TRACEABLE

INDUSTRY RESEARCH REPORT

2024 State of API Security: Financial Services

Contents

A Letter from Richard Bird, Chief Security Officer

Dear Friends and Industry Colleagues,

As a former CISO and security executive who has led security programs for large financial institutions, I've seen firsthand how quickly the landscape can shift. With years of experience navigating the complexities of financial organization security, I understand the challenges you face daily. APIs have become the backbone of our digital world, enabling us to innovate and deliver seamless experiences to our customers. However, with this growth comes a new set of security risks that we simply cannot ignore.

The findings of this report should serve as a reality check for our industry. It's clear that while financial organizations understand the importance of API security, many are still struggling with basic challenges like preventing unauthorized access, stopping data exfiltration, and effectively finding and fixing vulnerabilities. When API-related breaches happen, the fallout is massive - it erodes customer trust, damages our reputation, and hits us where it hurts most, our bottom line.

There are numerous challenges in front of us. As security leaders, it's our job to protect our organizations' assets and our customers' data, and make sure we're complying with tough regulations. The regulatory landscape is changing fast, and we need to stay ahead of the game. Attack types are also changing.

We can't afford to be caught off guard by the growing threats of fraud and malicious bots that are constantly looking for ways to exploit API vulnerabilities and steal sensitive data.

Moving forward, we need to take a proactive and comprehensive approach to API security. We can't just react to problems as they happen or rely on piecemeal solutions. This means getting security teams, developers, and business stakeholders on the same page, working together to prioritize and implement effective security measures.

This report is designed to give you the insights, guidance, and practical recommendations you need to bolster your API security posture. It's a call to action for all of us to take a hard look at what we're doing now, invest in the right solutions, and give our teams the tools and resources they need to succeed.

The stakes are high, and the trust our customers, partners, and stakeholders have placed in us is not something we can take for granted. We need to step up, and lead the charge in securing our API ecosystems.

Together, we can build a stronger, more resilient future for financial services.

Richard Bird
Chief Security Officer
Traceable

Introduction

To better understand the current state of API security in the financial services industry, we conducted a survey of over 150 cybersecurity professionals in the United States. The survey aimed to uncover the challenges, risks, and strategies employed by financial organizations to safeguard their API ecosystems.

The financial services industry is a prime target for cybercriminals due to the sensitive nature of the data it handles. Our survey reveals that APIs in financial organizations commonly handle highly sensitive information, including personally identifiable information (PII) (60%), account authentication data (60%), payment card details (56%), and device and location data (55%). The exposure of such sensitive data through APIs can have severe consequences, ranging from financial losses and regulatory penalties to reputational damage and erosion of customer trust.

Moreover, financial organizations face the added burden of complying with stringent industry regulations. Our survey findings highlight that a staggering 82% of financial institutions express moderate to extreme concern about complying with federal financial regulations such as FFIEC, OCC, and CFPB in relation to their API inventory and security posture. Additionally, 76% of respondents indicate similar levels of concern regarding PCI-DSS compliance. The regulatory landscape surrounding API security adds another layer of complexity and urgency for financial organizations to address API vulnerabilities and safeguard sensitive customer data.

The stakes are high, as the impact of API-related breaches extends far beyond technical realms. Data loss, brand reputation damage, financial losses, and customer attrition are among the top repercussions faced by financial institutions in the wake of API security incidents.

This report covers the current state of API security within the financial services sector, uncovering the pressing challenges, risks, and strategies employed by organizations to safeguard their API ecosystems. Through comprehensive survey findings and expert insights, we aim to provide a roadmap for financial institutions to navigate the complexities of API security, strengthen their defenses, and fortify customer trust in the digital age.

TRACEABLE

Top Findings at a Glance

82% express concerns about complying with federal financial regulations (FFIEC, OCC, CFPB) in relation to their API inventory and security posture.

76% of respondents indicate moderate to extreme concern regarding PCI-DSS compiance in relation to API security.

73% A staggering 73% of respondents state that malicious bots are a moderate to critical threat to API security in financial services.

64% 64% of financial organizations DO NOT have the ability to understand the context between API activity, user activity, data flow, and code execution.

41% Data loss and brand reputation damage (both 41%) are the top consequences of API-related breaches, followed by financial loss (36%) and customer attrition (35%).

15% Only 15% of financial organizations are extremely confident in their ability to detect and prevent API-based fraud and abuse.

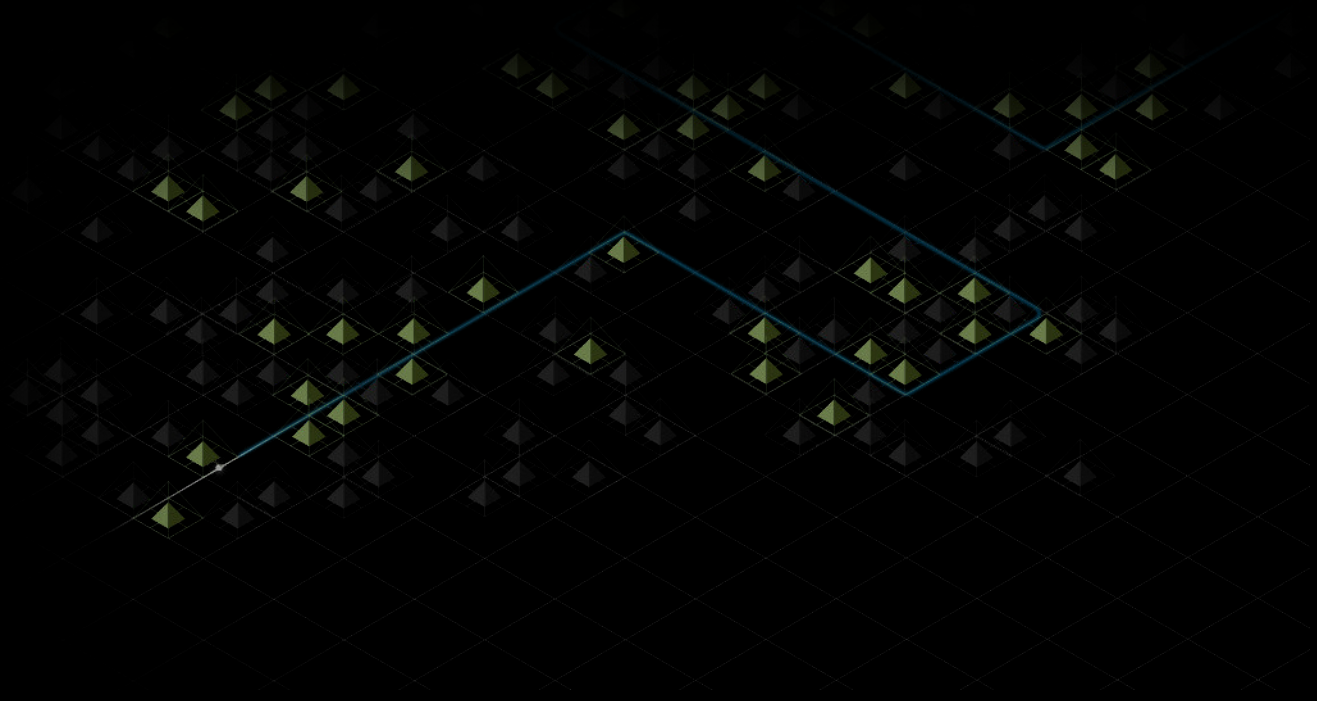
45% Less than half of respondents state that they can prevent approximately 50% or fewer of API attacks in their environment.

TRACEABLE

Key Findings

The “Key Findings” section of the “State of API Security for Financial Services” report delves into the most significant insights uncovered by our comprehensive survey. This section examines the critical challenges faced by financial institutions in securing their APIs, the prevalence and impact of API-related breaches, and the effectiveness of current security measures.

The findings shed light on the complex regulatory landscape, the types of sensitive data handled by APIs, and the real-world consequences of API security incidents. By exploring these key aspects, the report provides a detailed understanding of the current state of API security in the financial services industry and offers valuable insights for organizations looking to strengthen their API security posture.



TRACEABLE

API Security Challenges: Unauthorized Access, Data Exfiltration, and Vulnerability Management

As financial institutions increasingly rely on APIs to drive innovation, streamline operations, and deliver seamless customer experiences, they must navigate a complex web of security risks. Our survey uncovers the most pressing concerns faced by organizations in their quest to secure their API ecosystems.

At the forefront of these challenges is the issue of **unauthorized access to accounts, with 35% of respondents** identifying this as a top concern. APIs often serve as the gateway to sensitive customer data and financial resources, making them an attractive target for cybercriminals. Unauthorized access can occur through various means, such as weak authentication mechanisms, compromised credentials, or exploitation of vulnerabilities.

Closely following unauthorized access is the challenge of **sensitive data exfiltration, reported by 33% of the respondents**. APIs, by their very nature, facilitate the exchange of data between systems and applications. However, when not properly secured, they can become conduits for the unauthorized transfer of sensitive information. Attackers may exploit vulnerabilities or misconfigurations in APIs to extract valuable data, such as personally identifiable information (PII), financial records, or intellectual property.

Identifying **API vulnerabilities emerges as another significant challenge, with 30% of the respondents** highlighting this concern. As the number and complexity of APIs grow, so does the attack surface. Vulnerabilities can arise from various factors, such as coding errors, misconfigurations, or outdated software components. Identifying these vulnerabilities requires a proactive approach to vulnerability management, including regular security testing, code reviews, and continuous monitoring. Failure to identify and address vulnerabilities promptly can leave APIs exposed to exploitation by malicious actors.

35%

At the forefront of these challenges is the issue of **unauthorized access to accounts, with 35% of respondents** identifying this as a top concern.

33%

Closely following unauthorized access is the challenge of **sensitive data exfiltration, reported by 33% of the respondents**.

30%

Identifying **API vulnerabilities emerges as another significant challenge, with 30% of the respondents** highlighting this concern.

TRACEABLE

Compliance and Regulatory Pressures: The Driving Force behind API Security Priorities

In the heavily regulated financial services industry, compliance with industry standards and regulations is a top priority.

As APIs become increasingly central to financial institutions' operations, ensuring that these interfaces meet the stringent regulatory requirements has become a critical concern. Our survey highlights the significant pressure that compliance and regulatory obligations place on financial organizations' API security initiatives.

A staggering **82% of financial organizations surveyed express moderate to extreme concern about complying with federal financial regulations**, such as those set forth by the Federal Financial Institutions Examination Council (FFIEC), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), in relation to their API inventory and security posture. These regulatory bodies enforce rigorous standards for data protection, risk management, and operational resilience, and their guidelines have a profound impact on how financial institutions approach API security.

In addition to federal financial regulations, **76% of respondents indicate moderate to extreme concern regarding compliance** with the Payment Card Industry Data Security Standard (PCI-DSS) in relation to their API security posture. PCI-DSS is a global information security standard designed to protect credit card data from theft and fraud. APIs that handle payment card information must adhere to the strict security requirements outlined in PCI-DSS, including encryption, access controls, and regular vulnerability assessments. Non-compliance with PCI-DSS can result in substantial fines, the revocation of the ability to process credit card transactions, and severe reputational damage.

82%

express concerns about complying with federal financial regulations (FFIEC, OCC, CFPB) in relation to their API inventory and security posture.

76%

express concerns about complying with federal financial regulations (FFIEC, OCC, CFPB) in relation to their API inventory and security posture.

TRACEABLE

Fraud and Malicious Bots in Financial API Ecosystems

Our survey reveals the alarming prevalence and impact of these malicious actions on the API ecosystems of financial institutions.

Among the respondents who experienced an API-related data breach, a staggering **42% attribute the root cause to fraud, abuse, and misuse**. This finding highlights the growing sophistication and frequency of attacks specifically designed to exploit vulnerabilities in financial APIs. Fraudsters are increasingly leveraging techniques such as credential stuffing, account takeovers, and API abuse to gain unauthorized access to sensitive financial data and execute fraudulent transactions.

The survey also uncovers a concerning lack of confidence among financial institutions in their ability to detect and prevent API-based fraud and abuse. **Only 15% of organizations express extreme confidence in their fraud detection and prevention capabilities**, indicating a significant gap in their defensive measures. This lack of confidence is particularly worrisome given the high stakes involved in financial API security, where a single breach can result in substantial financial losses and irreparable damage to an institution's reputation.

Compounding the threat of fraud is the growing menace of malicious bots targeting financial APIs. **An alarming 73% of respondents perceive malicious bots as a moderate to critical threat** to their API ecosystems. Malicious bots are automated programs designed to carry out nefarious activities, such as scraping sensitive data, executing fraudulent transactions, or overwhelming APIs with traffic to cause denial-of-service attacks.

The rise of malicious bots can be attributed to the increasing accessibility and affordability of bot-building tools and services on the dark web. Attackers can easily create and deploy armies of bots to target financial APIs at scale, making it increasingly difficult for institutions to distinguish between legitimate and malicious traffic.

73%

An alarming 73% of respondents perceive malicious bots as a moderate to critical threat to their API ecosystems.

42%

Among respondents who experienced an API-related data breach, a staggering 42% attribute the root cause to fraud, abuse, and misuse of APIs.

15%

Only 15% of organizations express extreme confidence in their API fraud detection and prevention capabilities.

TRACEABLE

The Consequences of API-Related Data Breaches

Reputation, Financial Loss, and Customer Attrition Top the List

The impact of API-related breaches extends far beyond the technical realm, striking at the heart of a financial institution's core business aspects. Our survey reveals that data loss and brand reputation damage are the most significant consequences faced by financial institutions in the wake of an API security incident, with both being reported by **41% of respondents**. This finding underscores the critical importance of protecting sensitive customer data and maintaining a trustworthy brand image in the highly competitive financial services industry.

Closely following reputation damage are the tangible financial **losses incurred due to API breaches, as reported by 36%** of respondents. These financial losses can stem from a variety of factors, including the direct costs of investigating and remediating the breach, potential regulatory fines and penalties, and the loss of business due to customer attrition. Speaking of customer attrition, **35% of respondents reported losing customers** as a direct result of an API-related data breach. In an industry where customer trust and loyalty are paramount, losing customers to a preventable security incident can have long-lasting effects on an organization's growth and profitability.

These findings serve as a stark reminder that API security is not merely a technical concern, but a business-critical issue that demands attention and prioritization from the highest levels of an organization. The consequences of an API breach can ripple throughout a financial institution, eroding customer trust, damaging brand reputation, and ultimately impacting the bottom line. It is therefore imperative that financial institutions take proactive measures to prevent API breaches from occurring in the first place. This includes implementing robust security controls, regularly testing and monitoring APIs for vulnerabilities, and providing adequate training and resources to development and security teams.

41%

Data loss and brand reputation damage (both 41%) are the top consequences of API-related breaches, followed by financial loss (36%) and customer attrition (35%).

36%

Closely following reputation damage are the tangible financial losses incurred due to API breaches, as reported by 36% of respondents.

35%

35% of respondents reported losing customers as a direct result of an API-related data breach.

TRACEABLE

Sensitive Data Exposure: APIs as the New Frontier for Data Protection

The findings reveal that APIs in financial institutions commonly handle a wide range of sensitive data, with personally identifiable information (PII) and account authentication data being the most prevalent, **both handled by 60% of organizations' APIs**. This comes as no surprise, as APIs often serve as the conduit for customer onboarding, account management, and authentication processes. However, the sensitivity of this data cannot be overstated – a breach involving PII or authentication data could lead to identity theft, account takeovers, and other forms of financial fraud.

Payment card details are another type of sensitive data frequently handled by APIs in the financial sector, with **56% of the respondents indicating that their APIs process this information**. Given the strict regulatory requirements surrounding the handling of payment card data, such as those outlined in the Payment Card Industry Data Security Standard (PCI DSS), any breach involving this information could result in significant financial penalties and reputational damage for the affected institution.

Furthermore, the survey finds that **55% of the respondents report that their APIs handle device and location data**. While this data may not seem as sensitive as PII or payment card details at first glance, it can still be exploited by malicious actors to gain insights into a user's behavior, preferences, and movements. In the wrong hands, this information could be used for targeted phishing attacks, social engineering, or even physical threats.

The exposure of any of these types of sensitive data through API vulnerabilities can have severe consequences for financial institutions. Beyond the direct financial costs of investigating and remediating a breach, organizations may face regulatory penalties, legal liabilities, and long-term reputational damage. In an industry built on trust, a single data breach can erode customer confidence and lead to significant client attrition.

60%

60% of financial organization APIs handle both personally identifiable information (PII) and account authentication data.

56%

Payment card details are another type of sensitive data frequently handled by APIs in the financial sector, with 56% of respondents indicating that their APIs process this information.

55%

55% of respondents report that their organization APIs handle device and location data.

TRACEABLE

Assessing the Effectiveness of API Security Controls: Progress and Pitfalls

The survey reveals that a range of security solutions are being employed, with encryption and signatures (50%), data loss prevention (DLP) (47%), and web application firewalls (WAFs) (47%) being the most widely adopted measures.

However, despite the implementation of these security measures, the survey highlights significant gaps in the effectiveness of these controls. Nearly half (45%) of the respondents estimate that they can prevent only 50% or fewer of API attacks, indicating that the current security solutions are not sufficient to combat the evolving threat landscape.

While 47% of respondents report having the ability to prevent API abuse, fraud, and sensitive data exfiltration in their production environments, and 44% can detect and block a variety of API and web-based attacks, there are notable limitations in other critical areas.

Only 39% of respondents have the ability to discover and track the use of third-party APIs and the sensitive data transmitted to and from them, leaving a potential blind spot in their API security posture. Similarly, just 38% can perform rapid scans to avoid pushing vulnerable APIs into production environments, increasing the risk of exposing unpatched vulnerabilities to attackers.

Another area of concern is the limited visibility into the full context of API activity. Only 36% of respondents have the ability to understand the context between API activity, user activity, data flow, and code execution. This lack of contextual insights hinders the ability to effectively investigate anomalous or suspicious activities and respond to security incidents in a timely manner.

These findings suggest that while financial organizations are actively deploying various API security solutions, they still face significant challenges in effectively managing and securing their API ecosystems.

64%

64% of financial organizations DO NOT have the ability to understand the context between API activity, user activity, data flow, and code execution.

47%

Only 47% of respondents report having the ability to prevent API abuse, fraud and sensitive data exfiltration.

39%

Only 39% of respondents have the ability to discover and track the use of third-party APIs and sensitive data transmitted to and from them.

32%

Only 32% of respondents have the ability to discover all APIs in use, including shadow, orphaned, and zombie APIs.

How Traceable Can Help - Proactive Steps for API Security

The path forward requires a proactive and comprehensive approach to API security. Financial institutions must adopt a strategic mindset that goes beyond mere compliance and focuses on building a robust and resilient API security framework.

- **API Discovery and Posture Management:** Traceable's API catalog automatically and continuously discovers and builds an inventory of every API in your organization, including internal, private, public or externally exposed, rogue, shadow, partner, and 3rd party APIs. Traceable continuously discovers and tracks changes to APIs via on-premise, cloud, in-code components, integrations with API management, network traffic endpoints, and even workloads via eBPF. In short, Traceable's data collection capabilities are unparalleled. Traceable provides a comprehensive view, cataloging every API, associated API data, sensitive data flows, and risk posture – even as your environment changes.
- **Attack Detection and Threat Hunting:** With Traceable, you can identify, assess, and mitigate API security threats to your organization, reveal unknown attacks, and visualize user behavior analytics to uncover fraud and abuse. Traceable's OmniTraceTM engine provides a comprehensive set of API security and data flow analytics that allows your SOC team, incident responders, and threat hunters, as well as red teams and blue teams, to find issues, detect threats, and discover attacks as they occur. Traceable's automated detection features and behavioral analytics quickly discover risk while the OmniTraceTM provides your security team the ability to hunt for specific details around issues unique to your business. Traceable surfaces the data that makes discovery of attacks and threats possible.
- **Attack Protection:** Using Traceable's contextual analysis of your APIs and the complete understanding of the inter-connectivity between the API activity, user activity, data flow, and code execution, Traceable automatically detects and blocks known and unknown API attacks, business logic abuse attacks, API fraud and abuse, as well as sensitive data exfiltration in your production environments.
- **API Security Testing:** Traceable empowers your security team to test and eliminate the risk of pushing vulnerable APIs into production environments by proactively assessing and targeting your APIs using real context from active API traffic. Requiring zero configuration, Traceable uses our extensive API security and operational context collected by the platform to discover vulnerabilities in APIs during the QA and security testing processes. With Traceable, security and development teams have the ability to perform fully informed API assessments, replacing outdated dynamic application security testing tools with a completely API context-aware process.

Appendix

Approximately how many APIs does your organization use?

501 to 1,000	20%
251 to 500	16%
100 to 250	16%
1,001 to 2,500	14%
Less than 100	14%
More than 2,500	13%

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

Internal APIs	67%
Private APIs	62%
Third-Party APIs	62%
Public APIs	48%
Open APIs	45%
Partner APIs	37%
Composite APIs	25%
Unknown	3%

Does your organization have a solution to discover, inventory and monitor APIs?

Yes	79%
No	11%

What are the top three challenges to securing APIs? (only three choices allowed)

Ability to detect and prevent unauthorized access to accounts	35%
Ability to detect and prevent the exfiltration of sensitive data such as PII, PHI, SSNs and banking information	33%
Identifying vulnerabilities in APIs	30%
Investigating API anomalies or suspicious activity	30%
Ability to detect suspicious and anomalous activity in APIs	27%
Maintaining an accurate inventory of APIs	26%
Prioritizing API vulnerabilities for remediation	25%
Managing API sprawl	23%
Third-party access to APIs	23%
Risk ranking APIs	21%
Lack of visibility into API traffic	17%
Lack of effective technologies	11%

How significant a concern are federal financial regulations (e.g., FFIEC, OCC, CFPB) in relation to your organization’s API inventory and security posture?

Very concerned	28%
Extremely concerned	28%
Moderately concerned	26%
Slightly concerned	11%
Not a concern	5%
Does not apply	1%

How significant of a concern is PCI-DSS compliance in relation to your organization’s API security posture?

Very concerned	33%
Moderately concerned	22%
Extremely concerned	21%
Slightly concerned	13%
Not a concern	7%
Does not apply	3%

How confident are you in your organization's ability to detect and prevent digital fraud and abuse carried out through APIs?

Very confident	38%
Moderately confident	33%
Extremely confident	15%
Slightly confident	11%
Not at all confident	3%

To what extent do you believe malicious bots pose a threat to your organization's APIs?

Moderate threat	40%
Significant threat	26%
Minor threat	23%
Critical threat	7%
Not a threat	5%

Please indicate which of the following sensitive data types your APIs handle: (check all that apply)

Third-Party Data (data obtained from external providers, such as, credit bureaus, risk assessment services)	63%
Personally Identifiable Information (PII)	60%
Account Authentication Information	60%
Payment/Credit Card Information	56%
Device Data (information collected through mobile apps or other devices that include device identifiers and location data that needs special protection)	55%
Behavioral Data (spending habits, transaction patterns, financial preferences)	44%
unknown	2%

Did your organization have a data breach caused by API exploitation in the past two years?

No	65%
Yes	26%
Unknown	9%

What was the root cause of the one or more data breaches? Please select all that apply.

Fraud, abuse and misuse	**42%**
Known attacks (attacks with known signatures)	33%
Account takeover	30%
DDoS	27%
Unknown attacks zero day	23%
Business logic attack	23%
Misconfiguration	21%
Enumeration	21%
Brute force	12%
Other (key in)	8%
Could not determine	5%

What were the consequences of the one or more data breaches? Please select all that apply.

Data loss	41%
Brand value erosion	41%
Financial loss	36%
Loss of customers	35%
Failure to comply with regulations and mandates	33%
Loss of business partners	29%
Failures in company operations	27%
Loss of IP	21%
Unknown	6%

Does your organization use any of the following solutions to achieve API security? Please select all that apply.

Encryption and signatures	50%
Data loss prevention (DLP)	47%
Web Application Firewall (WAF)	47%
An API key	42%
Tokens	40%
Web Application and API Protection (WAAP)	38%
API gateway	37%
API security platform	36%
Basic authentication	35%
Identification of vulnerabilities	34%
API lifecycle management tools	28%
DAST (Dynamic Application Security Testing)	25%
OpenID Connect (OIDC)	21%
Quotas and throttling	15%
None of the above	3%

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

8	36%
9	20%
10	18%
7	16%
5	4%

6	3%
4	2%
3	1%

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

> 50%	45%
31% to 40%	14%
41% to 50%	14%
21% to 30%	10%
10% to 20%	9%
unknown	7%
< 10%	1%
Zero	0%

Do your current solutions enable your organization to do the following? Please select all that apply.

Ability to prevent API abuse, fraud and sensitive data exfiltration in your production environments	47%
Ability to detect and block a variety of API and web-based attacks	44%
Block threats based on threat actor, IP range, geolocation or attack type	44%
Monitor how your API endpoints are communicating and how your application services are behaving	42%
Ability to discover and track the use of 3rd-party APIs and sensitive data transmitted to/from them	39%

Ability to investigate anomalous or suspicious activity and security events in APIs	39%
Ability to perform rapid scans to avoid pushing vulnerable APIs into production environments	38%
Ability to track where APIs are deployed, how they are used and routing information	38%
Detect anomalous events or behaviors in APIs	38%
Ability to detect and remediate known and unknown API attacks, business logic abuse attacks	36%
Ability to have a customizable, downloadable report of vulnerabilities in your APIs and recommendations for remediation	36%
Ability to understand the context between API activity, user activity, data flow and code execution	36%
Ability to easily search for and discover deployed APIs and the tooling used	33%
Ability to discover all APIs in use including shadow, orphaned, and zombie APIs	32%

Does your organization have policies and procedures in place to manage and oversee the inventory and use of APIs?

Yes	86%
No	8%

Who owns your organization's API security program? Please select only one person/department.

CISO or CSO	28%
CTO	18%
CIO	14%

Head of software development	8%
Head of Enterprise Architecture	8%
Engineering	6%
Business units (LOB)	6%
No one person or department	5%
Head of quality assurance	4%
Unknown	3%

What is your organization’s total IT security budget?

$100,000,001 to $250,000,000	26%
$10,000,001 to $50,000,000	19%
$50,000,001 to $100,000,000	16%
Less than $10,000,000	16%
$250,000,001 to $500,000,000	13%
More than $500,000,000	11%

Approximately, what percentage of the 2024 IT security budget are allocated to API security activities?

11% to 20%	30%
20% to 30%	27%
30% to 50%	16%
Less than 10%	13%
Don’t know	10%
Greater than 50%	4%

TRACEABLE

About Traceable

Traceable is the industry's leading API Security company that helps organizations achieve API visibility and attack protection in a cloud-first, API-driven world. Traceable is the only intelligent and context-aware solution that powers complete API security – API discovery and posture management, API security testing, attack detection and protection, anywhere your APIs live. Traceable enables organizations to minimize risk and maximize the value that APIs bring their customers.

www.traceable.ai