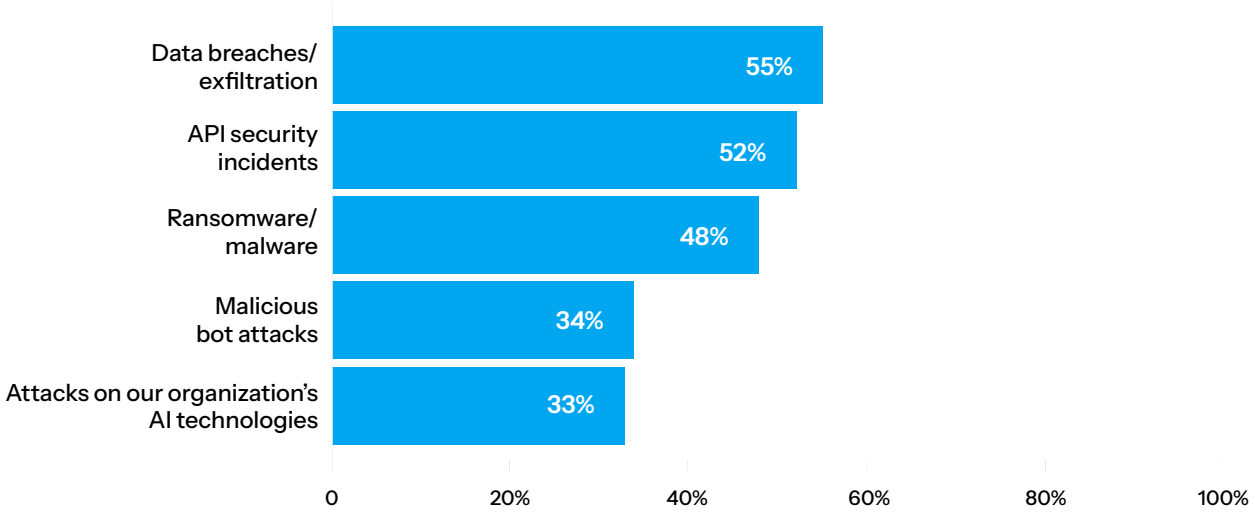
22% of respondents say they have a full API inventory and know which APIs return sensitive data.

43% of organizations were hit by attacks on APIs linked to their AI applications and LLMs.

40% cite poor visibility into APIs and the resulting risks as their biggest worry regarding APIs linked to AI apps and LLMs.

API attacks viewed as a top threat to APAC enterprises' cyber resilience

Q: What are the top 5 cyberthreats that are most important to your organization from the perspective of achieving cyber resilience?



Akamai Security

Featured insights: API security in four APAC countries

China

- 63% of respondents in China experienced an API security incident in the past 12 months.
- Average cost per incident: **US$818,000**
- #1 type of incident: Data breaches and/or data leaks via APIs (43%)
- Percentage who increased focus on API security in the past 12 months: **85%**

Interesting finding: In China, the most frequently cited cause of API security incidents was that WAFs help, but additional protections are still needed. And yet, 80% of Chinese enterprises use WAFs, and only 27% use dedicated API security solutions.

India

- 93% of respondents in India experienced an API security incident in the past 12 months.
- Average cost per incident: **US$497,000**
- #1 type of incident: AI-linked API attacks (40%) and incidents involving unmanaged APIs (40%)
- Percentage who increased focus on API security in the past 12 months: **76%**

Interesting finding: 81% of respondents say their organization has personnel specifically responsible for API security, the highest figure among the four markets. Yet 93% still report incidents, suggesting that ownership alone is not enough without stronger visibility and day-to-day protection.

Japan

- 84% of respondents in Japan experienced an API security incident in the past 12 months.
- Average cost per incident: **US$1.59 million**
- #1 type of incident: Attacks involving APIs linked to AI, e.g. apps, agents, or LLMs (48%)
- Percentage who increased focus on API security in the past 12 months: **64%**

Interesting finding: Japan combines relatively high incident exposure with weak visibility. Only 11% of respondents say they have a full API inventory and know which APIs return sensitive data, down sharply from 37% in 2025.

Singapore

- 90% of respondents in Singapore experienced an API security incident in the past 12 months.
- Average cost per incident: **US$1.33 million**
- #1 type of incident: Attacks involving APIs linked to AI, e.g. apps, agents, or LLMs (48%)
- Percentage who increased focus on API security in the past 12 months: **57%**

Interesting finding: Singapore combines very high incident exposure with some of the largest API estates in the four surveyed markets. While the typical organization sits in the range of 5,000 to less-than 10,000 APIs, the mean inventory is much higher at 46,639.

The financial cost of weak API security

The dedication to API security in China, Japan, India, and Singapore is clear, but organizations in these markets have not yet consistently protected themselves from repeat attacks or their financial impact.

An average API security incident in the region costs more than US$1 million.

The financial impact is greatest in Japan and Singapore. The average incident cost in Japan is particularly notable because it has increased by nearly 200% (196.8%) year-on-year, reaching more than US$1.5 million in 2026. Repeat incidents also remain common, with more than half of incident-hit organizations reporting four or more incidents.

The financial impact of incidents

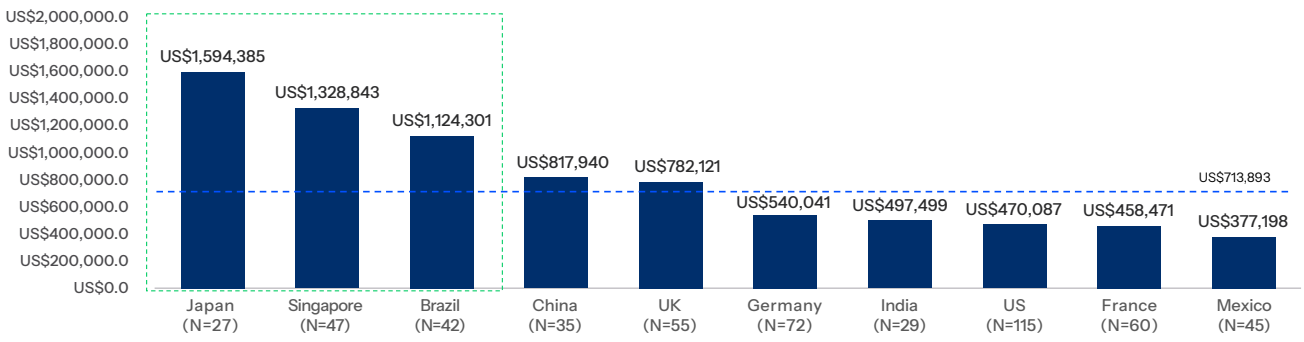
US$1 million

The average cost of an API security incident in APAC stands at **more than US$1 million**.

The largest overall costs result from repairs, remediation, and downtime from **unavailable services**.

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

Average financial cost of API security incidents in 2025 vs. 2026

Country/benchmark	2025 Avg. incident cost (USD)	2026 Avg. incident cost (USD)	Change (2026 vs. 2025)
China	$780,236	$817,940	$37,704
India	$708,617	$497,499	($211,118)
Japan	$537,127	$1,594,385	$1,057,258
Singapore		$1,328,844	

Organizations in the region may be paying more attention, assigning more responsibility, and testing their APIs more thoroughly, but repeat incidents and high costs show that visibility and protection are still not strong enough.

Top six impacts of API security incidents in APAC

What costs and/or impacts, if any, have API security incidents had or are likely to have on your business?

Rank	Cost/impact	APAC average	China	Japan	Singapore	India
1	Loss of customer goodwill and churned accounts	37%	35%	46%	30%	33%
3	Loss of trust and reputation	34%	40%	35%	30%	31%
3	Loss of productivity	33%	30%	33%	33%	35%
4	Costs incurred to help fix the security issue	30%	48%	21%	29%	28%
5	Service downtime/outage	24%	26%	25%	22%	24%
6	Negative impact on department's reputation with senior leaders and/or board of directors	24%	15%	23%	29%	29%

Akamai Security

Three key regional insights

Regional insight 1:

Visibility is getting harder to sustain as APAC's API estates grow

Across the four surveyed APAC markets, the typical organization now has about 5,700 APIs in its inventory, while the largest estates in the top quartile exceed 32,300 APIs. As these estates continue to grow larger and more complex, keeping track of APIs and establishing which return sensitive data becomes harder.

Weak visibility has consequences for APAC enterprises' AI investments. 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, it is the API that finds the data and brings it to the requestor, no questions asked.

While nearly all (95%) of respondents across the four surveyed APAC markets *say* their organization factors APIs into regulatory compliance requirements, far fewer are taking the practical steps needed to support that claim.

- **40% factor APIs** into regulator-required reporting
- **59% factor APIs** into security plans
- **63% factor APIs** into risk assessments

This shortfall indicates a significant compliance weakness because APAC regulations increasingly expect organizations to prove they understand and protect API-linked data flows. For example:

- **China's Data Security Law** requires strong measures to secure customer data exchanged across APIs.
- **Japan's Act on the Protection of Personal Information** requires impact assessments for high-risk processing activities that can include APIs.
- **India's Digital Personal Data Protection Act** requires mechanisms to detect breaches, including those occurring via APIs.

Without clear visibility into which APIs exist, which expose sensitive data, and how they are protected, organizations cannot easily produce the evidence regulators now expect.

Regional insight 2:

Repeated incidents reveal where API security is inadequate

API security incidents remain widespread across APAC. Four-fifths of respondents say their organization experienced an API security incident in the past 12 months, and repeat attacks remain common once organizations are hit.

However, regional averages mask sharp differences between markets. For example, 93% of Indian and 90% of Singaporean organizations experienced an API security incident in the past year, while 63% of Chinese respondents said their APIs had been targeted. Satisfaction with current resilience against attacks is also uneven, with 54% of Chinese respondents saying they are content, compared to 42% in India, 25% in Japan, and 18% in Singapore.

API security incident frequency across China, Japan, India, and Singapore

81%

81% of respondents say their organization experienced an API security incident in the past 12 months.

The average number of incidents in APAC is 3.6.

Among incident-hit organizations, over half (56%) say they experienced four or more API-related incidents.

The high number of repeat incidents suggests the challenge for APAC organizations is no longer simply preventing attacks; it is understanding that they are inevitable and will grow in scope as attackers embed AI into their own tactics. Repeat incidents point to underlying weaknesses in day-to-day API protection and response.

The regional incident mix reveals where API governance and security is weakest

The most common incident types across the four countries involve APIs that are hardest to govern: AI-linked APIs, unmanaged APIs, misconfigured APIs, and insufficiently secured third-party APIs.

That pattern shows that the hardest-to-locate APIs are also the ones most often involved in incidents.

There is also a clear disconnect between the C-suite and frontline AppSec and DevSecOps teams in how prepared they believe their organizations are for API-related attacks.

In APAC, overall, 50% of respondents say they are well or fully prepared for attacks involving AI-linked API. However, when we examine the responses by role, it's clear that IT security leaders (CISO, CIO, CTO) are consistently more confident than implementation teams (AppSec and DevSecOps practitioners). Across the full sample, 56% of C-suite respondents say they are well prepared or fully prepared for this incident type, compared with 44% of AppSec.

Regional insight 3:

The region is making progress on API security, but not all markets are equal

Across the four markets surveyed, organizations are increasing focus on API security, assigning clearer responsibility for it, and strengthening testing. However, regional averages tell only part of the story. China and India are helping pull APAC forward, while Japan and Singapore show that progress is still inconsistent and, in some cases, fragile.

Measure	APAC	China	India	Japan	Singapore
Focus on API security increased over past year	72%	85%	76%	64%	57%
Personnel specifically responsible for API security	58%	56%	81%	44%	49%
Advanced, security-focused API testing	40%	58%	29%	33%	40%
Security testing fully embedded across API SDLC and CI/CD	19%	28%	17%	15%	14%

China is the clearest pacesetter. Eighty-five percent of respondents say focus on API security has increased, and 58% report advanced security-focused testing, which entails:

- Full integration across software development lifecycle (SDLC) and CI/CD pipelines
- Analyzing APIs for OWASP API Security Top 10 risks
- Running automated tests that simulate malicious traffic
- Prioritizing vulnerabilities by impact for rapid remediation

This regional leadership is not new. In 2025, China was the only APAC market we surveyed to rank "securing APIs from threat actors" as its top cybersecurity priority. In 2026, that priority has shifted toward securing AI technologies against attacks, in line with the global picture. But the connection remains direct: Secure APIs are part of what helps make the AI applications, agents, and LLMs they connect to more resilient.

India stands out on ownership. Eighty-one percent of respondents say their organization has personnel specifically responsible for API security, and 76% report increased focus on API security over the past year. Japan is weaker on some core measures. Only 44% say their organization has dedicated API security personnel, and 33% report advanced testing. Singapore trails on momentum, with 57% saying focus on API security has increased.

Full API testing integration remains limited

While 40% of APAC respondents report advanced, security-focused API testing, only 19% say security testing is fully embedded across the API SDLC and CI/CD. That indicates stronger testing is becoming more common, but full integration into development and deployment remains limited.

Takeaway: *APAC has real strengths to build on, but they are unevenly spread. Some countries are increasing focus, assigning clearer responsibility, and putting better testing in place, while others still lag on the basics that support API resilience.*

Conclusion

APAC is moving forward, but the governance and security gap is still real

The four APAC countries we surveyed are making real progress on API security. More organizations are increasing focus, assigning clearer responsibility, and strengthening testing as APIs become more central to digital services and AI applications.

But that progress has not yet translated into consistent protection

Many organizations still do not have a clear view of which APIs expose sensitive data, and repeated incidents suggest those gaps are not being closed fast enough.

Progress is also uneven across the four markets surveyed. Some are building stronger day-to-day API security practices, while others remain more exposed to poor visibility, weaker testing, and heavier incident impact.

The region has clear strengths to build on. The task now is to transfer that momentum into everyday security practice, especially across the APIs that are hardest to track, govern, and secure. That will become increasingly important as business-critical AI applications depend on APIs that organizations need to see clearly and secure consistently.

Learn how Akamai can help you secure your enterprise against common API attack methods highlighted in the OWASP API Security Top 10 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 05/26.