2024 API SECURITY IMPACT STUDY

Government

API incidents are on the rise. Learn how the government is addressing this top security concern — and what your organization can do to stay safe.

Governments around the world are under growing pressure to secure digital services in an API-first era. In 2024, 86.1% of public sector organizations reported an API security incident — a sharp jump from 76.8% the year before. This increase places the public sector above the all-industry average of 84%, underscoring the growing scale of the challenge. From meeting General Data Protection Regulation (GDPR) requirements to enforcing data residency across multicloud systems and confronting sovereign security threats, agencies face a universal need for greater visibility, stronger governance, and built-in resilience.

The true cost of government API security incidents

Government agencies are increasingly adopting APIs to enable digital services, facilitate interagency data sharing, and modernize infrastructure. But this trend has introduced a host of new vulnerabilities that threat actors are eager to exploit. Poor authentication mechanisms, API misconfigurations, and insufficient awareness of critical risk indicators have left the government particularly susceptible to API security breaches. The consequences of these incidents extend far beyond data theft by posing risks to operational continuity, regulatory compliance, and public trust.

How do we know this? Akamai surveyed more than 1,200 IT and security professionals — from chief information security officers to application security staff — to learn about their experiences with API-related threats.

Here, we've filtered our findings for government respondents, who said the top impacts of their API security incidents were:

- "Increased stress and/or pressure for the team/department" (28.5%)
- "It hurt our department's reputation with senior leaders and/or board of directors" (27.2%)
- "Fines from regulators" (25.2%)

These intertwined consequences are easy to understand, given that your peers placed the cost of addressing API incidents at US$717,500 — 21.3% higher than the average across all eight industries surveyed.

Read on to gain industry-specific insights from the 2024 API Security Impact Study.

As attacks rise, visibility is a growing concern

When asked to cite the top causes of their API security incidents, your peers identified two key vulnerabilities:

- Lack of API authentication controls (25.2%)
- Traditional tools used for securing APIs (25.2%)

Despite mounting evidence of the consequences of API threats — from high remediation costs to an erosion of trust — our findings suggest many government teams have yet to make API security a top priority. In fact, API security ranks sixth among cybersecurity priorities for the year ahead at 17.9%.

86.1% of government organizations reported experiencing an API security incident in 2024 — a significant increase from 76.8% in 2023

$717,500 is the average financial cost of an API security breach for government organizations in the United States, exceeding the all-industry average of $591,404

66.9% of government entities maintain an API inventory, yet only 18.5% have full visibility into which APIs handle sensitive data, leaving critical information at risk

Top 3 impacts

1. **Increased stress and pressure on security teams**
2. **Damaged team's reputation with leaders and board**
3. **Regulatory fines for noncompliance**

Source:
2024 API Security Impact Study

For government agencies, the costs of API attacks are steep — including financial and human impacts. Losing trust at the leadership level because of breaches can mean increased scrutiny, operational disruptions, and more work for teams that are already stretched thin and struggling to meet compliance demands.

Akamai

Just like in the private sector, it's challenging for government agencies to distinguish between genuine and malicious API activity. This is due, in part, to low visibility into precisely where APIs are vulnerable. While 66.9% of your peers say they have a full inventory of their APIs, only 18.5% of that subset know which ones return sensitive data, including personally identifiable information (PII) such as national ID number, biometric data, and contact information.

Consider what can happen to an unauthorized API deployed by a department or subsidiary of a government organization without collaboration or oversight of up-to-date central IT or security teams.

That API may have been:

- Designed to provide access to citizens' personal or financial data without proper authorization controls, potentially exposing sensitive information
- Replaced by a new version but not properly decommissioned, leaving an outdated endpoint vulnerable to exploitation
- Operating outside the visibility of central IT and security teams, evading traditional monitoring tools and compliance checks
- Exploited by malicious actors to gain unauthorized access to government systems, potentially leading to data breaches, identity theft, or financial fraud

This isn't just hypothetical — the cybersecurity landscape for U.S. government agencies presents significant challenges. According to the Cybernews Business Digital Index, many government agencies and departments are struggling to maintain robust security postures, with nearly 4 in 10 (38.8%) receiving "critical risk" ratings in their assessments, and 75% experiencing a data breach.

These statistics reflect the complex reality facing government security teams, who must balance mission objectives, legacy systems, and evolving threats while operating under unique constraints and scrutiny. As these challenges intensify, especially in the realm of API security, agencies need partners who understand their specific requirements and can provide solutions tailored to government environments.

How API incidents impact confidence, cost, and team stress

Given the frequency and costs of API attacks, it's no surprise that securing APIs is a growing priority for governments worldwide. In the United States, the Data.gov initiative, managed by the General Services Administration, standardizes APIs across federal agencies to improve consistency, security, and interoperability. Similar efforts are underway globally — from open data frameworks in the European Union and United Kingdom to digital transformation initiatives across the Asia-Pacific and Middle East regions, where governments are adopting standardized APIs to ensure secure and seamless data exchanges.

Many of these initiatives align with regional regulations such as the EU's GDPR, Australia's Notifiable Data Breaches scheme, and Japan's My Number Act. By enforcing common standards and frameworks, governments are working to ensure secure data exchange while reducing risks from third-party integrations and unauthorized access.

	Government	Average of all industries
United States	**$717,500.50**	**$591,404.01**
United Kingdom	**£378,140.69**	**£420,103.18**
Germany	**€296,975.79**	**€403,453.26**

Q3. If you have experienced an API security incident, what has been the estimated total financial impact of these incidents combined? Please include all related costs such as system repairs, downtime, legal fees, fines, and any other associated expenses.

It’s clear that government agencies are keenly aware of the consequences of API threats. For the first time, we asked respondents in the three countries we surveyed to share the estimated financial impact of the API security incidents they experienced in the past 12 months.

While the financial impacts are significant, we heard loud and clear from study participants that the costs go far beyond the bottom line.

When asked to list the top impacts of an API security incident, it wasn’t cost. As mentioned earlier, our respondents indicated “increased stress and/or pressure for the team/department” and “it hurt our department’s reputation with senior leaders and/or board of directors” as the top two.

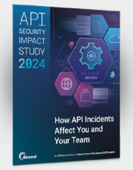
These consequences leave a lasting impact. Breaches erode trust, which can jeopardize future funding and weaken public confidence. At the same time, productivity losses in already stretched agencies can drive burnout and lower workforce engagement.

But the pressure isn’t limited to a few regions. Although this report focuses on select markets, API security has become a critical issue for public sector organizations worldwide, as agencies in Asia-Pacific, Latin America, and beyond face similar challenges in securing digital infrastructure, meeting compliance standards, and protecting sensitive data from evolving threats.

Reduce risk and stress through proactive API security

API attacks against the government are growing in scope, scale, sophistication, and cost. This includes GenAI-fueled bot attacks that quickly adapt to bypass traditional API security tools and other perimeter defenses. Many security teams in your industry are experiencing these threats firsthand and feeling the impacts, both financial and human. But even when organizations understand the significance of API threats, they’re left with the question: What can we do about it?

Taking measures now to better secure your APIs — and the data they exchange — can empower your organization to protect its revenue and sensitive data, and alleviate the burden from security teams, all while preserving the hard-earned trust of boards of directors and government leaders. These measures include building your team’s knowledge about advanced API threats and the capabilities you need to defend against them.



To read the full report and learn about best practices for API visibility and protection, download the **2024 API Security Impact Study**.

Ready for a conversation about your challenges and how Akamai can help?

Request a customized Akamai API Security demo

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 and LinkedIn. Published 05/25.