API
SECURITY
IMPACT
STUDY
2024

How API Incidents Affect You and Your Team

Akamai

Contents

Executive summary

Now in its third year, the API Security Impact Study (formerly the API Security Disconnect Report) explores the state of API protection based on a survey of 1,207 leaders and practitioners across the U.S., U.K., and (new in 2024) Germany. The study examines how enterprises experience API security events — their frequency, causes, and impacts — and how security departments are addressing APIs as an attack vector.

To gain the fullest picture, we surveyed a balance of:

CISOs, CIOs, CTOs, senior security professionals, and AppSec team members from organizations ranging in size from under 500 to more than 1,000 people

Eight industries: financial services, retail/ecommerce, healthcare, government/public sector, manufacturing, energy/utilities, and (new in 2024) automotive and insurance

Introduction

APIs are often viewed as an *emerging* attack vector, even amid data that shows them to be prevalent and damaging. Consider these statistics:

- 108 billion API attacks were recorded from January 2023 through June 2024, according to a recent Akamai State of the Internet (SOTI) report.

- "Current data indicates that the average API breach leads to at least 10 times more leaked data than the average security breach," according to the May 2024 Gartner® Market Guide for API Protection.*

- Attacks are also increasing. The SOTI also reports web application and API attacks together rose by 49% between Q1 2023 and Q1 2024.

These increases are not surprising. Behind the scenes, APIs facilitate communication and exchange data among nearly all the technologies driving your digital initiatives: GenAI tools, customer-facing apps, cloud services, and more. Yet many APIs are insufficiently protected — whether built with no authentication, misconfigured, or totally forgotten — making them an attractive and cost-effective attack vector to cybercriminals. They only need to find one vulnerable API and, *boom*, they gain direct access to all the data it returns when called, which can be thousands of records.

At a high level, our research showed that API security has yet to become a key element in a comprehensive security strategy. Organizations mostly treat API threats as emerging, when the attack data — as well as the financial impacts and stress to teams that surfaced in our study — showed they are growing in number and often successful. Our 2024 findings offer a window into how API security incidents affect your peers and their organizations. We hope this data will help position your own team to better assess API protections and improve them where needed.

> Many APIs are insufficiently protected — making them an attractive and cost-effective attack vector to cybercriminals.

* GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

High-level findings: API incidents affect the business and stress teams

Our 2024 study's findings showed that APIs are an attack vector that is growing and creating considerable security challenges for teams. Our respondents demonstrated remarkable consensus on:

- Seeing API security incidents rise for three years straight

- Spending more than half a million dollars on average to address and recover from API-related incidents (US$943,162 is the average financial impact, according to our U.S. C-suite respondents)

- Feeling the human toll of API incidents, with the impact of stress and reputational damage to their teams (especially internal scrutiny that amplifies this pressure) ranking even higher than costs to fix the incidents

Respondents offered mixed views on the completeness of their API inventories, and this variability was even more pronounced when broken down by role (see page 11). Strikingly, enterprises with full API inventories that also know which of their APIs return sensitive data dropped from an already low 40% in 2023 to just 27% in 2024.

Respondents also indicated that the traditional tools they've relied on to protect APIs do not fully cover risk. Those tools, such as web application firewalls (WAFs), API gateways, and network firewalls, are often the first to be blamed for an attack's success (see full list of causes on page 17 and a note on WAF and WAAP on page 12).

Our study findings also allow us to infer a few main reasons why API security strategies have yet to take greater priority — despite evidence that they merit focus. One key factor: a lack of alignment among key security roles on the number, location, and risk attributes for APIs that need protecting — likely because of poor visibility to APIs and no single source of truth.

We also observed a lack of consensus between security leaders and practitioners on causes of API attacks. Is it the tools they use, the mistakes their coders made in development, or attacks on loopholes in GenAI innovations? Depends on who you ask.

Of course, the other reason API security hasn't taken more prominence strategically is that teams are already stretched to cover other pressing threats, which are also likely taking up the majority of budget, team focus, and effort. Let's dive deeper into the results.

> Security professionals are feeling the human toll of API incidents, with the impacts of stress and reputational damage to their teams ranking even higher than costs to fix the incidents.

API Security Impact Study — 2024
Snapshot of Key Findings

84% of respondents experienced an API security incident in the past 12 months

Average cost to address API incidents over the past 12 months:

🇺🇸 U.S.	🇬🇧 U.K.	🇩🇪 Germany
$591,404	**£420,103**	**€403,453**

Low visibility
Only 27% of enterprises with full API inventories know which APIs return sensitive data — down from 40% in 2023.

High stress
#1 impact of API incidents
CISOs: It hurt our department's reputation with senior leaders/board.
CIOs: It increased stress and/or pressure for my team/department.

Scant testing
Only 13% and 18% of respondents test their APIs in real time and daily, respectively, from API development through production.

The financial cost of API security incidents exacerbates the impact on teams and leaders. Costly breaches draw scrutiny and can make it appear — to influential stakeholders like the board of directors — that teams are not doing their jobs successfully. That's stressful. In fact, participants across geographies cited stress on their teams as the top impact of an API security incident.

The current state of API security

For the past three years, the number of organizations reporting API security incidents has consistently risen, reaching a high of 84% in 2024 (see below). How are these API attacks affecting organizations? What are they doing — or not yet doing — to lower their risk? We've structured our findings as answers to these questions.

Are API attacks having a significant impact on organizations and their security teams?

The short answer is yes. This was the first year we collected data on the financial impact of an API security incident, and it turned out to be significant: the cost, on average, to remediate API incidents (including system repairs, downtime, legal fees, fines, and any other associated expenses) for those 84% who experienced them over the past 12 months was:

- **$591,404** in the U.S.
- **£420,103** in the U.K.
- **€403,453** in Germany

Certain roles viewed the costs as much higher, particularly U.S. C-suite respondents who reported $943,162 — nearly 60% more than the average of total U.S. respondents.

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

Year	Total	U.S.	U.K.	Germany
2022	76%	75%	77%	—
2023	78%	85%	69%	—
2024	84%	83%	83%	84%

No matter the exact number, the financial cost of API security incidents exacerbates human impacts. Costly breaches draw scrutiny and can make it appear — to influential stakeholders like the board of directors — that teams are not doing their jobs successfully. That's stressful. In fact, participants across geographies cited "stress" (specifically, stress on their teams) as the top impact of an API security incident, followed by "it hurt our department's reputation with senior leaders and/or board of directors," with "costs to fix" in third. Notably, the internal impacts that most affect morale reappear and dominate the bottom three impacts, which are nearly tied (see below).

Results were similar when broken down by industry: "Increased stress and/or pressure for the team after an API breach" was also the top-ranked impact across four of the eight industries we surveyed (see sidebar on). This includes financial services, which notably reported the highest financial impact of all industries at US$832,801.

The relationship between the financial and human costs of API attacks also came through.

Top cited impacts of API security incidents

1. Increased stress and/or pressure for the team or department − **27.0%**

2. It hurt our department's reputation with senior leaders and/or board of directors − **26.6%**

3. Costs incurred to help fix the issue − **25.8%**

4. Fines from regulators − **25.4%**

5. Loss of customer goodwill and churned accounts − **25.0%**

6. Loss of productivity − **24.1%**

7. Loss of trust and reputation − **23.8%**

8. Loss of employee goodwill − **23.8%**

9. Led to increased internal scrutiny of our team/department by the business − **23.5%**

Based on the question: What costs and/or impacts, if any, have API security incidents had on your business? (Select up to 3); n=1,207

loud and clear in responses from IT and security leaders on the impacts of incidents (each respondent was allowed to pick up to three). One area showing general consensus among all roles in all regions was that the greatest impacts of API security incidents are on staff.

- The top two reported by CISOs — "it hurt our department's reputation with senior leaders/board" and "loss of customer goodwill and churned accounts" — revealed an exact tie between the human and financial impacts at 31%.

- Similarly, the top impacts reported by CIOs indicated a tie between "increased stress and/or pressure for my team/department" and "costs to fix" at 34%.

These results make sense for CISOs and CIOs: What if the teams they lead keep getting slammed with security incidents that create poor working conditions, blow budgets out of the water, and upset customers? These leaders don't want to see quality talent leave or their department's reputation plummet. Add to that such financial pressures such as remediation costs and/or customer churn, and the stress on CISOs and CIOs ratchets up considerably. In fact, "loss of customer goodwill and churned accounts" was the top-ranked impact of an API security incident for respondents from both the insurance and automotive industries (see sidebar on the next page for more industry findings).

Top responses for the remaining roles were:

- CTO, 30%, "loss of employee goodwill"

- Senior security professional, 27%, "it hurt our department's reputation with our senior leaders/board"

- AppSec team, 31%, "led to increased stress and or pressure for my team/department"

Top cited impacts of API security incidents by industry

Automotive	Loss of customer goodwill and churned accounts – **33%**
Energy/Utilities	It hurt our department's reputation with our senior leaders and/or board of directors – **36%**
Financial Services	Tie: Led to increased stress/pressure for my team/department + regulatory fines – both **29%**
Gov't/Public Sector	Led to increased stress/pressure for my team/department – **29%**
Healthcare	Tie: Loss of trust and reputation + loss of productivity – both **29%**
Insurance	Loss of customer goodwill and churned accounts – **28%**
Manufacturing	Led to increased stress and or pressure for my team/department – **34%**
Retail/Ecommerce	Led to increased stress and or pressure for my team/department – **29%**

Based on the question: What costs and/or impacts, if any, have API security incidents had on your business? (Select up to 3); n=1,207

Is there adequate visibility to APIs and potential risks?

No. More to the point, it's actually gotten worse. This year, the percentage of participants who have a full API inventory and also know which APIs exchange sensitive data dropped from an already low 40% in 2023 to just 27% in 2024. (This finding might have an upside, if we consider that more organizations are attempting to undertake a full inventory but lack the tools needed to locate every API and identify the activity happening within each one.)

The percentage of participants who have a full API inventory and also know which APIs exchange sensitive data **dropped from an already low 40% in 2023 to just 27% in 2024**.

Current state of API inventories and awareness, all respondents

	2024	2023
Yes, **and we know** which return sensitive data	27%	40%
Yes, **but we don't know** which return sensitive data	43%	32%
We have a partial inventory of our APIs **and we know** which return sensitive data	23%	24%
We have a partial inventory, **but we don't know** which return sensitive data	6%	4%
No, **we don't** have any inventory	1%	—

Based on the question: Do you have a full inventory of your APIs, and do you know which return sensitive data?
(Select from five options); n=1,207

Looking at leaders across all three countries and eight industries surveyed, CIOs tend to believe —
by a significant margin over CISOs — that their organizations have complete API inventories. At the
practitioner level, both senior security professionals and AppSec team members are largely aligned
with the average CIO's view that all APIs are accounted for.

But how do the five roles on average compare, when it comes to knowing (or not knowing) which
of their APIs return sensitive data when called? The answer is important, because many of these
calls come from malicious sources, seeking to exploit common API vulnerabilities.

Four types of unmanaged APIs that attackers target to access data

1. **Shadow APIs** (aka undocumented APIs) exist and operate outside the official, monitored channels
within an organization.

2. **Rogue APIs** are unauthorized or malicious APIs that pose a security risk to a system or network.

3. **Zombie APIs** include any API that has been left running, even after being replaced by new versions
or other APIs entirely.

4. **Deprecated APIs** are no longer recommended for use, due to changes in the API.

These findings offer some curious takeaways about visibility into API risk. The majority of CISOs and CTOs replied that either they had a full inventory *without* knowing which APIs return sensitive information (let's refer to this knowing as "sensitive data knowledge") or had a partial inventory *with* sensitive data knowledge.

The majority of CIOs reported having a full API inventory, and of those CIOs, 42.9% reported also having full sensitive data knowledge — while 36.3% reported not having that knowledge. Senior security professionals were in line with CIOs (75% reported a full inventory), but it broke down *in the reverse* regarding sensitive data knowledge: 32.5% of senior security professionals said they have sensitive data knowledge and 42.5% said they do not.

Finally, AppSec staff members, probably the most hands-on of all respondents, reported the single largest majority across all five roles. Almost half reported a full inventory without sensitive data knowledge — the other half was roughly split between:

- Full inventory with full knowledge of sensitive data
- Partial inventory with full sensitive data knowledge of those APIs

We can see that measuring inventories has not yet been standardized enough to produce a single-source API count. Given the variability, it's also likely that more enterprises with full inventories *do not* have full sensitive data knowledge. Knowing which APIs return sensitive data is always significant. However, a partial inventory can be the most dangerous, since shadow, rogue, zombie, and deprecated APIs are highly targeted, poorly protected, and usually slip past traditional security tools.

Current state of API inventories and awareness, broken down by role

	CISO	CIO	CTO	Sr Sec Pro	AppSec
We have a full inventory, **and we know** which return sensitive data	17.2%	42.9%	16.5%	32.5%	26.4%
We have a full inventory, **but we don't know** which return sensitive data	41.4%	36.3%	34.8%	42.5%	47.4%
We have a partial inventory of our APIs **and we know** which return sensitive data	32.5%	15.4%	39.9%	18.3%	20.4%
We have a partial inventory, **but we don't know** which return sensitive data	8.3%	5.5%	8.2%	5.8%	5.2%

Based on the question: Do you have a full inventory of your APIs, and do you know which return sensitive data? (Select from five options); n=1,207

At a time when unmanaged APIs have sprawled and proven to be elusive to traditional security tools, these findings reveal a common security gap that makes the API attack vector more attractive to threat actors.

Of course, unmanaged APIs are just one of at least five API attributes that a security team needs to see and evaluate. The range includes:

- **APIs with known vulnerabilities** that haven't been patched
- **APIs that are unmanaged or forgotten** (shadow, rogue, zombie, deprecated)
- **APIs with external exposures** (such as credentials, keys, and variables outside your control)
- **APIs with operator errors** (security misconfigurations in infrastructure and services)
- **APIs with undiscovered vulnerabilities** and bugs that threat actors identify and exploit

At a minimum, the range of responses across roles regarding API inventories and visibility into API vulnerabilities suggests that:

- Enterprises are still relying on security products that are not designed specifically for discovering and securing APIs — especially the high-risk, unmanaged ones.
- Security departments have yet to define the risk attributes of an API that need to be seen and assessed or to build consensus across their many business units, developer teams, and vendors on their strategy for API discovery and inventorying.

Addressing such disconnects can be a great first step in making an effective case for investing in stronger capabilities to secure and secure all APIs (see "How to move toward a more mature posture for API security" on). As it stands, the focus and advocacy needed to receive budget allocation are often not in place for API security, making it difficult to prioritize and fund initiatives that could advance not only API and web app defenses but an organization's overall security posture.

👍 **Better together: WAAP + API-specific protections**

Designed to quickly identify and mitigate threats from multiple attack vectors, web application and API protection (WAAP) extends the traditional protections of a WAF. **An API security solution — working in tandem — extends protections even further beyond the firewall to create the strongest defense possible**.

Are APIs being tested often enough to lower risk of abuse or breaches?

No, not often enough. Public-facing APIs that are misconfigured, lacking authentication controls, embedded with coding errors, or harboring other preventable risks are exactly what attackers are looking for — and those attackers are getting better and better at finding them.

So every time your development team sends APIs like these into production — without comprehensively testing them first — is like unintentionally planting a future workload for your security team (a workload that's no doubt urgent and contributing to what our findings revealed about stress).

But note that we said *preventable* risks.

If you test APIs in dev — frequently and efficiently by way of automation — *before* they are released to production, you place your organization, your developers, and your security team at an advantage. And that advantage is immediate in terms of lowering stress caused by unknown vulnerabilities and knowing that errors won't be found in production when they're exponentially more difficult and costly to fix.

So far, however, testing is not gaining ground, according to our respondents. Frequent API testing — real-time and daily — declined from last year, across the API lifecycle, including in production.

- In 2023, 18% of U.S. and U.K. respondents said they tested in real time. Among the same cohort **in 2024, that figure fell to 13%**.

- In 2023, 37% of U.S. and U.K. respondents said they tested at least once a day. **In 2024, only 13% tested at this frequency**, although 26% of German respondents tested once a day.

> If you test APIs in dev — frequently and efficiently by way of automation — *before* they are released to production, you place your organization, your developers, and your security team at an advantage.

Weekly API testing is most common for participants across geographies, but in no geo did it reach 50%. In addition, frequency of API testing varied widely across geos, from *real time* to *not at all*. Notably, only 6% of respondents answered "We only test APIs' security before releasing them into production." Ideally, teams will move to continous testing throughout the API lifecycle.

What does it mean to continuously test APIs?

Vulnerabilities can be introduced to APIs at any point in their lifecycle, from coding errors made in development to security gaps that surface once users begin interacting with the API. That's why, ideally, API testing is done in development (shift-left) and also continuously while they are in production (shift-right).

Examples of API testing in development:

- Run automated tests that simulate malicious traffic.
- Inspect API specifications against established governance policies.
- Test APIs on demand or as part of a CI/CD pipeline.

Examples of API testing in production:

- Continuously monitor API traffic and assess traffic metadata.
- Identify changes in your existing APIs via automated analysis.
- Find issues in real time and remediate before attackers notice.

Do your API security protocols meet compliance mandates?

In many data protection regulations, APIs aren't mentioned by name, but the requirements clearly focus on securing the applications and infrastructure within which APIs operate. Compliance mandates are always evolving, and additional regulations are on the way with API implications, including the American Privacy Rights Act (currently in draft legislation) and the EU Cyber Resilience Act.

Regulations and frameworks with current, direct implications for API security include:

- PCI DSS (currently v4.0.1)
- General Data Protection Regulation (GDPR)
- Digital Operational Resilience Act (DORA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Network and Information Security (NIS2) Directive

API security gets attention but remains on the back burner

If API attacks are costly and inflict fines, if they contribute to loss of customer trust, if they cause rising stress on staff and lost credibility with enterprises' boards, why aren't teams taking more decisive action? Answers to the following questions help us understand.

How are different enterprise roles prioritizing API security?

We asked our participants to identify their main cybersecurity priorities for the next 12 months, allowing them to select up to three from an extensive list (see sidebar). The top six priorities differed only by 2% and the bottom six by only 1%, suggesting that priorities are similar across geographies and industries — and that teams are often compelled to juggle them all.

In some industries, however, the ranking differences central to APIs tell a different story. For example, energy/utilities ranks API security as the lowest priority vs. all other sectors at 13.2% (and below the all-survey participant average of 18%). At the same time, energy/utilities also had the highest reporting of API security incidents at 91%, the highest of all eight sectors and above the 84% average. What adds up here? The low priority given to API security, and the high attack rate.

Top cited security priorities over the next 12 months

1. Defending against GenAI-fueled attacks – **21.2%**

2. Defending against ransomware – **20.5%**

3. Securing authentication for workforce users – **19.7%**

4. Managing and securing developer secrets – **19.6%**

5. Securing endpoints – **19.2%**

6. Cloud security solutions – **19.1%**

7. Securing privileged IT access – **18.6%**

8. Data loss prevention – **18.6%**

9. Securing APIs from threat actors – **17.9%**

10. Securing applications – **17.7%**

11. Security information and event management – **17.6%**

12. Incident response and management – **17.6%**

Based on the question: What are your business's main cybersecurity priorities in the next 12 months?
(Please select up to 3); n=1,207

More telling data emerged from cutting the response data by role:

- CISOs cited GenAI-assisted attacks and API protection the highest, at **25.5%** and **24.8%**, respectively.

- AppSec staff aligned with CISOs, citing GenAI-assisted attacks as their highest priority at **22.5%**.

- CIOs and CTOs both focused on privileged access, with CTOs adding incident response in a tie.

- Senior security professionals alone ranked ransomware their highest priority.

These differences lead us again to ask questions such as: Why are different layers of the IT security organization seemingly operating from different playbooks? And why do top security leaders and frontline workers both seem aligned on the hefty role APIs — and their risks — play in GenAI-assisted attacks, while other roles are not?

Perhaps it's because the CISOs see their business units hastily rolling out innovations like GenAI-fueled apps to meet demand, while the AppSec team members see the same; only *they* know the extent of the unknowns regarding the vulnerabilities of AI components (like LLMs) that touch sensitive data. Added to that, this team has a front-row seat to the many warning signs that attackers are building GenAI into their attack methods.

But the main reason might be the simplest one: Top-down and bottom-up communications don't happen frequently enough — in large enterprises especially — leading to a disconnect between priorities at the top vs. what teams *must* handle day to day.

Finally, let's compare respondents' top cybersecurity priorities with the causes they gave for their API security incidents. As shown on page 17, three of their top-cited causes refer to traditional application security tools that were unable to catch API issues. The comparison offers a good opportunity to open a discussion on how API discovery and testing solutions could enhance not only their API security but nearly all of their other top security priorities.

In other words, if the right API security tools can protect not only APIs, but also improve security for fields such as data, cloud, and applications, this makes API security look less like a siloed, niche field to your stakeholders. Speaking to the big picture can make it easier to win approval to elevate APIs on the priority list.

> If the right API security tools can protect not only APIs, but also improve security for fields such as data, cloud, and applications, this makes API security look less like a siloed, niche field to your stakeholders.

Does lack of alignment on API security incidents indicate no single source of truth?

We've highlighted differences between the C-suite and frontline staff in their overall security priorities, and those differences persist in issues more specific to API threats. For example, CIOs are aligned with the AppSec team in terms of awareness of API attacks (about 88% in each role report having experienced incidents). Meanwhile, the CISO, CTO, and senior security professional all came in about eight percentage points lower, with about 80% reporting they had experienced incidents.

The top-cited cause behind API security incidents also varied by role, with most CISOs and senior security professionals citing that the API gateway didn't catch it, while the other three roles each named a different culprit:

- CISO: API gateway didn't catch it – **26.8%**
- CIO: Unintended internet exposure – **28.6%**
- CTO: WAF didn't catch it – **25.9%**
- Senior security professional: API gateway didn't catch it – **23.3%**
- AppSec team: API misconfiguration – **23.2%**

Top cited causes of API security incidents, all respondents

1. API had unintended exposure to the internet – **21.8%**
2. Web application firewall didn't catch it – **21.8%**
3. API gateway didn't catch it – **20.2%**
4. APIs in GenAI tools/technologies, e.g., LLMs – **20.0%**
5. API misconfiguration – **19.9%**
6. Network firewall didn't catch it – **19.6%**
7. Well-known tech tool/service, e.g., Microsoft – **19.2%**
8. Vulnerability due to API coding errors – **19.1%**
9. Unmanaged APIs, e.g., dormant or zombie APIs – **18.9%**
10. Lack of API authentication controls – **18.8%**
11. Authorization vulnerabilities – **18.7%**
12. Software solution downloaded from the internet – **17.6%**
13. Mid-tier software solution, e.g., Slack – **16.3%**

Based on the question: What do you believe are the causes of the API security incidents your organization has experienced? (select up to 3); n=1,207

Reported cost of API security incidents also showed a lack of alignment from top roles down, though it's important to note that cutting the data by role *and* region naturally results in a smaller sample size. Still, the differences in these subsets are worth noting, especially in the U.S., where CIOs and CTOs reported the cost of incidents to be about US$1M and CISOs about US$737,000, while senior security professionals and AppSec staff reported about US$375,000 and US$444,000, respectively.

In the U.K., costs were generally more aligned across role-specific subsets, although AppSec team members there reported the highest figure at £749,000 and the CISOs the lowest at £190,000. (The middle roles ranged top-down from £374,000 to £222,000.) Germany's disparity in cost reporting was similar to the U.K.'s, with the highest estimate coming from the lowest-ranking, most hands-on staff at €345,000 and the lowest cost by the highest ranking CISOs at £197,000 (opposite findings from the U.S.). One area showing general consensus among all roles in all regions was that the greatest impacts of API security incidents are on staff (see Impacts, page 7).

How to move toward a more mature posture for API security

As mentioned, our findings make it clear that members of security teams at different strata of the organization are not viewing API security through the same lens. But there's a flip side: What's also clear is that they have common ground to build upon. They know the costs (financial and human), and they acknowledge that the tools they've relied on aren't enough.

With API security having such a large impact on organizations, your next steps could be deciding what to build on, what to change, and showing leaders how securing APIs can help the bottom line. Gaining alignment within your security department, from CISO to the AppSec team, on how to prioritize API security is a good place to start, followed by promoting open communication between leadership and frontline AppSec team members, as well as the managerial layers in between.

Steps you can take

To close our study, we've put together a series of progressive steps your security team can use to start, or build upon, your API security strategy and move toward mature API protection.

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 (see sidebar on page 10) 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 correctly to perform their intended function. Ideally, testing is performed prior to 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, implicitly or explicitly (see page 14).

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're able to 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 WAAP), 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 that enable proactive threat hunting using a combination of sophisticated tools and human intelligence.

Conclusion

This year's report made it loud and clear that security — in this case, API security — isn't just about threat lists or tools; it's about people.

Our study confirms that security teams are overstretched and that the notion of adding a whole new attack vector to your team's workload might seem daunting. But the proliferation of APIs is not going to let up, and taking steps to secure your APIs has a strong ripple effect on several other high priorities, such as GenAI vulnerabilities (to protect the APIs that exchange data with LLMs) and cloud security (to reduce risk in every API included in the workloads you migrate).

We deeply believe that being proactive on API security not only protects your business but also positions your team to become much more credible and trusted in its view of this critical attack vector — among peers, leaders, and the board. This has the huge benefit of reducing stress levels in your team, which our study showed are highly affected by API security incidents and the scrutiny and loss of goodwill they engender, in both fellow employees and customers.

Taking steps now also preemptively eases your compliance planning and reporting, not to mention the timely prevention of regulatory fines. So why not get started?

- If you're ready to consider the next steps on your journey to a mature API security posture, we recommend starting with our white paper, API Security Fundamentals.

- If you're ready for a conversation about your challenges and how we can help, it's easy to request a customized Akamai API Security demo.

About the API Security Impact Study

The research for the 2024 API Security Impact Study was conducted by Opinion Matters between June 12, 2023, and July 7, 2024. Their team surveyed a total of 1,207 respondents with the following breakdown by residence of the company: 404 from the U.K., 402 from the U.S., and 401 from Germany. One-third of respondents were CIOs or CISOs; one-third were senior security professionals; and one-third were from application security teams working in companies ranging in size from under 500 to more than 1,000 people, across eight key industries: 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.
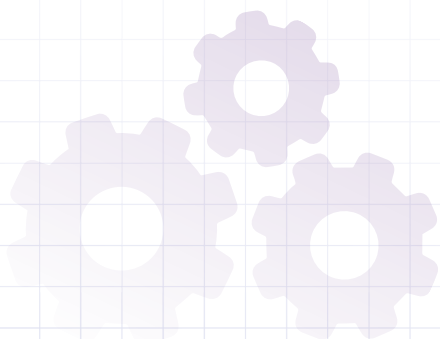
State of the Internet/Security

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**