Google Cloud



API Security: Latest Insights & Key Trends

2022 Research Report

How API security is impacting the pace of innovation at enterprises and what IT leaders are doing to mitigate risks

Table of Contents

Executive Summary	3
Threats abound	4
Affecting the pace of innovation	5
Active API security posture is necessary	6
Current Assessment	7
Confident in the face of threats	7
Is this confidence misplaced?	8
Companies prioritize being proactive with API security	8
Opportunities	9
Consolidation, end-to-end monitoring, oversight needed	9
More training and certification in this space is needed	9
Most agree their strategy needs improvement	10
API security strategy not always a top priority	11
The impact of API management and API gateway solutions	11
API security is a key element	
of a larger API strategy	12

Executive Summary



With the increasing adoption of digital experiences, the use of Application Programming Interfaces, or APIs is on the rise. As such, APIs represent a significant area of vulnerability for organizations worldwide. The following report examines the landscape of API security threats and their impact on the pace of innovation. It delves into the worldview of the technology leaders as it pertains to API security posture and strategy, and offers a perspective on opportunities to improve API security health.

This report is based on research conducted by Google Cloud between May and June 2022 among technology leaders from companies in the United States with at least 1,500 employees who have a significant influence or decision-making authority on purchases of technology solutions related to API initiatives within their organization.

"Why API Security Is a Key Element of a Larger API Strategy" explains that API security posture is a growing concern for IT executives due to the prevalence of threats, but that most organizations need to improve their API security strategy. There is a need for proactive security capabilities and measures as well as end-to-end API security solutions such as Apigee, a full life cycle API management platform.

The Threat Landscape

Threats abound

Companies worldwide rely on Application Programming Interfaces, or APIs, to facilitate digital experiences and unleash the potential energy of their own data and processes. APIs are a critical link in blending proprietary data with assets from third parties. They also serve a critical role in the race to modernize applications, fueling interoperability and, in turn, efficient functionality.

But the proliferation and importance of APIs comes with a risk. As a gateway to a wealth of information and systems APIs have become a favorite target for hackers.

Our research confirms the widespread impact of these threats. We surveyed over 500 technology leaders in the United States. Half of them report experiencing an API security incident in the past 12 months. That percentage is higher or lower depending on who you ask. 62% of C-Suite executives surveyed indicated that they've had a security incident in the past 12 months while only 37% of those who are a couple levels removed from the C-Suite said the same.

This could point toward the limited purview of functional IT teams, or it could be an indication of how salient the issue is for those with greater responsibility. Or both.

More than three out of five C-Suite ITDMs report experiencing an API security incident in the past 12 months.

"The rate at which APIs are developed today exceeds the rate at which our organization can ensure the security of each of these APIs."

- IT Supervisor/Manager, Computer Hardware/ Software/Services

API Security Incidents





To compound the issue, threats surface from a myriad of API security areas with IT leaders each identifying more than three areas on average. While no single area stands out as a glaring vulnerability, the three most common sources of potential threats are security misconfigurations, outdated APIs/data/components, and bots/spam/abuse.

Misconfigurations, as a category, are the most identified threat area with 2 of 5 IT leaders selecting either security misconfiguration or misconfigured APIs.

Sources of API Security Threats



Affecting the pace of innovation

These threats and incidents have real-world implications. API security is slowing the pace of innovation for many organizations. More than half (53%) of organizations have delayed the rollout of a new service or application due to API security concerns. For those who have experienced an incident in the past 12 months, more than three quarters (77%) have delayed the rollout of a new service or application.

Delayed the Rollout of a New Service or Application Due to API Security Concerns



Active API security posture is necessary

With security vulnerabilities being introduced from a variety of sources throughout development, it will come as no surprise that security issues are identified at every phase of the API lifecycle from design to testing to deployment and beyond. Naturally, security issues are most commonly discovered during testing performed as part of the release management process (67%), but a substantial number of vulnerabilities are identified as part of the process to deploy to production (64%). This indicated an area of risk for vulnerabilities to be deployed to production as a considerable percent of possible security issues are identified in the later stages of API lifecycle.

Notably, issues and vulnerabilities are identified with real-time monitoring in production by three out of five (62%) IT leaders, emphasizing that the need for an active security posture is a necessity in this environment.

C-Suite respondents were more likely than IT leaders who report up to executives to say vulnerabilities are caught during the software development process (66%).

Stage of the API lifecycle where API security issues and vulnerabilities are identified



Current Assessment

Confident in the face of threats

Despite the precarious API threat landscape, most organizations believe they have the tools and solutions to ensure end-to-end API security. In fact, more that three quarters (77%) of respondents said they have the required tools and solutions and another 16% said they partially have what they need to implement end-to-end API security, there were very few who said they don't have the tools they need.

What's more interesting, most technology leaders (66%) would rate their security posture as *Advanced*. Specifically, they believe that they have a comprehensive and centralized API security center of excellence, and their security tools and solutions are not disjointed in any way.

Certain groups are more confident of their security posture than others. The following rate their API Security as *Advanced*:

- Cloud Native (71%)
- Hybrid Cloud environment (71%)
- C-Suite IT executives (71%)
- Had an Incident in Past 12 Months (71%)



Advanced API security Posture

Cloud Native organizations responded in the survey that their security posture is advanced at a higher rate despite being more likely to have had an incident and delayed a rollout in the past year.

Is this confidence misplaced?

It would appear that there is a gap between the existence of security incidents and confidence that the tools are doing the job. Could it be that organizations are ignoring the prevalence of security incidents (50% had an incident in the last year) as well as the impact API security is having on innovation (53% have delayed a rollout in the past year)? Or is it simply that security incidents are accepted as a cost of doing business in the digital space?

The reality is likely somewhere in the middle. Some may be underestimating threats and the extent to which they impact their organization, while also being realistic that API security is constantly evolving, and threats are a part of life.

Companies prioritize being proactive with API security

To stay ahead of security threats, many organizations look for solutions that allow them to be proactive while minimizing the burden on their security teams. According to our research, capabilities that proactively identify security threats (60%) and improve automation (57%) are at the top of most IT leaders' wish lists for the next year. However, most are not ready or willing to prioritize taking the leap toward incorporating Artificial Intelligence and Machine Learning into their API security yet.

Technologies priorities for API security



Opportunities

Consolidation, end-to-end monitoring, oversight needed

So, what are IT leaders looking for in an API security solution given a relentless threat landscape and a litany of vulnerabilities to account for across every stage of the API lifecycle?

Aside from factors that are near table stakes, like easy integration with existing tools and support for the latest technologies, consolidation and end-to-end solutions are some of the most important factors to look for when evaluating API security solutions. This is especially true for those reporting to the C-Suite (C-1). While the C-Suite themselves are more focused on easy integration with existing API tools, the level below them is also looking for a solution that will cover a lot of ground.

When evaluating API security solutions, the C-Suite tends to value 3rd party recommendations more than C-1 while C-1 values solutions that are built for cloud-native security with the latest technologies. Moreover, a considerably higher percentage of C-1 prefer consolidated API security solutions over point solutions.

Factors used to Evaluate API Security Solutions (Top-5)



More training and certification in this space is needed

Aside from technological solutions, many look to training and procedural improvements as a means of combating threats. Top priorities for API security include establishing an API security learning and certification standard (38%), improving their documentation to incorporate security best practices (38%), and modifying existing processes to catch API security and vulnerability issues (37%). But IT leaders tend to take a "yes, please" approach to improving their API security with no single initiative standing out above others.

Most agree their strategy needs improvement

According to our research, most organizations don't have a complete API security strategy in place. A majority (60%) would say that their strategy needs improvement at the very least.



Like other security areas, there's a slight disconnect between the perceptions of IT leaders in the C-Suite and those reporting to them (C-1). In this case, 53% of C-Suite would say their API security strategy needs improvement. That number increases to 61% for those reporting to the C-Suite (C-1), and 69% among those two levels removed (C-2).





API security strategy not always a top priority

While many organizations simply lack the resources and know-how to enact a comprehensive strategy, IT leaders in those organizations often feel as though API security isn't prioritized. This can lead to some animosity within the ranks of the security team.

Even those with a plan are likely to have API security solutions littered across their organization with responsibilities often divided among teams. In fact, API security responsibilities frequently vary from company to company depending on needs, industry, and company structure.

The impact of API management and API gateway solutions

More than three quarters (78%) of organizations say they have an organization-wide API management/API Gateway solution implemented.

Those organizations are less likely to feel that their security strategy needs improvement (52%), they are more likely to have a comprehensive and centralized API security center of excellence (74%), and more likely to believe they have the required tools and solutions implemented to ensure end-to-end API security (91%).

"The VP does not see it as a priority within the budget."

- IT Supervisor/Manager, Financial Services

We do not have a strategy "due to lack of organizational insight and leadership."

- Director/VP of IT, Health Care

Companies with organization-wide API management (APIM) solution implemented



API security is a key element of a larger API strategy

Attacks on APIs are common, but incidents don't have to be.

End-to-end solutions enable organizations to identify and sure-up vulnerable API security areas such as misconfigurations as well as outdated APIs, data, and components. And while point solutions can deliver a fractured solution, it's clear that, given the breadth of attacks across the API lifecycle and the variety of vulnerabilities, a comprehensive solution offers the best chance of avoiding delays and stymied innovation. Long term API security needs to be prioritized as part of a larger API management plan and when possible, an organization-wide API strategy.



About Apigee API Management Platform

Google Cloud's Apigee API management platform delivers full lifecycle API management to help businesses unlock the value of data and securely deliver modern applications and digital experiences. Apigee offers a rich set of capabilities to enable enterprises to gain control over and visibility into API traffic, including the ability to automate troubleshooting and problem resolution and to derive insights from API usage.

Ready to learn more? Visit cloud.google.com/apigee, or connect with us directly at apigee@google.com.

