TRACEABLE

2025 Global State of API Security

The Battle Continues: Assessing Persistent Breaches, Generative AI Risks, and Rising Bot and Fraud Attacks

About This Research

Traceable conducts this annual research to provide organizations with an objective assessment of API security risks and trends. By tracking these patterns and emerging threats, we aim to offer security leaders the knowledge needed to make informed decisions and prioritize the most important security challenges.

Our commitment is to ensure that as APIs continue to be central to business operations, organizations have the insights they need to protect their critical assets.

www.traceable.ai

TRACEABLE

Report Contents

Executive Summary: The Urgent Need for API Security in Enterprise Organizations 4

Top Findings At-A-Glance 5

Research Methodology 7

Key Findings 8

Part I: API-related Data Breaches Continue to Wreak Havoc 9

Part II: Traditional Solutions Fall Short 17

Part III: The Escalating Threat of Bot Attacks on APIs 21

Part IV: Generative AI Adoption and Associated API Security Risks 23

Part V: Governance, Ownership and Budget: The Strategy and Finance of API Security 25

Where Do We Go From Here? 28

Executive Summary

The 2025 Global State of API Security Report, our second annual study, provides a comprehensive analysis of the escalating security challenges associated with APIs across industries like technology, financial services, healthcare, and retail. Drawing on insights from 1,548 IT and security professionals worldwide, this report uncovers critical vulnerabilities, attack trends, and emerging risks impacting enterprise organizations.

This year's findings reveal that 57% of organizations reported at least one data breach caused by API exploitation in the past two years. Despite these breaches, organizations are still testing only 38% of their APIs for vulnerabilities on average, with a low confidence level—companies estimate they can only prevent 24% of API-related attacks. This underscores the need for more robust and comprehensive API security measures, especially as 61% of organizations expect API risk to increase or significantly increase over the next 12 to 24 months.

A significant challenge highlighted is preventing API sprawl, with 54% of respondents stating difficulty in managing and controlling the expansion of APIs in their environments. This lack of control makes it increasingly challenging for organizations to protect their systems and data.

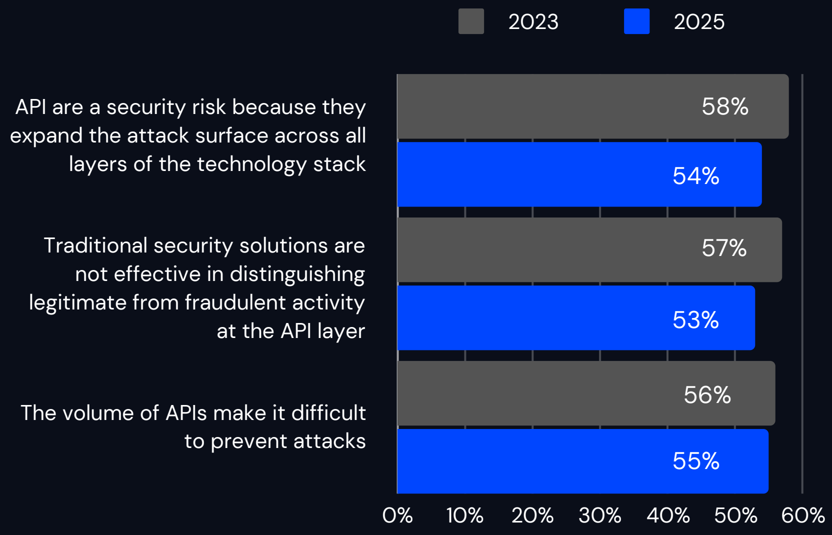
DDoS and fraud remain the top methods of API exploitation, revealing the limitations of traditional security solutions. While many organizations deploy tools like web application firewalls (WAFs) and web application and API protection (WAAP) platforms, these measures are often ineffective. The data indicates that these approaches frequently fall short in mitigating threats, prompting enterprises to reassess their strategies.

New to this year's report is a focus on the security challenges associated with generative AI applications. As 67% of organizations are adopting generative AI, risks have multiplied. Concerns include expanded attack surfaces (60%), potential data exfiltration (60%), and unauthorized access (60%). Furthermore, 66% of respondents cite a lack of in-house expertise in securing generative AI APIs, emphasizing the need for specialized knowledge and solutions.

57%
had an API related breach in the past two years

37%
only 37% can understand the context of their APIs

Reasons why APIs are at risk



Top Findings At a Glance

The following findings illustrate the growing API crisis and what steps should be taken to improve API security

- Organizations are having multiple data breaches caused by an API exploitation in the past two years, which results in financial and IP losses. These data breaches are likely to occur because on average only 38 percent of APIs are continually tested for vulnerabilities. As a result, organizations are only confident in preventing an average of 24 percent of attacks. To prevent API compromises, APIs should be monitored for risky traffic performance and errors.

- Targeted DDoS attacks continue to be the primary root cause of the data breaches caused by an API exploitation. Another root cause is fraud, abuse and misuse. When asked to rate the seriousness of fraud attacks, almost half of respondents (47 percent) say these attacks are very or highly serious.

- Organizations have a very difficult time discovering and inventorying all APIs and as a result they do not know the extent of risks to their APIs. Many APIs are being created and updated so organizations can quickly lose control of the numerous types of APIs used and provided. Once all APIs are discovered it is important to have an inventory that provides visibility into the nature and behavior of those APIs.

- According to the research, the areas that are most challenging to securing APIs and should be made a focus of any security strategy are preventing API sprawl, stopping the growth in API security vulnerabilities and prioritizing APIs for remediation.

- Third-party APIs expose organizations to cybersecurity risks. In this year's research, an average of 131 third parties are connected to organizations' APIs. Recommendations to mitigate third-party API risk include creating an inventory of third-party APIs, performing risk assessments and due diligence and establishing ongoing monitoring and testing. Third-party APIs should also be continuously analyzed for misconfiguration and vulnerabilities.

- To prevent API exploitations, organizations need to make identifying API endpoints that handle sensitive data without appropriate authentication more of a priority. An API endpoint is a specific location within an API that accepts requests and sends back responses. It's a way for different systems and applications to communicate with each other, by sending and receiving information and instructions via the endpoint.

Bad bots impact the security of APIs.

- A bot is a software program that operates on the Internet and performs repetitive tasks. While some bot traffic is from good bots, bad bots can have a huge negative impact on APIs. Fifty-three percent of respondents say their organizations experienced one or more bot attacks involving APIs. The security solutions most often used to reduce the risk from bot attacks are web application firewalls, content delivery network deployment and active traffic monitoring on an API endpoint.

Top Findings At a Glance Continued...

Generative AI and API security

- Generative artificial intelligence is being adopted by many organizations for its many benefits such as in business intelligence, content development and coding. In this research, 67 percent of respondents say their organizations have currently adopted (21 percent), in the process of adopting (30 percent) or plan to adopt generative AI in the next year (16 percent). As organizations embrace generative AI they should also be aware of the security risks that negatively affect APIs.

- The top concerns about how generative AI applications affect API security are the increased attack surface due to additional API integrations, unauthorized access to sensitive data, potential data leakage through API calls to generative AI services and difficulty in monitoring and analyzing traffic to and from generative AI APIs.

- The main challenges in securing APIs used by generative AI applications are the rapid pace of generative AI technology development, lack of in-house expertise in generative AI and API security and the lack of established best practices for securing generative AI API.

- The top priorities for securing APIs used by generative AI applications are real-time monitoring and analysis of traffic to and from generative AI APIs, implementing strong authentication and authorization for generative AI API calls and comprehensive discovery and cataloging of generative AI API integrations.

- Organizations invest in API security for generative AI-based applications and APIs to be able to identify and block sensitive data flows to generative AI APIs and safeguard critical data assets, improve efficiency of technologies and staff and real time monitoring and analysis of traffic to and from LLM APIs to quickly detect and respond to emerging threats.

Methodology

This research report is a collaborative study with the Ponemon Institute that surveyed 1548 respondents, across roughly 100 countries and over 6 major industries. This included organizations with at least 1000 employees, to those with over 75,000 employees.

The acquired data were analyzed using descriptive and inferential statistics to uncover trends and challenges in API security. Participants' involvement was voluntary, with responses collected and analyzed anonymously. The goal is to help stakeholders better comprehend the intricate landscape of API security, so they are able to make more informed decisions about the security strategy of their organization.

1548
respondents

100+
countries

Key Findings

The 2025 Global State of API Security Report reveals critical insights into the challenges organizations face today. Key findings highlight the persistent and frequent data breaches tied to APIs, the increasing difficulties in cataloging and managing extensive API ecosystems, and the rising risks posed by third-party API integrations. The report also underscores the growing prevalence of bot attacks, the surge in API fraud, and the heightened security concerns as organizations adopt generative AI applications.

These findings collectively emphasize the urgent need for comprehensive API security strategies and greater visibility across an organization's entire API ecosystem.

Part I:

API-related Data Breaches Continue to Wreak Havoc

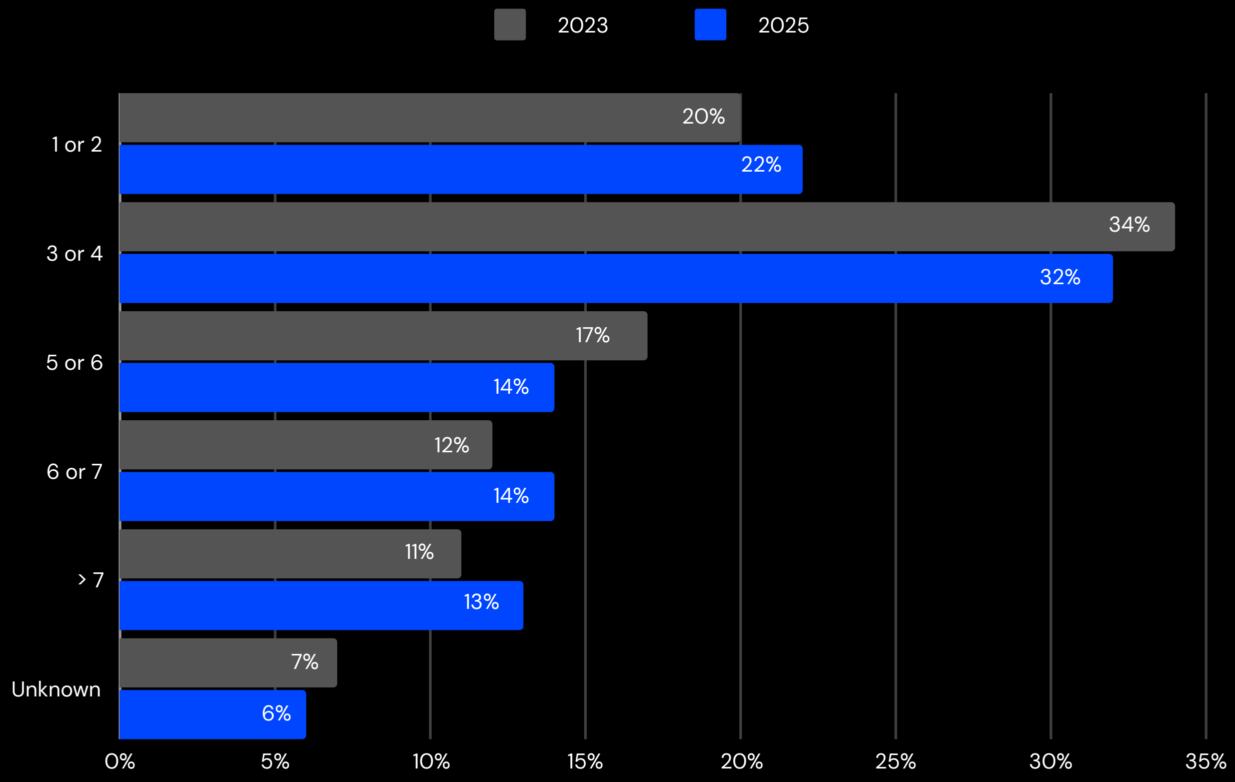
API breaches remain a critical issue for organizations, with incidents continuing to occur at an alarming rate. This chapter discusses the root causes of these breaches, examining the methods most commonly exploited by attackers, such as DDoS, fraud, and brute force attacks. It also highlights the persistent challenges organizations face in detecting and mitigating these threats, emphasizing the urgent need for more effective API security strategies.

57% of organizations experienced an API-related data breach in the past two years. Of those that experienced a breach, 73% had at least three API-related breaches.

This year's survey shows that 57% of organizations experienced at least one data breach caused by an API exploitation in the past two years, underscoring the ongoing risk that APIs present. The distribution of these incidents reveals both stability and shifts in the number of breaches organizations face. While 1 to 2 breaches were reported by 22% of respondents (up from 20% in 2023), the percentage of those experiencing 6 to 7 breaches rose from 12% to 14%, and those reporting more than 7 breaches increased from 11% to 13%.

These shifts suggest that while some organizations may have experienced fewer incidents, a significant number continue to face multiple API-related data breaches. This indicates that API security remains a complex and ongoing challenge, requiring careful attention from security teams.

How many data breaches did your organization have that were caused by an API exploitation in the past two years?



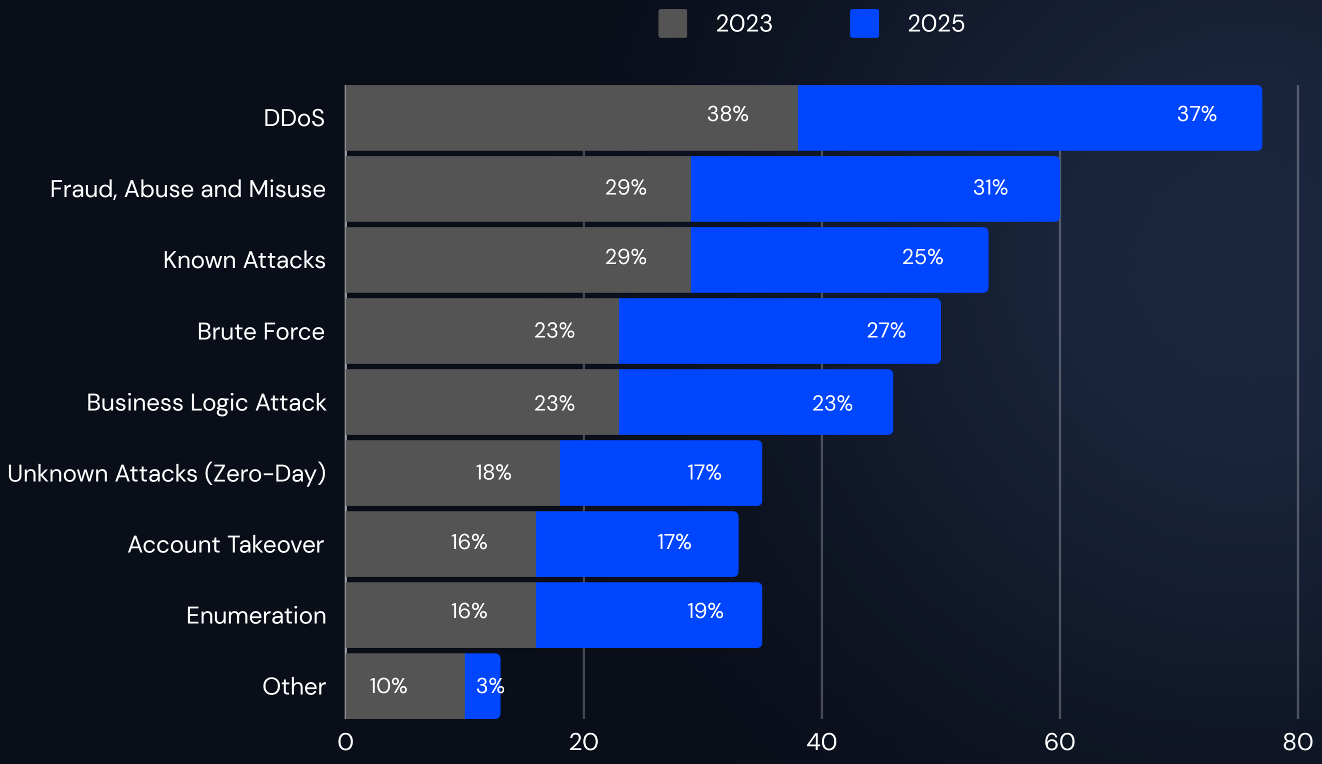
DDoS and Fraud Continue to be the Primary Breach Method; Brute Force Enters the Top 3.

The data presents a multifaceted landscape of the root causes behind data breaches, painting a picture of the complex challenges organizations face in today's digital environment. Leading the charge are DDoS attacks, reported by a significant 38% of respondents.

Such attacks, which flood systems with traffic to cause service interruptions, demonstrate the pressing need for organizations to bolster their defenses against volumetric threats.

Equally concerning is the fact that both known attacks, which have established signatures, and fraud, abuse, and misuse were cited by 29% of participants. This highlights a dual challenge: while organizations are struggling to fend off threats they should theoretically be prepared for, they're also wrestling with deceptive activities that might slip under traditional security radars.

The root causes of the one or more data breaches caused by an API exploitation in the past two years. More than one response permitted.



Financial Loss, Loss of Intellectual Property, and Brand Value Erosion are Top Consequences of API-related Data Breaches.

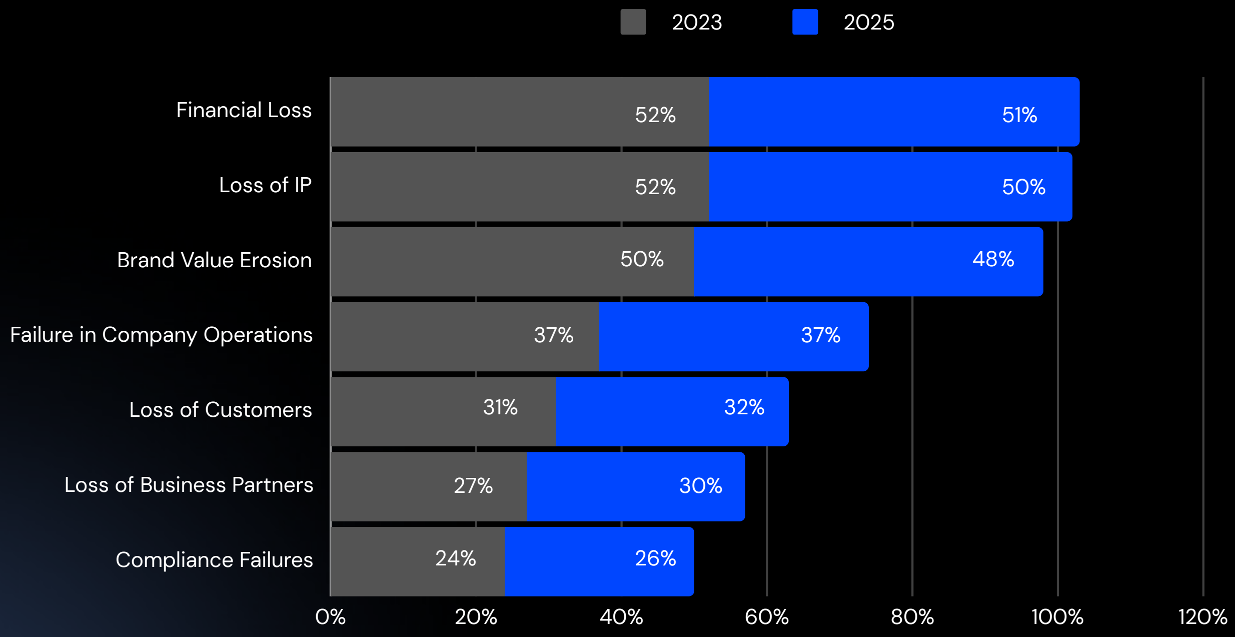
Financial consequences and loss of intellectual property (IP) equally resonating as the most severe, both experienced by 51% of the affected organizations.

Not far behind, brand value erosion was reported by 48% of respondents, underlining the substantial reputational risks involved. Operational disruptions were faced by 37%, indicating how breaches can fundamentally affect a company's core functionality.

Additional consequences include a decline in customer base (32%) and 30% faced a loss of business partners.

Notably, 26% struggle with non-compliance to regulations, highlighting the legal implications that come with security lapses.

The consequences of the one or more data breaches caused by an API exploitation. More than one response permitted.

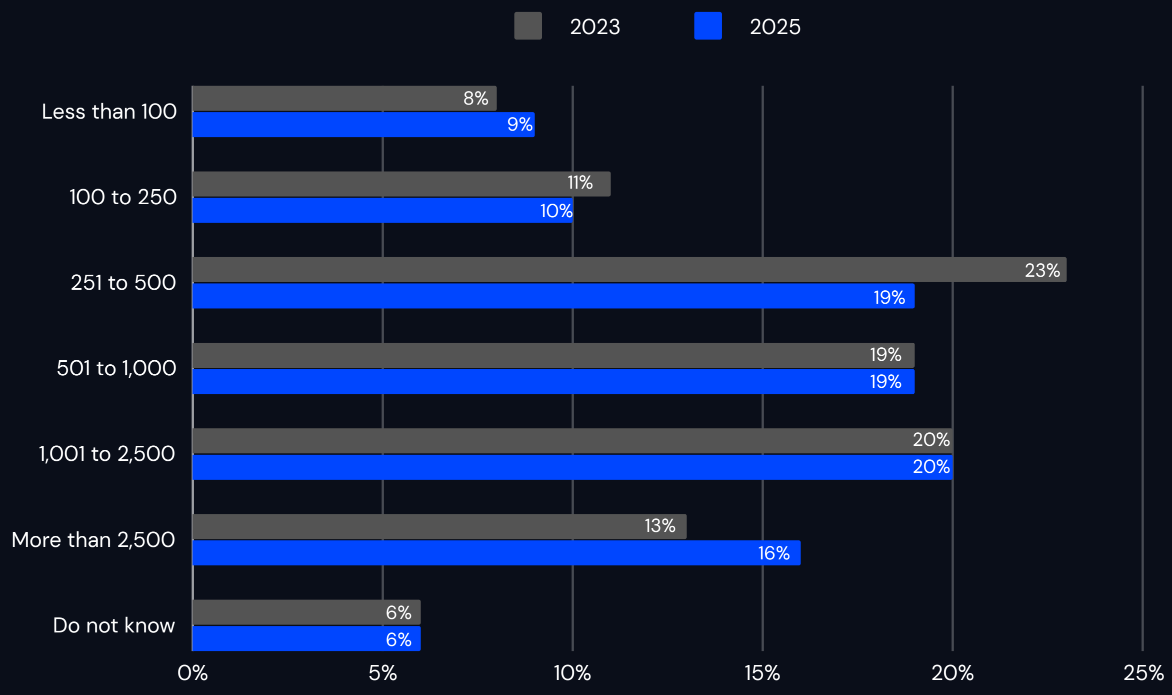


Over Half (55%) of Organizations Have at Least 500 APIs

The proliferation of digital platforms and services has led to a surge in the number of APIs used by organizations.

- **Only 9% use less than 100 APIs**, hinting at budding digital initiatives.
- **10% using 100-250 APIs** and **19% managing 251-500**, represent businesses scaling digital operations and integrations.
- **19% utilizing 501-1,000 APIs** and **20% navigating 1,001-2,500** suggests a complex ecosystem involving third-party integrations, extensive cloud usage, and global operations. It may reflect a highly digital-first business model, perhaps even a platform-based approach. While the flexibility and scalability offered by such a vast number of APIs are evident, so are the security challenges. The larger and more varied the API network, the more potential entry points for cyber threats.
- **16% operate with over 2,500 APIs** (up from 13% in 2023), indicative of vast enterprises with intricate digital touch points.
- 6% still **lack clarity on their API count**, signaling lack of visibility and potential security blind spots.

How many APIs does your organization use?



Diverse API Types and Their Implications for Security

Recent data unveils that organizations are widely using a range of APIs, and it's largely unchanged from the previous year – from Open APIs at 33%, Public APIs at 31%, to Private APIs at 30%. Additionally, Partner APIs (25%), Composite APIs (17%), Internal APIs (25%), and Third-party APIs (15%) also find their place in the organizational framework.

The assortment of API types in modern organizations highlights their intricate digital ecosystems:

Breadth of Integration Points: The prevalence of Open APIs (33%), Public APIs (31%), and Private APIs (30%) underscores the various integration points businesses operate with. Open and Public APIs often indicate external partnerships or services offered to a broader audience, while Private APIs are crucial for internal processes, linking various systems within an enterprise.

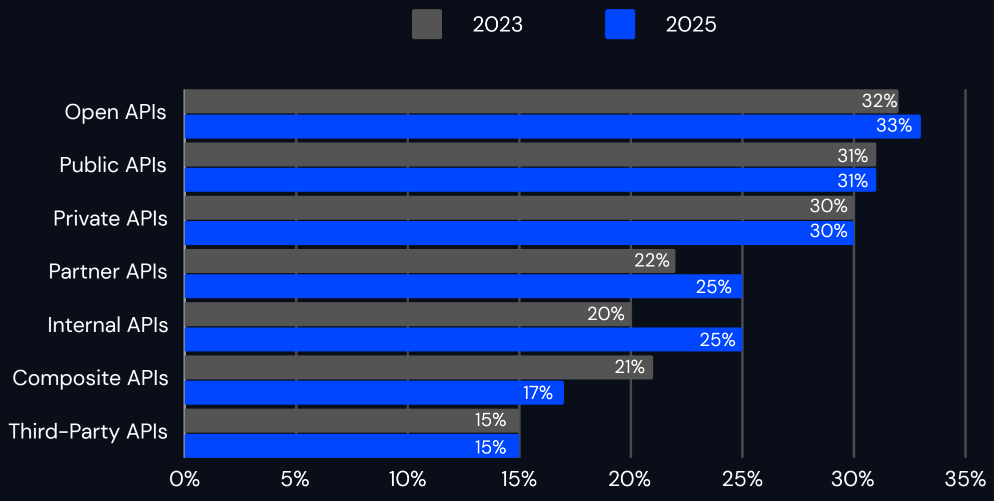
Collaborative Ventures: The utilization of Partner APIs (25%) suggests that a significant number of organizations are involved in collaborative ventures, relying on shared services or data to deliver value to their end-users. Such collaborations, while fruitful, can introduce additional vectors for vulnerabilities if not managed judiciously.

Internal Workflows and Flexibility: The use of Internal APIs (25%) and Composite APIs (17%) points towards the inclination of businesses to streamline their internal workflows and create flexible systems that can adapt to changing business needs. Composite APIs, which allow multiple data and service calls to be combined, demonstrate the push for efficiency in system design.

Reliance on Third Parties: The 15% usage of Third-party APIs reveals an external dependency wherein businesses leverage outside platforms or tools. This reliance can be for augmenting functionality, enhancing service offerings, or simplifying certain processes. However, it also means organizations are entrusting a portion of their operations, and potentially their data, to external entities, necessitating rigorous security scrutiny.

A Spectrum of Trust: The differentiation between Public, Private, and Partner APIs inherently indicates levels of trust. Public APIs are exposed to a wider audience, perhaps with limited access to certain functionalities. In contrast, Private APIs are often closely guarded. Meanwhile, Partner APIs represent a middle ground, where access is granted based on collaborative agreements.

What types of APIs does your organization use and/or provide?



Over half of the respondents (56%) echo the sentiment that the sheer volume of APIs makes it difficult to prevent attacks. As shown below, APIs' capacity to expand the attack surface across all layers of the technology stack is seen as a significant risk by a total of 58% of respondents, who either strongly agree or agree with the statement.

Fifty-seven percent of respondents say traditional security solutions are not effective in distinguishing legitimate from fraudulent activity at the API layer. The increasing number and complexity of APIs makes it difficult to track how many APIs exist, where they are located and what they are doing. As a result, 56 percent of respondents say the volume of APIs makes it difficult to prevent attacks.

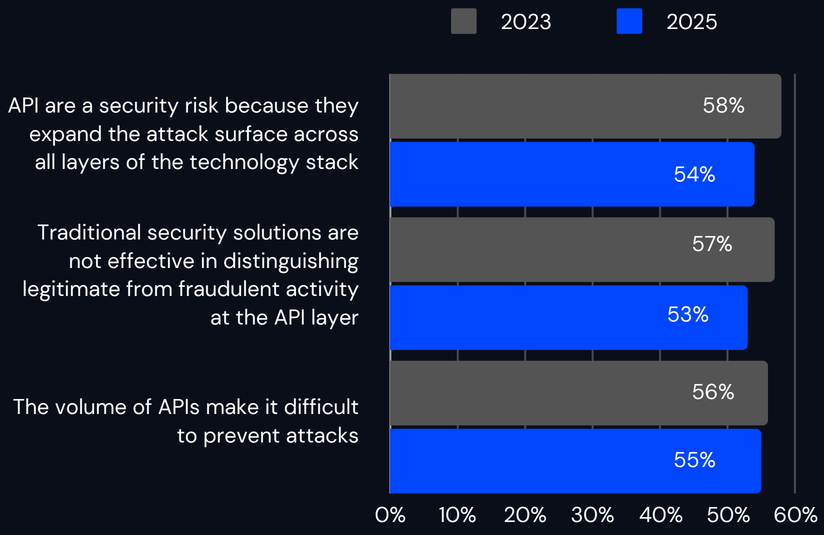
This finding underscores the need for new, effective security methodologies and solutions tailored for API protection.

54% say APIs expand the attack surface

53% say legacy solutions not effective

55% say volume of APIs make it difficult to stop attacks

Reasons why APIs are at risk



API sprawl continues to be the top API security challenge

It's clear that the API threat landscape is set to intensify. A substantial 61% of respondents anticipate that API risks will either significantly increase or increase over the next 12 to 24 months. Despite APIs' pivotal role, organizations struggle with significant challenges in securing them. Over half of respondents (54%) highlight preventing API sprawl as a top issue, while maintaining an accurate API inventory and prioritizing APIs for remediation, also emerged as considerable hurdles.

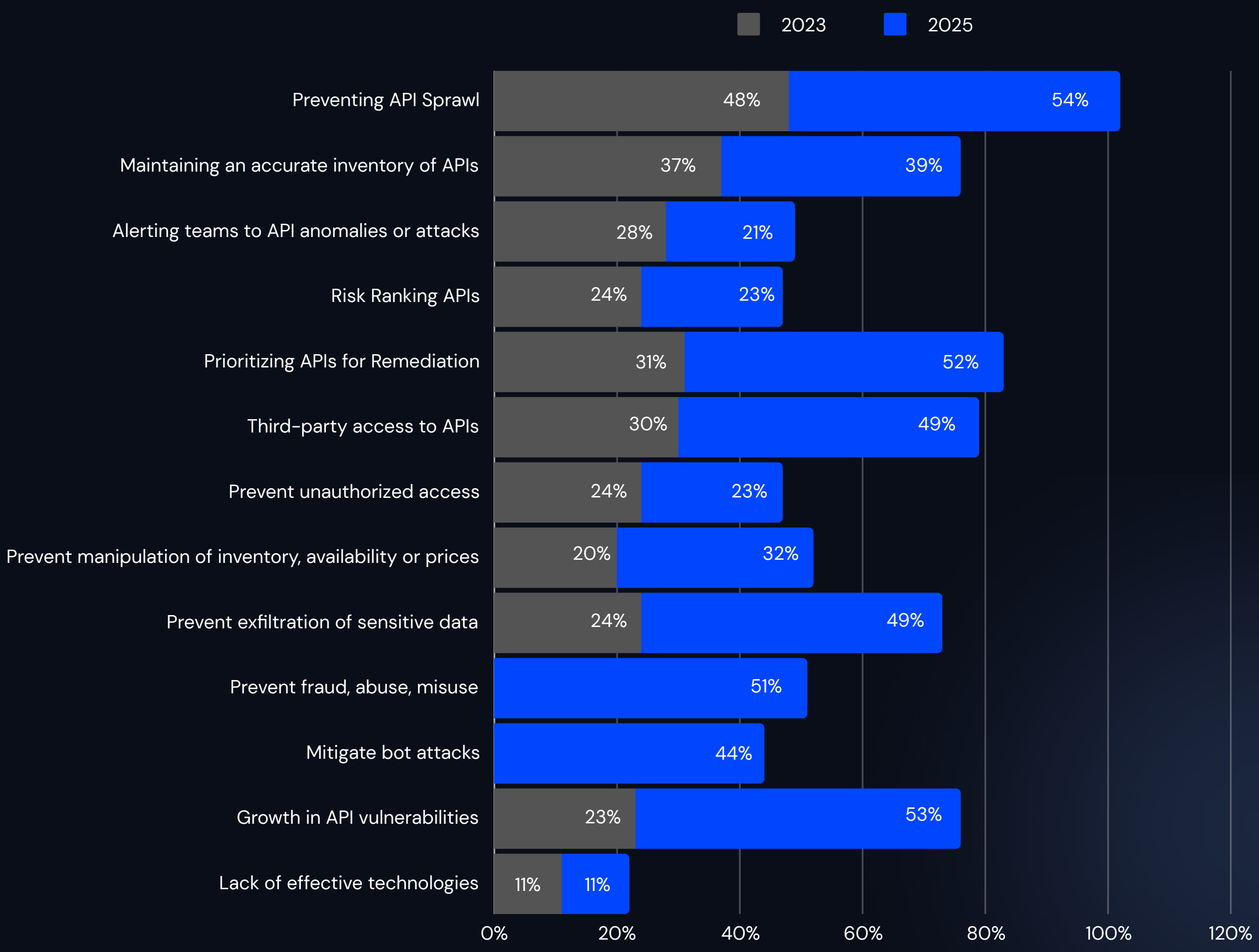
54%
preventing API Sprawl

53%
Growth in API vulnerabilities

52%
prioritizing remediation

51%
Prevent fraud, abuse, misuse

What are the top three challenges to securing APIs?
Respondents chose their top 3 challenges.



Part II:

Traditional Solutions Fall Short

Despite widespread deployment of traditional security tools like web application firewalls (WAFs) and API gateways, many organizations still struggle to secure their APIs effectively.

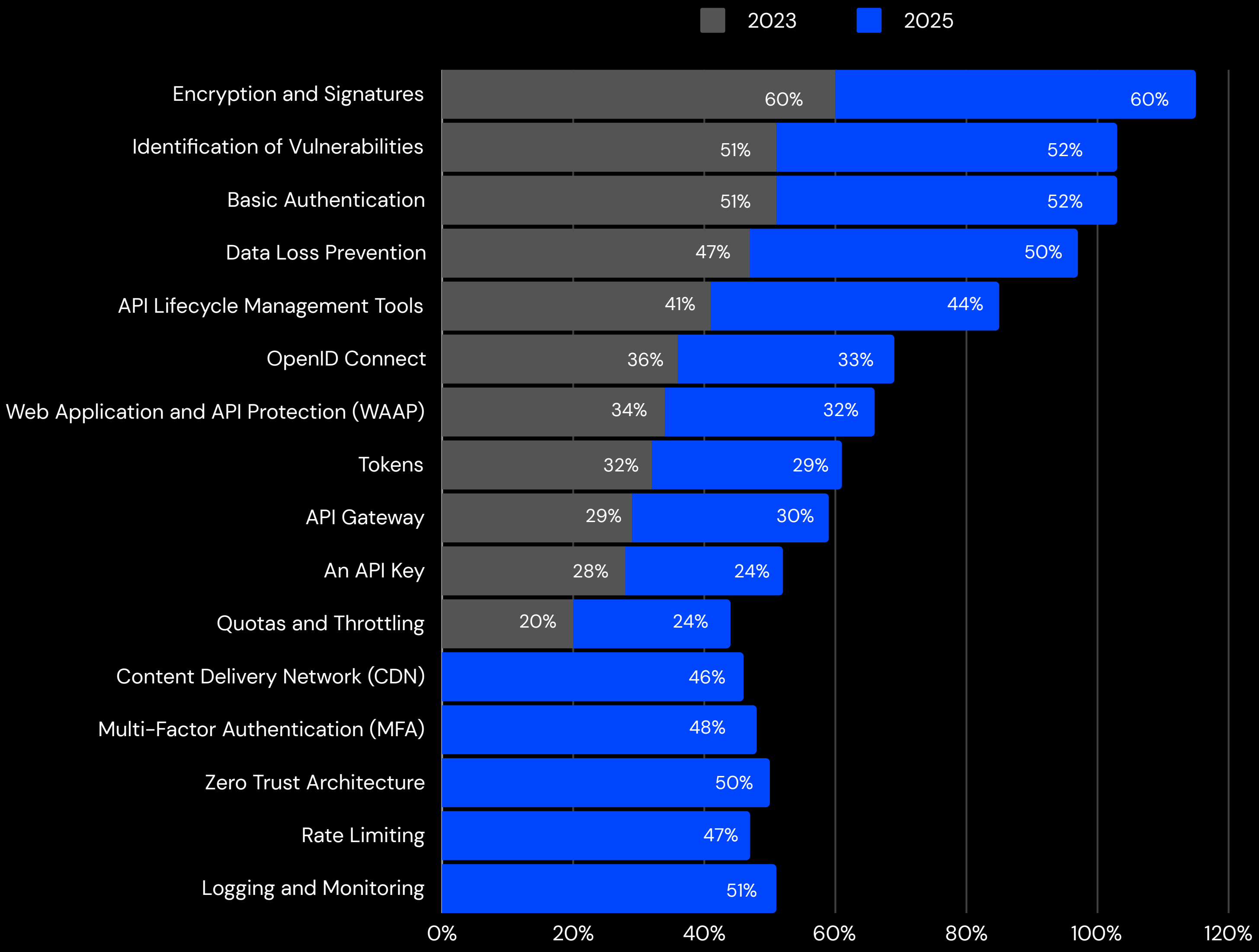
This chapter explores the limitations of these conventional approaches, highlighting their inability to address the unique and evolving threats posed at the API layer. It underscores the need for organizations to adopt more advanced and integrated security strategies that go beyond traditional measures.

Organizations deploy multiple solutions to protect their APIs.

Different solutions are deployed by organizations to secure their APIs, with encryption and signatures (60%), identification of vulnerabilities (52%), and basic authentication (52%) emerging as the most popular options. These are followed by API lifecycle management tools (44%), , and Data Loss Prevention (DLP) (50%).

New methods were noted this year with Content Delivery Networks (CDN) (46%), Multi-Factor Authentication (48%), Zero Trust architecture (50%), Rate Limiting (47%) and Logging and Monitoring (51%) being used for API protection.

Solutions used to achieve API security.
More than one response permitted.



Persistent Reliance on Ineffective API Security Solutions

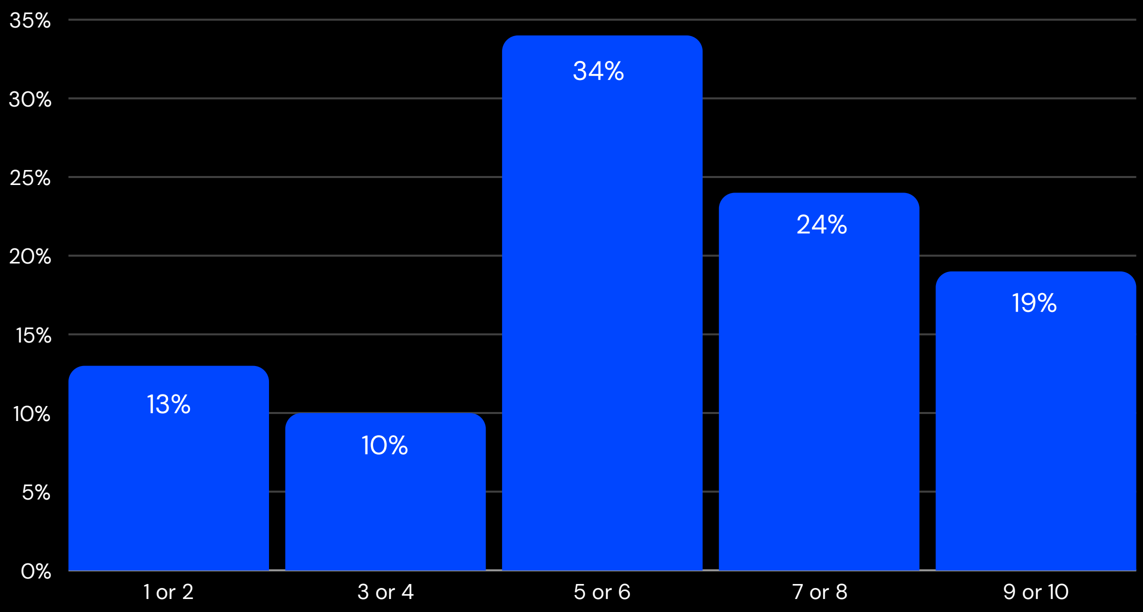
Despite the growing complexity of API threats, organizations continue to rely on the same traditional security solutions, even as their effectiveness remains questionable. **Only 19% of respondents rate their API security solutions as "highly effective" (scores of 9 or 10).**

The majority of organizations express far less confidence: 34% rate their tools as merely moderate (scores of 5 or 6), indicating ambivalence about their effectiveness.

Alarmingly, a combined 23% of respondents give their solutions low effectiveness scores (1 to 4), signaling a significant portion of organizations that acknowledge their current approaches are failing.

These numbers reveal a critical gap between the perceived need for API security and the actual performance of the solutions being deployed. As threats continue to evolve, the industry's reliance on outdated measures leaves organizations vulnerable, underscoring the urgent need for innovation in securing the API layer.

Please rate how effective the solutions your organization uses to achieve API security from 1 = not effective to 10 = highly effective.

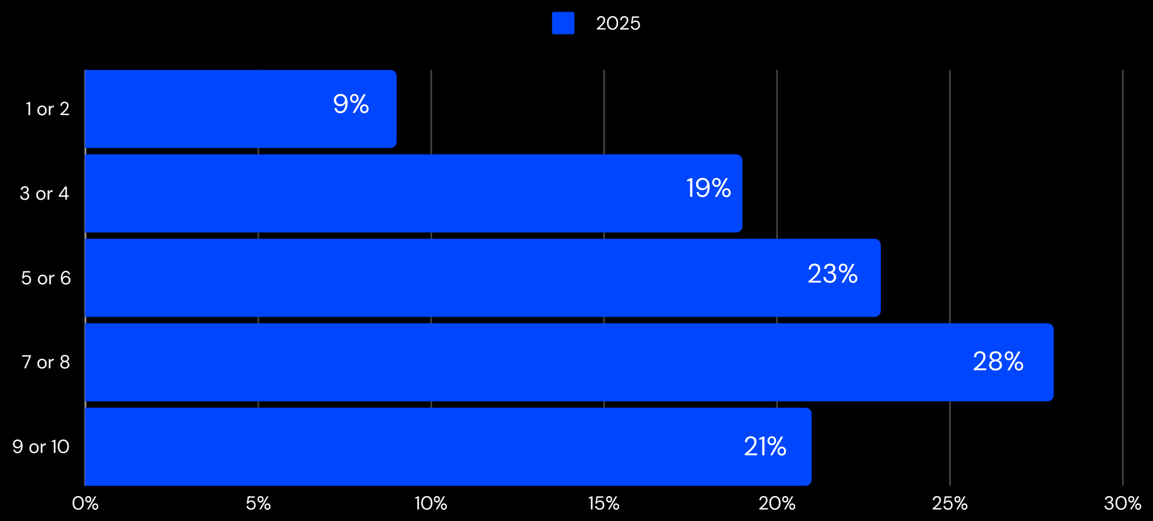


API Attack Protection: Gaps in Detection and Prevention

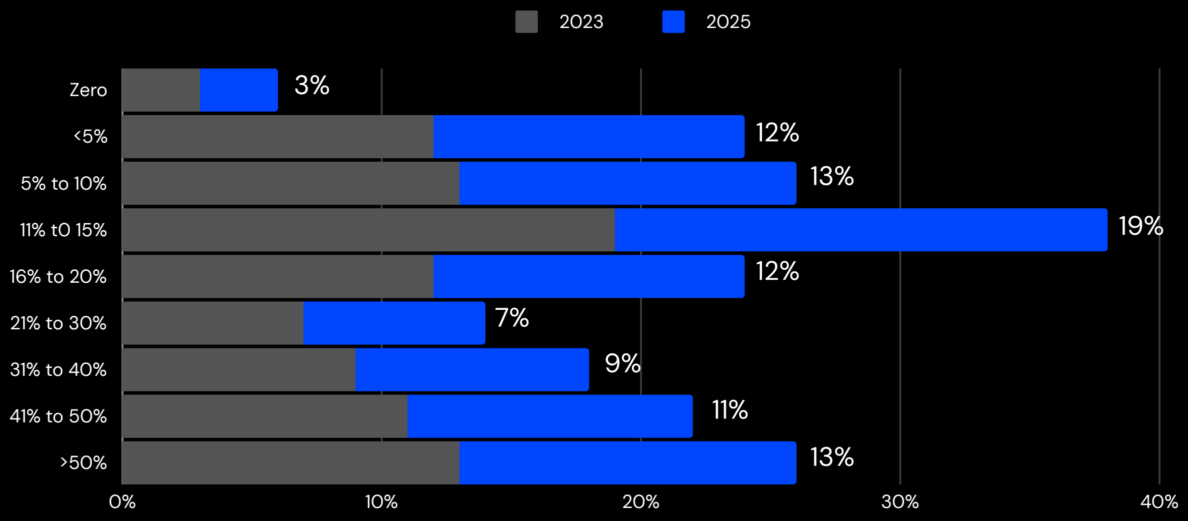
Organizations continue to face significant gaps in their ability to detect and prevent API attacks. Only 21% of respondents rate their detection capabilities as high (9 or 10), while 28% report moderate effectiveness (7 or 8), and 28% fall on the low end (1–4). These figures highlight the limited monitoring and response capabilities at the API layer.

In terms of prevention, only 13% of organizations can prevent more than half of API attacks—a number unchanged from last year. The majority are unable to block even 20% of attacks, with 19% preventing just 11–15%. This stagnation underscores the need for improved tools and strategies to secure API environments and address the evolving threat landscape.

Rate the ability of your organization to detect attacks at the API layer from 1 = no ability, to 10 = high ability



What percentage of all attacks against APIs can your organization prevent?



Part III:

The Escalating Threat of Bot Attacks on APIs

APIs are a growing target for bot attacks, which can disrupt services, steal data, and compromise systems. The 2025 Global State of API Security Report highlights the increasing prevalence of these attacks and the ongoing struggle organizations face in effectively mitigating them.

53% of organizations reporting at least one bot-related incident targeting their APIs

Bot attacks represent a growing challenge in the API security landscape, with 53% of organizations reporting at least one bot-related incident targeting their APIs. This prevalence underscores the persistent and evolving nature of the threat. Notably, 44% of organizations cite bot attacks as a significant obstacle in securing their API environments, indicating that many businesses struggle to manage these attacks effectively.

Despite awareness of the issue, only 21% of organizations describe their ability to mitigate bot traffic as "high." This suggests a gap between the recognition of the threat and the effectiveness of the measures currently in place. Organizations are deploying a range of tools to combat bot attacks, but the results are mixed.

The most commonly used solutions include web application firewalls (WAFs), deployed by 52% of organizations, and content delivery networks (CDNs), used by 49%. These tools are designed to filter and block malicious traffic, but their efficacy in the context of API-specific threats is limited. Active traffic monitoring, employed by 48% of organizations, helps track API endpoint activity, providing real-time data that can be valuable in detecting and responding to attacks.

API rate limiting, a strategy implemented by 42%, and assertive rate-limiting policies (used by 33%) are additional methods aimed at curbing the frequency and volume of API calls, effectively reducing the attack surface.

However, these measures, while helpful, are not sufficient on their own. The variety of tools and strategies deployed reflects an industry grappling with a complex issue, yet the lack of a unified, high-confidence approach indicates that many organizations remain vulnerable.

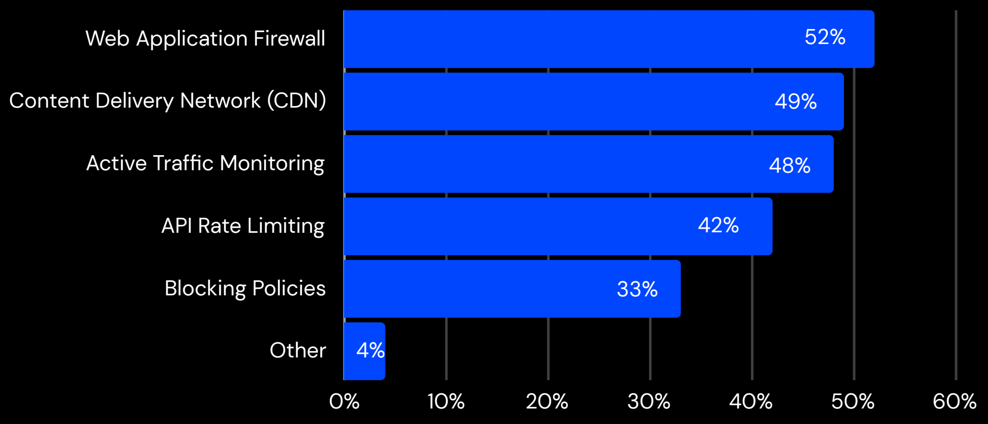
The findings highlight a critical need for more advanced, integrated solutions that can proactively identify and respond to bot traffic.

As bot attacks grow in sophistication, organizations must move beyond reactive measures and develop robust, coordinated strategies to secure their APIs effectively.

53%

of organizations reporting at least one bot-related incident targeting their APIs.

Organizations employ various tools to defend APIs against bot attacks (respondents could choose more than one)



Part IV:

Generative AI and API Security

As generative AI adoption accelerates, organizations face new challenges and risks related to API security. With 67% of respondents either currently adopting or planning to adopt generative AI, the expanded attack surface, data leakage concerns, and unauthorized access risks become increasingly significant.

This section explores these emerging threats, the priorities for securing APIs in AI applications, and the primary challenges organizations encounter as they work to safeguard their generative AI API integrations.

Key API Security Concerns with Generative AI Applications

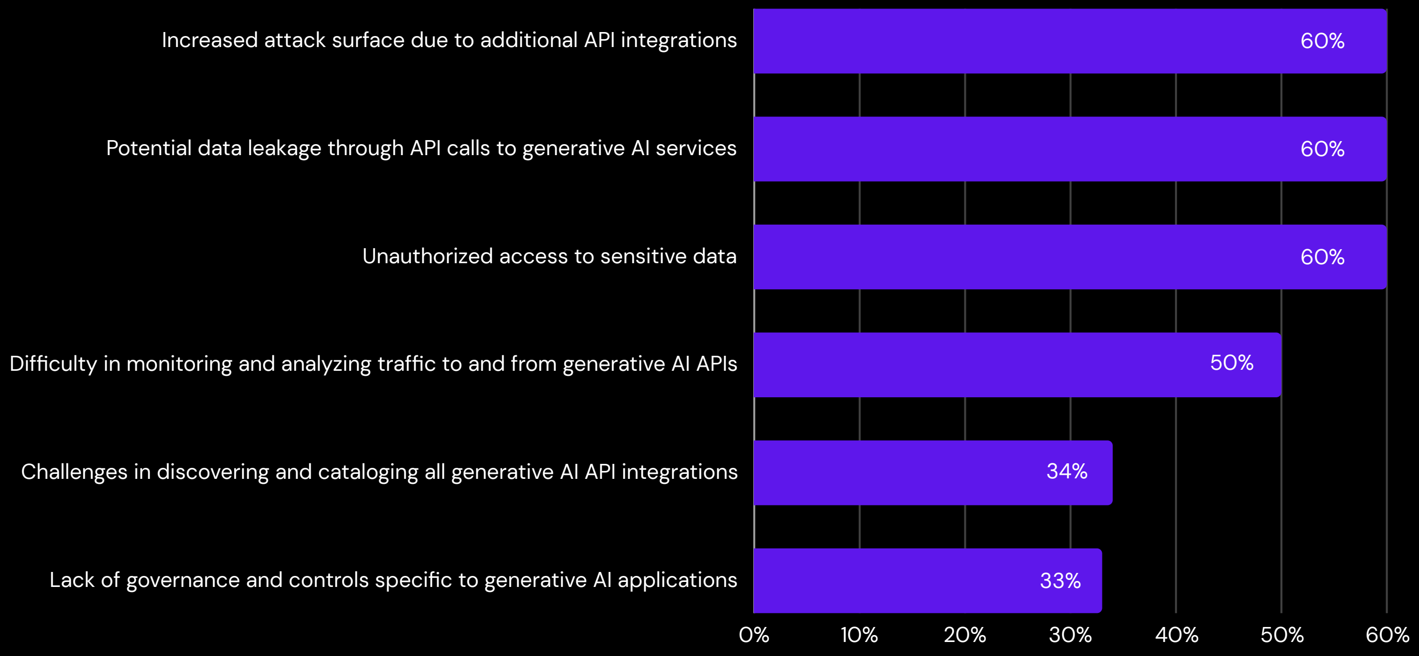
Organizations cite several top concerns with integrating generative AI into their API ecosystems. The most significant issues include:

- Increased attack surface due to additional API integrations (60%): With generative AI comes a surge in new API connections, each expanding the potential entry points for attackers.
- Potential data leakage through API calls (60%): As AI systems exchange large volumes of data, the risk of sensitive information exposure grows.
- Unauthorized access to sensitive data (60%): Organizations fear that poorly secured generative AI APIs could become a gateway for attackers to access critical information.

Other notable concerns include the difficulty in monitoring and analyzing traffic to and from AI APIs (50%), as well as the challenges in cataloging and managing generative AI API integrations (34%).

The lack of governance and controls specific to generative AI applications also poses a risk for 33% of respondents, emphasizing the need for more structured management approaches.

What are the top concerns regarding API security in relation to generative AI applications? Respondents selected top 3 concerns only.



Part V:

Governance, Ownership and Budget: The Strategy and Finance of API Security

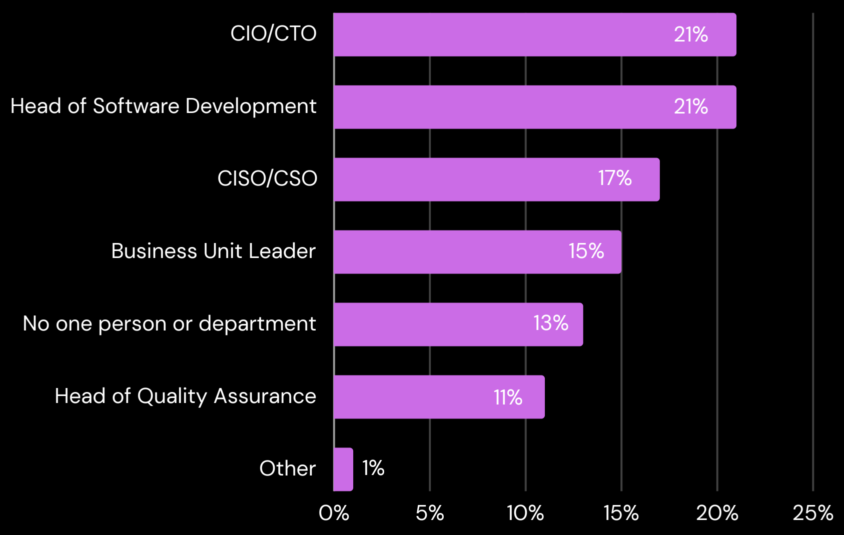
Effective API security goes beyond technology—it requires clear ownership, strategic governance, and well-aligned budget priorities. This chapter examines how organizations allocate responsibility for API security, the influence of compliance and risk management on budget decisions, and the impact of leadership structures on securing API ecosystems.

By exploring these critical factors, the chapter highlights the importance of a unified approach that integrates strategy, accountability, and financial investment.

API Security Ownership: A Mixed Bag

Ownership of API usage and security programs remains fragmented across organizations, with no single role or department taking a dominant lead.

Who within your organization "owns" the API usage and security program?



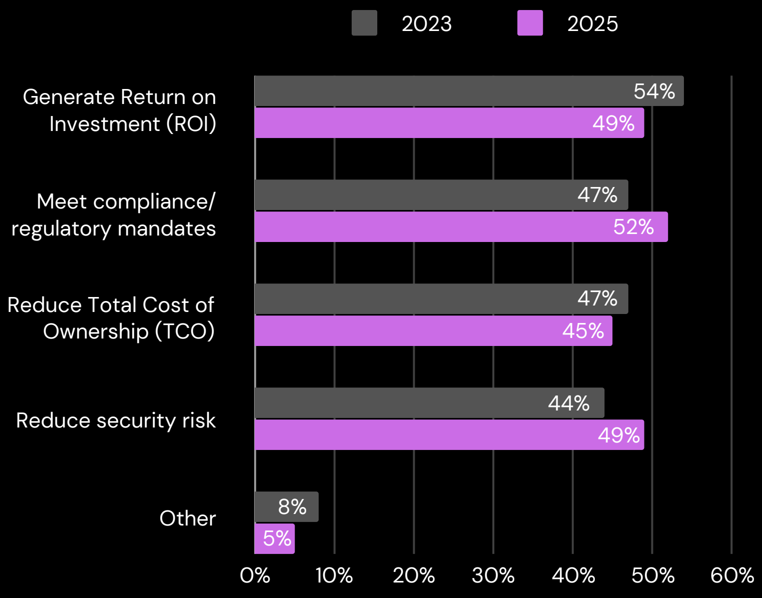
According to the data, 21% of organizations assign this responsibility to the CIO/CTO, while another 21% place it under the head of software development. 17% have their CISO or CSO overseeing API security, and 15% leave it to line-of-business (LOB) leaders. Interestingly, 11% delegate this role to the Head of Quality Assurance.

However, 13% of organizations report that no one person or department officially owns the API security program, indicating a lack of clear accountability. This fragmented approach underscores the need for unified leadership and ownership to effectively manage and secure API environments across enterprises.

Compliance Drives Security Budget Decisions in 2025

In 2025, compliance has become the most influential factor driving security budget and investment decisions, cited by 52% of organizations—up from 47% in 2023.

What are the most important drivers for your organization's security budget and investment decisions? Two responses permitted.



This shift highlights an increasing focus on regulatory requirements and industry standards as organizations prioritize meeting compliance obligations.

While ROI and risk reduction remain significant drivers at 49% each, the emphasis on compliance underscores the growing pressure organizations face to align their security strategies with regulatory demands.

Additionally, reducing total cost of ownership (TCO) continues to influence decisions, with 45% of organizations listing it as a key consideration.

Where do we go from here?

APIs are now a critical part of the digital infrastructure, but their rapid growth has brought significant security challenges. This year's survey shows that API security is not just important—it's essential. 57% of organizations reported at least one API-related breach in the past two years, yet only 19% rate their existing security measures as effective. This highlights a serious gap between the need for API security and the capability of current solutions.

Traditional methods, like web application firewalls and API gateways, are proving inadequate in the face of evolving threats such as bot attacks, fraud, and the risks associated with generative AI. Despite clear evidence of their limitations, organizations continue to rely on these outdated approaches. This reluctance to adapt and evolve their security measures is leaving them exposed to increasingly sophisticated threats.

The challenge of managing API sprawl further complicates the situation. 54% of organizations report difficulties in tracking and managing the expanding number of APIs in their environments. Without proper inventory and control, the risk of unauthorized access and breaches remains high. Moreover, many organizations struggle to apply consistent policies and standards across their API ecosystems, which increases their exposure.

AOwnership of API security remains fragmented. Responsibilities are divided among CIOs, heads of development, CISOs, and others, leading to a lack of clear accountability and making it difficult to build a cohesive security strategy.

This disjointed approach weakens overall efforts to secure APIs and protect critical data. Looking ahead, 61% of organizations expect API risks to increase over the next 12 to 24 months. This trend suggests that, unless organizations rethink their strategies and move away from traditional, ineffective solutions, they will continue to face significant vulnerabilities.

The data underscores the need for a more proactive, unified, and effective approach to API security.

About Traceable

Traceable is the industry's leading API Security company that helps organizations achieve API protection in a cloud-first, API-driven world. With an API Data Lake at the core of the platform, Traceable is the only intelligent and context-aware solution that powers complete API security – security posture management, threat protection and threat management across the entire Software Development Lifecycle – enabling organizations to minimize risk and maximize the value that APIs bring to their customers. To learn more about how API security can help your business, book a demo with a security expert.

www.traceable.ai

TRACEABLE