API SECURITY IMPACT STUDY 2025

The Costs of API Attacks in 4 APAC Countries

How security teams in China, Japan, India, and Australia view the impacts of compromised APIs

Akamai

An affiliate publication of **Akamai State of the Internet (SOTI) reports**

Contents

Introduction

Attacks on application programming interfaces (APIs) are becoming more frequent, more sophisticated, and grander in scale. In fact, **108 billion API attacks were recorded from January 2023 through June 2024**, according to a recent Akamai State of the Internet (SOTI) report.

And yet, despite the rapid proliferation of APIs in the enterprise and the access to sensitive data that many of these APIs require, research indicates that securing them has not been a top priority for most security teams. As organizations struggle with poor visibility into APIs and their risks, the findings align with industry concerns that enterprises lack centralized responsibility for API security, from tracking vulnerabilities to measuring the impact of breaches.

The latest installment of the API Security Impact Study collects responses from more than 800 individuals in roles across cybersecurity to determine the state of API security in four of the largest economies in the Asia-Pacific (APAC) region: China, India, Japan, and Australia. It builds upon an annual survey conducted by Noname Security (now a part of Akamai Technologies) asking security professionals how APIs have fit into their security initiatives over the past three years. Consistently, our research has found that despite a growing awareness of API vulnerabilities, the commitment to API security from senior leadership has not kept pace, as both CISOs and CIOs struggle to address a growing scope of competing priorities.

In 2024, the **API Security Impact Study** expanded its traditional scope of organizations in the United States and the United Kingdom to encompass Germany. It found that:

- API security incidents had risen for the third straight year.
- Estimates of the cost of responding to these incidents averaged more than half a million dollars (nearly a million, according to IT and security leaders).
- Most respondents recognized the stress and reputational damage that these incidents cause for security teams.

This survey's respondents comprised C-suite executives (CISOs, CIOs, and chief technology officers), senior security staff, and AppSec team members working in companies in eight sectors:

- Automotive
- Financial services
- Retail/ecommerce
- Healthcare
- Insurance
- Government/public sector
- Manufacturing
- Energy/utilities

The findings reveal valuable insights into API security practices and priorities, including:

- The causes of API security incidents
- Overall cybersecurity priorities
- Costs associated with API security incidents, such as fines and remediation expenses
- API security incidents' impacts on security teams
- The state of API inventorying and testing practices
- Awareness of which APIs return sensitive information
- The status of API security in regulatory compliance efforts

What is an API security incident?

Incidents can include API abuse, API attacks, API-focused data breaches, and overall attempts to compromise APIs by malicious actors.

Executive summary

The results of this survey provide valuable insights for security teams and leadership across the APAC region and several industries, but a few high-level trends stand out.

1. **China is making API security a vital part of its cybersecurity strategy.** This stands in contrast to other regions who may not be paying sufficient attention to API security. In China, respondents listed "securing APIs from threat actors" as their top priority. In the 2024 API Security Impact Study, respondents from the U.S., the U.K., and Germany ranked "securing APIs from threat actors" as their ninth-highest priority, after other priorities like "defending against generative AI (GenAI)-fueled attacks" and "defending against ransomware." China also had the highest estimate of the cost of addressing API security incidents over the 12 months prior, at CN¥5,687,373 (US$778,271*).

> **"Securing APIs from threat actors"** | #1 cybersecurity priority in the next 12 months for Chinese respondents

2. **A disconnect remains between crucial enterprise roles.** The results varied by role, country, and industry, but one clear message emerged overall: C-suite, senior security professionals, and AppSec teams are misaligned in their understanding of the costs, causes, and organizational impacts of API security incidents as well as their organizations' visibility into APIs.

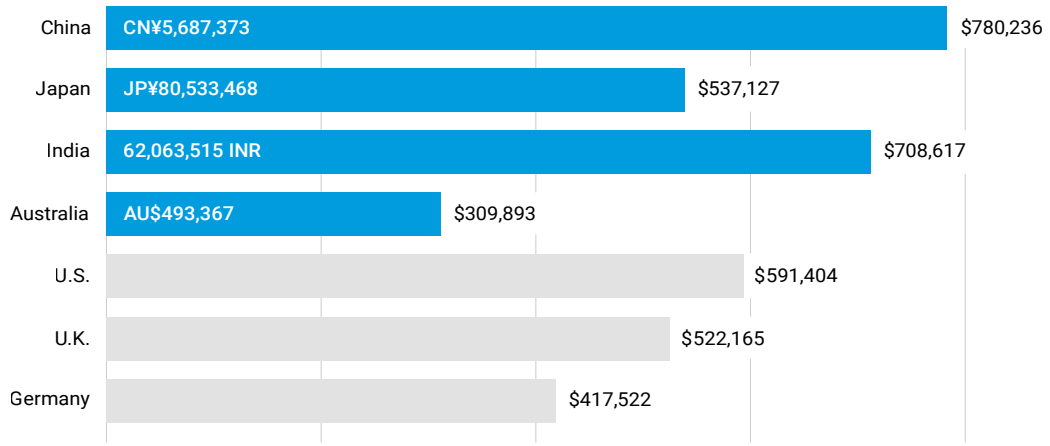
For example:

- In China, C-suite respondents' estimates of the costs of API security incidents were almost double other roles' estimates.
- In Japan, there was no agreement among enterprise roles regarding the top causes of the API security incidents their organizations experienced.
- In India, far more C-suite (77%) and senior security professionals (75%) reported having a full inventory of their APIs than did AppSec teams (41%).
- Overall, 92% of C-suite respondents said their organizations had experienced an API security incident in the last 12 months, compared with 80% of AppSec teams.

*All currency conversions as of March 27, 2025

If you have experienced an API security incident, what has been the estimated total financial impact of these incidents combined?

Average estimated cost of API incidents over the past 12 months

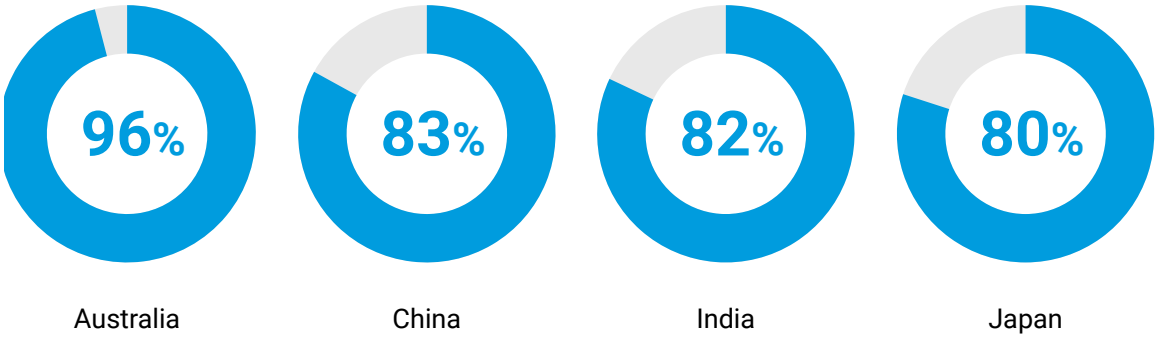


3. **The impacts of API security incidents are not limited to a single, overwhelming event.** Rather, the survey results reveal that the impacts of API attacks and abuse reach far and wide. The respondents viewed the top impacts differently depending on their roles and regions. Some viewed the financial impact (e.g., cost of remediating an API attack the security team didn't see coming) as the most important, while others saw the loss of trust following an attack (e.g., damaged reputation with the board of directors) as the largest impact; Japanese respondents ranked this as the number one impact.

> **"It hurt our department's reputation with our senior leaders and/or board of directors."**

#1 impact of API security incidents, according to Japanese respondents

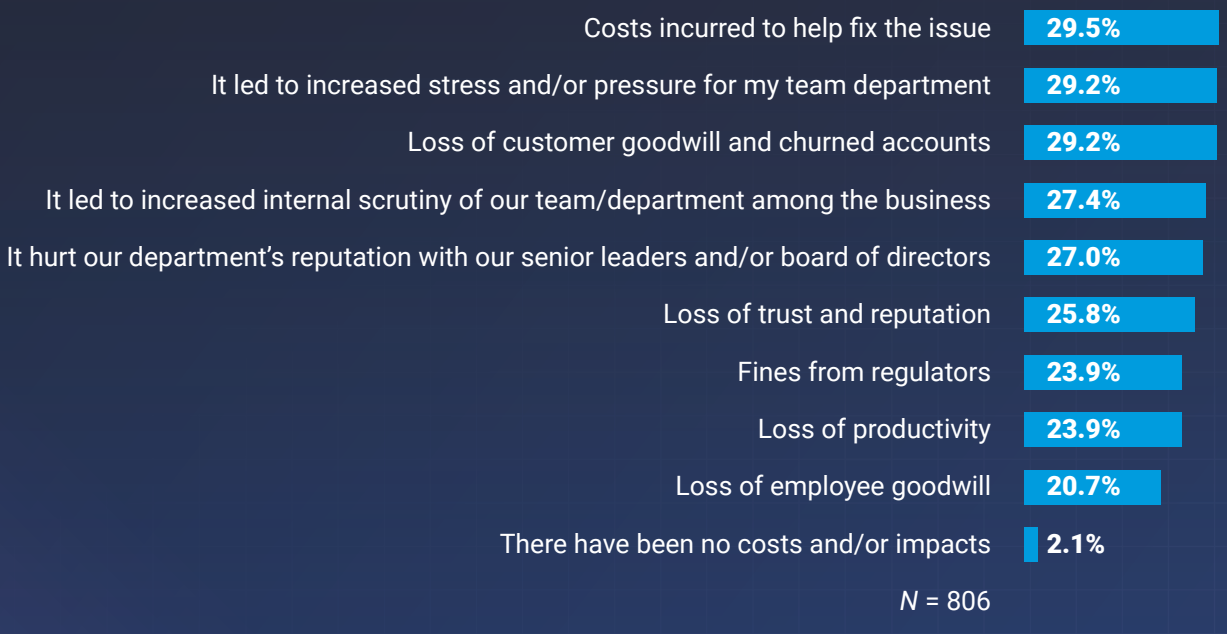
4. Organizations across the four countries are facing regular API security incidents right now.



These results closely align with those of our last report, in which 84% of respondents from the U.S., the U.K., and Germany said they had experienced an incident in the last 12 months.

Ranking API security incidents' impacts in China, Japan, India, and Australia

What costs and/or impacts, if any, have API security incidents had on your business? *(Select up to 3)*



Regional trend snapshot

While the four countries have significant regulatory, political, and economic differences, the results do provide valuable insights into the maturity of API security initiatives in general. The study's findings also provide useful benchmarking data for professionals establishing their own API security priorities. Clearly, attackers are setting their sights on APIs. Akamai's **2024 State of the Internet Report on API Security: Shining a Light on API Threats** showed that API attacks are becoming a greater concern in APAC. The Akamai research revealed that 15% of all web attacks in the APAC region targeted APIs. On a global basis, the APAC region had the third-highest percentage of API attacks, behind Europe, the Middle East, and Africa (EMEA) at 48% and North America at 27%.

As organizations prepare to meet the challenge of this growing attack vector, these survey results demonstrate that upper management and front-line staff need to reach a consensus on important baseline issues like the number of API security incidents they're facing, their root causes, and the costs associated with them in terms of both the bottom line and reputational damage.

How much of a priority is API security?

For China, API security is the top priority. All respondents were asked to rank their cybersecurity priorities for the coming year. China, the world's second-largest economy, was a bit of an outlier here, being the only country to list "securing APIs from threat actors" as its top priority.

What are your business's main cybersecurity priorities in the next 12 months? (Select up to 3)

China

1. Securing APIs from threat actors — 27.6%
2. Securing privileged IT access — **24.6%**
3. Securing applications — **24.1%**
4. SIEM — **24.1%**
5. Data loss prevention — **22.2%**

Japan

1. Defending against ransomware — **25.5%**
2. SIEM — **25.5%**
3. Data loss prevention — **25.0%**
4. Securing APIs from threat actors — 22.0%
5. Securing applications — **22.0%**

India

1. Cloud security solutions — **26.9%**
2. Managing and securing developer secrets — **24.9%**
3. Securing applications — **23.4%**
4. Securing APIs from threat actors — 22.9%
5. Securing privileged IT access — **29.9%**

Australia

1. Securing endpoints — **26.2%**
2. Managing and securing developer secrets — **24.3%**
3. SIEM — **23.8%**
4. Securing APIs from threat actors — 22.8%
5. Data loss prevention — **22.8%**

China's focus on APIs may be a function of Chinese security staff's estimates of API security incidents' costs:

- Senior security professionals: CN¥6,733,916 (US$924,000)
- AppSec teams: CN¥6,622,503 (US$920,000)

In each of the other countries, "securing APIs from threat actors" ranked as the fourth-highest priority. In the aggregate, "securing APIs from threat actors" ranked second, behind security information and event management (SIEM).

Little consensus on cost

While senior security professionals (CN¥6,733,916, or US$925,478) and AppSec teams (CN¥6,622,503, or US$910,166) in China had high estimates for the costs of API security incidents, their C-suite counterparts' estimates were far lower (CN¥3,750,897, or US$517,293, on average). This discrepancy among roles was also observed in Japan and India but not in Australia. However, the discrepancy was not just between the C-suite and front-line staff. In Japan, for example, senior security professionals had the highest cost estimates, while AppSec teams had the lowest. This discrepancy between roles suggests a lack of common understanding of how much API security incidents cost organizations. It also explains the disconnect between roles regarding how much they should prioritize API security. If these roles can't agree on the financial impacts of API security incidents on their business, API security is unlikely to be high on their priority list.

Organizations recognize that API security incidents are happening but are confused about how often

There is also a disconnect about the frequency of API security incidents. Previous API Security Impact Studies in other regions have shown a steady rise in the number of incidents in those regions over time. But without previous years' data on China, Japan, India, and Australia to compare, it's impossible to measure how much API security incidents have risen in these countries. Still, it is clear that organizations are aware of the threat. Overall, 85% of the surveyed organizations said they had experienced an API security incident in the past 12 months, with Australia exhibiting the highest frequency at 95%.

API security incidents prevalent across China, Japan, India, and Australia

Overall, 85% of organizations said they had experienced an API security incident in the past 12 months, with Australia exhibiting the highest frequency at 95%.

The results also show a gap between leadership's and front-line staff's understanding of the frequency of API security incidents. Overall, 92% of C-suite respondents said they had experienced an API security incident in the last 12 months, compared with 83% of security professionals and 80% of AppSec teams. This gap was larger in some countries, notably China, where 97% of C-suite respondents reported incidents, compared to 78% of security professionals and 74% of AppSec teams.

Impact of API security incidents widespread

Attacks on a vulnerable API can have profound impacts across an organization that extend beyond the costs associated with correcting them and the damage to the organization's public reputation. The impacts of an attack can also include regulatory fines, loss of customers (or churn), and internal reputational damage, as well as increased employee stress for security teams (the top impact cited by respondents in the U.S., the U.K., and Germany).

The results suggest that organizations in the four APAC countries are feeling the impact in many places. When asked about the costs and impacts of API security incidents for their businesses, none of the four countries identified a single overwhelming factor. When the four countries were asked to provide up to three costs or impacts, "costs incurred to help fix the issue" emerged as the top factor (29.5%), followed closely by "it led to increased stress and/or pressure for my team/department" (29.2%) and "loss of customer goodwill and churned accounts" (28.8%). Among the other options, "loss of employee goodwill" (20.7%) had the lowest score, followed distantly by "there have been no costs and/or impacts" (2.1%).

Lack of clarity on causes of API security incidents

According to the respondents, "API misconfigurations" was the most likely cause of an API security incident, being the most cited cause in Australia and India and the second most cited in China. However, no API vulnerabilities clearly stood out in any of the countries surveyed. In the aggregate results, when respondents were asked to select up to three responses, "API misconfigurations" (22.3%) was followed by "the network firewall didn't catch it" (20.8%), "API gateway didn't catch it" (20.7%), and "authorization vulnerabilities" (20.6%).

The top six responses were within a couple of percentage points of one another. This suggests that organizations realize that API vulnerabilities persist across vectors and that there are widespread weaknesses in their API security efforts. These are the takeaways for security teams:

- The shared focus on API misconfigurations is probably justified. Security misconfiguration is the number eight risk on the widely followed OWASP API Security Top 10 list and can lead to vulnerabilities like Broken Object Level Authorization (OWASP's number one), broken authentication (OWASP's number two), and excessive data exposure (OWASP's number three).
- The prevalence of commonly used security tools (e.g., network firewalls, web application firewalls [WAFs]) that are not designed to catch the growing number of more sophisticated attacks could also be cause for concern. While these tools provide baseline protections, fast-evolving API attack methods call for more comprehensive API security.

Ranking API security incidents' causes in China, Japan, India, and Australia

What do you believe are the causes of the API security incidents your organization has experienced?
(Select up to 3)

Aggregate findings for the four surveyed APAC countries

API misconfigurations	**22.3%**
The network firewall didn't catch it	**20.8%**
API gateway didn't catch it	**20.7%**
Authorization vulnerabilities	**20.6%**
API had unintended exposure to internet	**19.6%**
APIs in GenAI tools such as large language models (LLMs)	**19.2%**
Vulnerability due to API coding errors	**18.7%**
Mid-tier software solution (Slack)	**18.7%**
Lack of API authentication controls	**18.1%**
Web application firewall didn't catch it	**17.5%**
Unmanaged APIs (e.g., dormant or zombie API)	**16.6%**
Software solution downloaded from the internet	**16.3%**
A well-known technology tool/service (Microsoft, etc.)	**15.8%**
We haven't ever experienced an API security incident	**2.6%**

N = 806

Awareness of sensitive data in APIs

Overall, more than 70% of respondents said they have a full inventory of their APIs. Knowing which of those APIs return sensitive data was trickier, however. Just 37% of respondents claimed to have a full inventory and to know which of their APIs return sensitive data. These results differed substantially by role as well. Forty-four percent of C-suite respondents said they know which APIs return sensitive data (although that dropped to 31% among CISOs alone), compared to 37% of AppSec teams and 28% of senior security professionals.

In Japan, far more AppSec respondents claimed to know which APIs return sensitive data (64%) than did C-suite respondents or senior security professionals (24%). Considering how easily an attacker can submit fraudulent calls to APIs and get sensitive data in return, this is an area where security teams cannot afford to have misalignment between roles.

API vulnerabilities extend to AI

Among all four countries, three times more CIOs than CISOs blamed their API security incidents on vulnerabilities in their organizations' GenAI technologies.

Their concern is justified.

The AI-powered applications and LLMs organizations deploy often depend on APIs for missing functionality, integration, and the exchange of data. Attackers can exploit AI security gaps through tactics such as:

- Prompt injection attacks: Attackers manipulate AI-generated responses to leak sensitive data or bypass security measures.
- Data exfiltration and model theft: Attackers attempt to extract proprietary knowledge from AI models.

With only 37% of respondents saying they know which of their APIs return sensitive data, the growing threat to GenAI applications and LLMs should be a high priority for both IT and security leaders.

Across all four countries surveyed, the top three industries that cited GenAI vulnerabilities as the number one cause of their API security incidents were:

1. Government/public sector
2. Energy/utilities
3. Insurance

Breakdowns by country

China prioritizes API security

In terms of cybersecurity priorities for the coming year, China stood out among the four countries for prioritizing API security. “Securing APIs from threat actors” received the highest overall score, topping the priority list for 27% of Chinese respondents. “Securing privileged IT access” came in second and was the top priority for energy/utilities, financial services, manufacturing, automotive, and healthcare.

Perhaps unsurprisingly given these results, China was also a leader in API testing. More than half of Chinese respondents said they conduct testing in real time (22%) or daily (28%). That figure was as high as 65% among AppSec teams. This focus on testing is important. Many of the API vulnerabilities that organizations cite as incident causes can be identified and remediated before a developer team releases an API to the public.

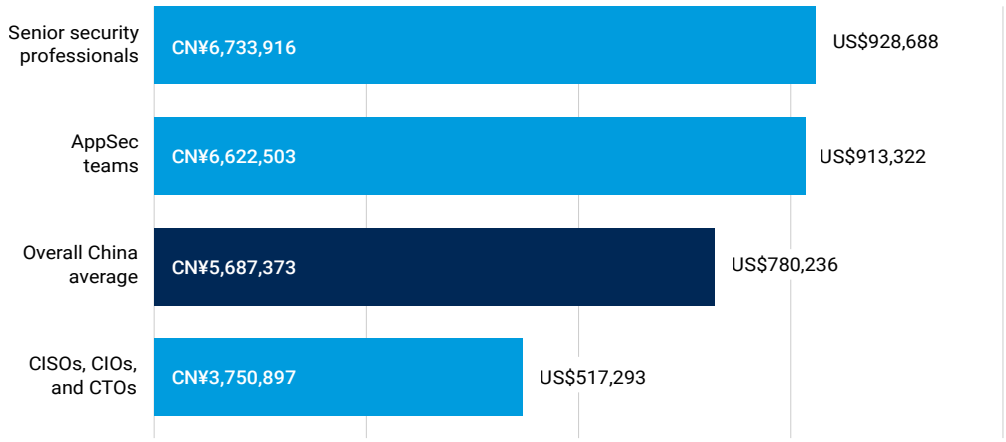
In China, senior leadership saw API security incidents as a clear issue in the last year. Nearly all C-suite respondents (97%) reported an API security incident, reflecting a 20-point gap between front-line staff. Retail was the industry with the highest prevalence of incidents in the past year, with 100% reporting an incident, whereas insurance had the lowest prevalence at 72%.

However, the C-suite thinks incidents cost far less than front-line staff do.

In China, 97% of CISOs, CIOs, and CTOs reported experiencing an API security incident, reflecting a 20-point gap between C-suite leaders and front-line security staff.

If you have experienced an API security incident, what has been the estimated total financial impact of these incidents combined?

Cost of API security incidents according to Chinese security leaders and practitioners



There was some disagreement among Chinese respondents about the biggest impacts of API security incidents. While AppSec teams cited financial impacts, C-suite respondents listed stress/pressure on their teams. This is perhaps unsurprising given that C-suite respondents had the lowest estimates for costs associated with API security incidents. Interestingly, automotive, government/public sector, and insurance were the only industries to rate "costs incurred to help fix the issue" as the top impact.

In line with this, the C-suite had a much more positive outlook (53%) than their practitioner counterparts about their knowledge of which APIs return sensitive data (senior security professionals: 25%; AppSec teams: 40%). These roles were roughly aligned on whether they have a full API inventory.

The top reported causes of API security incidents in China were:

- "The network firewall didn't catch it"
- "API misconfigurations"
- "API gateway didn't catch it"

"Vulnerability due to API coding errors" came in a close fourth, even though many of the Chinese respondents reported testing in real time. A total of 50% of retail/ecommerce respondents listed "the network firewall didn't catch it" as the top cause of incidents, representing the highest level of consensus among the industries for China. Among the other industries, the top causes were only mentioned by roughly 40% of respondents or less, and other industries blamed factors inherent to the APIs themselves, such as API misconfigurations. Chinese respondents in retail/ecommerce also exhibited greater consensus in terms of their top cybersecurity priority for the next 12 months, with 50% citing "data loss prevention."

Do you know which of your APIs return sensitive data?

Only 39.4% of Chinese respondents with full API inventories said they know which of their APIs return sensitive data. C-suite respondents had a much more positive outlook than their practitioner counterparts about their knowledge of this important API risk factor:

- CISO, CIOs, CTOs: 53%
- Senior security professionals: 25%
- AppSec teams: 40%

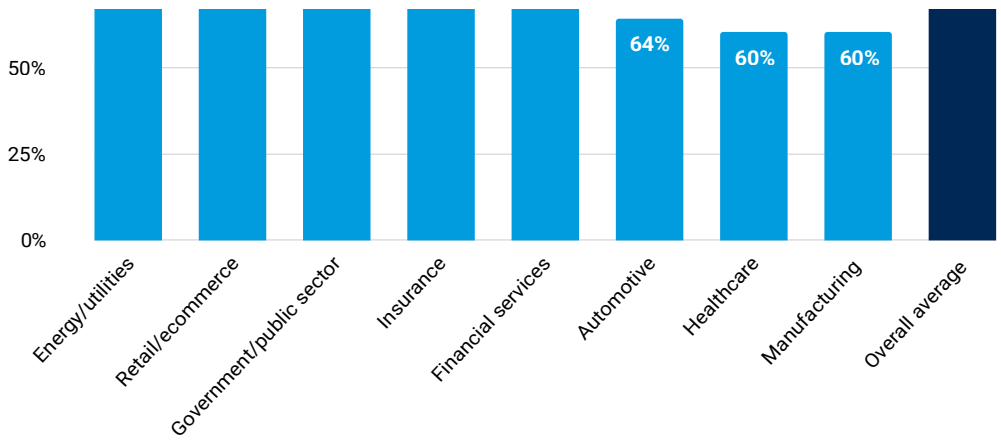
Japan gives lower priority to APIs, while API-rich industries see fewer incidents

In Japan, “securing APIs from threat actors” was the fourth-highest security priority, behind “defending against ransomware,” “SIEM,” and “data loss prevention.” However, “securing APIs from threat actors” was more important for senior security professionals, who listed it as their top priority alongside “defending against ransomware.” “Securing APIs against threat actors” was also a top priority in Japan’s automotive industry, an important data point given that only 8% of respondents in that industry said they know which of their APIs return sensitive data.

While roughly 80% of respondents in Japan reported an API security incident in the 12 months prior (much lower than in China), surprisingly, only 60% of Japanese respondents in API-rich industries like automotive, healthcare, and manufacturing reported incidents. In terms of roles, the C-suite was in line with AppSec teams, with approximately 83% of both reporting incidents.

Have you experienced an API security incident in the past 12 months?

How Japanese industries stack up versus the country’s overall average



Fewer respondents in Japan cited security tools as a top cause of incidents than in other countries, and more cited external tools. “Software solution downloaded from the internet” (22%) was the most reported cause, while “mid-tier software solution (Slack)” came in fourth (21%). Interestingly, “a well-known technology tool/service (Microsoft, etc.)” came in last (15%).

Estimated cost of an API security incident in Japan:

- Overall: JP¥80,500,000 (US$528,000)
- C-suite: JP¥74,000,000 (US$485,000)
- Healthcare: JP¥33,216,389 (US$218,000)
- Senior security professionals: JP¥115,000,000 (US$754,000)
- AppSec teams: JP¥56,000,000 (US$367,000)
- Automotive: JP¥228,000,000 (US$1,500,000)

In Japan, the internal impacts of an API security incident were felt most strongly by AppSec team members. “It hurt our department’s reputation with our senior leaders and/or board of directors” was the top result among the AppSec subset, while “it led to increased internal scrutiny of our team/department among the business” came in third place. “It led to increased stress and/or pressure for my team/department” was fourth.

The second-largest impact for Japanese respondents overall involved damage to a company’s external reputation, namely “loss of customer goodwill and churned accounts.” And this wasn’t just the case for businesses. Japanese government organizations also cited goodwill and churn as they apply to citizens as the largest impact.

Nearly 80% of Japanese respondents said they have a full API inventory. Meanwhile, 37% said they know which APIs return sensitive data, but there was a significant disparity across industries. Only 8% of respondents in the Japanese automotive and financial services industries reported that they know which APIs return sensitive data, a stark contrast with retail/ecommerce (80%) and government/public sector (64%).

There was also a discrepancy across roles, with just 23% of C-suite and senior security professionals claiming to know which APIs return sensitive data, compared to 64% of AppSec teams.

Only 11% of Japanese respondents conduct API testing in real time, significantly lagging China’s 22%. However, nearly 20% of Japanese senior security professionals said they test in real time, while 12% said they don’t test their APIs at all because of a lack of resources. Similarly, in the Japanese healthcare industry, 20% of respondents said they don’t test at all because of a lack of resources. There is some level of API testing happening in most organizations, however. For Japan overall, just 4% of respondents said they don’t test their APIs at all.

Japanese automakers lack visibility into API risks

Only 8% of Japanese auto companies know which of their APIs return sensitive data. Given the importance of the automotive sector to Japan’s economy — and how frequently companies are embedding API-rich technology into products like connected vehicles — this is somewhat of a surprise. It’s difficult to secure what you cannot see.

API security and compliance in Japan

Nearly 90% of respondents in China, India, and Australia say they factor API security into meeting regulatory requirements. This is less likely in Japan, where 22% of respondents say they do not factor API security into their compliance efforts, citing:

- Lack of time or resources
- Belief that regulators aren’t requiring it yet

Japan’s overall response was heavily informed by the C-suite: 28% of Japanese CISOs, CIOs, and CTOs say APIs don’t have a place in their compliance programs.

India results show significant disconnect between staff and leadership

India was fairly in line with Japan in terms of the prevalence of API security incidents. Overall, 82% of respondents in India said they had experienced an API security incident in the past year, with every respondent in the energy/utilities industry (100%) reporting an incident. The insurance industry had the lowest prevalence, with 60% of respondents reporting an incident.

Similarly to the overall results in other countries, in India, "API misconfigurations" was the most reported cause of API security incidents (23%), followed closely by "a well-known security tool/service (Microsoft, etc.)" (22%) and "APIs in GenAI tools" (22%). Here are a few additional highlights on API security incidents' causes in India:

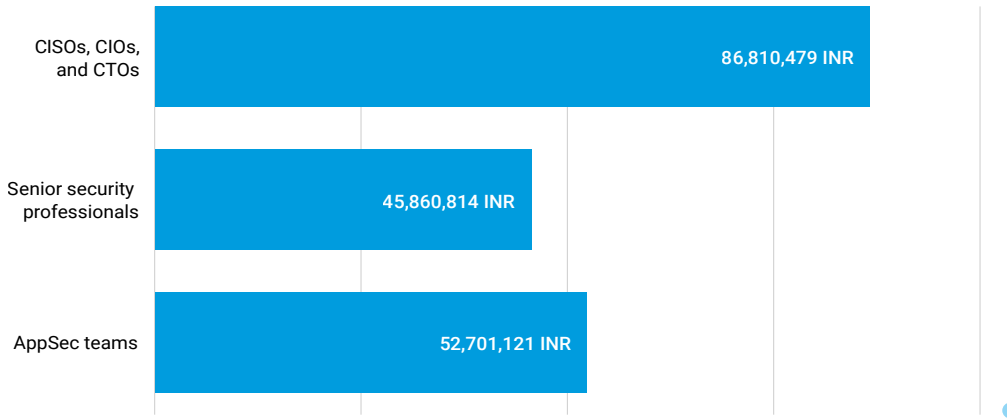
- Respondents blamed "vulnerability due to API coding errors" the least.
- Energy/utilities and healthcare were the industries that blamed APIs in GenAI tools such as LLMs the most.
- Senior security professionals' top-cited cause was vulnerabilities in GenAI tools, nearly 10 percentage points above the overall average in India.
- Manufacturing and retail/ecommerce blamed well-known external tech tools or services the most.

API security incidents tended to affect Indian businesses in terms of internal, employee-based factors, with most respondents citing "it led to increased internal scrutiny of our team/department among the business" (32%) and "it led to increased stress and/or pressure for my team/department" (31%) as the largest effects. The insurance and retail/ecommerce industries cited "loss of customer goodwill and churned accounts" as the biggest impact.

The average reported cost of an API security incident in India was 62,063,515 rupees (INR), and here, too, C-suite executives' estimates were much higher than those of front-line security staff.

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

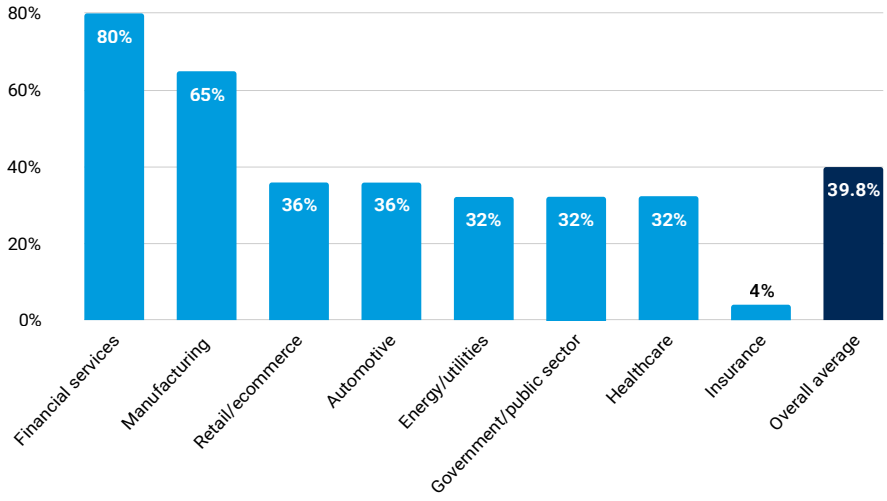
How Indian security leaders and staff view the costs of API incidents



Two Indian industries in particular brought the overall average cost up: financial services (128,288,777 INR, or US$1,480,552) and retail/ecommerce (117,978,722 INR, or US$1,361,566).

In India, 64% of respondents reported having a full inventory of APIs, but among them, 39% said they know which APIs return sensitive data. This result is fairly in line with China (39.4%) and Japan (37%) but higher than Australia (27.9%). Most respondents in financial services (80%) and manufacturing (65%) said they know which APIs return sensitive data, while only 4% of those in insurance said they know.

Do you have a full API inventory *and* do you know which APIs return sensitive data?
How Indian industries compare to the country's overall average



The gap in visibility was more pronounced by role:

- C-suite (77%) and senior security professionals (75%) were far more likely to report having a full inventory of APIs than AppSec teams (41%).
- C-suite (65%) and senior security professionals (43%) were also far more likely to report knowing which APIs return sensitive data than AppSec teams (11%).

This may be why AppSec teams listed "securing APIs from threat actors" as their top priority (24%), versus C-suite executives, who were more likely to prioritize "cloud security solutions" (35%). Meanwhile, senior security leaders cited "managing and securing developer secrets" (36%) as the top priority on average.

Overall, "securing APIs from threat actors" (21%) came in as the fourth-highest cybersecurity priority in India, behind "cloud security solutions" (27%), "managing developer secrets" (25%), and "securing applications" (23%).

This brings us to an important topic: the role of API testing. Of the four countries surveyed, India blamed "vulnerability due to coding errors" the least for their API security incidents — ranking it last among 13 causes. Because coding errors happen during development, it's worth exploring how frequently organizations test APIs. The challenge is that without real-time testing, it can be difficult to even know if an API attack was caused by a coding error. And if an enterprise can't see a vulnerability, it's not likely to cite it as the cause of an attack.

We asked respondents how often they undertake API security testing (during production and throughout the full API lifecycle) for signs of abuse. Here is a breakdown of overall API testing frequency in India:

- Weekly: 31%
- Daily: 21%
- In real time: 15%

Focusing solely on organizations that test their APIs in real time, here is a breakdown showing how Indian industries stack up versus the overall average of 15%:

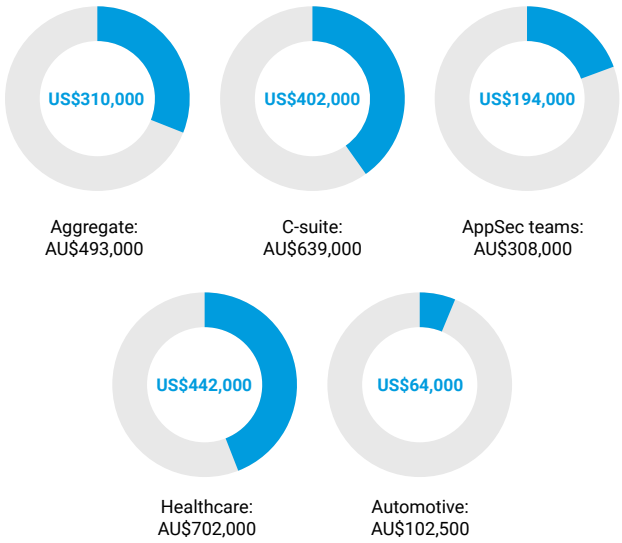
- Financial services: 24%
- Healthcare: 20%
- Manufacturing: 19%
- Automotive: 4%
- Energy/utilities: 4%

Australia experienced the most API security incidents

Of the four surveyed APAC countries, Australia had the highest prevalence of API security incidents in the past 12 months, with 95% of respondents reporting an incident. Most respondents blamed these incidents on "API misconfigurations" (23%) or "API gateway didn't catch it" (23%), but many other respondents cited internal processes, including "authorization vulnerabilities," "vulnerability due to API coding errors," and "API had unintended exposure to the internet" (approximately 21% each).

If you have experienced an API security incident, what has been the estimated total financial impact of these incidents combined?

How five groups of Australian respondents view API incidents' costs



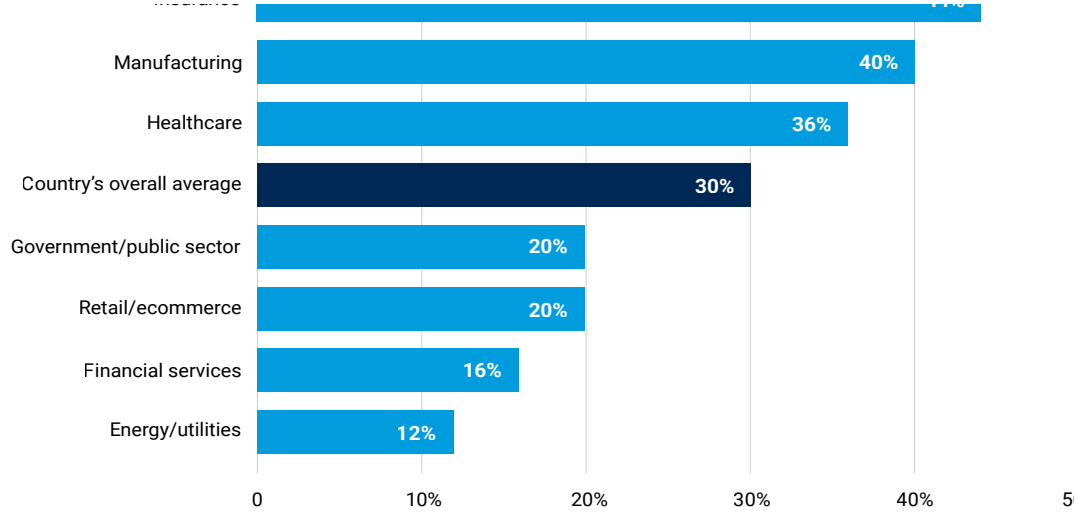
The costs of API security incidents were also viewed as a larger impact in Australia than in the other surveyed APAC countries, ranking second (32%) after "it hurt our department's reputation with our senior leaders and/or board of directors" (33%). While "fines from regulators" was the fourth most cited impact overall, it was the most cited impact among senior security professionals and three industries: insurance, energy/utilities, and manufacturing.

Australian CISOs, CIOs, and CTOs were highly focused on API security incidents' internal consequences. Their top-cited impacts were tied at 32.8%: "it led to increased stress and/or pressure for my team/department" and "it hurt our department's reputation with our senior leaders and/or board of directors."

Australia also had the highest percentage of respondents who claimed to have a full API inventory among the countries surveyed (81%), but that group had the lowest percentage of respondents who said they know which APIs return sensitive data (30%). Only one company said they don't have an inventory of APIs at all.

Do you have a full API inventory *and* do you know which APIs return sensitive data?

How Australian industries stack up versus the country's overall average



Despite the high frequency of API security incidents in Australia, "securing APIs from threat actors" was not a top priority for Australian respondents, ranking fourth overall among cybersecurity priorities (21%), after "securing endpoints" (26%), "managing and securing developer secrets" (24%), and "SIEM" (24%). "Securing APIs from threat actors" was tied with "data loss prevention" at roughly 21% each among Australian organizations' top priorities.

When it comes to spotting API vulnerabilities early in the lifecycle, Australian respondents had the lowest rate of real-time API testing among the four countries (6%), with most testing daily (34%) or weekly (35%). No respondents in the Australian financial services, healthcare, or manufacturing industries reported that they test in real time.

The lack of real-time testing in Australia is concerning and worth exploring. As noted in the next section about API security and compliance, Australia's Consumer Data Right regulation includes standards to ensure that companies' developers build APIs in a standardized and secure manner.

APIs that are embedded with coding errors or other preventable risks are exactly what attackers seek. When an organization tests APIs early and frequently, it places its security and developer teams at an advantage.

Do enterprises factor API risks into their compliance programs?

Worldwide, regulatory agencies are increasingly requiring organizations to document and account for APIs, and their message seems to be getting through. Across the four countries surveyed, respondents showed a strong awareness of how APIs and API security factor into regulatory requirements.

Nearly 90% of respondents in China, India, and Australia said they factor API security into meeting regulatory requirements. This was less common in Japan, where 22% of respondents said they do not, citing a lack of time or resources or a belief that regulators aren't requiring it yet. Japan's overall response was heavily informed by the C-suite; 28% of Japanese CISOs, CIOs, and CTOs said APIs don't have a place in their compliance programs.

However, not enough organizations across the four surveyed countries are taking the necessary actions to integrate APIs into their compliance programs. Of the majority that said they do factor in APIs, less than half include them in three essential areas that most regulators demand: risk assessments, reporting, and security plans. In fact, just 41% factor APIs into risk assessments, and 40% factor APIs into reporting requirements.

Why are these discrepancies important? Attackers know they can simplify their approach to data breaches by directly targeting poorly protected APIs.

Act on the Protection of Personal Information (Japan):

Requires conducting data protection impact assessments to identify and mitigate risks for APIs processing large volumes of personal data or involving high-risk data processing activities

Data Security Law of the People's Republic of China:

Requires implementing strong measures to secure access to customers' data via technologies such as APIs that exchange information across applications, systems, and cloud environments

Digital Personal Data Protection Act (India):

Requires having mechanisms to detect data breaches, including those occurring via APIs, and to conduct regular compliance audits that entail accounting for APIs and efforts to secure them

Consumer Data Right (Australia):

Includes standards to ensure that developers build APIs in a uniform, secure manner while emphasizing protocols to protect consumer data in transmission and access, including via APIs

Key takeaways and next steps for security teams

For security leaders and team members seeking guidance on where API security should fit into their priorities, these survey results offer a few compelling starting points:

- API security incidents — such as attacks, abuse, and data breaches — are happening frequently in the four countries surveyed.
- There is a significant disconnect between C-suite (CISO, CIO, CTO), senior security professionals, and AppSec teams about the cost of these incidents, as well as other impacts such as lost trust. These roles are also misaligned in terms of their visibility into their APIs and their knowledge of whether those APIs return sensitive data.
- Either organizations have a limited understanding of how their APIs are vulnerable, the vulnerabilities for threat actors to take advantage of are widespread, or both. This is likely due to poor internal processes as well as weaknesses within existing API security solutions.

To achieve an effective approach to API security that protects critical data, customer relationships, and internal team members, organizations first need to reach a consensus on the causes, impacts, and priority level of API security incidents. From there, they'll benefit from creating clear and comprehensive processes to protect APIs in both development and production. Finally, they need security tools that can help with these tasks.

The following is a step-by-step approach to building a lasting API security strategy:

1. **Start with API discovery and visibility**
   To undertake a full inventory of your entire API estate, seek out tools with an automated approach to discovering APIs and the microservices they support. Breadth of coverage is critical, as unmanaged APIs are a prime target for threat actors.

2. **Invest in testing**
   Select an API security solution that allows you to easily test whether APIs are coded to perform their intended function. Ideally, testing is performed before deployment, but it's also important to test all APIs already in production with real-time analysis of traffic and potential vulnerabilities.

3. **Undertake full API documentation**
   Auditing your entire API environment to identify misconfigured APIs or other errors is essential. Your auditing capabilities should also ensure adequate documentation of every API and whether it contains sensitive data or lacks appropriate security controls. This also helps you prepare for compliance mandates that involve API security, whether implicitly or explicitly.

4 **Use runtime detection**

An API security solution with automated runtime detection allows you to differentiate between normal and abnormal API activity. By monitoring API interactions this way, you can detect behaviors indicating a threat in real time and take action.

5 **Respond to suspicious behavior**

By integrating an API security solution with your existing security stack (e.g., WAF or web application and API protection), you'll be able to spot high-risk behavior and block suspicious traffic before it can access critical resources.

6 **Investigate and hunt for threats**

In the most mature API security stage, you'll use forensic analysis on past threat data to learn whether alerts correctly identified threats and whether patterns emerged, enabling proactive threat hunting that combines sophisticated tools and human intelligence.

For more insights into API security best practices, access the two following papers:

- **Protect Against OWASP's Top 10 API Security Risks**
- **11 Critical Capabilities of API Threat Detection and Response**

For additional help, schedule a customized **Akamai API Security demo**.

About the API Security Impact Study

The research for the 2025 Security Impact Study edition, focusing on organizations in China, Japan, India, and Australia, was conducted by Opinion Matters between October 14 and 30, 2024. Opinion Matters surveyed a total of 806 respondents, with at least 200 respondents from each country. One-third of the respondents were CIOs, CTOS, or CISOs; one-third were senior security professionals; and one-third were from application security teams in companies ranging in size from 250–400 to more than 1,000 employees across eight key industry sectors: automotive, financial services, retail/ecommerce, healthcare, insurance, government/public sector, manufacturing, and energy/utilities.

Opinion Matters abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Opinion Matters is also a member of the British Polling Council.

Credits

Lead writer
Barney Beal

Managing editor and content strategist
John Natale

Copy editor
Cullen Pitney

Promotions
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 API Security

Learn how Akamai protects APIs throughout their entire lifecycle, from development to production — with critical capabilities across API discovery, posture management, runtime protection, and API security testing. **https://www.akamai.com/products/api-security**

Access data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided that Akamai is duly credited as a source and the Akamai logo is retained. **https://akamai.com/api-security-study-asia-data**