TRACEABLE

State of API Security - RSA Conference 2023

The first annual RSA Conference survey of security professionals reveals insights and increased risk in API Security, and where organizations still have gaps in protecting their APIs.

State of API Security - RSA Conference 2023

EXECUTIVE SUMMARY

The cybersecurity industry has evolved considerably in recent years, and with the onslaught of new technologies like Web3 and Generative AI, API security has become that much more important to the world at large, and the 2023 RSA Conference reflected that reality.

For 10 years, APIs have been exploding in use, with virtually no guard rails to keep them safe. For starters, while **69% of organizations factor APIs into their cybersecurity strategy**, an alarming **40% do not have an API security solution in place.**

What makes APIs so dangerous is that they expand the attack surface across all vectors. They present the largest attack surface we have ever encountered in the industry. In the past, hackers had to find ways of bypassing existing solutions, such as WAFs, DLP, API Gateways, etc., in order to find data and disrupt systems. Now, they can simply exploit an API, and obtain access to sensitive data, and not even have to exploit the other solutions in the security stack.

In simple terms, APIs hold the keys to Pandora's box. They are the number one method of gaining access to sensitive data, systems, infrastructure, and a whole host of other surfaces that result in numerous consequences for organizations and their customers.

It doesn't help security initiatives that ownership of API security was a mixed bag. While **38% of respondents stated that the CISO owns API security**, **25% stated that Dev/DevOps owns it**, while another **24% did not know** who owns API security in their organization.

Finally, advanced methods of API threat protection also proved to be a hot button for respondents. To be able to understand, detect, and protect against modern API-based attacks, you must have an intelligent understanding of the complete behavior of your APIs. This includes intended usage (context), and the data they interact with, to form a baseline of the expectation of that API, over time.

An alarming **50% of respondents** did not know if their API security solution could baseline behavior to detect anomalies.

Research Methodology

To better understand the state of API security at the RSA Conference 2023, Traceable conducted the first annual survey on the show floor. The team spoke with over 100 security professionals about their recent experience, struggles, and how they are dealing with a new era of threats – specifically API security risks in their organization. Traceable anonymized and compiled this data to produce a report to inform the industry on the trends and patterns of API security.

Contents

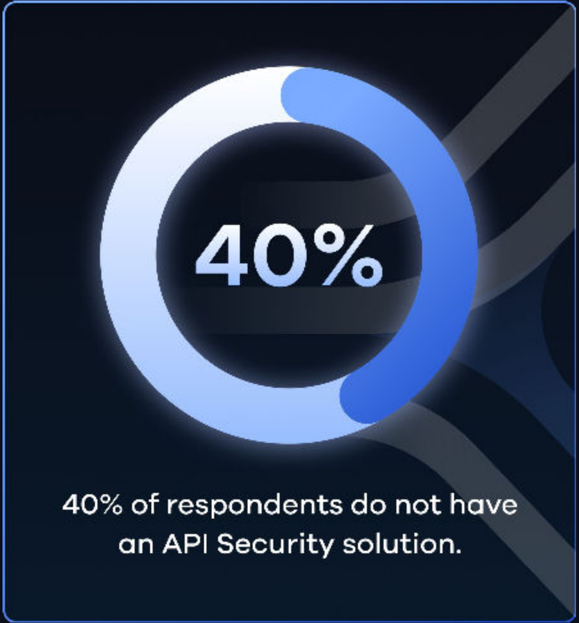
40% of organizations do not have an API security solution

Despite 69% of organizations factor APIs into their cybersecurity strategy, most don’t have a solution in place.

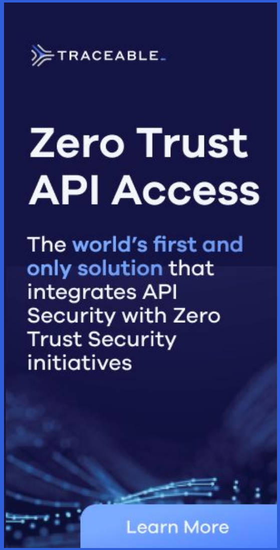
APIs are now the biggest concern when it comes to abuse, fraud and data loss. These kinds of security incidents have a massive impact on organizations in terms of financial loss, brand value erosion, as well as compliance, given mandates such s FFIEC, and other regulatory guidance on data protection.

While it’s reassuring to know that **69% of organizations factor APIs into their cybersecurity strategy**, it’s concerning that **40% of organizations do not have an API security solution in place**.

This is a disconnect. For 10 years, APIs have been exploding in use, with virtually no guard rails to keep them safe. Without an API security solution in place, organizations will not know when they are being exploited.



40% of respondents do not have an API Security solution.



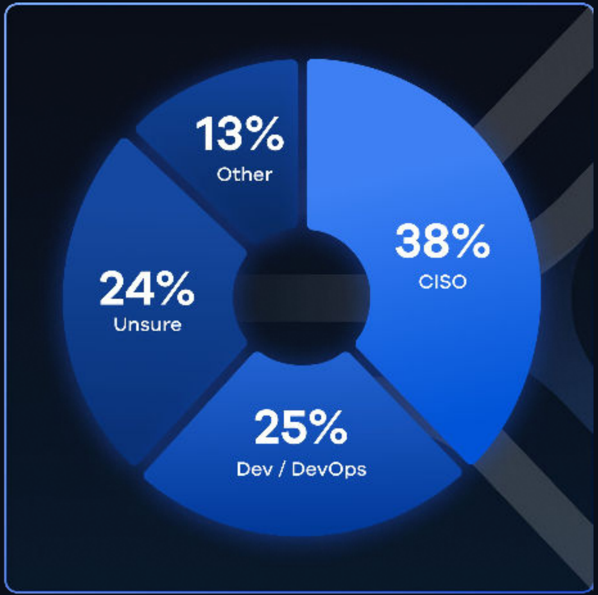
API Security ownership remains fragmented in organizations

38% of respondents claim the CISO owns API security, while 25% claim that Dev/DevOps takes ownership; 24% of respondents do not know who owns API security in their company.

API security ownership can be a complex endeavor. You may have used open APIs from other companies to access specific datasets from their applications. This effectively means that the organization as an entity owns the API. However, when you look closer, different personas are responsible for a variety of aspects of every API. One person may have come up with the idea, and someone else might have written the code. Yet another person may be in charge of maintaining them, and another for securing them.

The complexity of API security ownership was reflected among our respondents, with **38% stating the CISO owns API security, while 25% claim that Dev/DevOps takes ownership. 24% of respondents stated that they do not know who owns API security in their company.**

The fragmented nature of ownership isn't a surprise, given how many teams are involved in both their development and security.

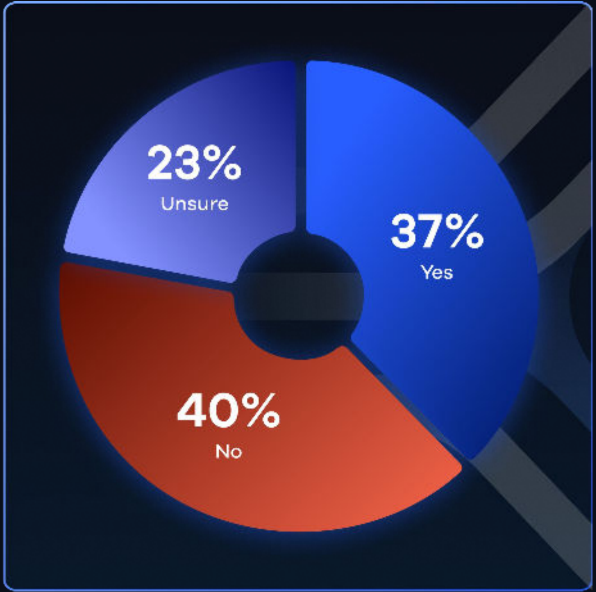


40% of organizations do not have a dedicated API Security Team

The industry is just now starting to see organizations create dedicated professionals and teams to API security. Large financial institutions, for example, have recently begun hiring for API governance initiatives. We didn't see this just one year ago. The tides are changing.

However, it's still slightly concerning that **40% of organizations do not have a dedicated API security team**. This could be for a number of reasons. Some organizations roll API security into other solutions, such as AppSec or Cloud Security,, or think they are covered if they have a WAF. The truth is, these solutions have never been sufficient, and many organizations are finding out the hard way.

It's time to get beyond the status quo methods of detecting and preventing attacks. APIs simply can't be protected with first-generation, one-dimensional, signature-based solutions – and they most definitely need a dedicated team to make sure they are safe.



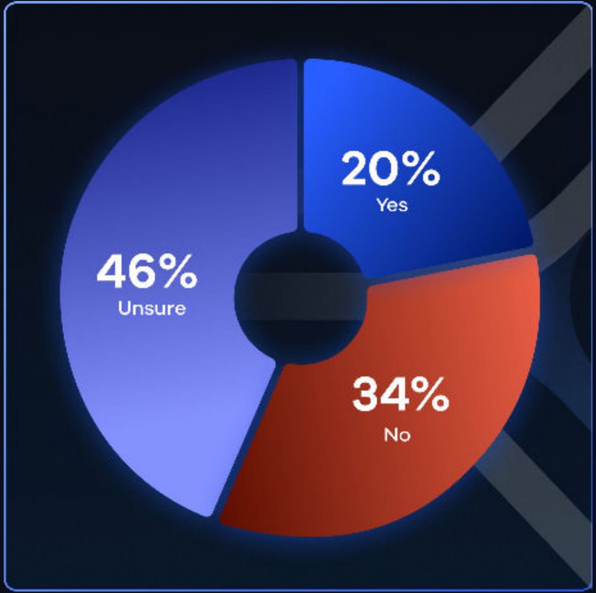
66% either struggle with API sprawl, or do not know if their company is managing API sprawl effectively.

20% stated that they, in fact, do struggle with API sprawl, 34% stated they do not, and a staggering 46% were unsure if their organization was managing API sprawl effectively.

When people think of software architecture, they often picture layers of code. But in recent years, there has been a shift from this model – known as the monolithic approach – toward a more modular development style. This new approach, known as microservices, has given rise to a phenomenon known as **API sprawl,** and it can have massive consequences**.**

The reality is that there are thousands of APIs in organizations, running on multiple clouds, and they are growing each day. Given this consistent rise in the number of APIs, **most organizations simply do not have visibility into how many APIs they have, where those APIs reside, and what those APIs are doing.**

The survey respondents reflected this reality. **20% stated that they, in fact, do struggle with API sprawl, 34% stated they do not, and a staggering 46% were unsure** if their organization was managing API sprawl effectively.



TRACEABLE
The Definitive Guide to API Sprawl
Download the Report
TRACEABLE
API Sprawl
Discover and secure your APIs, address systemic risk, and maintain stakeholder trust.

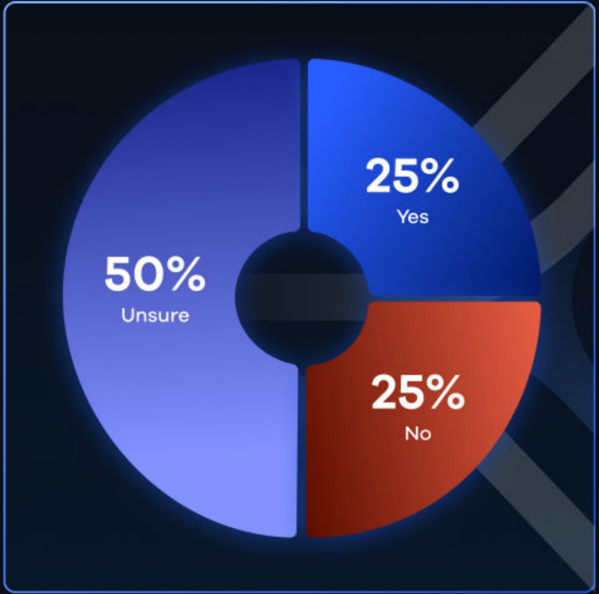
50% of respondents were not sure if they could baseline API behavior and identify abnormal activity

APIs are now the largest attack vector for abuse, data loss and fraud, across nearly every industry. In addition, organizations are using outdated, unreliable approaches to API security, and aren't yet including APIs in those plans.

Given that reality, it's no surprise that **50% of respondents were unsure if their solution could actually baseline API behavior**.

It's often said that *all* API attacks are zero-days – the unknowns. This means, you need to know and understand the "unknown unknowns". API security solutions can tell you what is abnormal if they already know about it – but not the unknowns.

To be able to understand, detect, and protect against modern API-based attacks, you must have an intelligent understanding of the complete behavior (both normal and abnormal) of your APIs. This includes intended usage (context), and the data they interact with, to form a baseline of the expectation of that API, over time.



Additional API Security Resources

TRACEABLE

INDUSTRY INSIGHTS

The Business Case for API Security

Why API Security? Why Now?

[The Business Case for API Security: Why API Security? Why Now?]

TRACEABLE

SOLUTIONS BRIEF

API Data Lake

The Basis for Context-Aware Security, Intelligence and Scalability

API Data Lake - Full Context for Complete API Security

SOLUTION HIGHLIGHTS

[API Data Lake: The Basis for Context-Aware Security]

TRACEABLE

SOLUTIONS BRIEF

Zero Trust API Access (ZTAA)

Traceable's Zero Trust API Access actively reduces your attack surface by minimizing or eliminating implied and persistent trust for APIs.

Why the Next Evolution of Zero Trust MUST Include API Security

SOLUTION HIGHLIGHTS

[Zero Trust API Access: Eliminate Implied and Persistent Trust for APIs.]

TRACEABLE

WHITEPAPER

API Sprawl

Discover and secure your APIs, address systemic risk, and maintain stakeholder trust.

[The Definitive Guide to API Sprawl]

Best practices for building and sustaining a robust API Governance program in your organization

What is API Governance?

[Best Practices for Building and Sustaining a Robust API Governance Program]

www.traceable.ai/request-a-demo

TRACEABLE

TRACEABLE

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

Trusted by World-Leading Businesses

Informatica Bullish JOBVITE

BlueVolt Outreach DigitalOcean

deserve FALCONX Globe

snap! finance Xolve harness

Traceable is Backed By:

UNUSUAL VENTURES svci Silicon Valley CISO Investments TIGERGLOBAL ivp