2024 State of API Security

Fearless API Security

SALT

Executive Summary

The State of API Security in Q1 2024

The Salt Security State of API Security Report for this year has brought to light an urgent need for action, as the usage of APIs has skyrocketed and security breaches have become more commonplace. Organizations are now managing more APIs than ever before, with 66% of them managing over 100. This has led to a massive increase in API traffic, which has created an expanded attack surface. As a result, there has been a staggering increase in API security breaches, with incidents more than doubling in the past year (37% of respondents experienced incidents). However, despite this alarming trend, too few organizations are implementing advanced API security strategies, with only 7.5% of organizations implementing dedicated API testing and threat modeling. Limited budgets (22%) and scarce resources (21%) further hinder the implementation of robust security measures.

While the security landscape is in a state of flux, some things remain the same—outdated or "zombie" APIs are the most critical concern for survey respondents (69.9%), following the trend of last year's report; however, now account takeover/misuse is also high ranked with 46% of respondents claiming it to be a main concern. Authentication weaknesses persist as a major vulnerability in production APIs, with a troubling number of organizations encountering authentication issues (38%) and sensitive data exposure incidents (38%) within the last twelve months. These security gaps underscore the need for a more comprehensive approach to API security.

Furthermore, organizations struggle to maintain a complete API inventory, with only 58% having an established API discovery process. This lack of visibility into the full API ecosystem creates significant security blind spots and makes it difficult to identify and address vulnerabilities. This incomplete API inventory provides immense challenges to providing posture governance strategies across all APIs.

Another trend we are seeing across the API space is the increased use of AI within API development pipelines. This allows organizations to rapidly expand the creation and use of APIs. While this can help progress digital transformation strategies it also can introduce more risk. It can be hard for security teams to keep track of all these newly created APIs manually so it becomes important to look at automation such as with AI based API security solutions.

To address these critical issues, API security must become a C-level priority with increased investment in specialized protections beyond traditional API gateways and WAFs. Robust API discovery processes are essential for gaining comprehensive visibility into the API landscape. Security must be integrated from the earliest stages of API development, alongside continuous monitoring for rapid threat detection and response. The time to act is now—this report underscores the critical need for organizations to overhaul their API security approach to protect their assets and reputation in this rapidly evolving threat landscape.

Table of Contents

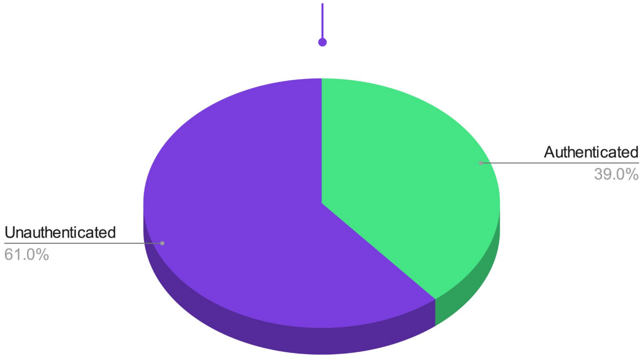
The Threat of API Attacks is Real and Growing

API security incidents more than doubled over past 12 months

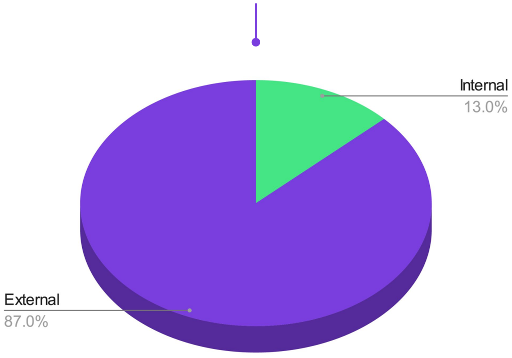
API security incidents have more than doubled in the past year due to the rapid increase in API usage, creating a vast and expanding attack surface for malicious actors to exploit. Salt Labs has found that attackers are using a diverse range of tactics, with a significant portion bypassing authentication protocols altogether (an astonishing 61% are unauthenticated). Therefore, don't be fooled into thinking that authentication protocols provide complete security—almost two-thirds of attackers can bypass them altogether. They exploit vulnerabilities such as Broken Object Level Authorization (BOLA), OAuth, and insecure API endpoints to gain unauthorized access to sensitive data and systems.

Even internal APIs are vulnerable, with 13% of attack attempts explicitly targeting them. This underscores the need for comprehensive API security across your entire ecosystem, from public-facing APIs to internal integrations. With a significant rise in breaches, 37% of organizations reported security incidents compared to only 17% in 2023, the threat is not just theoretical—it's happening now and impacting businesses of all sizes.

Salt customer data: Attack attempts from authenticated vs unauthenticated attackers



Salt customer data: Attack attempts against internal and external facing API endpoints



Don’t Let API Vulnerabilities Become your Next Boardroom Crisis

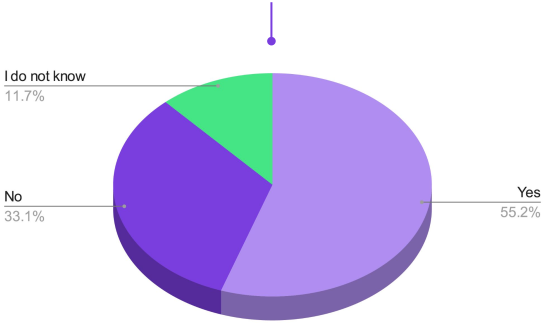
55% have delayed an application rollout over API security issues, and the C Suite is getting involved in the discussion

APIs are crucial in modern digital business by driving innovation and customer interactions. However, without proper security measures, APIs can be vulnerable to attacks that can put sensitive data at risk, disrupt operations, and damage customer trust. In fact, a recent survey revealed that 55% of respondents experienced delays in application rollout due to security issues with their APIs. This underscores the real-world impact of inadequate API security, including delayed innovation, frustrated customers, and lost revenue.

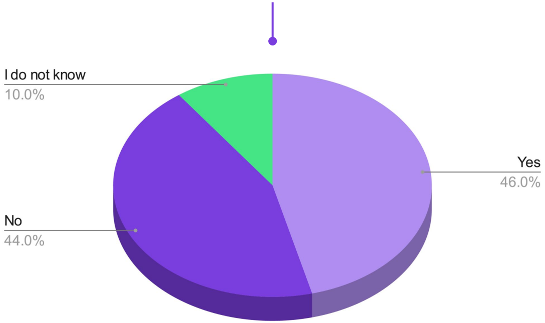
Moreover, the survey revealed that C-level executives increasingly recognize the importance of API security, with 46% of respondents reporting that it has become a topic of executive discussion. This highlights the growing awareness of the business risks involved in API security.

Ensuring robust API security isn't just an IT issue, it's a critical business continuity imperative. By prioritizing strong API security measures, Chief Information Security Officers (CISOs) can protect their organization's reputation, prevent costly downtime, and ensure the smooth operation of mission-critical applications. In fact, investing in robust API security can be viewed as a strategic advantage that enables organizations to deliver applications faster and more securely, ultimately driving business growth.

Have you ever slowed the rollout of a new application into production because of API security concerns?



Has the security of your APIs become a C-level discussion at your organization?



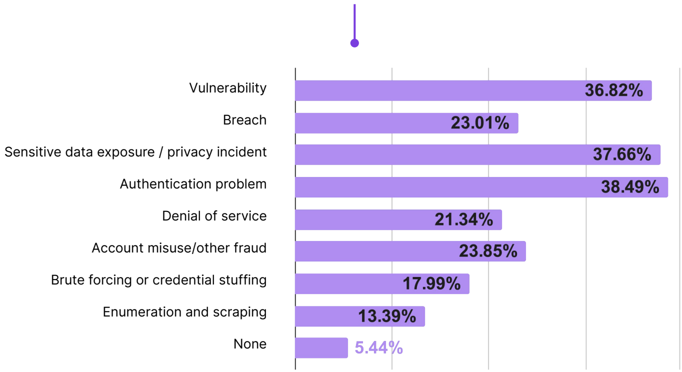
The Stark Reality of API Risks

95% of respondents have experienced security problems in production APIs, with 23% having experienced a breach

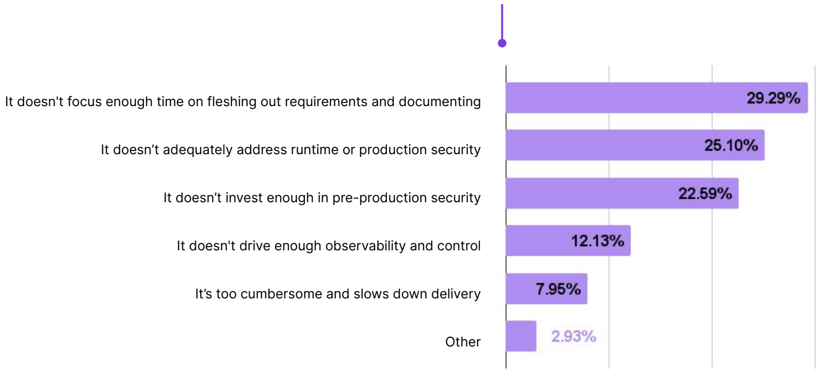
Respondents revealed that a significant number of organizations are facing difficulties in controlling security incidents related to their APIs. In fact, 95% of organizations are struggling to contain these incidents. This is further compounded by the fact that 23% of organizations have experienced a breach, which means that their sensitive data and critical systems have been compromised. This is a major concern and highlights the need for improved security measures.

Organizations that fail to invest in adequate API runtime protection are at risk of falling prey to an ever-increasing threat landscape. Therefore, it is essential for organizations to prioritize specialized API security measures to safeguard their sensitive data and ensure business continuity in today's dynamic digital environment. By doing so, they can mitigate the risk of breaches, protect their reputation, and maintain a competitive edge.

In the past 12 months, what security problems have you found in production APIs?



What is your biggest concern about your company's existing API program?



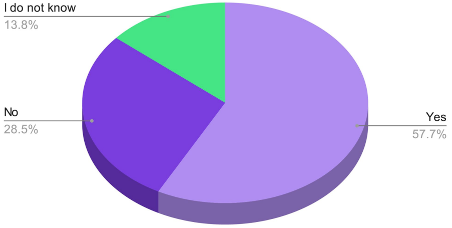
Attackers are Following the OWASP Top 10. Are you?

80% of attack attempts leverage one or more of OWASP API Top 10 methods, but only about 58% of respondents focus on this industry list

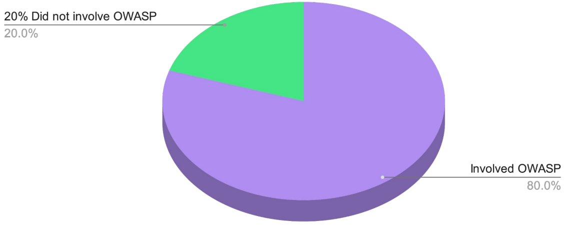
The OWASP API Security Top 10 is a crucial resource for professionals working in API security. It highlights the most common and high-risk vulnerabilities that attackers exploit. A large percentage of API attacks target these well-known weaknesses, which shows that malicious actors have a clear understanding of how to bypass security controls. However, despite this established knowledge base, only 58% of organizations prioritize protection against these threats. This is a concerning gap between awareness and action that leaves many organizations dangerously exposed. Salt Security aims to bridge this divide by empowering businesses to defend against OWASP API Top 10 vulnerabilities proactively. Our comprehensive solutions use AI/ML and expert-curated threat intelligence from Salt Labs to identify and neutralize these critical threats, safeguarding your APIs from well-worn attack vectors.

When mapping attempted attacks to the OWASP API Security Top 10, we saw a myriad of #8: injection attacks (54%)—which may happen due to high activity of vulnerability scanners, as most of their payloads are injections. The next most common attacks were ties with #2: broken user authentication, #4: lack of resources & rate limiting (which is an API issue that requires that attack activity be investigated at the user level vs. the aggregate level, a nuance traditional tools like WAFs simply can't distinguish), and #5: broken function level authorization are all the next highest at 12%. These attacks take advantage of business logic gaps, and the resulting exploitation potential is quite high because these attacks simply cannot be detected by traditional tools.

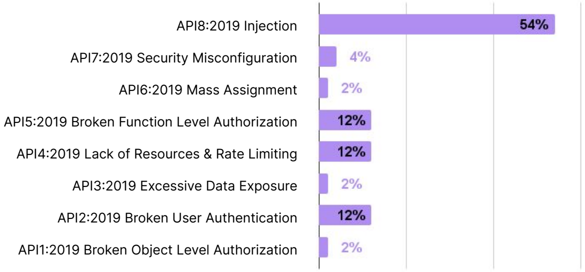
Has your security team highlighted the OWASP API Top 10 Threats as a focus area for your security program?



Salt customer data: Attack attempts leveraging the OWASP API Security Top 10 vs other attack types



Salt customer data: Attack attempts that map to the OWASP API Security Top 10



Get Ahead of the Curve: Master API Posture Governance

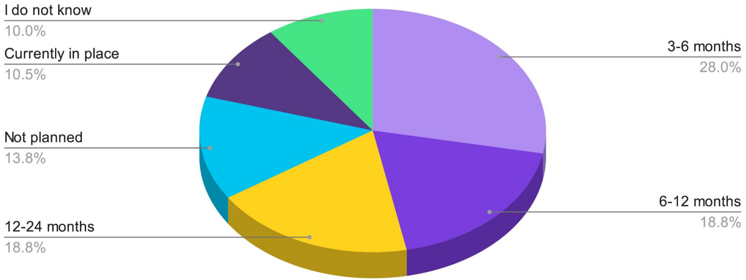
Only 10% currently have a strategy in place, while 47% plan to implement such strategy within the next 12 months

API security requires a proactive and comprehensive approach that traditional methods struggle to maintain, especially with the increasing complexity of the modern API landscape, further amplified by the rise of AI-built APIs. To effectively mitigate risks throughout an API's lifecycle, organizations need to adopt an API posture governance strategy. This strategy provides a structured framework for managing and securing the entire API ecosystem, from design and development to deployment and ongoing maintenance. However, the Salt Security survey revealed a significant gap, with only 10% of organizations currently having an API posture governance strategy in place.

To address this gap, it's becoming more important to deploy a robust API posture governance engine. It empowers organizations to gain complete visibility into their API landscape, eliminating blind spots and ensuring no critical API goes unnoticed. It also enables the establishment and enforcement of corporate-wide security standards and regulations across the entire API ecosystem. This fosters a unified approach to API security, where all stakeholders, from developers to security teams, are aligned on best practices and compliance requirements.

Organizations can no longer afford to wait until a security breach occurs. By proactively implementing an API posture governance strategy and leveraging a powerful engine, organizations can reduce the risk of breaches—even before APIs are deployed to production—to protect their valuable data, and maintain the trust of their customers and partners. This is especially important as the complexity of API ecosystems continues to grow, making it increasingly difficult to manage and secure APIs without a comprehensive and well-defined strategy.

Do you currently have plans in place for an API posture governance strategy?



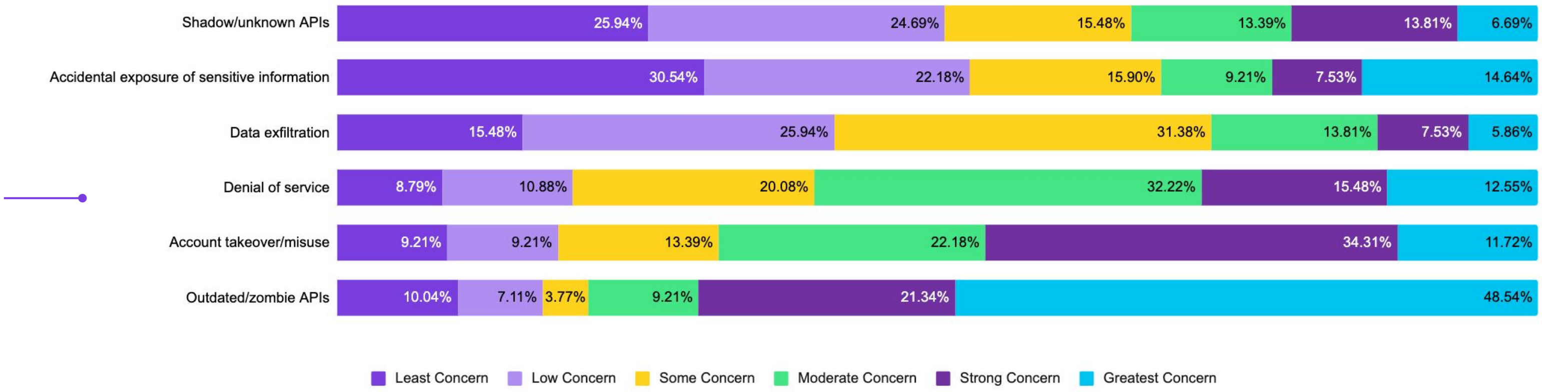
Zombie APIs: The Undead Threat Lurking in the Dark

Zombie APIs remain a top concern amongst respondents

Similar to last year, respondents have expressed high levels of concern about the potential risks associated with "zombie" APIs; however, this year we saw a striking result of 69.9% compared to last year’s 54%. Zombie APIs are outdated and forgotten APIs that exist within an organization's systems. Since they are no longer maintained or updated, they often lack essential security patches, making them easy targets for malicious actors. Attackers can exploit vulnerabilities in zombie APIs to gain unauthorized access to sensitive data, disrupt operations, or carry out further attacks within a network. The prevalence of zombie APIs is likely due to the dynamic nature of application development, where APIs are frequently created, updated, and sometimes decommissioned. However, the decommissioning process for APIs is often incomplete, leaving zombie APIs behind and posing a significant security risk.

The survey also found that 46% of respondents consider account takeover/misuse a top concern, highlighting the growing threat of unauthorized access to user accounts through compromised API credentials. Account takeover (ATO) attacks targeting APIs are on the rise. In an ATO attack, malicious actors steal a user's login credentials (username and password) and use them to impersonate the legitimate user to gain access to accounts and potentially sensitive data. API credentials can be compromised through various methods, including phishing attacks, malware infections, or brute-force attacks targeting weak passwords. Once attackers gain access to valid API credentials, they can bypass traditional security measures designed to protect user accounts accessed through web interfaces. This can give them unrestricted access to a user's account data and the ability to perform actions on the user's behalf, such as transferring funds, changing personal information, or even launching further attacks within the system.

Rank your top API security-related concerns



SALT

Is your API Security Playing Catch-up?

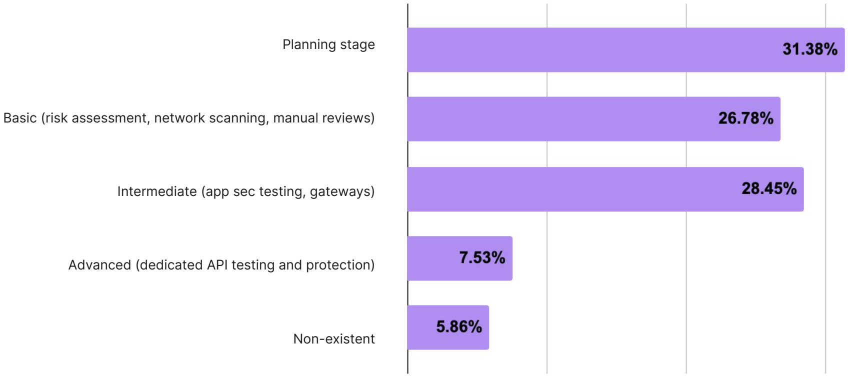
Only 7.5% of respondents consider their API security programs to be advanced, 31% are just in the planning stage

According to our recent survey, the level of API security maturity in organizations is a cause for concern. The survey revealed that only 7.5% of organizations consider their API security programs advanced, leaving the vast majority with significant room for improvement. In addition is the fact that over half of the organizations surveyed (55%) are still at the basic or intermediate stages of API security, relying on traditional security measures that may be inadequate against modern API threats.

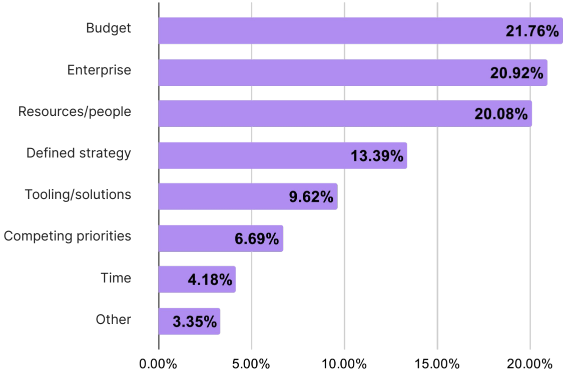
The survey also uncovered that over one-third (37%) of the respondents, who all have APIs running in production, do not have a current API security strategy in place. This includes nearly 6% of respondents who admit that their programs are non-existent, and 31% who say their API security strategy is still in the planning stages. This is a significant gap between the crucial role APIs play in modern business and the security measures taken to protect them.

It's important to take API security seriously to prevent your sensitive data and operations from becoming the next headline-making breach.

How would you describe the security strategy for your API development program?



What is the biggest obstacle keeping you from implementing an optimal API security strategy?



Don’t let Hidden APIs Turn into Headline-making Breaches

Only 58% of organizations have processes in place to discover APIs across their organization

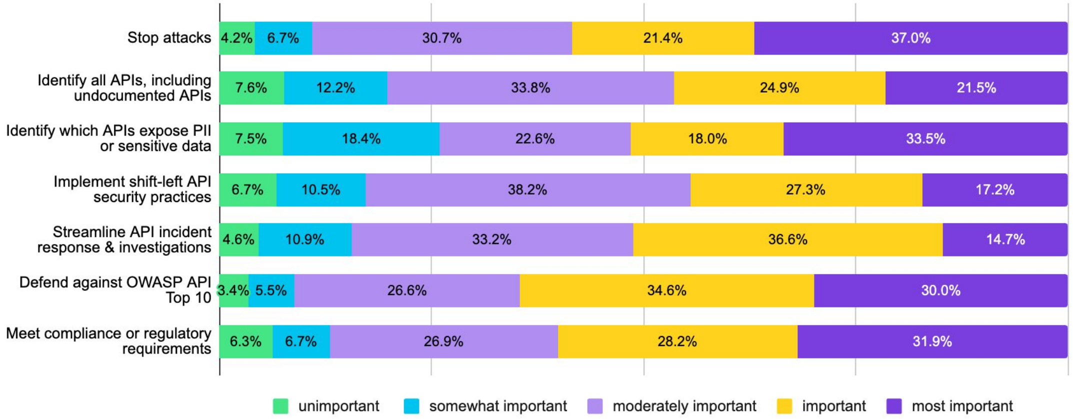
API discovery is a major challenge for many organizations, which means that a significant number of APIs are at risk of being exploited. Attackers are always looking for hidden APIs to use as a backdoor to your systems.

The attributes of an API security platform that respondents identified as most valuable were the ability to stop attacks (37%), identify which APIs expose PII or sensitive data (33.5%), and meet compliance or regulatory requirements (31.9%). Which are the same top three as last year’s report.

Although only 17.2% of survey respondents found "shift left" security practices highly important, focusing on immediate API security concerns is understandable.

A comprehensive discovery engine can help by illuminating your entire API landscape, even identifying the most obscure APIs and closing critical security gaps. This allows you to protect your entire API ecosystem, regardless of where or how they were created. Additionally, with the ability to identify APIs exposing sensitive data (valued by 33.5% of respondents), you can prioritize security for your most critical assets.

How do you rate the value of each of these attributes of an API security platform?



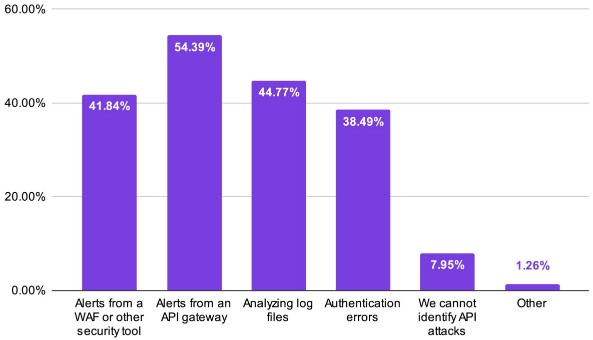
API Attacks are Evolving. Is your Security Strategy?

Only 21% of respondents believe their existing security approaches are very effective at preventing API attacks

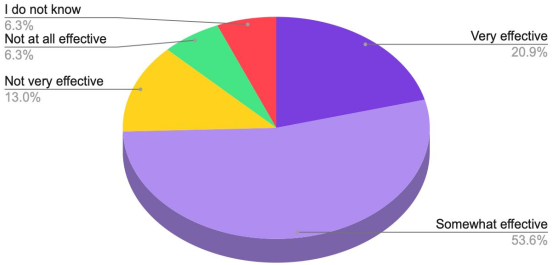
In our survey only 21% of the respondents believe that their current security approaches are effective in preventing API attacks. This indicates that traditional security tools have some limitations. Among the most commonly used tools, API gateways (used by 54% of respondents) mainly focus on coarse-grained authentication, authorization, encryption, and rate limiting. However, these measures can be easily bypassed by modern attackers. Analyzing log files (used by 45% of respondents) is a reactive approach and can be quite tedious. By the time a security analyst can identify an attack from log data, it's likely the attackers have already infiltrated your systems and stolen valuable data or caused other harm.

WAFs (utilized by 42% of respondents) are known to be ineffective against modern API attacks. Their reliance on signature-based detection and proxy architectures leaves them blind to complex attack patterns that don't match known threats like XSS, SQLi, or JSON injection. WAFs simply can't stitch together the data points needed to detect the advanced behavior that characterizes modern API attacks.

How do you identify an attack or attacker targeting your APIs?



How effective are your existing security tools in preventing API attacks?



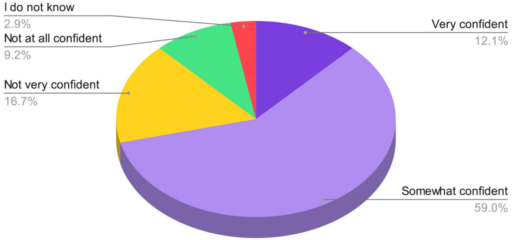
Yesterday’s Documentation = Today’s Vulnerability

25.5% update their APIs at least weekly, while 22% update their documentation rather infrequently

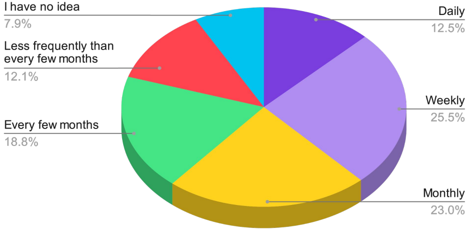
In today's fast-paced digital world, APIs are constantly changing. Almost half of all organizations update their APIs at least once a week (38%), and a significant portion (12.5%) make daily updates. Outdated documentation and poor visibility into your API landscape can leave you exposed to security risks. Only 12% of respondents feel very confident in the accuracy of their API inventory, highlighting a widespread lack of trust in their security posture. This lack of confidence is justified, given that nearly a third of respondents (29%) don't feel confident at all in the accuracy of their documentation.

Furthermore, OAS and Swagger files, designed to streamline API documentation, often fall behind the fast update cycles of modern APIs. Only 19% of organizations update these critical files as frequently as their APIs change. A significant portion (16%) update documentation with no regular cadence at all, and a concerning 11% wait a full six months between updates. As a result, there is often a significant gap between the actual state of your APIs and what your documentation reflects.

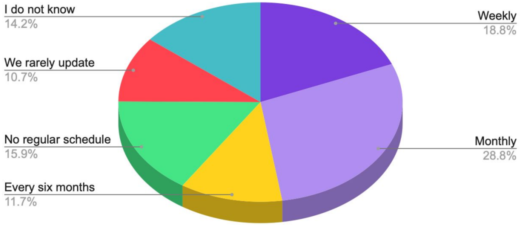
How confident are you that your API inventory is complete?



On average, how often are your primary APIs updated?



How frequently do you update your OAS or Swagger files?



Don’t let PII Exposure Become a Costly Compliance Nightmare

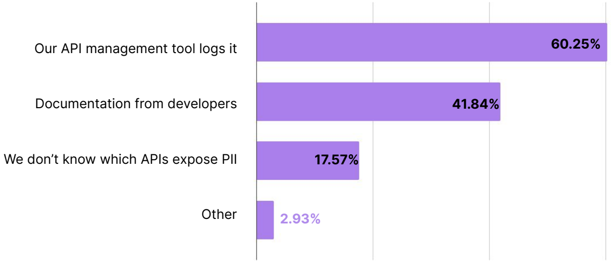
Under 15% are very confident they understand which APIs expose PII data

The survey revealed that many organizations lack confidence in their ability to identify and secure sensitive data exposed through APIs. Shockingly, only about 15% of those surveyed expressed a high level of confidence in their ability to identify which APIs expose Personally Identifiable Information (PII) data. This lack of clarity poses a significant risk for data breaches and regulatory noncompliance.

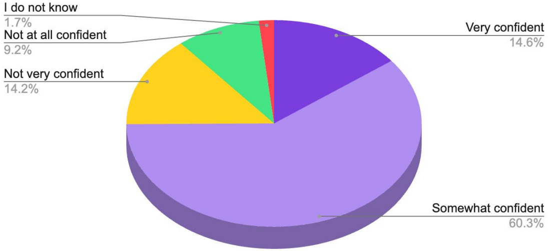
The survey found that around 60% of organizations are only somewhat confident in their understanding of PII exposure through APIs, while 25% are unsure or lack confidence altogether. This presents a serious challenge for organizations, leaving them vulnerable to security incidents involving the exposure of sensitive data. In fact, 38% of survey respondents had already experienced such a security incident, highlighting the real-world consequences of inadequate PII protection.

Traditional methods of PII discovery, such as logs from API management tools and developer documentation, have proven to be inadequate; however, 60% and 42%, respectively, of respondents still rely on these methods.

How do you know which APIs expose sensitive data or PII?



How confident are you that your API inventory provides enough detail about your APIs, including exposure of sensitive data or PII?



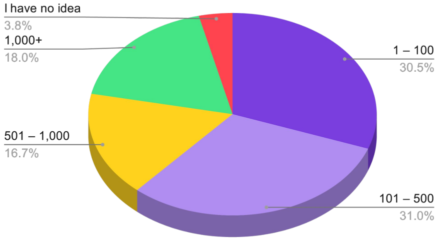
Your API Landscape is Growing Exponentially. Is your Security Keeping up?

66% of respondents manage more than 100 APIs, compared to 59% in 2023

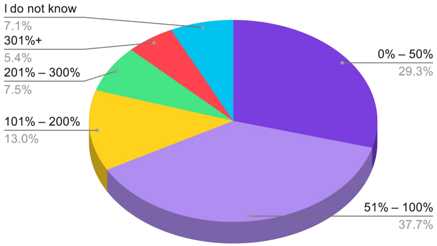
The use of APIs has skyrocketed in recent years. As of now, 66% of organizations manage more than 100 APIs, compared to 59% in 2023. A significant percentage (35%) of these organizations are dealing with the security implications of managing over 500 APIs. Many organizations have experienced a rapid increase in API growth over the past year. 38% of respondents have reported an increase of 51-100%, and another 26% have reported an increase of over 100%. This expansion has created a vast and constantly changing attack surface that is hard to secure with traditional security tools.

To add to the challenge, around 67% of organizations are dealing with over 10 million API requests each month. Some APIs are being bombarded with as many as 500 million requests, making it difficult to identify malicious activity hidden amongst legitimate requests. The trend of AI-generated APIs has added to this complexity. These APIs often have dynamic functionality that is not completely understood, making it even harder to maintain security and visibility.

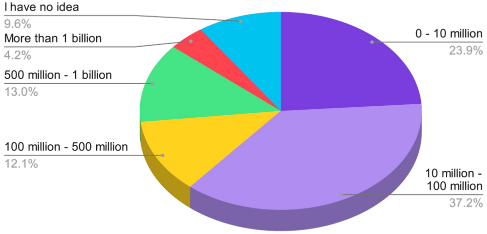
How many APIs does your organization develop, deliver, and/or integrate?



By how much has the number of APIs increased over the past 12 months?



How many requests are sent to your applications' APIs each month?



Vulnerabilities Discovered in the Wild

Salt Labs uncovers API security vulnerabilities and an increase in APIs

Salt Labs is the extraordinarily talented research division of Salt Security, and as such our mission is to constantly identify and surface API vulnerabilities in major online websites and services. Our researchers are continuously probing these services—old and new, big and small, across all geographical regions and business sectors. We opt to publish a subset of these important findings as part of our efforts to educate the industry about API security.

In this section of the report, we wanted to augment the survey and empirical data to showcase some vulnerabilities and trends that the Salt Labs team has recently discovered. While these particular vulnerabilities have been disclosed to the companies involved and the issues have been resolved, we have chosen to anonymize the companies and applications—the focus should be on the nature of the security gap, not on a particular company who had that gap, because our research shows that when one service has a flaw like one of these, many others do as well.

To start out, the count of APIs are increasing, having gone up by 167% in the past year. Additionally, the amount of endpoints went up by 400% since last year, and a factor growth of 5.0, meaning APIs are now five times larger compared to the beginning of 2023 (the number of endpoints in an API can represent its size).

It is interesting to note that 38% of survey respondents stated that they had identified a vulnerability in their production APIs. While that may not seem like a lot, this number has fluctuated between 38% and 55% since we began conducting this survey, but Salt Labs research indicates this number is substantially higher.

Additionally, the number of traffic (requests) can show how much API usage there is. It's important to note that the amount of traffic is part of the agreement we have with the customer, so there may be a cap or limitation in this area. Throughout the duration of 2023, the count of API calls experienced steady growth, with a percentage increase of 96% and a factor growth of 2.0. This signifies that the usage has doubled over the course of the year. At the end of the day, from the start of 2023 through its end—our customers have more APIs, they are getting larger (endpoint count), and accessed more than ever (request count).

One unique and important point to consider when dealing with API security is that, as opposed to many other fields in security and offensive research, success rates (cases in which we found a significant API security issue) are very high. If we can find these security gaps, you can bet attackers will too.

These findings provide yet another very strong indication that API security is one of the most vital security disciplines today and that every organization employing a web service should make a concerted effort to invest time and resources into securing their APIs.

Found in the Wild: Threat Landscape and an Uptick in OAuth Vulnerabilities

APIs are the building blocks of today's interconnected digital ecosystem, powering the seamless communication between applications that drive modern business operations. However, there's a rapidly expanding API threat landscape that poses a significant risk to organizations. In this brief report, we'll explore key data points that highlight this growing risk.

Analysis of CVE data shows concerning trends. Web vulnerabilities such as SQL Injection and XSS are on an alarming upward trajectory, with SQL Injection CVEs witnessing a staggering 363.30% increase from 2020 to 2023. This exponential growth underscores the heightened risk these vulnerabilities pose to the security of APIs.

OAuth vulnerabilities are also a cause for concern. The number of OAuth-related CVEs is steadily rising, highlighting a potentially weak link within the authentication mechanisms employed by many APIs. These vulnerabilities provide a potentially exploitable entry point for attackers seeking to gain unauthorized access to sensitive data or disrupt critical business processes.

Bug bounty program data offers valuable insights into the real-world exploitation attempts targeting APIs. There's been a surge in the reporting of SSRF and IDOR vulnerabilities, which mirrors a core theme in the OWASP API Top 10 2023. These findings substantiate the growing prevalence of these specific attack vectors. Conversely, a decline in CSRF reports suggests that this particular vulnerability may be diminishing as a threat.

Salt Security's internal data corroborates these external trends. In fact, the numbers from 2024 are 1.5 times higher than those recorded in 2023 within the key categories—'SQL injection', 'Shell Code', 'XSS' and 'Path Traversal'. This substantial rise emphasizes the persistent and concerning presence of these well-established API security threats.

The data presented here paints a clear picture: API vulnerabilities pose a heightened risk to modern organizations. Traditional web vulnerabilities remain highly relevant within the context of the API economy. This necessitates a shift in security strategies. CISOs must prioritize API security measures that address not only these classic threats but also the emerging attack vectors outlined in the OWASP API Top 10.

Proactive defense is paramount in today's dynamic threat landscape. Investment in dedicated API security solutions is essential for achieving comprehensive threat visibility. These solutions empower CISOs to identify and mitigate API vulnerabilities before they can be exploited by malicious actors. Furthermore, proactive identification of security weaknesses allows for timely remediation, preventing costly data breaches and operational disruptions.

Recommendations and Conclusions

Implications for API security

The results from the Q1 2024 State of API Security survey are clear. Respondents overwhelmingly told us that reliance on APIs is continuing to grow as APIs become ever more imperative to their organizations' success. At the same time, APIs are getting harder to protect as current tools and processes can't keep pace with new attack trends.

Organizations must move from traditional security practices and last-generation tools to a modern security strategy that addresses security at every stage of the API lifecycle and provides a broad range of protections that foster collaboration

Define a robust API security strategy

WAFs and API gateways leave significant gaps when defending against API attacks, so companies need to define and execute an API security strategy that covers the complete API lifecycle and addresses cross-functional responsibilities. A comprehensive program must include API design analysis and drift analysis, automatic and continuous discovery, augmented runtime protections, a feedback loop for developers to use runtime insights to harden APIs, training for SecOps teams to understand and triage API security incidents, and a clear model for shared responsibility across functional groups.

Assess your current level of risk

Validate current API designs against API security best practices, checking whether authentication and authorization controls are in place throughout the sequence of API calls for a given business function, for example. Launch simulated attacks based on the OWASP API Security Top 10 list to understand the gaps in protection from WAFs and API gateways. Emulate the tactics of well-known API security incidents of 2022 to see whether similar business logic flaws exist in your APIs.

Enable frictionless API security across all your application environments

With APIs being the foundation of all application development today, you can't afford to leave some of your environments unprotected. You must be able to apply API discovery and runtime protection on prem and in the cloud and on legacy apps, as well as your container and Kubernetes deployments. How you connect the API security tooling into your environments is also crucial—avoid inline deployments, agents, or the need to instrument code to keep your API security platform from being blamed for any application impact.

Focus on robust runtime security

Even with the most rigorous development practices, achieving perfectly secure code is virtually impossible. This is where robust runtime protection becomes essential, offering immediate and continuous defense against malicious actors. Threat actors are constantly probing for vulnerabilities and gaps in API business logic. They often employ sophisticated tactics to evade detection, masking their malicious intent within seemingly legitimate API traffic. To combat this, advanced API security platforms must go beyond simple anomaly detection. They analyze vast amounts of data over extended periods, leveraging AI and ML to identify patterns indicative of malicious intent, such as reconnaissance activities, unauthorized access attempts, and data exfiltration efforts. By focusing on identifying malicious intent rather than just anomalies, these platforms can more effectively detect and thwart attacks before they cause significant damage. This level of sophisticated analysis requires cloud-scale big data and mature AI algorithms, capabilities beyond the reach of on-premises API security solutions and immature AI/ML implementations. By prioritizing robust runtime security, organizations can proactively defend against malicious actors and safeguard their APIs from exploitation.

Shifting Left with API Posture Governance for Comprehensive Security

Shift-left tactics are useful, but API security requires a more comprehensive approach. A strong API security strategy integrates posture governance throughout the entire Software Development Lifecycle (SDLC), from the initial design phase to runtime protection. Posture governance, with a powerful engine at its core, sets security standards early in the development process and consistently enforces them throughout the API lifecycle. This proactive approach not only reduces risk by identifying and addressing potential vulnerabilities early on, but also establishes a strong foundation for effective runtime protection. By ensuring that APIs are built with security in mind from the very beginning, organizations can significantly reduce the attack surface and simplify the process of implementing runtime protection measures.

About the Data

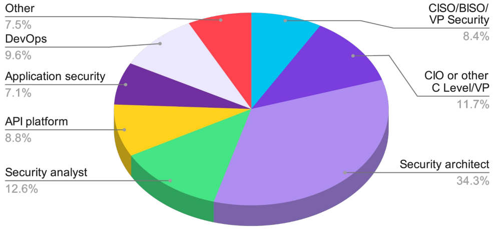
Insights from nearly 250 security professionals and API developers, plus analysis of real-world API attack attempts

These report findings combine live Salt customer data and the survey responses of around 250 respondents. The survey respondents were fairly evenly distributed across a broad range of job responsibilities, industries, and company sizes. 20% of respondents are executive-level security or IT leaders, and 18% sit within the platform or DevOps teams. Technology and financial services companies—widely viewed as at the forefront of API use—comprise 37% of respondents. Companies large and small were evenly represented.

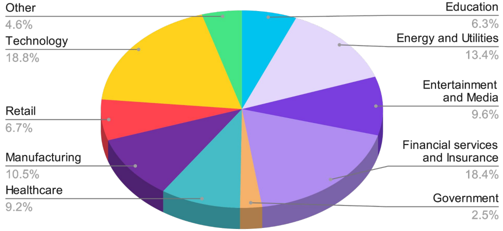
The report also includes real-world API attack attempt data from the Salt Security API Protection Platform. This empirical customer data is anonymized, aggregated, and then analyzed by Salt API security researchers to identify critical trends that can help educate the broader security industry.

Finally, the "in the wild" vulnerability research comes from our in-house research arm. Salt Labs, the industry's only dedicated API research team, undertakes projects to more deeply understand the evolution of API attacks to improve the Salt platform detection models and educate the companies involved and the industry as a whole.

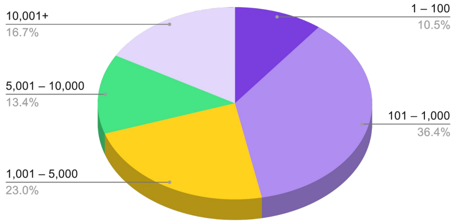
What area best represents your functional role?



Size of company (employee count)

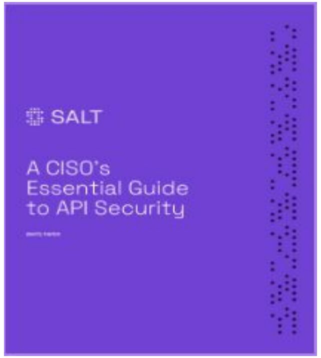


Industry



Additional Resources

These key assets will help you get even smarter about API security


SALT

A CISO's Essential Guide to API Security

[A CISO's Essential Guide to API Security](#)

Gartner

Innovation Insight for API Protection

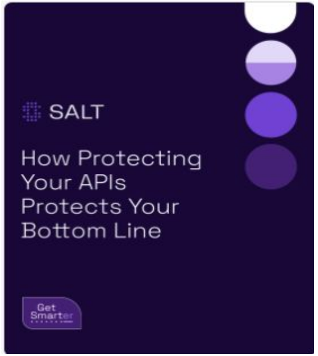
Overview

Key Findings

Recommendations

Strategic Planning Assumptions

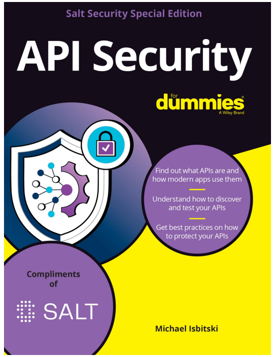
[Gartner® Innovation Insight for API Protection](#)


SALT

How Protecting Your APIs Protects Your Bottom Line

Get Smarter

[The Business Value of API Security](#)


Salt Security Special Edition

API Security

for dummies

A Wiley Brand

Find out what APIs are and how modern apps use them

Understand how to discover and test your APIs

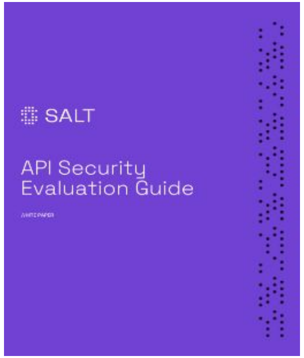
Get best practices on how to protect your APIs

Compliments of

SALT

Michael Isbitski

[API Security for Dummies](#)


SALT

API Security Evaluation Guide

WHITE PAPER

[API Security Evaluation Guide](#)

About Salt Security

Salt protects the APIs that form the core of every modern application

The Salt Security API Protection Platform secures your APIs across the full API lifecycle. The Salt platform collects a copy of API traffic across your entire application landscape and uses big data, machine learning (ML), and artificial intelligence (AI) to discover all your APIs and their exposed data, stop attacks, and eliminate vulnerabilities at their source. The Salt platform:

Discovers all APIs and exposed data – Automatically inventory all your APIs, including shadow and zombie APIs, and highlight all instances where your APIs expose sensitive data. Continuous discovery ensures your APIs stay protected even as your environment evolves and changes with agile DevOps practices.

Stops API attackers – Pinpoint and stop threats to your APIs by identifying attackers early, during their reconnaissance phase, and prevent them from advancing. The Salt platform correlates activities back to a single entity, sends a consolidated alert to avoid alert fatigue, and blocks the attacker rather than transactions.

Improves your API security posture – Salt proactively identifies vulnerabilities in your APIs even before they serve production traffic. The platform also uses attackers like pen testers, capturing their minor successes to provide insights for dev teams while stopping attackers before they reach their objective.

About Salt Labs

Salt Labs identifies API threats and vulnerabilities in customer deployments and in the wild. Our in-depth API threat research reports document the steps of an exploit, including the processes and tooling, to reveal an attacker’s approach, the details of an exploit, the risk to the business, and the steps an organization can follow to avoid falling victim to a similar attack. We also apply our research findings to improve the ML and AI algorithms at the heart of our API security platform, so that all our customers benefit from our ongoing research. Our industry reports, such as this State of API Security Report, tap empirical and survey data to educate the market on API security trends.