TRACEABLE

2023 State of API Security:

A Global Study on the Reality of API Risk

The industry's first global report investigates API data breaches, API sprawl, ownership, governance, zero trust, and the path to a secure future.

Ponemon INSTITUTE

TRACEABLE

Table of Contents

TRACEABLE.

A Letter from Traceable CEO, Jyoti Bansal

Dear Friends and Industry Colleagues,

As the digital landscape continues to evolve at an accelerated pace, one thing remains clear: APIs have become a crucial backbone to nearly every business operation in existence. However, with their ubiquitous adoption comes an equally pressing concern – API security. As the CEO of Traceable, I am committed to ensuring we understand, confront, and adapt to the ever-changing dynamics of this complex field.

Recognizing the critical nature of this area, we found a pressing need for a more comprehensive understanding of the State of API Security across different sectors and geographies. Despite APIs being critical to the modern enterprise, until now, there has not been an extensive, multi-country, industry-wide study offering a panoramic view of the API security landscape. We believed that it was time to fill this gap and embarked on this research journey with the Ponemon Institute.

Our joint effort has culminated in this extensive survey. Titled, The 2023 State of API Security: A Global Study on the Reality of API Risk, the report explores the complex worlds of API-related data breaches, API sprawl, API ownership, fraud and abuse, Zero Trust, and an analysis of organizations' current API security practices.

We gathered and analyzed data from a diverse range of enterprise organizations, aiming to provide a holistic view of current practices, challenges, and opportunities in API security. Our aim is to enable informed decisions, foster strategic dialogue, and ultimately contribute to the collective goal of bolstering security in our interconnected digital world.

This report is more than a compilation of data points—it's a reflection of our shared experiences, struggles, and triumphs in navigating the complex terrain of API security. My hope is that the insights contained within these pages will guide conversations, influence strategies, and help us all navigate our organizations effectively and confidently into the future.

As we delve into the state of API security, I would like to express my gratitude to the hundreds of professionals who contributed their time and insights to this research. Your participation has made this report a valuable asset for executives, decision-makers, and security professionals across the globe.

Together, we are building the foundation for a more secure digital future. I invite you to read, reflect, and engage with the findings of this report as we continue this important mission.

Sincerely,

Jyoti Bansal
Co-Founder and CEO, Traceable

Introduction

In an era where technology is the lifeblood of business, understanding the intricacies of API security is paramount. Sponsored by Traceable, this research delves deep into the pulse of global organizations, gauging their awareness and strategies towards mitigating API security risks. The Ponemon Institute, in partnership with Traceable, engaged 1,629 cybersecurity experts spanning the United States, the United Kingdom, and EMEA. This research offers a unique window into the evolving landscape of API security.

APIs, the unsung heroes of our digital age, are the bridges that allow disparate applications to converse seamlessly. As the conduits for everything from sensitive medical records to financial data, their role in modern organizations cannot be overstated. Indeed, 57% of our respondents underscored the critical importance of APIs in their digital transformation journeys. Yet, with great power comes great responsibility. APIs, if left vulnerable, can be the Achilles' heel of an organization. A staggering 60% of participants revealed that their organizations had suffered a data breach due to API vulnerabilities, leading to significant intellectual property theft and financial repercussions.

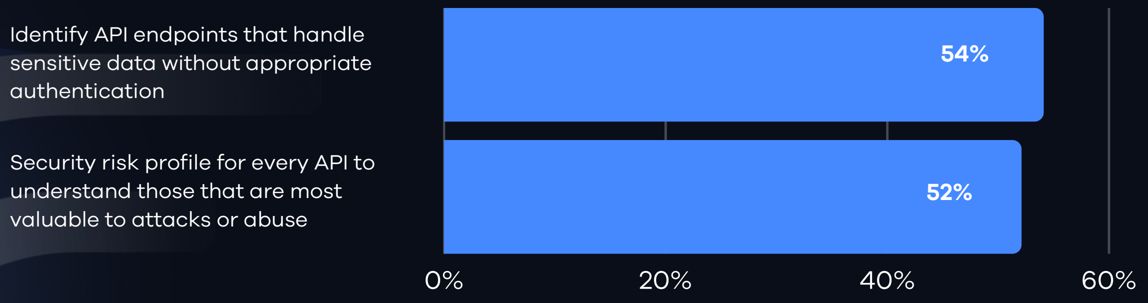
One of the most illuminating insights from this study is the juxtaposition of the potential for major security incidents against the apparent complacency of organizations. When asked to prioritize the importance of having a comprehensive security risk profile for every API and the ability to pinpoint API endpoints managing sensitive data without adequate authentication, the responses were telling.

As depicted in Figure 1, a mere 52% felt the urgency to understand the most vulnerable APIs based on a security risk profile, while 54% deemed the identification of sensitive data-handling API endpoints as a high priority.

In the grand scheme of IT security budgets, which average at a robust $35 million for the organizations in this study, only a fraction, approximately $4.2 million, is channeled towards API security endeavors. Intriguingly, the mantle of API security budget predominantly rests with 35% of IT and IT security functions.

Figure 1. Organizations are ignoring the API security risk

On a scale from 1 = not a priority to 10 = a very high priority, 7+ responses presented



Top Findings At-A-Glance

Organizations Are Losing the Battle to Secure APIs

One reason is that organizations do not know the extent of API risk. Specifically, on average, only 40 percent of APIs are continually tested for vulnerabilities. As a result, organizations are only confident in preventing an average of 26 percent of attacks and an overage of only 21 percent of API attacks can be effectively detected and contained.

60% of organizations experienced an API-related data breach in the past two years; 74% experienced at least 3 API-related breaches.

60% of organizations reported a breach in the past two years. It is not a one-time event as a significant 34% reported experiencing 3-4 breaches, indicating deep-rooted risk, vulnerabilities and insufficient remediation measures. Alarmingly, 40% of these organizations suffered from five or more breaches, emphasizing the need for stronger API security measures. The most vulnerable group, 11%, reported more than seven breaches, highlighting chronic security issues.

DDoS, Fraud, and API Attacks Are Top API Breach Methods

Our survey underscores that DDoS attacks stand out as the predominant API attack method resulting in a breach, with 38% of respondents confirming this. Intriguingly, fraud and known attacks are neck and neck for the second spot, each cited by 29% of participants as a major cause of data breaches.

Solutions are needed to reduce third-party risks and detect and stop data exfiltration events happening through APIs

An average of 127 third parties are connected to organizations' APIs and only 33 percent of respondents say they are effective in reducing the risks caused by these third parties' access to their APIs. Only 35 percent of respondents say they are effective in identifying and reducing risks posed by APIs outside their organizations and 40 percent say they are effective in identifying and reducing risks within their organizations. One reason is that most organizations do not know how much data is being transmitted through the APIs and need a solution that can detect and stop data exfiltration events happening through APIs.

TRACEABLE

Top Findings At-A-Glance cont...

Majority of Respondents Are Not Confident in Traditional Solutions to Protect APIs

Fifty-seven percent of respondents say traditional security solutions are not effective in distinguishing legitimate from fraudulent activity at the API layer. Further, 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 (56 percent of respondents).

61% of organizations anticipate that API risk will increase or significantly increase over the next 24 months

The anticipation of API risk in the near future showcases a notably cautious outlook among organizations. A significant majority, totaling 61%, expect the risk associated with APIs to either increase or significantly increase over the next 12 to 24 months. This suggests a prevailing sentiment that as the digital landscape continues to evolve, so too do the challenges and threats associated with it. Only 15% of respondents believe the risk will decrease, hinting at the urgent need for better API management and security solutions in the rapidly changing tech environment.

58% of respondents state that APIs expand the attack surface

A significant 58% of respondents either strongly agree or agree with the assertion that APIs expand the attack surface across all layers of the technology stack. This highlights a widespread recognition of the risk introduced by APIs, despite their indispensable role in the digital landscape.

48% of organizations report that API sprawl is their top challenge

Securing APIs presents a dynamic set of challenges for organizations. Topping the list, as reported by 48% of respondents, is preventing API sprawl, reflecting the rapid proliferation of APIs in the modern enterprise. The second most pressing challenge, identified by 39%, is maintaining an accurate inventory of APIs, followed by managing third-party access to APIs, at 30%.

Methodology

This research report is a collaborative study with the Ponemon Institute that surveyed 1629 respondents, across 32 countries and over 6 major industries. This included organizations with at least 1000 employees, to those with over 75,000 employees. The survey tackles the complexities of API-related data breaches, API sprawl, API ownership, attacks and exploits, fraud and abuse, as well as the adoption of Zero Trust methodologies.

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.

1629 respondents

100 countries

Key Findings

The 2023 State of API Security offers valuable insights into the challenges, trends, and solutions employed by organizations in protecting their APIs. By examining the survey data, we gain a deeper understanding of the risks, vulnerabilities, and emerging strategies related to API security.

These global findings serve as a foundation for organizations seeking to enhance their security posture and mitigate potential risks.

Note: The complete findings are presented in the appendix of this report.

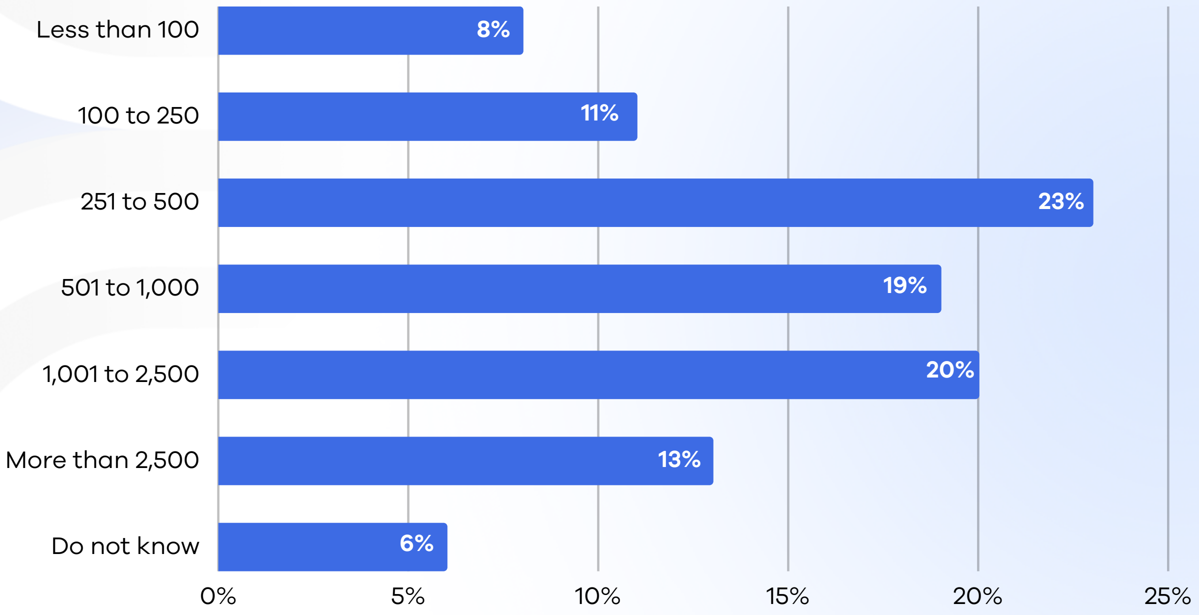
Part I: APIs: With Great Use Comes Great Responsibility

The Vast API Landscape: Numbers Don't Lie

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

- 8% handle less than 100 APIs, hinting at budding digital initiatives.
- 11% using 100-250 APIs and 23% 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.
- 13% operate with over 2,500 APIs, indicative of vast enterprises with intricate digital touchpoints.
- 6% lack clarity on their API count, signaling lack of visibility and potential security blind spots.

Figure 2. How many APIs does your organization use?



Diverse API Types and Their Implications for Security

The use of diverse API types is reflective of today's interconnected digital ecosystems and highlights the dynamic nature of modern businesses. Recent data unveils that organizations are widely using a range of APIs - from Open APIs at 32%, Public APIs at 31%, to Private APIs at 30%. Additionally, Partner APIs (22%), Composite APIs (21%), Internal APIs (20%), 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 (32%), 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.

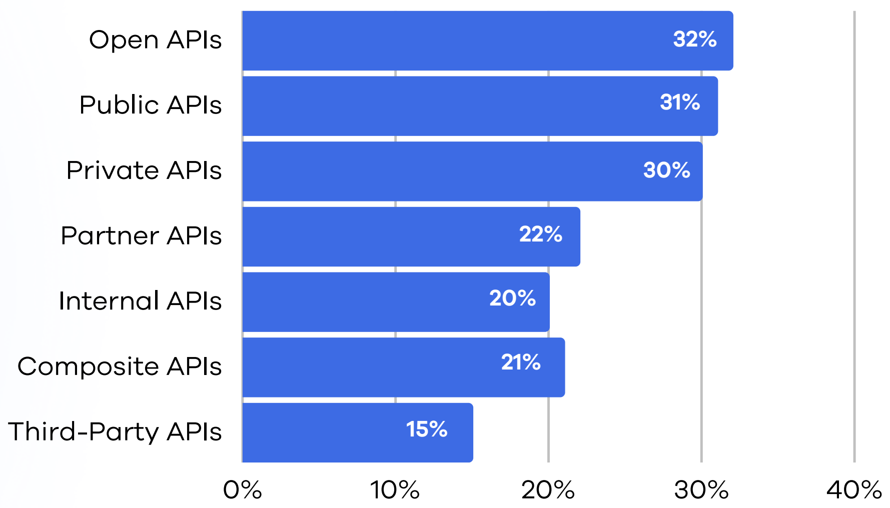
Collaborative Ventures: The utilization of Partner APIs (22%) suggests that a significant number of organizations are involved in collaborative ventures, relying on shared services or data to deliver value to their end-users. Such collaborations, while fruitful, can introduce additional vectors for vulnerabilities if not managed judiciously.

Internal Workflows and Flexibility: The use of Internal APIs (20%) and Composite APIs (21%) 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.

Figure 3. What types of APIs does your organization use and/or provide?



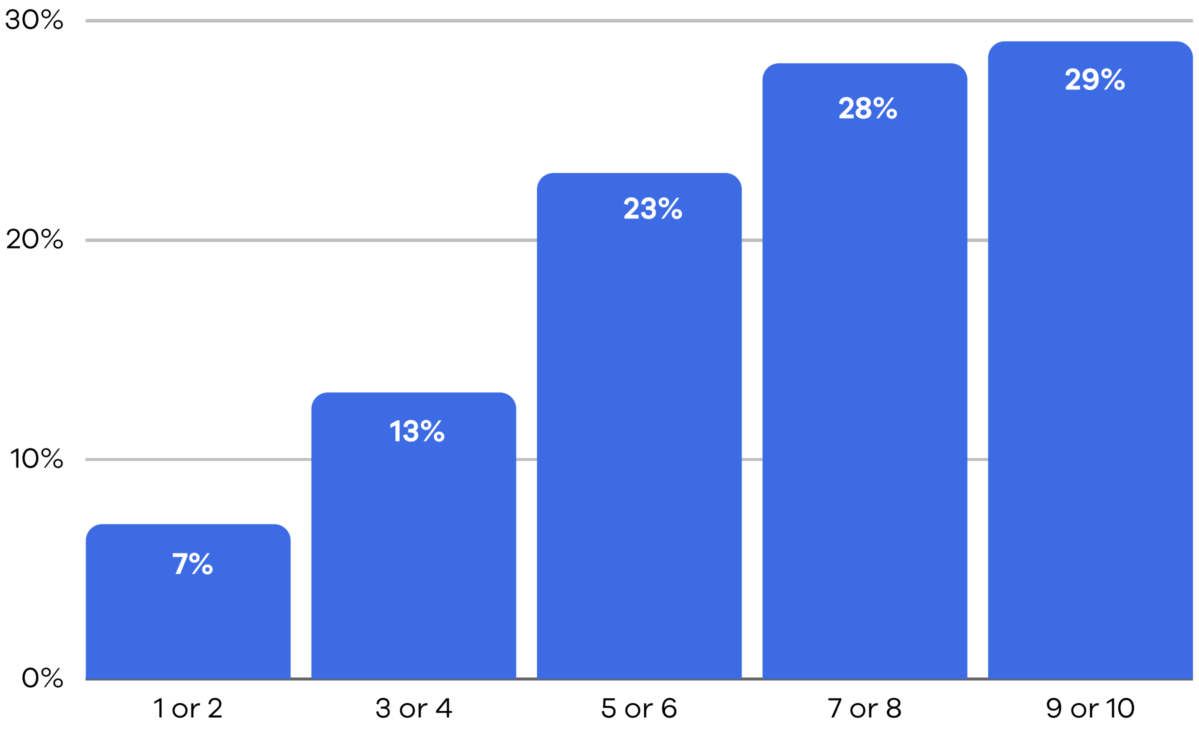
APIs Are the Cornerstone of Digital Initiatives

APIs are undeniably significant to the digital transformation agendas of organizations globally. An analysis of the data shows that a majority of organizations (57%) rate the importance of APIs at a 7 or higher on a scale of 1 to 10. Particularly telling is the combined 29% of respondents who rank APIs at the utmost levels of importance, with scores of 9 or 10.

Conversely, only a minority, 20% of participants, deem APIs to have low to moderate importance (scores of 1 to 4). The middle ground, represented by ratings of 5 or 6, is held by 23% of organizations, indicating a neutral stance.

The data underscores a collective acknowledgment: As digital transformation accelerates, APIs are not just supplementary; they are foundational. Most organizations are cognizant of their pivotal role, with only a small segment undervaluing their significance. This points towards a trend of increasing integration and digitization, with APIs serving as essential building blocks in the modern digital landscape.

Figure 4. Please rate how important APIs are to your organization's digital transformation programs from 1 = not important to 10 = highly important.

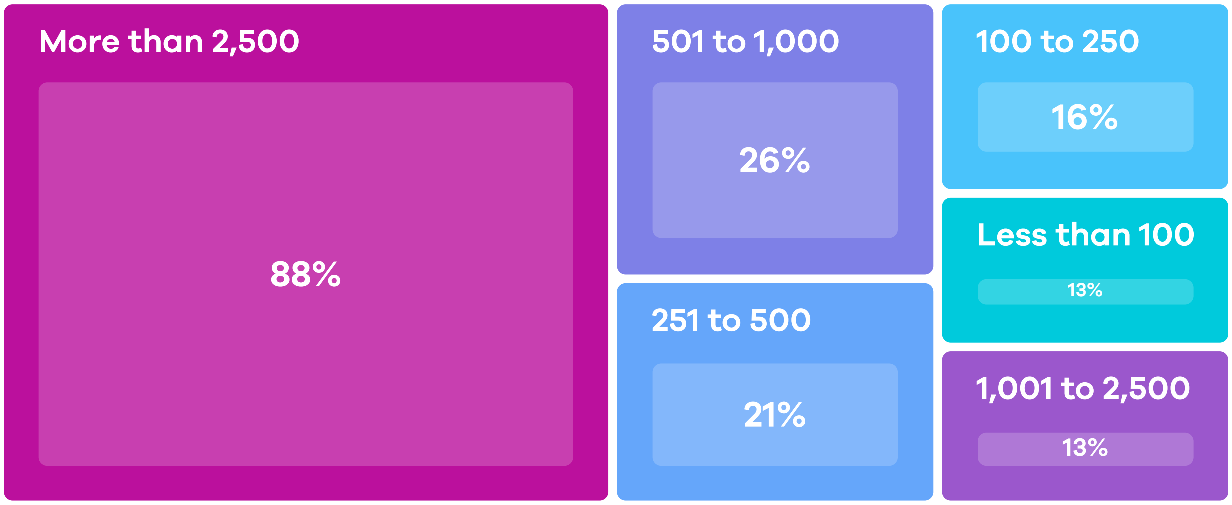


When Thousands Meet Thousands: The Growth of Cloud Applications in an API-Driven Age

A staggering 88% of organizations use more than 2,500 cloud applications.

This mass adoption is representative of an era where digital infrastructures have evolved rapidly, scaling operations to unprecedented levels. The versatility offered by cloud applications is undeniable, but as we said, with great use comes great responsibility.

Figure 5. How many cloud applications does your organization use?



The increasing reliance on these applications has correspondingly elevated the role and importance of APIs. These integration points allow different software tools to communicate, which is crucial for the smooth functioning of vast cloud ecosystems. But as with all technology, APIs come with their own set of challenges, especially when it comes to security.

And here lies the crux of the matter: with the rise in the use of cloud applications and a complex API ecosystem, there's an inherent increase in associated risks. A significant 61% of organizations anticipate that API risk will increase in the next 12 to 24 months, whereas only 15% expect a decrease. This looming risk is bound to impact the expansive growth in cloud application use and the multiplicity of API types in play.

Further, 58% of respondents agree or strongly agree that APIs extend the attack surface across all layers of the technology stack. This expansion of the attack surface is a cause for concern, particularly when considering the vast number of cloud applications that enterprises deploy. Each API acts as a potential vulnerability point, making the large-scale use of cloud applications a veritable minefield if not properly managed.

Over half of the respondents (56%) echo the sentiment that the sheer volume of APIs makes it difficult to prevent attacks. As shown in Figure 6, 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.

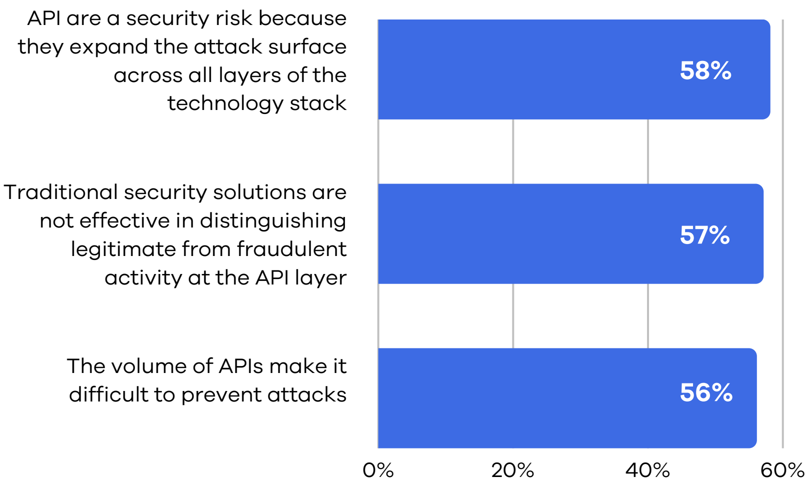
This finding underscores the need for new, effective security methodologies and solutions tailored for API protection.

58% say APIs expand the attack surface

57% say legacy solutions not effective

56% say volume of APIs make it difficult to stop attacks

Figure 6. Reasons why APIs are at risk



Part II:
Persistent and Escalating API Breaches: A Deep Dive into the Numbers

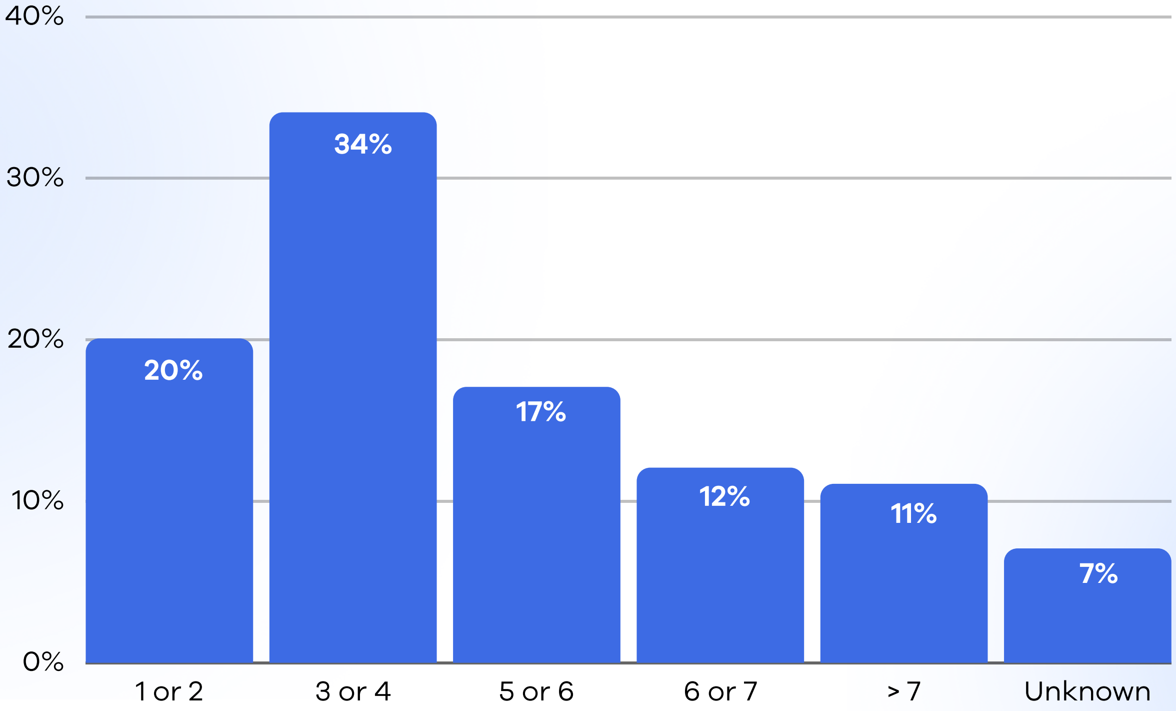
60% of organizations experienced an API-related data breach in the past two years. An overwhelming 74% experienced at least three breaches.

Multiple API-related breaches are alarmingly common. Here's the breakdown:

A striking 60% of organizations have been victim to an API-related data breach within the recent two years, highlighting the escalating threats aimed at APIs. Out of these, a substantial 74% suffered from three or more breaches, suggesting either a consistent security gap or recurrent threat actors exploiting these vulnerabilities. A notable 34% of respondents encountered 3 to 4 breaches, suggesting repeated vulnerabilities. Additionally, while one in five organizations experienced just 1 to 2 breaches, a nearly equal proportion (17%) faced 5 to 6 incidents, highlighting the recurring nature of these intrusions.

Worse, 23% (12% from 6 to 7 and 11% for more than 7) endured over six breaches, accentuating the persistent threats facing today's digital infrastructures. Of note, 7% of the respondents were unable to determine the exact number of API-related breaches, pointing towards potential undetected intrusions or gaps in monitoring and reporting.

Figure 7. How many data breaches did your organization have that were caused by an API exploitation in the past two years?



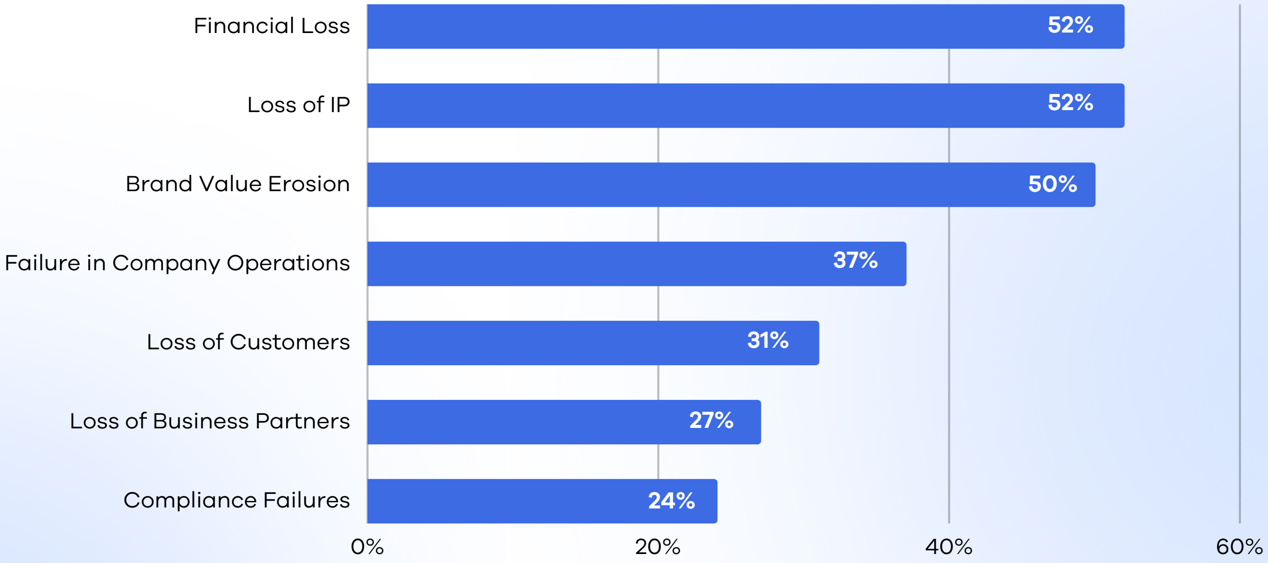
Financial Loss, Loss of Intellectual Property, and Brand Value Erosion are Top Consequences of API-related Data Breaches.

Financial consequences and loss of intellectual property (IP) equally resonating as the most severe, both experienced by 52% of the affected organizations.

Not far behind, brand value erosion was reported by 50% 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.

Additionally, relational consequences are evident, with 31% seeing a decline in customer base and 27% facing a loss of business partners. Notably, 24% also grappled with non-compliance to regulations, highlighting the legal implications that come hand in hand with security lapses.

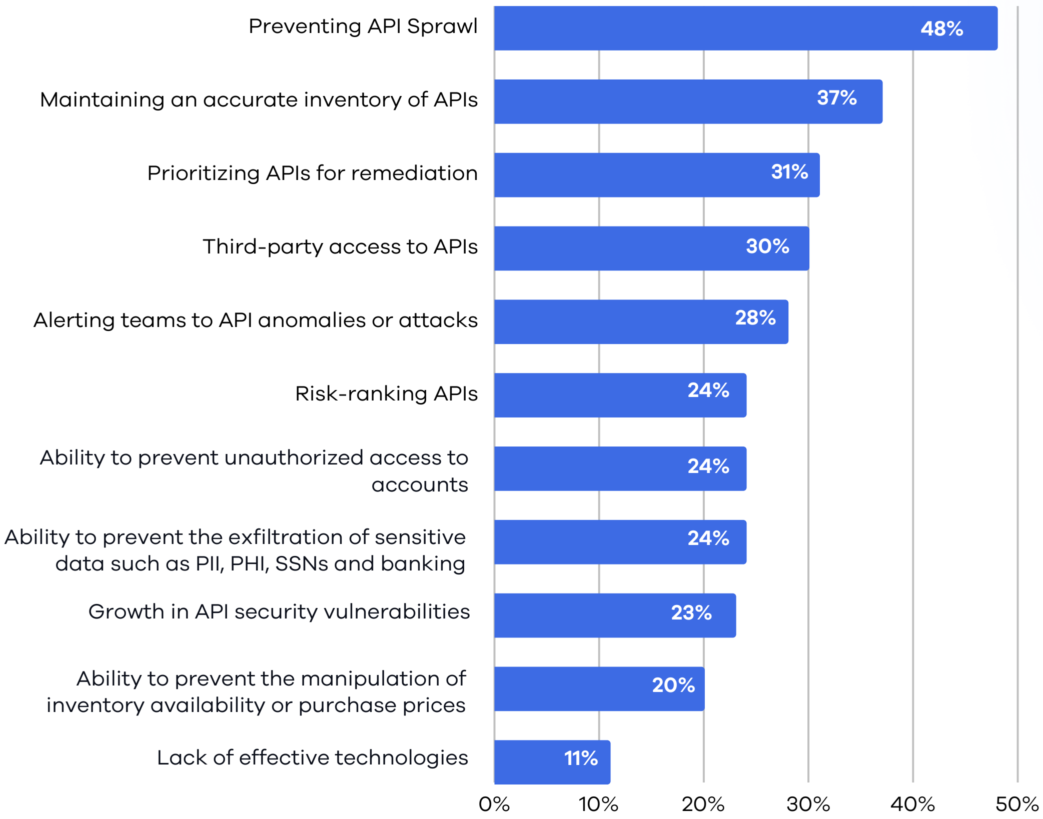
Figure 8. The consequences of the one or more data breaches caused by an API exploitation. More than one response permitted.



API Sprawl: The Silent Threat Multiplying in the Shadows

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 grapple with significant challenges in securing them. Nearly half of respondents (48%) highlight preventing API sprawl as a top issue, while maintaining an accurate API inventory and prioritizing APIs for remediation, also emerged as considerable hurdles.

Figure 9: What are the top three challenges to securing APIs?
Respondents chose their top 3 challenges.



48% preventing API Sprawl

37% maintaining accurate inventory

31% prioritizing remediation

30% third-party access to APIs

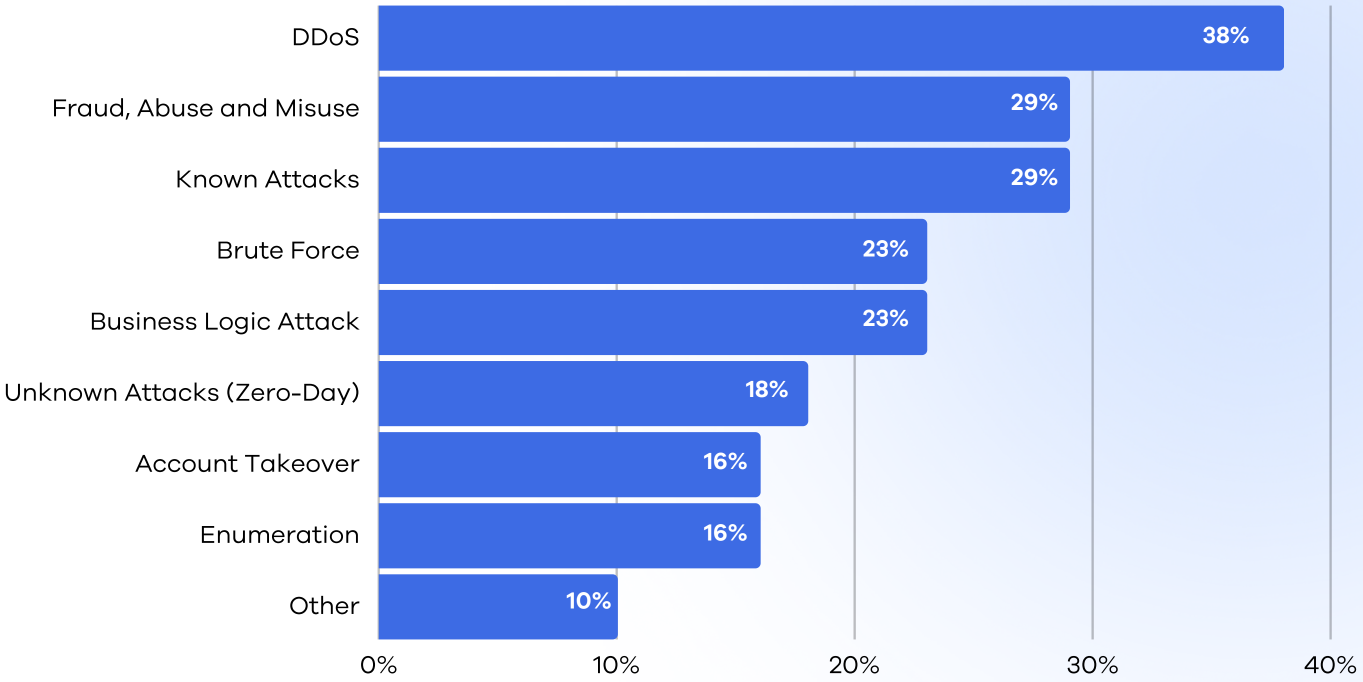
DDoS and Fraud Are Top Attack Vectors

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.

Figure 10. 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.

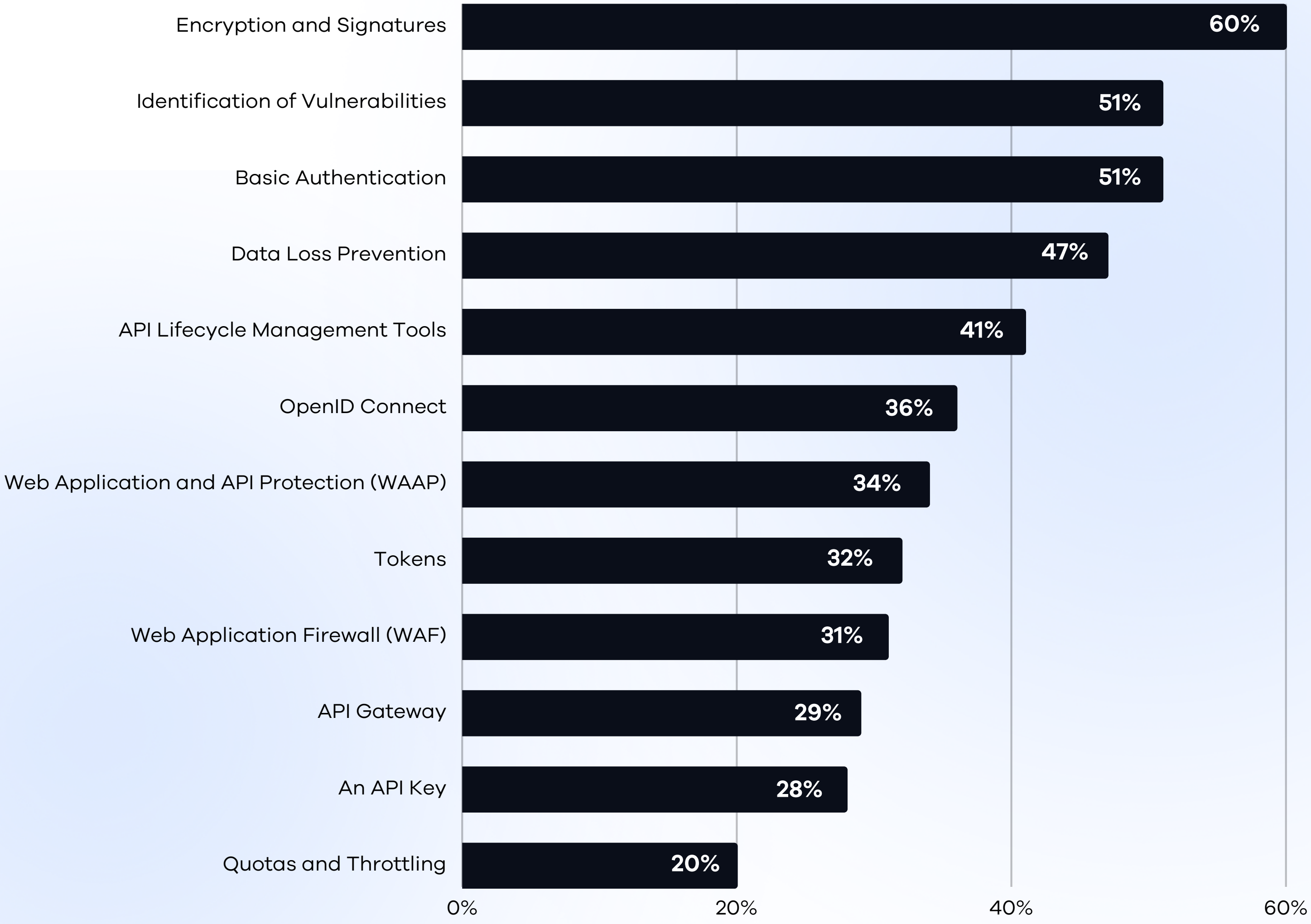


Part III: Guarding the Gate: API Security in Action

Various solutions are utilized by organizations to secure their APIs, with basic authentication (51%) and encryption and signatures (60%) emerging as the most popular options. These are followed by API lifecycle management tools (41%), identification of vulnerabilities (51%), and Data Loss Prevention (DLP) strategies (47%).

Other methods such as API keys, API gateways, OpenID Connect (OIDC), tokens, quotas and throttling, Web Application and API Protection (WAAP), and Web Application Firewall (WAF) are used to varying extents, reflecting the diverse array of tools available for API security.

Figure 11. Solutions used to achieve API security. More than one response permitted.



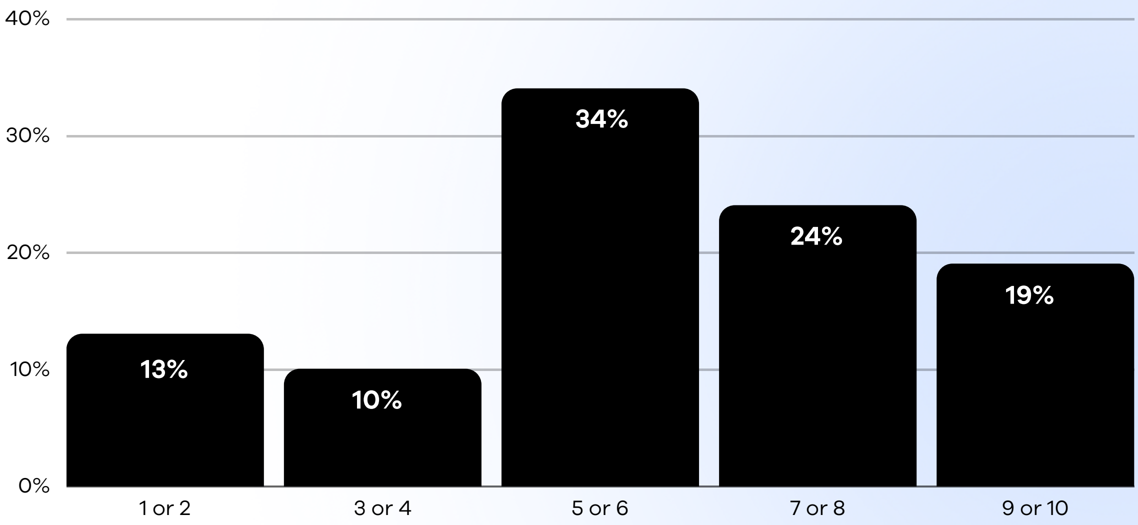
However, the effectiveness of these solutions leaves much to be desired.

The efficacy of traditional security solutions in securing the API layer has emerged as a pressing concern among organizations. A combined 57% of respondents either "agree" or "strongly agree" that traditional security mechanisms falter in distinguishing legitimate API activities from fraudulent ones. This sizable consensus paints a rather disconcerting picture of the state of API security, suggesting that many existing solutions may not be adept at dealing with the nuanced security challenges posed by APIs.

Further supporting this assertion is the perceived effectiveness of organizational solutions targeting API security. A significant 34% of organizations are ambivalent about the efficiency of their tools, marking their solutions as middling in effectiveness (ratings of 5 or 6). More alarmingly, 23% explicitly rate their solutions on the lower end of the scale, with effectiveness scores ranging from 1 to 4. While a combined 43% of organizations view their solutions as relatively more effective (ratings of 7 to 10), this still leaves over half of respondents with suboptimal confidence in their API security measures.

Piecing this data together, it becomes evident that a substantial proportion of organizations harbor reservations about the efficacy of traditional security solutions in the API realm.

Figure 12. Please rate how effective the solutions your organization uses to achieve API security from 1 = not effective to 10 = highly effective.



API Attack Protection: Perception Meets Reality

When focusing on prevention, a striking 41% of respondents believe that their organizations can prevent only up to 15% of all API attacks. This suggests a significant vulnerability and a possible underestimation of the importance of proactive measures. In contrast, confidence slightly improves when discussing detection and containment, with 51% of respondents feeling capable of detecting and containing up to 20% of API attacks. This might indicate a shift in strategy, where organizations, acknowledging the difficulty of outright prevention, invest more in damage control and mitigation after an attack occurs.

Yet, it's worth noting that even on the detection front, only 24% of respondents are confident in their organizations' ability to detect and contain more than 30% of attacks. This percentage, albeit higher than that for prevention, remains unsettlingly low given the potential risks and damages associated with undetected breaches.

Figure 13. In your opinion, what percentage of all attacks against APIs can your organization prevent?

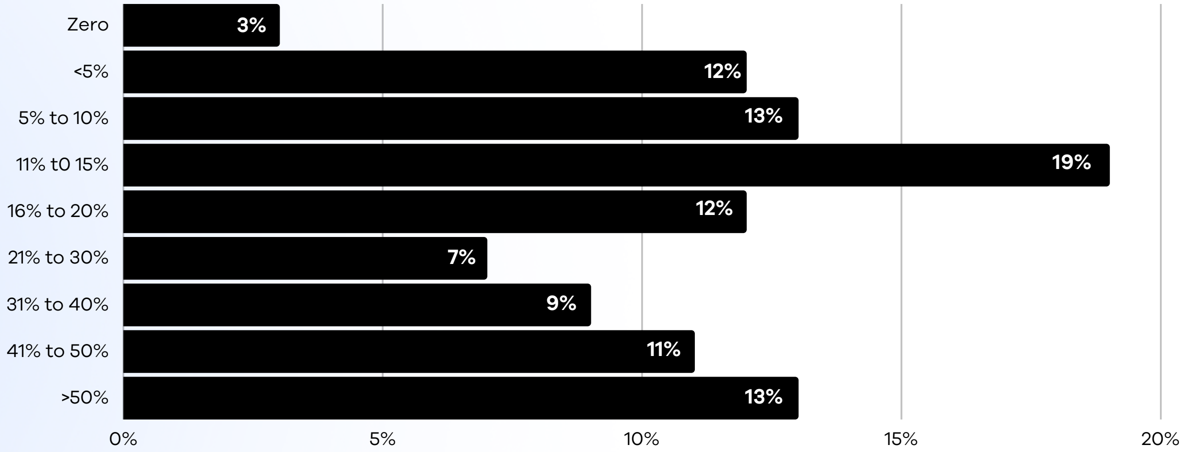
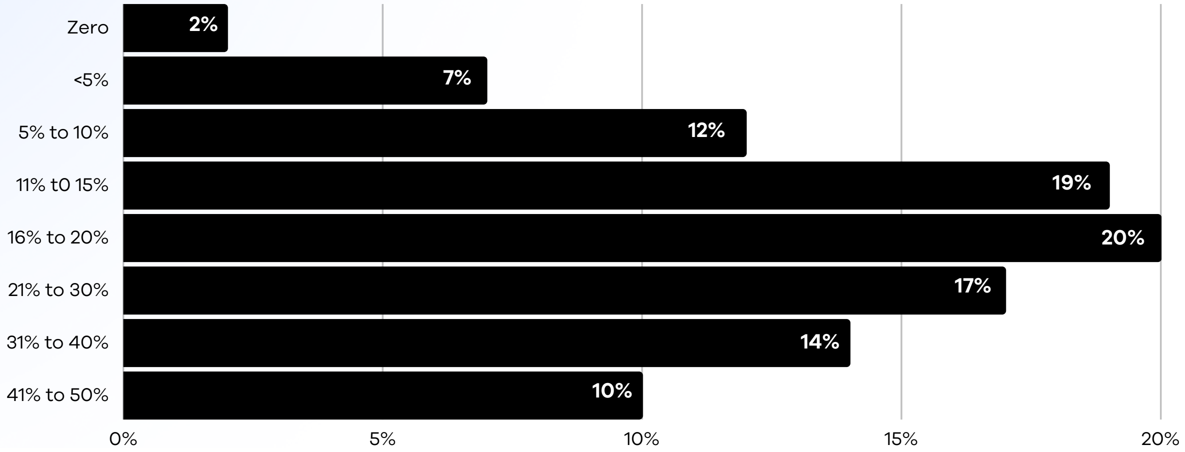


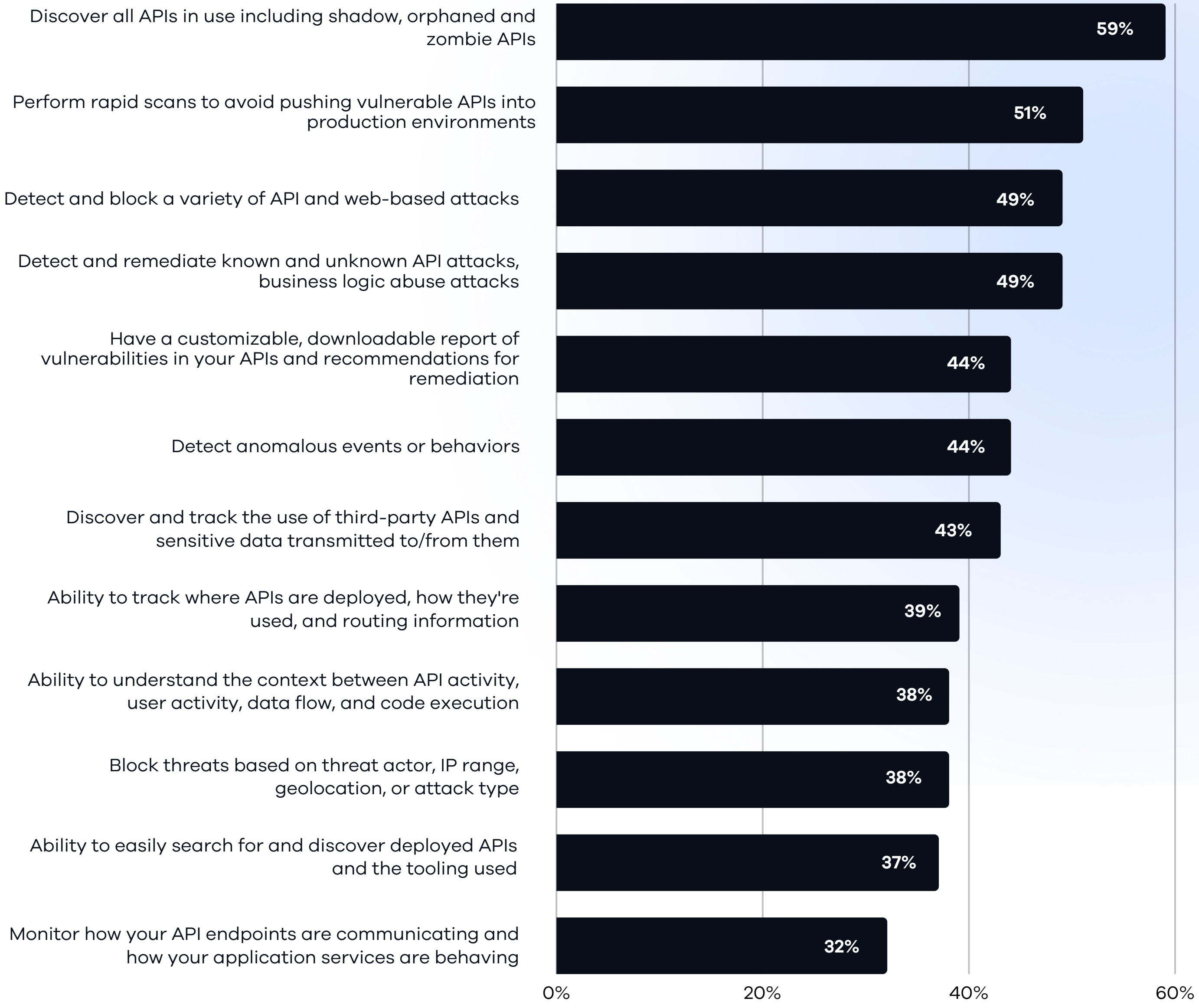
Figure 14. In your opinion, what percentage of all attacks against APIs can your organization effectively detect and contain?



Many organizations' current solutions enable them to discover all APIs in use (59%) and perform rapid scans to avoid pushing vulnerable APIs into production environments (51%).

However, among the most vital components of API security are the abilities to understand context between API activity, user activity, data flow, and code execution; to block threats based on threat actors, IP ranges, geolocations, or attack types; to detect anomalous events or behaviors; and to monitor how API endpoints are communicating and how application services are behaving. Alarmingly, less than 40% of organizations possess these capabilities. This reveals a significant vulnerability in the prevailing API security landscape and suggests a potential underestimation of the nuanced challenges inherent in today's digital interfaces.

Figure 15. Do your current solutions enable your organization to do the following to secure APIs? More than one choice was permitted.



Part IV: Embracing Zero Trust: The New Norm for API Security?

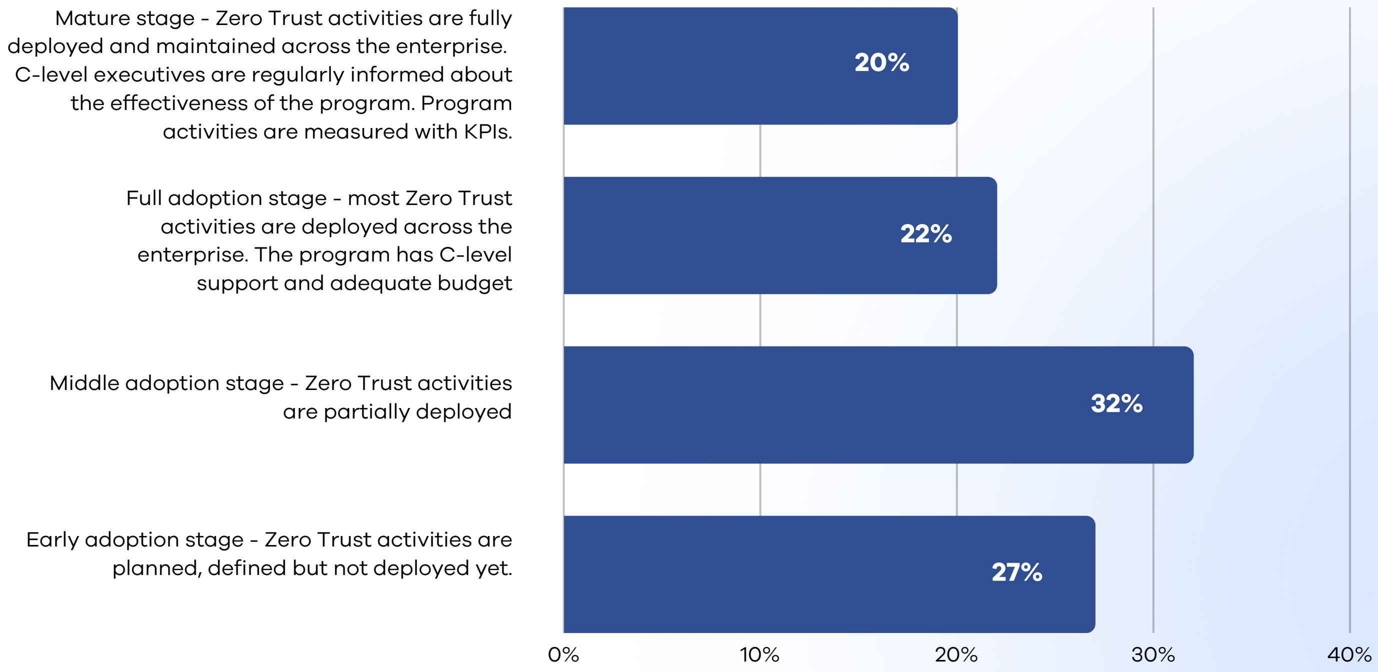
A Zero Trust framework is considered to improve API security. Forty percent of organizations in this research have adopted a Zero Trust framework and of these respondents, 55 percent of respondents say their Zero Trust strategy includes API security.

A zero-trust architecture aims to move defenses from static, networked-based perimeters to users, assets, and resources. Zero Trust segments access and limits user permissions to specific applications and services and assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location or asset ownership.

The maturity of most organizations' Zero Trust strategy is at the early adoption or middle adoption stages as shown in Figure 16. Most organizations are early adopters (27 percent of respondents) or at the middle adoption stage (32 percent of respondents) as described.

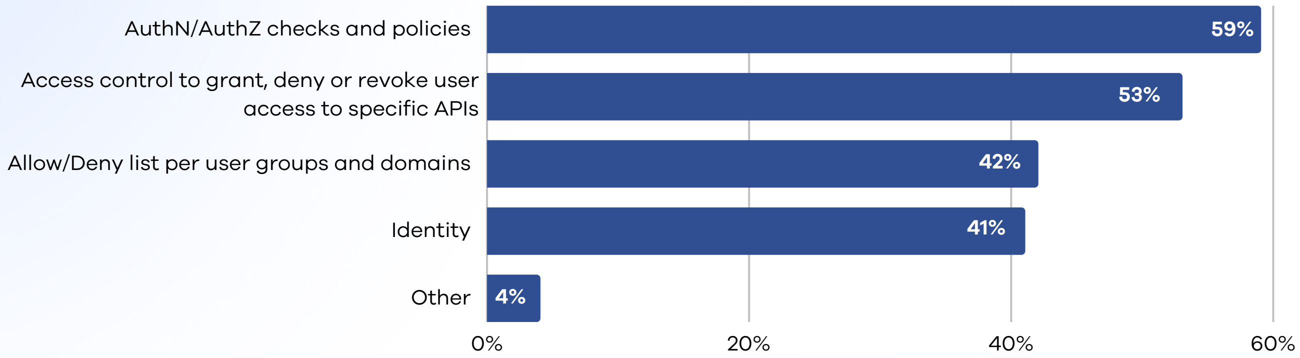
Traditional perimeter-based security solutions such as WAFs, WAAP, VPNs, next-gen firewalls, and network access control (NAC) products are ineffective at securing the expanding API attack surface.

Figure 16. What best describes the maturity of your organization's zero-trust strategy?



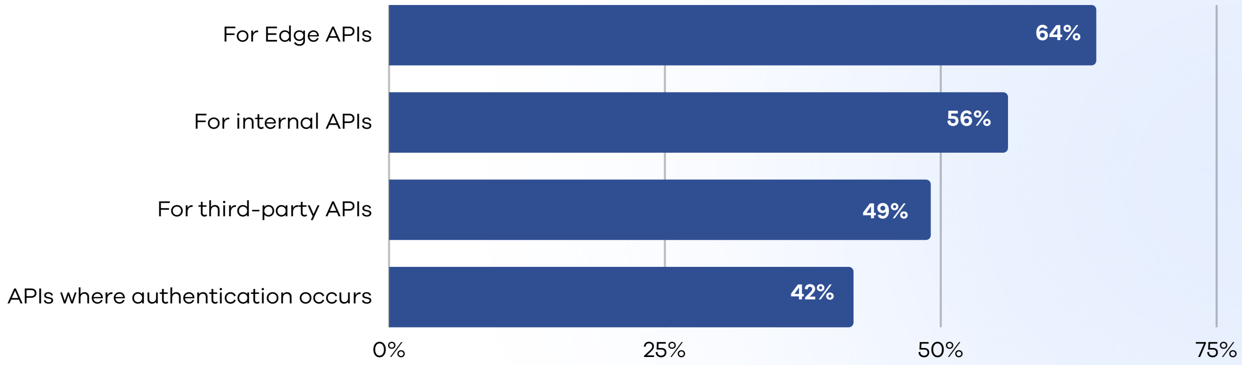
A Zero Trust strategy including API access is most likely to include AuthN/AuthZ checks and policies (59 percent of respondents) and access control to grant, deny or revoke access to specific APIs (53 percent of respondents), as shown in Figure 17.

Figure 17. What are the top considerations for your organization's zero-trust strategy around API access? Two responses permitted.



Most organizations would implement zero trust for APIs for Edge APIs (64 percent of respondents) and for internal APIs (56 percent of respondents), as shown in Figure 18.

Figure 18. Where would you consider implementing zero trust in your deployment? More than one response permitted.

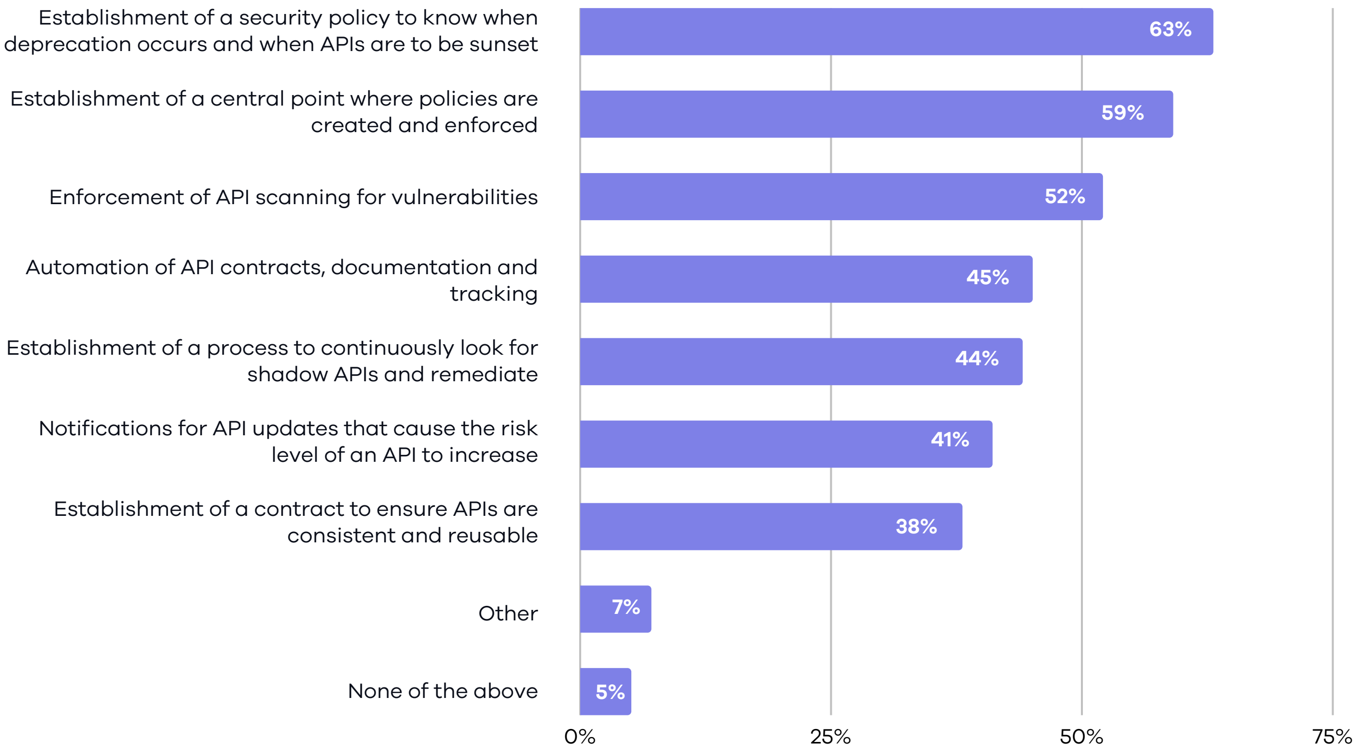


Part V: Governance, Ownership and Budget: The Strategy and Finance of API Security

Only 43 percent of organizations have policies and procedures in place to manage and oversee the use of APIs. Only 44 percent of respondents say their organizations are highly effective in ensuring APIs are consistent across an organization.

According to Figure 19, most organizations' governance practices focus on policies that indicate when deprecation occurs and when APIs are to be sunset (63 percent of respondents). Fifty-nine percent of respondents say their organizations centralize the creation of policies and their enforcement. Only 38 percent of respondents say their organizations establish a contract to ensure APIs are consistent and reusable.

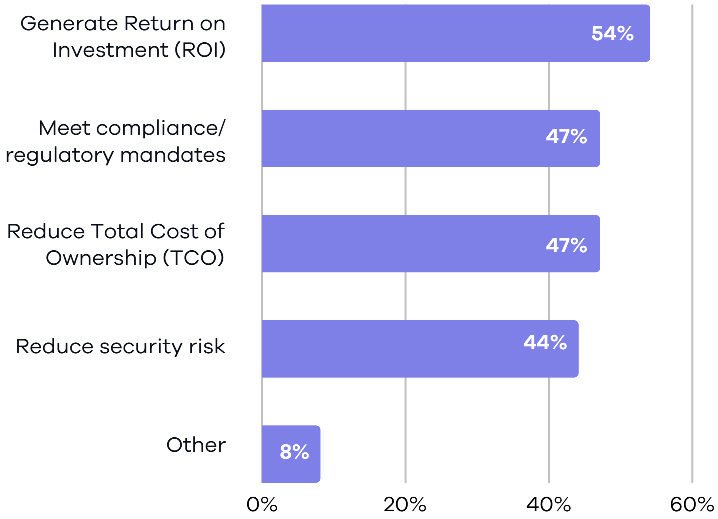
Figure 19. What policies and procedures are in place to manage and oversee the use of APIs?



Top Drivers?
ROI, Compliance, Risk.

ROI and compliance with regulations are the two main drivers for organizations security budget and investment decisions. The average IT security budget is $35 million and an average of $4.2 million is allocated to API security activities.

Figure 20. What are the most important drivers for your organization's security budget and investment decisions? Two responses permitted.



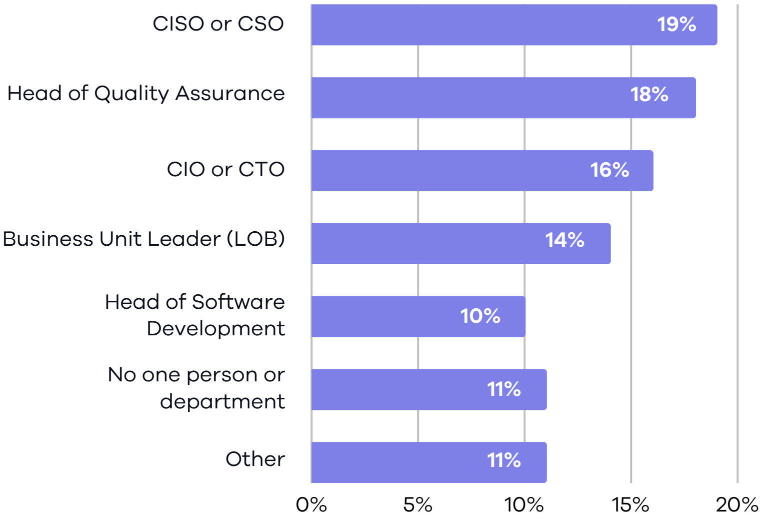
Organizations are most likely to base their investment decisions on the ROI that can be generated followed by meeting compliance and regulatory mandates. Compliance is particularly important for the financial services industry. On October 3, 2022, The FFIEC announced a significant update to meet cybersecurity mandates for financial institutions. This update explicitly calls out APIs as a separate attack surface in regulatory guidelines that represent a significant shift in compliance trajectories.

As a result, financial institutions have been including the inventory of APIs as part of their overall inventory of information systems and risk assessments.

API Security Ownership: A Mixed Bag

The varied ownership of API security budgets underscores today's digital and cybersecurity landscape. Roles from CISO/CSO at 19% to Head of Software Development at 10% all bear this crucial duty without a dominant leader.

Figure 21. Who within your organization "owns" the API security budget?



This diffusion might indicate several underlying dynamics. Firstly, the fact that roles like CISO/CSO, CIO/CTO, and the Head of Quality Assurance are all within a few percentage points of each other suggests there's no universal consensus on where the responsibility for API security should ideally reside.

This can be a double-edged sword.

On the one hand, it could be a sign of the interdisciplinary nature of API security, which necessitates collaboration across departments. On the other, it might point to a lack of clarity or potential silos within organizations, leading to possible inefficiencies or overlaps in efforts.

What the Future Holds

APIs, once seen as mere tools of interconnectivity, have clearly established their centrality in the modern digital ecosystem. This extensive survey not only sheds light on their current significance but also underscores their escalating role in the future.

The data reveals an undeniable reality: API security is not an optional or secondary consideration. It's a necessity, a lifeline. Organizations have come to recognize that APIs, while being enablers of digital transformation, are also potential entry points for compromise.

Traditional security measures, although widely adopted, have shown mixed effectiveness in protecting APIs. The challenges of API sprawl and the necessity for consistent standardization emerge as key concerns. Despite many organizations establishing API management policies, there remains a significant gap in ensuring their consistent application.

There's hope in the statistics: the embrace of Zero Trust security strategies, with a particular focus on APIs, is a step in the right direction. Moreover, the acknowledgment that APIs broaden the attack surface reaffirms their criticality. With a prevailing sentiment that API risks will surge in the future, the imperative to bolster security measures becomes even more pronounced.

As we gaze into the future of API security, two things are clear: the increasing integration of APIs will bring both promise and challenges. Their security will not only be an operational requirement but a cornerstone of enterprise strategy. The digital realm's resilience hinges on how securely we traverse the intricate web of APIs.

The call to action is clear: view APIs not just as bridges, but as fortifications in the digital world. As we chart our path forward, let's embrace both the challenges and opportunities they present, and let this understanding guide us towards a fortified API-driven future.

Embrace the journey, and craft a future that's both interconnected and secure.

Appendix: Detailed Survey Results

Which industry are you employed in?	Pct%
Financial Services	26%
Insurance	21%
Retail	20%
Healthcare	11%
SAAS (Software as a Service)	15%
High technology and software	9%
None of the above (stop)	0%
Total	100%

What is your organization's headcount?	Pct%
1,000 to 2,500	18%
2,501 to 5,000	15%
5,001 to 10,000	23%
10,001 to 25,000	18%
25,001 to 50,000	11%
50,001 to 75,000	8%
75,000+	7%
Total	100%
Extrapolated value (FTE)	20,807

Part 2. Background on API usage

Does your organization have a solution to discover, inventory and track APIs?	Pct%
Yes	53%
No	47%
Total	100%

If yes, how many APIs does your organization use?	Pct%
Less than 100	8%
100 to 250	11%
251 to 500	23%
501 to 1,000	19%
1,001 to 2,500	20%
More than 2,500	13%
Do not know	6%
Total	100%
Extrapolated value (FTE)	1,099

Please rate how difficult it is to discover and inventory all APIs in the organization from 1 = not difficult to 10 = highly difficult.	Pct%
1 or 2	11%
3 or 4	15%
5 or 6	20%
7 or 8	33%
9 or 10	21%
Total	100%
Extrapolated value	6.27

Please rate how important APIs are to your organization's digital transformation programs from 1 = not important to 10 = highly important.	Pct%
1 or 2	7%
3 or 4	13%
5 or 6	23%
7 or 8	28%
9 or 10	29%
Total	100%
Extrapolated value	6.66

Does your organization make it a priority to have a security risk profile for every API to understand those that are most vulnerable to attacks or abuse? On a scale from 1 = not a priority to 10 = a very high priority	Pct%
1 or 2	8%
3 or 4	16%
5 or 6	23%
7 or 8	25%
9 or 10	27%
Total	100%
Extrapolated value	6.45

Does your organization make it a priority to identify API endpoints that handle sensitive data without appropriate authentication? On a scale from 1 = not a priority to 10 = a very high priority.	Pct%
1 or 2	9%
3 or 4	15%
5 or 6	22%
7 or 8	26%
9 or 10	28%
Total	100%
Extrapolated value	6.50

How many cloud applications does your organization use.	Pct%
Less than 100	13%
100 to 250	16%
251 to 500	21%
501 to 1,000	26%
1,001 to 2,500	13%
More than 2,500	88%
Total	100%
Extrapolated value	977

What types of APIs does your organization use and/or provide? Please select all that apply.	Pct%
Open APIs	32%
Public APIs	31%
Private APIs	30%
Partner APIs	22%
Internal APIs	20%
Composite APIs	21%
Third-party APIs	15%
Total	170%

Part 2. API Risks

Do you expect API risk to increase, decrease or stay at the same level over the next 12 to 24 months?	Pct%
Significantly increase	21%
Increase	40%
Stay the same	24%
Decrease	15%
Total	100%

What are the top three challenges to securing APIs? Please select the top three choices only.	Pct%
Preventing API sprawl	48%
Maintaining an accurate inventory of APIs	37%
Alerting the team to API anomalies or attacks	28%
Risk ranking APIs	24%
Prioritizing APIs for remediation	31%
Third-party access to APIs	30%
Ability to prevent unauthorized access to accounts	24%
Ability to prevent the manipulation of inventory availability or purchase prices	20%
Ability to prevent the exfiltration of sensitive data such as PII, PHI, SSNs and banking information	24%
Growth in API security vulnerabilities	23%
Lack of effective technologies	11%
Total	300%

Did your organization have a data breach caused by an API exploitation in the past two years?	Pct%
Yes	60%
No (please skip to Q12)	31%
Unsure (please skip to Q12)	9%
Total	100%

If yes, how many data breaches did your organization have that were caused by an API exploitation in the past two years?	Pct%
1 to 2	20%
3 to 4	34%
5 to 6	17%
6 to 7	12%
More than 7	11%
Could not determine	7%
Total	100%

What was the root cause of the one or more data breaches? Please select all that apply	Pct%
Known attacks (attacks with known signatures)	29%
Unknown attacks zero day	18%
Account takeover	16%
Business logic attack	23%
DDoS	38%
Fraud, abuse and misuse	29%
Brute force	23%
Enumeration	16%
Other (please spcify)	10%
Total	200%

What were the consequences of the one or more data breaches? Please select all that apply	Pct%
Financial loss	52%
Brand value erosion	50%
Failures in company operations	37%
Failure to comply with regulations and mandates	24%
Loss of customers	31%
Loss of business partners	27%
Other (please specify)	5%
Total	279%

How many third parties are connected to your organization's APIs?	Pct%
Less than 50	15%
50 to 75	13%
76 to 100	23%
101 to 250	22%
More than 250	21%
Cannot determine	7%
Total	100%

Please rate the ability of your organization to identify and mitigate risks posed by third-party access to your APIs from 1 = no ability to 10 = high ability.	Pct%
1 or 2	15%
3 or 4	24%
5 or 6	28%
7 or 8	18%
9 or 10	15%
Total	100%

Please rate the ability of your organization to identify and mitigate risks posed by APIs outside your organization from 1 = no ability to 10 = high ability.	Pct%
1 or 2	14%
3 or 4	21%
5 or 6	29%
7 or 8	19%
9 or 10	16%
Total	100%

Please rate the ability of your organization to identify and mitigate risks posed by APIs within your organization from 1 = no ability to 10 = high ability.	Pct%
1 or 2	16%
3 or 4	21%
5 or 6	23%
7 or 8	26%
9 or 10	14%
Total	100%

Please rate the ability of your organization to have visibility into the API ecosystem from 1 = no ability to 10 = high ability.	Pct%
1 or 2	18%
3 or 4	21%
5 or 6	26%
7 or 8	20%
9 or 10	15%
Total	100%

Please rate the ability of your organization to detect attacks at the API layer from 1 = no ability to 10 = high ability.	Pct%
1 or 2	13%
3 or 4	10%
5 or 6	33%
7 or 8	26%
9 or 10	18%
Total	100%

Please rate the ability of your organization to ensure consistency in API design and functionality from 1 = no ability to 10 = high ability.	Pct%
1 or 2	10%
3 or 4	15%
5 or 6	31%
7 or 8	31%
9 or 10	13%
Total	100%

Attributions: Please use the scale below each statement.

The volume of APIs makes it difficult to prevent attacks.	Pct%
Strongly agree	29%
Agree	27%
Unsure	21%
Disagree	14%
Strongly disagree	9%
Total	100%

APIs are a security risk because they expand the attack surface across all layers of the technology stack.	Pct%
Strongly agree	29%
Agree	29%
Unsure	20%
Disagree	14%
Strongly disagree	8%
Total	100%

Traditional security solutions are not effective in distinguishing legitimate from fraudulent activity at the API layer.	Pct%
Strongly agree	28%
Agree	29%
Unsure	20%
Disagree	14%
Strongly disagree	9%
Total	100%

Part 3. API security practices

Does your organization use any of the following solutions to achieve API security? Please select all that apply.	Pct%
An API key	28%
API gateway	29%
API lifecycle management tools	41%
Basic authentication	51%
Data loss prevention (DLP)	47%
Encryption and signatures	60%
Identification of vulnerabilities	51%
OpenID Connect (OIDC)	36%
Quotas and throttling	20%
Tokens	32%
Web Application and API Protection (WAAP)	34%
Web Application Firewall (WAF)	31%
Total	458%

Please rate how effective the solutions your organization uses to achieve API security from 1 = not effective to 10 = highly effective.	Pct%
1 or 2	13%
3 or 4	10%
5 or 6	34%
7 or 8	24%
9 or 10	19%
Total	100%

In your opinion, what percentage of all attacks against APIs can your organization prevent?	Pct%
Zero	3%
< 5%	12%
5% to 10%	13%
11% to 15%	19%
16% to 20%	12%
21% to 30%	7%
31% to 40%	9%
41% to 50%	11%
> 50%	13%
Total	100%

In your opinion, what percentage of all attacks against APIs can your organization effectively detect and contain?	Pct%
Zero	2%
< 5%	7%
5% to 10%	12%
11% to 15%	19%
16% to 20%	20%
21% to 30%	17%
31% to 40%	14%
41% to 50%	10%
Total	100%

Approximately, what percent of APIs are continuously tested for vulnerabilities?	Pct%
Less than 5%	8%
5% to 10%	11%
11% to 25%	13%
26% to 50%	13%
51% to 75%	24%
76% to 100%	19%
Cannot determine	13%
Total	100%

Who owns your organization's API security risk testing program? Please select only one person/department.	Pct%
Business units (LOB)	19%
CIO or CTO	21%
CISO or CSO	21%
Head of quality assurance	11%
Head of software development	14%
No one person or department	14%
Total	100%

How much of a priority is API security in your organization?	Pct%
A very high priority	23%
A high priority	25%
A priority	21%
Somewhat of a priority	17%
Not a priority	14%
Total	100%

What prevents your organization from making API security a priority? Please select the top two reasons.	Pct%
Management underestimates the risk to APIs	49%
Difficulty in understanding how to reduce the threats to APIs	37%
Other security risks are considered more of a threat	42%
Not enough resources	33%
Lack of in-house expertise	12%
We consider APIs part of cloud security	13%
We consider APIs part of application security	8%
Other (please specify)	7%
Total	200%

Do your current solutions enable your organization to do the following? Please select all that apply.	Pct%
Ability to detect and block a variety of API and web-based attacks	49%
Ability to discover all APIs in use including shadow, ophaned and zombie	59%
Ability to discover and track the use of third-party APIs and sensitive data transmitted to/from them	43%
Ability to detect and remediate known and unknown API attacks, business logic abuse attacks	49%
Ability to easily search for and discover deployed APIs and the tooling use	37%
Ability to have a customizable, downloadable report of vulnerabilities in your APIs and recommendations for remediation	44%
Ability to perform rapid scans to avoid pushing vulnerable APIs into production environments	51%
Ability to track where APIs are deployed, how used and routing information	39%
Ability to understand the context between API activity, user activity, data flow and code executive	38%
Block threats based on threat actor, IP range, geolocation or attack type	38%
Detect anomalous events or behaviours	44%
Monitor how your API endpoints are communicating and how your application services are behaving	32%
Total	523%

Has your organization adopted a Zero-Trust framework?	Pct%
Yes	41%
No (please skip to Q32a)	59%
Total	100%

What best describes the maturity of your organization's Zero-Trust strategy? Please select one choice only.	Pct%
Early adoption stage - Zero trust activities are planned, defined but not deployed yet	27%
Middle adoption stage - Zero Trust activities are partially deployed	32%
Full adoption stage - most Zero Trust activities are deployed across the enterprise. The program has C-level support and adequate budget.	22%
Mature stage - Zero Trust activities are fully deployed and maintained across the enterprise. C-level executives are regularly informed about the effectiveness of the program. Program activities are measured with KPIs	20%
Total	100%

Does your organization's Zero-Trust strategy include API security?	Pct%
Yes	55%
No (please skip to Q32a)	45%
Total	100%

What would be top considerations for your organization's Zero-Trust strategy around API access? Please select the top two choices.	Pct%
Identity	41%
Access control to grant, deny or revoke user access to specific APIs	53%
AuthN/AuthZ checks and policies	59%
Allow/Deny list per user groups and domains	42%
Other (please specify)	4%
Total	200%

Where would you consider implementing Zero Trust in your deployment? Please select all that apply.	Pct%
For Edge APIs	64%
For internal APIs	56%
For third-party APIs	49%
APIs where authentication occurs	42%
Total	211%

Part 4. Governance and budget

Does your organization have policies and procedures in place to manage and oversee the use of APIs?	Pct%
Yes	43%
No (please skip to Q33)	57%
Total	100%

If yes, what do these policies and procedures include? Please select all that apply.	Pct%
Automation of API contracts, documentation and tracking	45%
Enforcement of API scanning for vulnerabilities	52%
Notifications for API updates that cause the risk level of an API to increase	41%
Establishment of a process to continuously look for shadow APIs and remediate	44%
Establishment of a central point where policies are created and enforced	59%
Establishment of a contract to ensure APIs are consistent and reusable	38%
Establishment of a security policy to know when deprecation occurs and when APIs are to be sunset	63%
Other (please specify)	7%
None of the above	5%
Total	353%

Please rate your organization's effectiveness in ensuring APIs are consistent across an entire organization from 1 = not effective to 10 = highly effective.	Pct%
1 or 2	9%
3 or 4	13%
5 or 6	34%
7 or 8	25%
9 or 10	19%
Total	100%

What are the most important drivers for your organization’s security budget and investment decisions? Please select the top two choices.	Pct%
Generate Return on Investment (ROI)	54%
Meet compliance/regulatory mandates	47%
Reduce security risk	44%
Reduce Total Cost of Ownership (TCO)	47%
Other (please specify)	8%
Total	200%

What is your organization's total IT security budget?	Pct%
Less than $100,000	11%
$100,000 to $500,000	12%
$500,000 to $1,000,000	12%
$1,000,000 to $5,000,000	13%
$5,000,000 to $10,000,000	15%
$10,000,001 to $50,000,000	15%
$50,000,001 to $100,000,000	11%
$100,000,001 to $250,000,000	8%
$250,000,001 to $500,000,000	3%
More than $500,000,000	0%
Total	100%
Extrapolated value (IT secuirty budget) US$	$34,600,000

Approximately, what percentage of the 2023 IT security budget are allocated to API security activities?	Pct%
Less than 1%	4%
1% to 2%	8%
3% to 5%	9%
6% to 10%	19%
11% to 15%	22%
16% to 20%	24%
More than 20%	9%
Don't know	4%
Total	100%

Who within your organization “owns” the API security budget? Please select one top choice.	Pct%
Business unit leader (LOB)	14%
CIO/CTO	16%
CISO/CSO	19%
Head of quality assurance	18%
Head of software development	10%
Other (please specify)	11%
No one person or department	11%
Total	100%

What best describes your position level within your organization?	Pct%
Business unit	9%
C-level executive/VP	11%
Director	15%
Manager	14%
Supervisor	16%
Staff/Technician	16%
Administrative	10%
Consultant/Contractor	4%
Total	100%

What best describes your direct line of reporting within your organization?	Pct%
Business owner/board level	8%
CEO/executive committee	8%
COO or head of operations	9%
CFO, controller or head of finance	7%
CIO or head of IT	15%
Business unit leader or general manager	5%
Head of compliance or internal audit	12%
Head of risk management	15%
Head of IT security	17%
Other	5%

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