SALT SECURITY

State of API Security

Q3 2022

Report by SALT LABS

State of API Security

Q3 2022

Executive Summary

The State of API Security Report from Salt Labs is the industry's only report on API security risks, challenges, and strategies. The fourth edition of this pioneering research offers security, DevOps, and risk management teams a deeper perspective into the dozens of factors that impact API security. It also provides insights on building strategies to reduce the growing API attack surface.

As with previous editions, the Q3 2022 report incorporates survey results and empirical data from the Salt SaaS platform hosting our customers' API metadata. The most eye-opening finding from the report comes from our customers. **Over the past year, Salt customers experienced a 117% increase in API attack traffic while their overall API traffic grew 168%.**

Unfortunately, attackers have also been busy. A review of our customer data found that **malicious traffic now accounts for 2.1% of all API traffic**. In fact, 34% of Salt customers have experienced 100+ attempted attacks per month, up from 30% a year ago. This attack activity is causing real business concerns, with **94% of survey respondents saying that they have experienced security problems in production APIs**. Most troubling, nearly **20% of respondents say their organizations have experienced a breach resulting from insecure APIs**.

Reliance on APIs is at an all-time high, with 60% of survey respondents managing 100+ APIs. The top drivers of this heavy API usage include development efficiency, platform/systems integrations, and digital transformation. However, with key strategic initiatives so closely tied to API usage, there is no room for deployment delays or rollbacks. Unfortunately, **over half of survey respondents say they have had to delay rolling out a new application because of API security concerns**.

In addition to growing attack volume, respondents are challenged by the increasing complexity of their own APIs. The pace of API change has skyrocketed, with **42% updating their APIs at least weekly**, and 11% updating them daily. In addition, 97% of respondents rely on multiple API protocols, which only increases the complexity of their API landscape.

Security and development teams are concerned about this convergence of API criticality and attack growth. When asked about their overall API program concerns, **38% of respondents ranked security as their top consideration**. However, **61% admit to lacking any API security strategy or to having only a basic one**. One of the best ways to start building a comprehensive API security program is by initiating controls to address the OWASP API Security Top 10 list. Interestingly, 62% of all attacks seen by Salt Labs over the past six months leveraged one or more of these vulnerabilities. Curiously, 45% of survey respondents admit this guide is not a focus area, which may help explain why so many have experienced API security concerns over the past year.

Respondents are also clear about the value they place on the various components of the API security landscape. **The ability to stop attacks was rated the most critical attribute by most respondents (41%), compared to only 22% who rated shift-left capabilities a top need**. Despite the higher value on runtime protection, the industry push towards "shift left" security has clearly influenced API security practices, with 53% attempting to identify and remediate API security gaps during development and 59% during testing. These steps are important, but with 94% of respondents citing recent API security incidents, shift-left tactics alone aren't adequately protecting them. Only 31% of respondents are addressing security gaps during runtime/production, which is troubling as most successful API attacks target gaps in logic flows that cannot be identified during pre-production testing.

Survey results also make it evident that traditional application security and API management tools simply aren't providing sufficient API protection – only **18% of respondents believe their existing tools are "very effective" in preventing API attacks**. Added to the fact that most rely on manual processes to document APIs and 86% lack confidence that this documentation is complete, security professionals are at a crossroads.

APIs are at the core of every modern application, and attackers continue their efforts at unprecedented rates. Survey responses and Salt customer data overwhelmingly demonstrate that **the time is now** for organizations to get serious about securing their APIs.

Research Methodology

To understand the state of API security today, Salt Labs – the API threat research arm of Salt Security – initiated and compiled this API security industry report. Our in-depth research combines survey responses and empirical data from Salt Security customers. The findings reflect the input of more than 350 security, DevOps, and app development professionals across companies big and small, in a variety of industries across the globe (page 17). Salt Labs also pulls aggregated and anonymized data from the SaaS component of the Salt Security API Protection Platform – this empirical data gives more context to the survey response findings.

Contents

Malicious traffic accounts for 2.1% of overall API traffic

API attack traffic has doubled in the past year

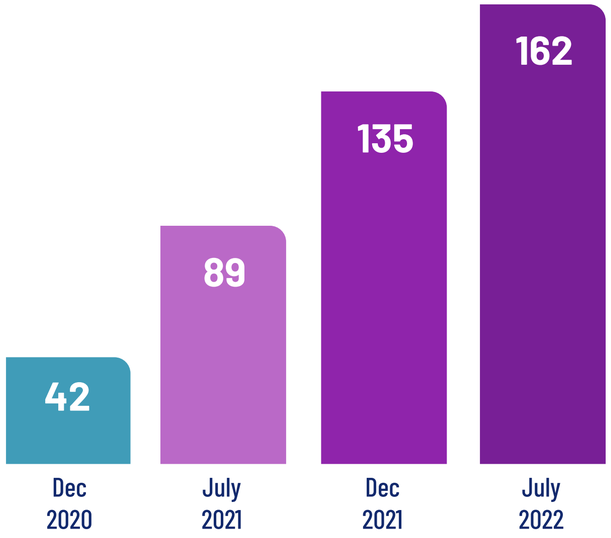
Organizations are embracing APIs to solve critical business problems and drive innovation at unprecedented levels, and Salt Security customers are at the forefront of this trend. Salt customer data shows the **average number of APIs per customer grew 82% over last year, up from 89 in July 2021 to over 162 in July 2022**. During the same period, **overall API traffic per customer grew 168%**, indicating that API usage is also exploding.

Attack activity continues to keep pace with this dramatic API usage growth and now accounts for 2.1% of overall API traffic for Salt customers. **Malicious API attack traffic surged 117%** over the past year, from an average of 12.22M malicious calls per month to an average of 26.46M calls.

We take some solace in noting that the rate of malicious traffic is lower than it has been for the past year, but it's still substantially higher than the 1.4% of traffic we found 18 months ago.

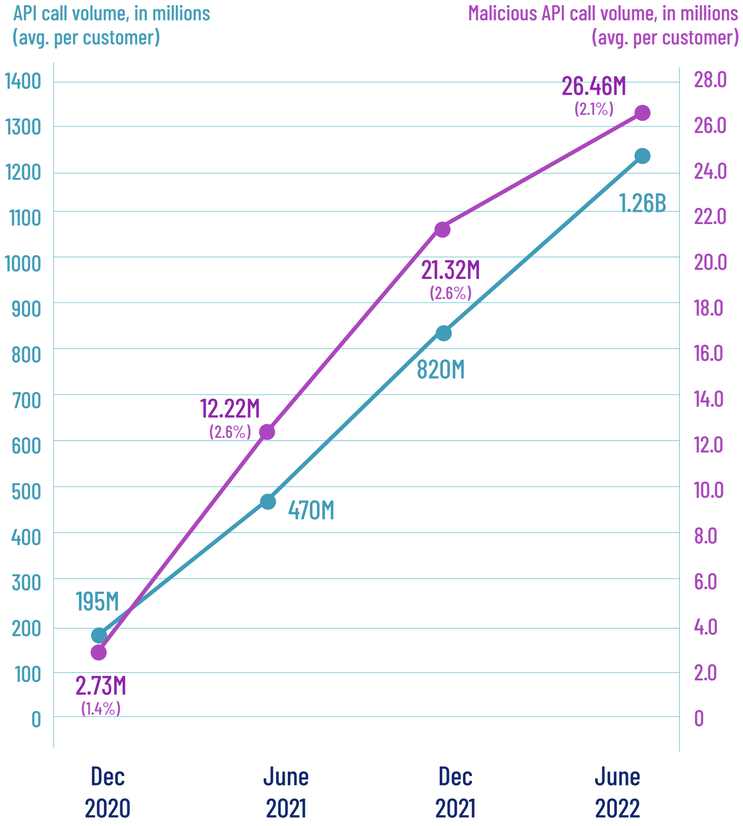
Salt customer data

Growth in average number of APIs per customer



Salt customer data

Growth in API call volume vs. malicious traffic



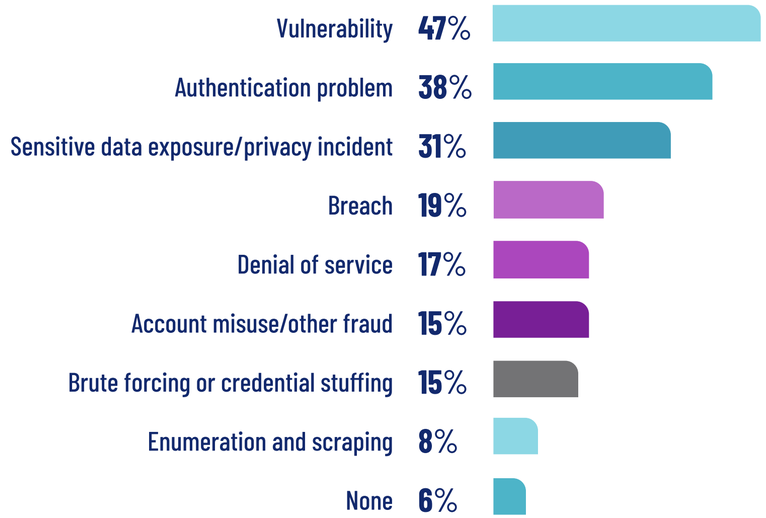
API attacks are on the rise and causing significant security concerns

94% of respondents have experienced security problems in production APIs

Not surprisingly, increased API usage and traffic have resulted in security concerns. Salt customer data reveals that **34% of customer accounts have experienced more than 100 attempted attacks per month**.

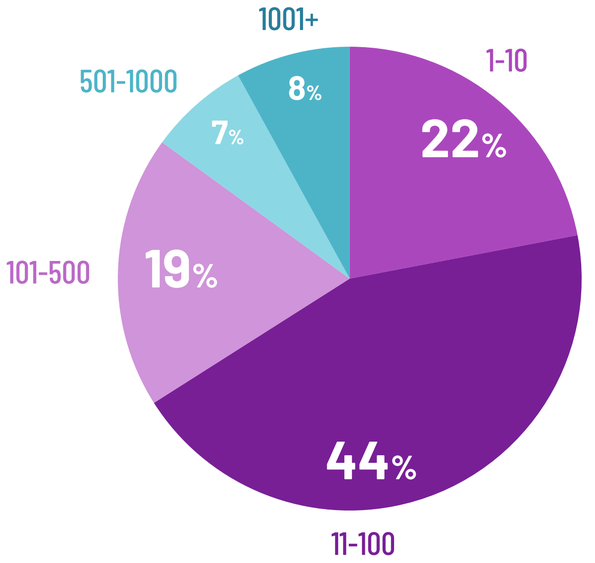
A resounding **94% of survey respondents reported they have experienced API security problems in production APIs**. Nearly half (47%) indicate that they have identified vulnerabilities in production APIs, 38% have experienced authentication problems, and 31% have seen sensitive data exposure and privacy incidents. Vulnerabilities in production have markedly increased by 8% over the past six months. And most frightening, **nearly 20% of respondents say their organizations have experienced a breach resulting from insecure APIs**.

In the past 12 months, what security problems have you found in production APIs? (*Select all that apply*)



Salt customer data

Average number of attacks per month per customer



The stakes are high, with application rollout delays and sensitive data exposures

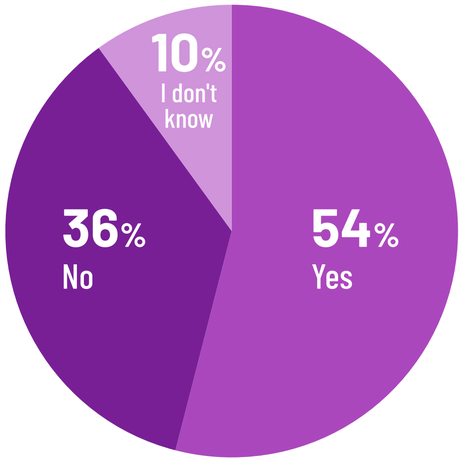
More than half of respondents have delayed rolling out a new application due to API security concerns

Companies rely on their APIs to build the applications that drive innovation and produce revenue, so there is no room for deployment delays. Unfortunately, **54% of respondents indicate that they have had to slow the rollout of a new application because of an API security concern**.

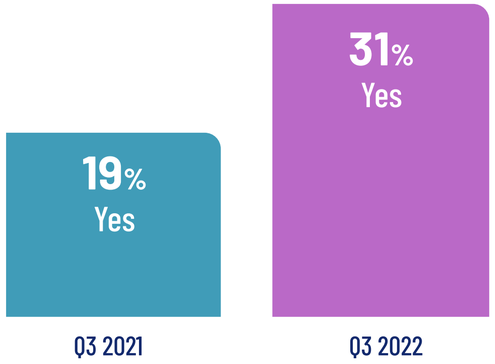
Furthermore, the increasing regulatory focus on sensitive data leaks is impacting profitability, and the public is taking notice. Poor API design and security practices are often at the root of sensitive PII data leaks, and this quarter's survey responses showcase this fact. **Nearly a third of respondents admit they have experienced sensitive data exposure or a privacy incident within their production APIs over the past year**, a sharp increase over last year's 19%.

Within Salt customers, **91% of APIs expose some PII or sensitive data**, so it's imperative to know where and how that sensitive data is transmitted and to protect those APIs with extra diligence.

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

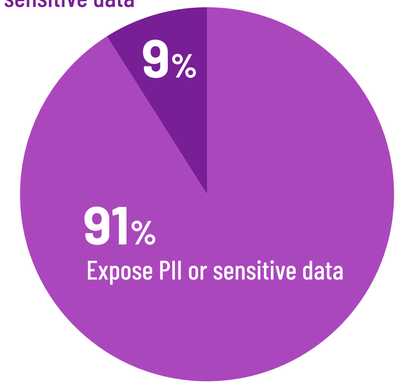


Have you found a sensitive data exposure or privacy incident in your production APIs?



Salt customer data

Percentage of APIs that expose PII or sensitive data



Security-related concerns top the list of API challenges

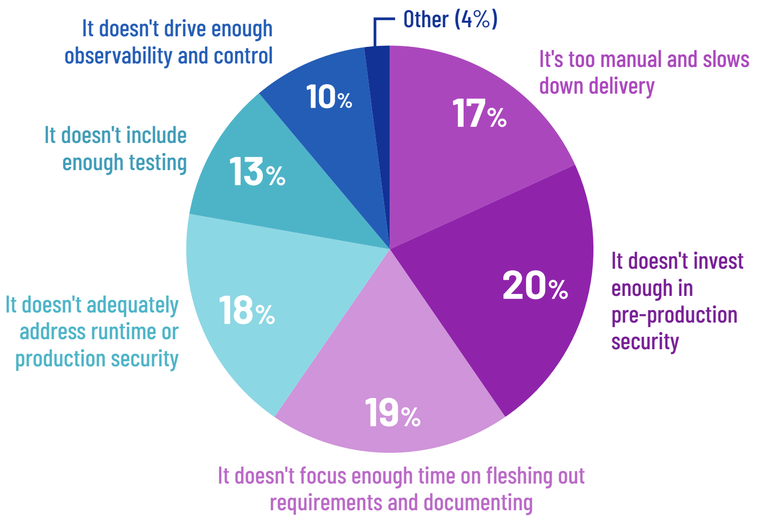
Out-of-date or "zombie" APIs create the greatest worries

As organizations continue to mature their API programs, it's no surprise that security-related considerations top their list of concerns. **Not investing enough in pre-production security (20%) and not adequately addressing runtime security (18%) were the top API concerns noted by respondents**. Also high on the list is a lack of focus on requirements and documentation (19%), which is paramount for those tasked with maintaining secure APIs.

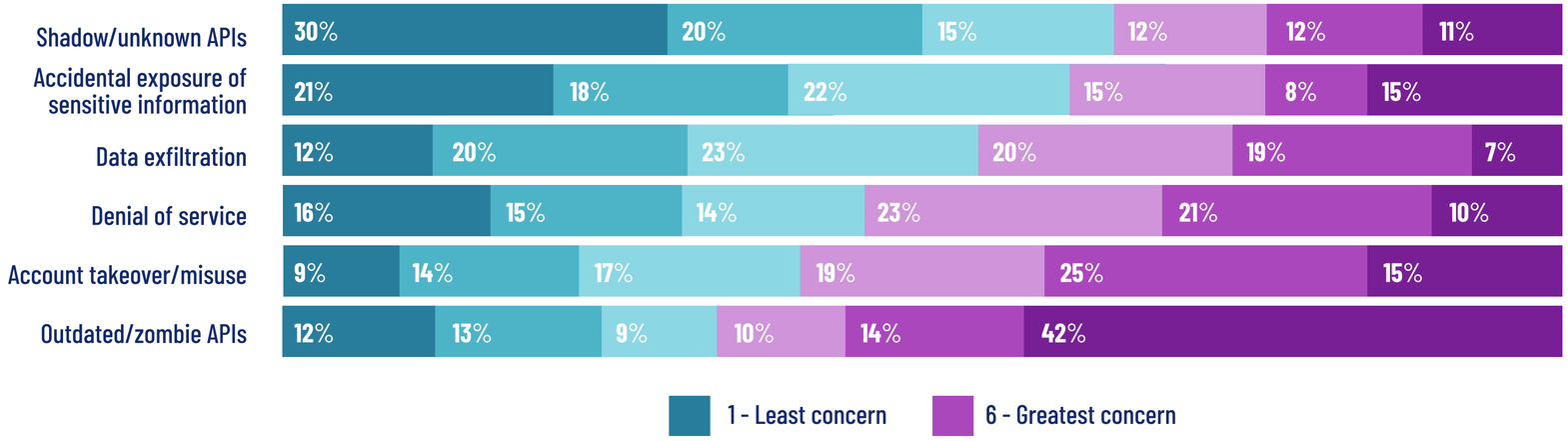
When asked about the most concerning API security risks, **42% of respondents said that their biggest worry is outdated or "zombie" APIs**. Zombie APIs have been consistently rated the #1 concern for the past four surveys, likely a direct result of the increasingly fast pace of development as companies seek to maximize the business value associated with APIs. As organizations build new APIs, they often fail to deprecate previous versions, leaving them vulnerable since nobody is patching or documenting these out-of-date APIs.

Account takeover and accidental exposure of sensitive information tied for the second-highest concern at 15%. Also interesting is an increasing level of **concern about "shadow" or unknown APIs, which rose from 5% rating it a top concern to 11% only six months later**. This news is welcome, showing that organizations are becoming more aware of the potential risk associated with these unknown and unsecured APIs.

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



Please rank the following risks, with 1 being your least concern and 6 your greatest concern, related to API security



Stopping attacks is the most highly valued API security attribute; shift left is lowest

The ability to stop attacks was rated the most critical attribute by the most respondents (41%), compared to only 22% who rated shift-left capabilities a top need

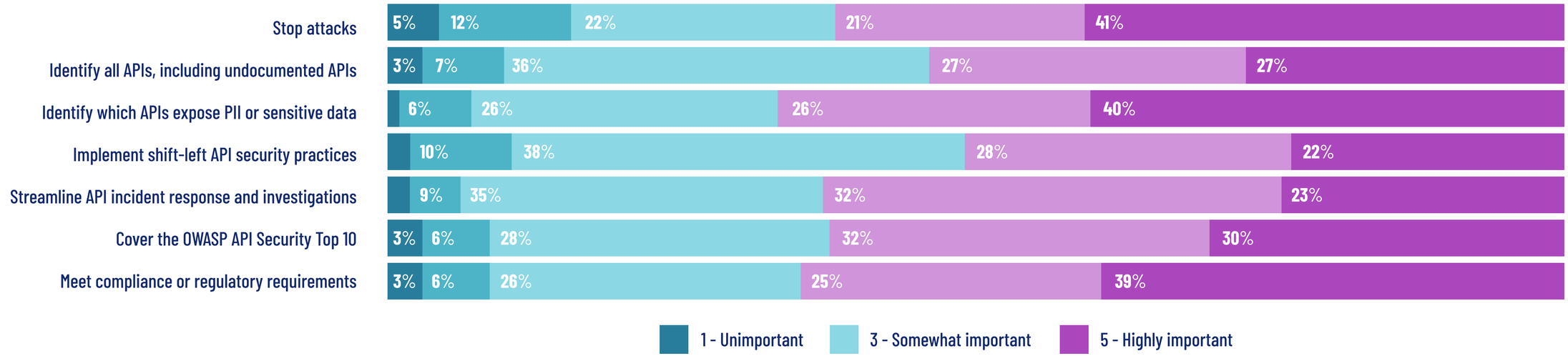
API security offers organizations a variety of capabilities and use cases, spanning discovery, attack prevention, incident response, and compliance. When asked to rate each attribute from unimportant to highly important, **the ability to "stop attacks" took the top spot of highly important capabilities**, with 41% giving it that most valued rating. It should come as no surprise that 30% of respondents also cited the ability to defend against the OWASP API Security Top 10 as highly important as well.

The ability to identify which APIs are exposing PII or sensitive data was second highest, with 40% of respondents ranking that capability as "highly important." These two areas – runtime protection and exposed sensitive data – represent the greatest sources of immediate risk for organizations.

Meeting compliance or regulatory requirements came in third on the list of "highly important" platform capabilities, with 39% rating it so. As with runtime protection and sensitive data, security audits present a "here and now" challenge for organizations who have to answer to auditors increasingly well informed on the risks that APIs present.

Coming in at the bottom of the list of most valued capabilities is shift-left capabilities, with only 22% citing it a "highly important" capability. It stands to reason that the delayed effect of shift-left practices, which protect only new assets yet to be released vs. those already running in production, would impact its perceived value. In addition, survey respondents may also recognize the lower overall value proactive security can provide, given the need for active API traffic to spot the business logic gaps that dominate today's API attacks.

On a scale of 1-5, how would you rate the value of each of these attributes of an API security platform? (*1 is unimportant and 5 is highly important*)



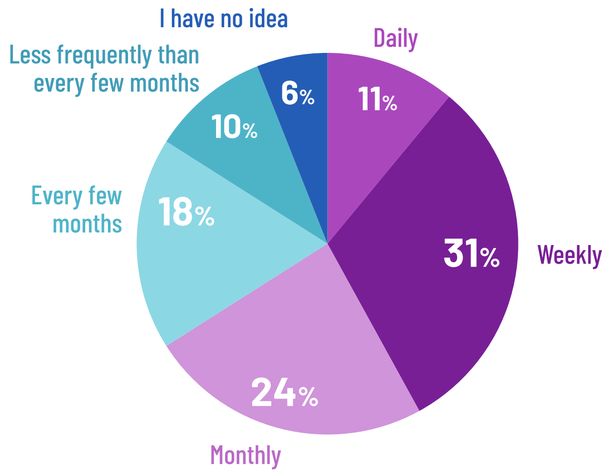
It's increasingly difficult to keep up with changing APIs

42% are updating their APIs at least weekly, and the majority are relying on multiple API protocols

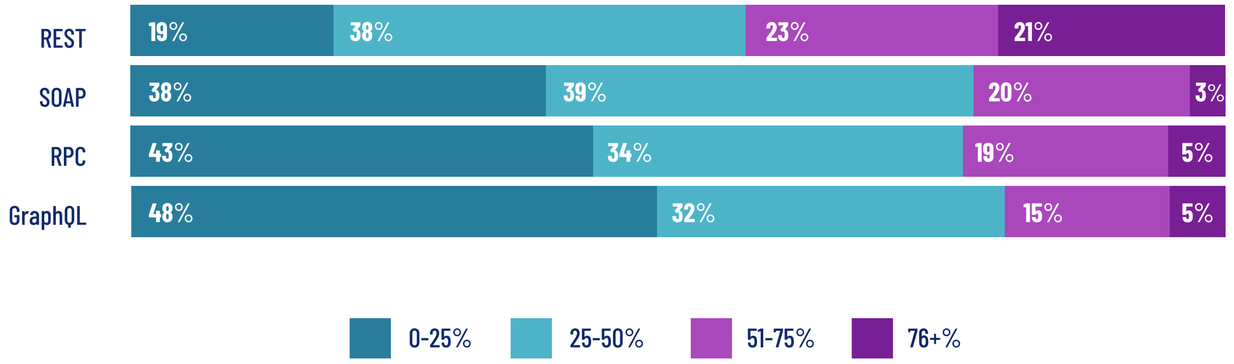
Beyond just a growing quantity, securing and maintaining APIs is further complicated by the fast pace of updates. One year ago, only 6% of survey respondents indicated that they update their APIs daily. Today, that number has increased to 11%. An additional **31% update their APIs weekly, while only 10% update them less frequently than every few months**.

Adding further complexity is the reliance on multiple API protocols as developers leverage the architecture that works best for each unique project. Nearly all respondents **(97%) utilize REST, 87% use SOAP, 82% use GraphQL, and 79% use RPC protocols**. The percentage of respondents who utilize GraphQL has remained relatively flat over the past several surveys, but what has changed is that 20% are now leveraging this architecture for more than half of their APIs. Therefore, it's more important than ever to discover and protect APIs of all protocol types – GraphQL poses particular challenges for security, given its nested query structure.

On average, how often do your primary APIs get updated?



How many of your APIs (in percentages) use which of the following protocols?



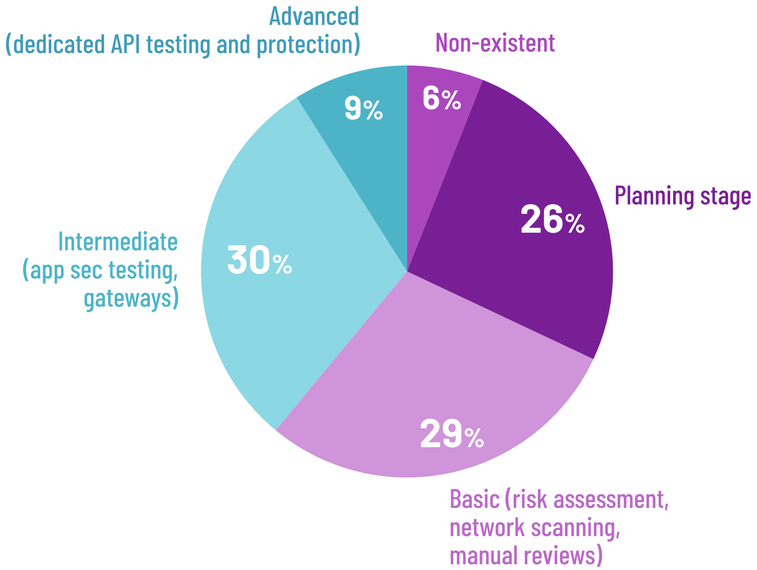
Multiple (solvable) obstacles are preventing strong API security strategies

61% of respondents admit they lack any or have only a basic API security strategy

With reliance on APIs at an all-time high and critical business outcomes relying upon them, it is even more imperative that organizations build and implement a strong API security strategy. Unfortunately, **only 9% of respondents can confidently state that they have an advanced API security strategy** that includes dedicated API testing and protection. **61% admit that they lack any API security strategy or have only basic protections** (risk assessment, network scanning, manual reviews).

The top reasons cited for the lack of a robust API security strategy include budget (24%), expertise (20%), resources (19%), and time (11%). With the current economic climate and budget cuts, it's not surprising that budget constraints rose from 20% to 24% over the past six months. Fortunately, these problems are surmountable: an existing security budget can be re-allocated to tackle API security with the right business justification. And a lack of expertise, people, and time can be remedied with the right API security tools, processes, and partners.

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?

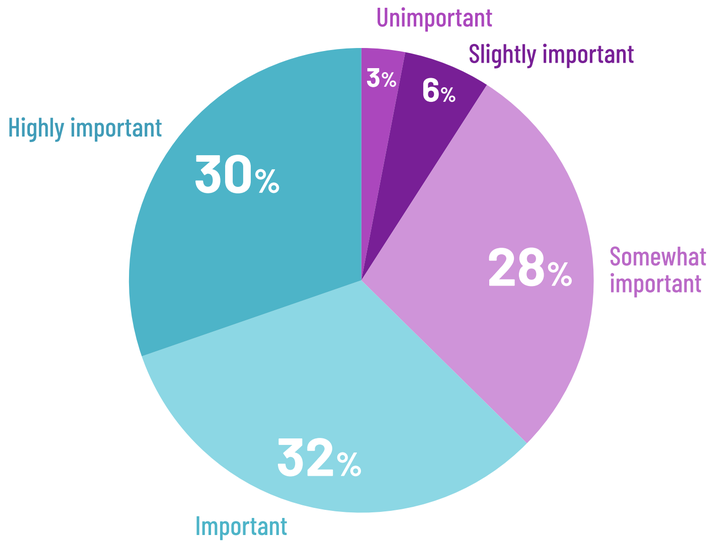
A critical - and obvious - first step in API security knowledge remains overlooked

The security teams at nearly half of organizations are not making the OWASP API Security Top 10 list a focus area

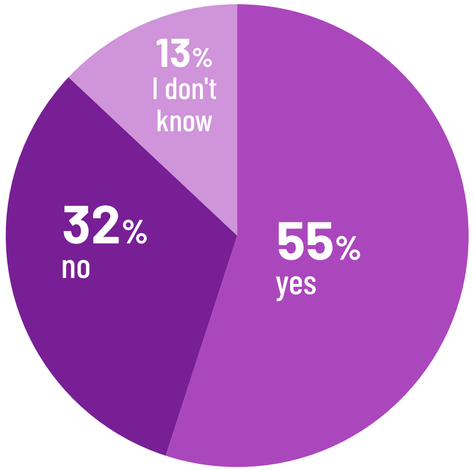
A shrinking number of respondents say they include the OWASP API Security Top 10 list as a focus area within their API security programs. A total of **62% of respondents consider "Defending against the OWASP API Security Top 10" to be highly important (30%) or important (32%)**. Unfortunately, **only 55% say their security team is actually highlighting the OWASP API Security Top 10 in their security program, down from 61%**.

This lack of focus is particularly troubling for the industry because the OWASP API Security Top 10 is a critical first step in security APIs. In fact, Salt customer data shows that **62% of all attack attempts leverage at least one of these ten security vulnerabilities**, and they are often leveraged in a layered approach to propagate more sophisticated attacks. With such a large percentage of attacks taking advantage of these most common and well-documented security flaws, organizations cannot afford to overlook this fundamental principle in API security.

Do you consider "Defending against the OWASP API Security Top 10" to be an important attribute of an API security platform?

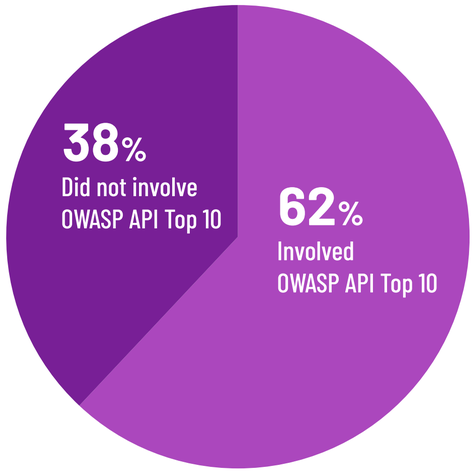


Has your security team highlighted the OWASP API Security Top 10 threats as a focus area for your security program?



Salt customer data

Attack attempts leveraging OWASP API Security Top 10 list



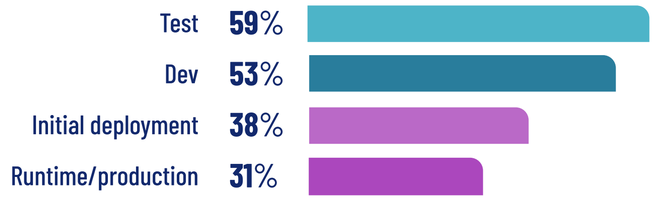
Organizations are continuing to "shift left," but it's failing to protect them

Respondents focus on fixing API security gaps during dev (53%) and test (59%), yet 94% still suffered API security incidents

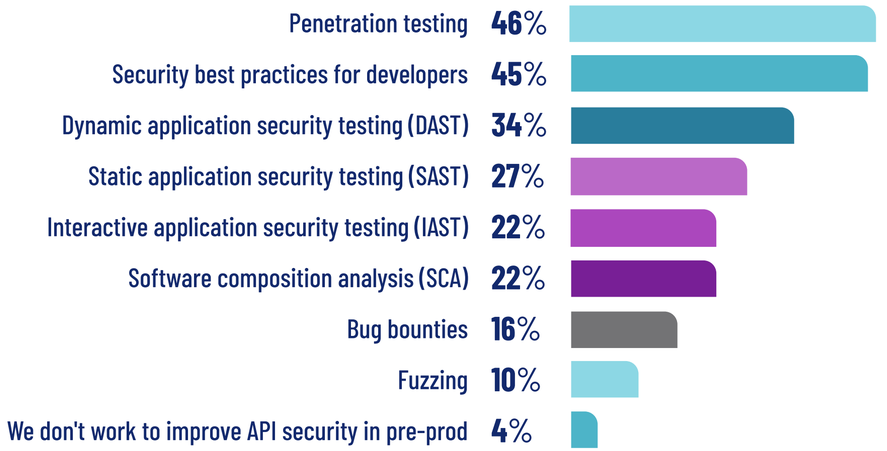
"Shift Left" security has been the topic of many industry conversations over the past year, and survey responses indicate that organizations are listening. **53% of respondents say they identify and remediate API security gaps during development, and 59% look for API issues in testing**. Tactics include penetration testing (46%) and leveraging security best practices for developers (45%). These steps are important, but with 94% of respondents admitting to API security incidents (page 4), shift-left tactics alone are not enough.

A troubling result of this survey is that **only 30% of respondents say they are identifying and remediating API security gaps in runtime**. Such a low number may help explain the high rate of API security incidents. Most successful attacks on APIs target gaps in logic flow, and API testing and scanning in pre-production can never uncover those gaps – finding them requires running traffic. Every organization wants to find security problems before code is released to production, but that tactic has fundamental limitations. Runtime security is the missing piece to achieving robust API security for many organizations.

At what point(s) in the development life cycle does your company identify and remediate API security gaps? *(Select all that apply)*



What tools/approaches do you use in pre-production to improve API security? *(Select all that apply)*



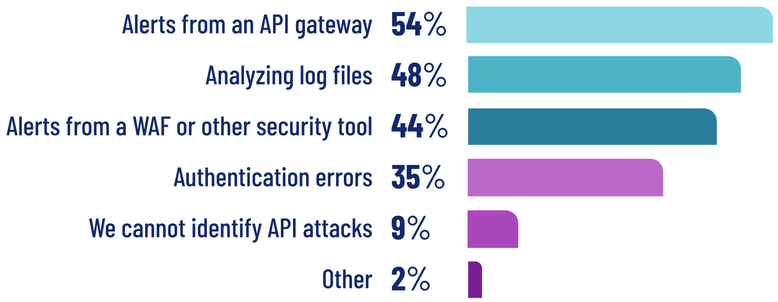
Traditional tools and processes are falling short in API protection

Most respondents rely on API gateways (54%) and WAFs (44%) to identify API attacks, yet 82% don't believe that their existing tools are very effective

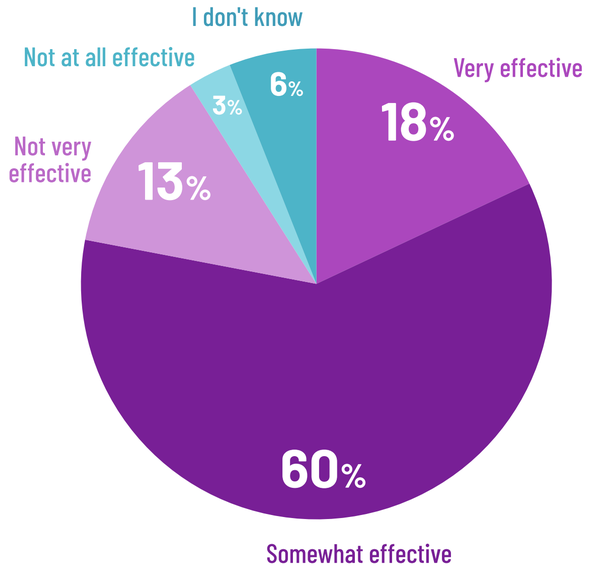
As in previous surveys, this quarter's respondents indicated that they primarily rely on traditional tools to manage APIs and protect against application attacks. However, it is interesting that they don't believe these methods are particularly effective, with **82% of respondents saying their existing tools aren't very effective in preventing API attacks. As a result, 73% admit that they lack confidence in their ability to respond to an API attack**.

Analyzing log files (48% of respondents) to identify API attacks is tedious, reactive, and highly ineffective – attackers will be long gone with valuable data by the time a security analyst can parse log files. WAF alerts (44% of respondents) are known to be ineffective, since WAFs use proxy architectures to apply signatures that detect only well-known attacks such as cross-site scripting (XSS), SQL injection (SQLi), and JSON injection. WAFs can't stitch together the data needed to spot today's API attacks. API gateways (54% of respondents) also employ traditional protections such as authentication, authorization, encryption, and rate-limiting. While these tools provide some coarse application protection, they cannot spot much less defend against the threats in the OWASP API Security Top 10.

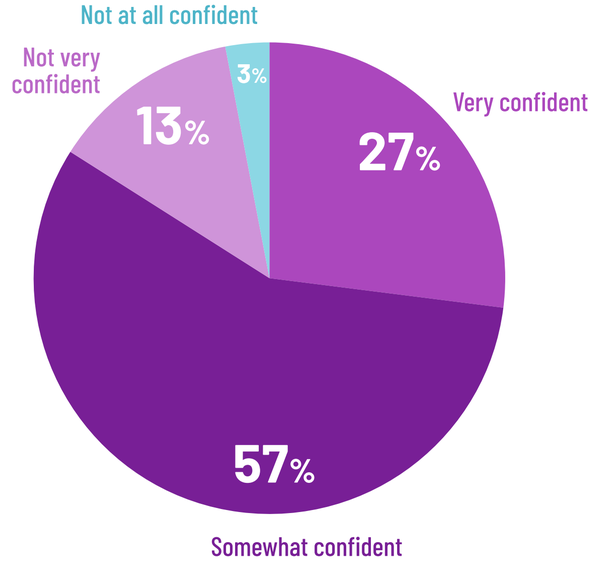
How do you identify an attack or attacker targeting your APIs? *(Select all that apply)*



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



How confident are you in your team's ability to effectively respond to an API attack?



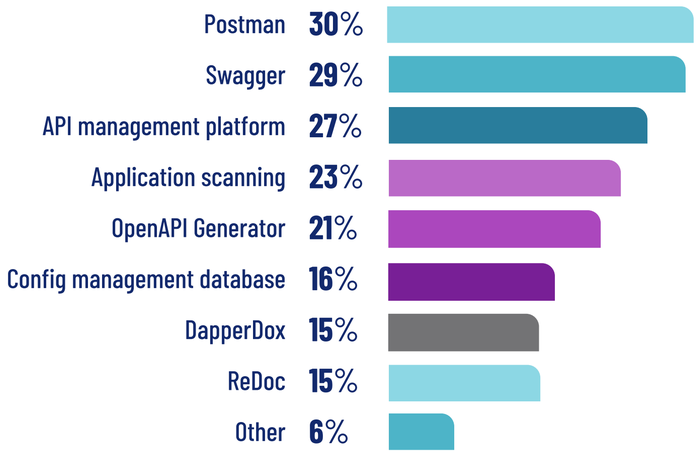
Most continue to rely on manual processes to document APIs

86% lack confidence that their API inventory is complete, and 14% admit they are entirely unaware about which APIs expose PII data

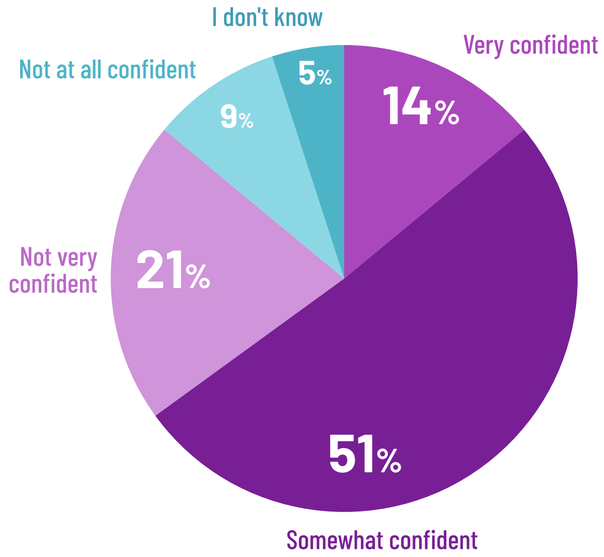
As the old security adage goes, you can't protect what you can't see (or have no idea even exists). This truism particularly holds for APIs because of the frequent pace of creation and change. Most respondents state they are relying on manual mechanisms to document their APIs, including Postman (30%), Open API Specification / Swagger (29%), and OpenAPI Generator (21%). Many are also using API management platforms (27%) and application scanning (23%). However, these tools and processes are falling short, since **86% lack confidence that their API inventory is complete. Only 14% have a high degree of confidence that they have all the information they need to understand their API resources**.

Even more alarming is that PII and other sensitive data are at risk. More than half (52%) of respondents rely only on documentation provided by developers to understand the potential PII exposure within their APIs, while 14% concede they have no idea which APIs contain sensitive data. It stands to reason that only **14% of respondents are highly confident that their API inventory provides enough detail about their APIs, including exposure of sensitive data or PII**.

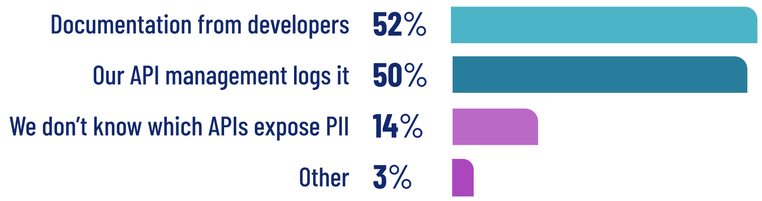
What mechanism(s) do you use to document and inventory your APIs? *(Select all that apply)*



How confident are you that your API inventory is complete?



How do you know which APIs expose sensitive data or PII? *(Select all that apply)*



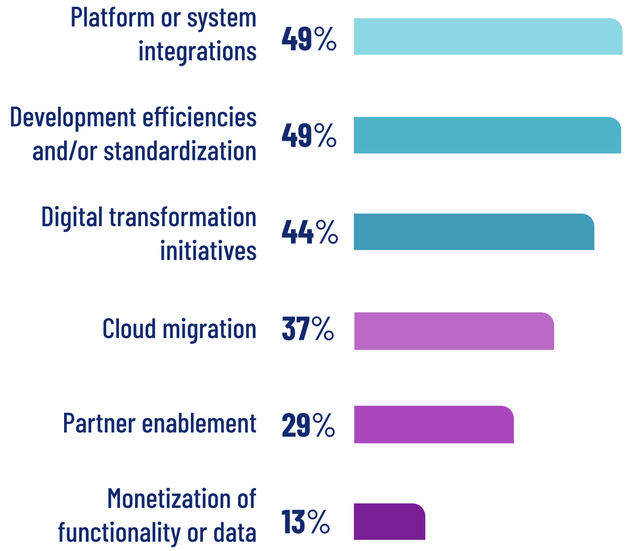
API usage grows as companies use them to drive efficiency and innovation

60% of respondents are managing 100+ APIs, and 50% are sending more than 10 million requests to their APIs each month

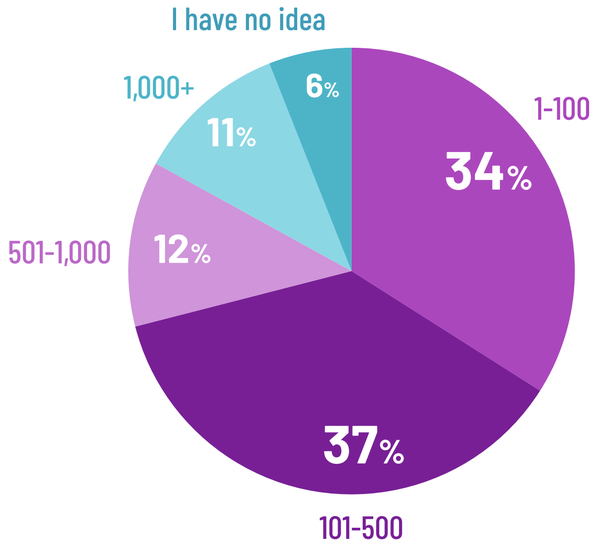
API usage continues to be pervasive and critical for organizational success. Almost two-thirds **(60%) of survey respondents develop, deliver, and/or integrate more than 100 APIs, and 11% manage in excess of 1000 APIs**. These APIs are seeing heavy traffic, with **50% of organizations surveyed sending 10+ million API requests per month and 26% sending 100+ million requests**.

What is driving this API adoption? Development efficiencies and platform/systems integrations tie for the top driver at 49%. But digital transformation initiatives are a close third with 44%, up 7% over the past six months. Cloud migration comes in a strong fourth, with 37% of respondents citing this driver as primary in their API usage. These strategic priorities are imperative to cost containment and revenue growth, so it's critical to embrace an API strategy that is scalable and secure.

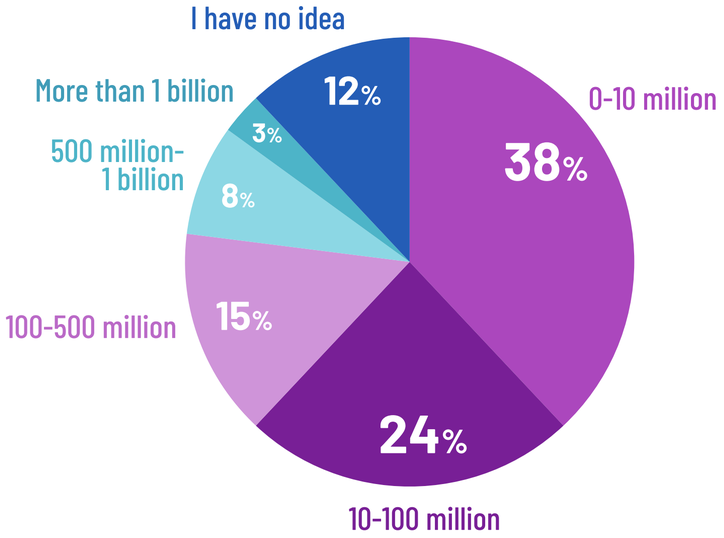
What are the main drivers behind the use of APIs in your organization? (*Select all that apply*)



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



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



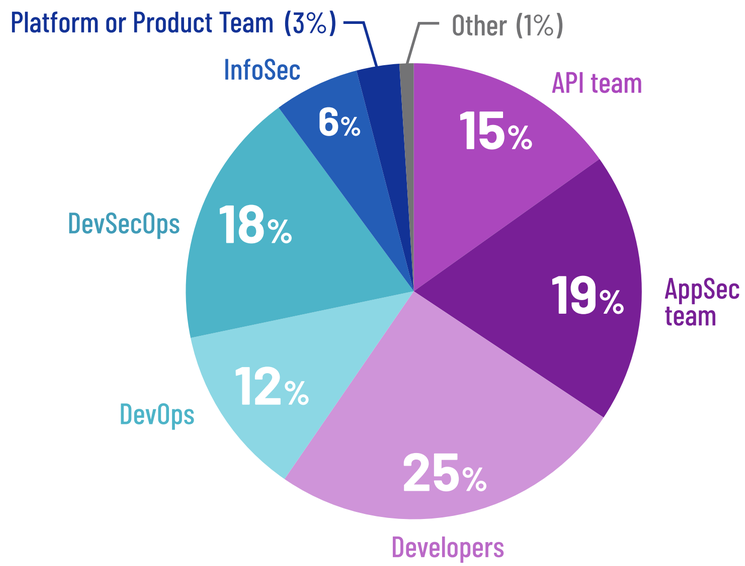
API security continues to change the game (for the better)

64% say that API security has helped security collaborate and even embed with DevOps teams

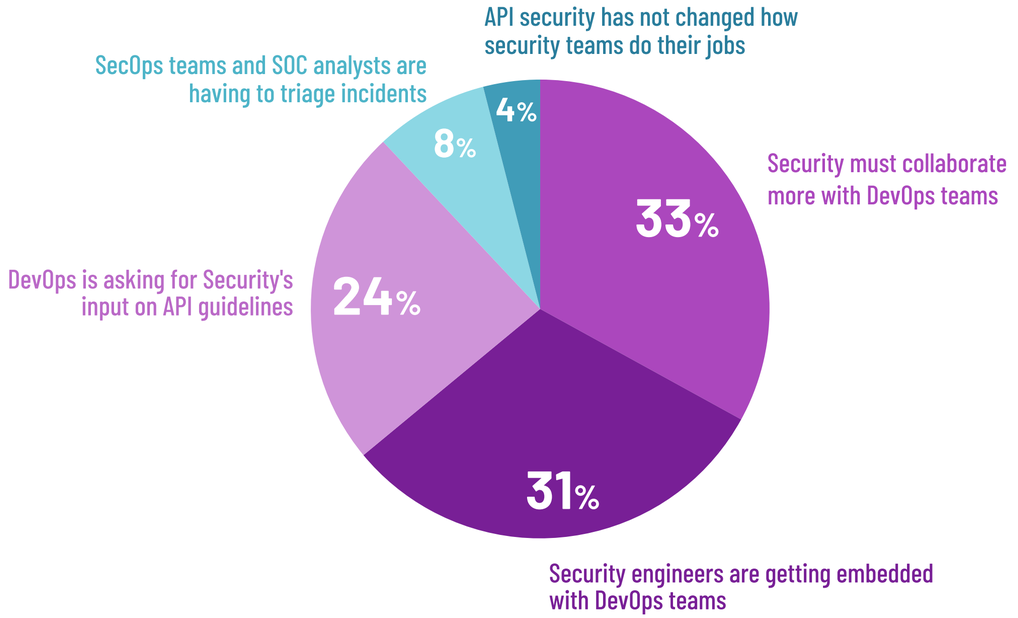
As API attacks continue to dominate the news, organizations are beginning to look closely at their development and security practices to ensure they can address this formidable challenge. Fortunately, API security is driving a positive shift in how security and DevOps teams collaborate. It is increasingly clear that all parties who touch APIs must work together to ensure they can both deliver the innovation companies need while keeping risks at bay. **Survey responses indicate confusion about who is ultimately responsible for securing APIs: 37% say developers and DevOps are responsible, 25% say AppSec and InfoSec, 18% say DevSecOps, and 15% say their dedicated API team**.

But change and clarity are increasing as teams seek to address the challenge. Development, operations, and security teams are collaborating to tackle the challenge of API security at a pace greater than seen in prior surveys. In fact, respondents say that **API security has compelled security and DevOps teams to collaborate more (33%) and even embed security engineers within DevOps teams (31%)**. Only 4% state that traditional roles and silos remain unchanged as teams tackle API security. The move towards bringing Dev and Sec closer together is promising for both API security and the cybersecurity industry as a whole.

Who is primarily responsible for securing APIs?



How do you feel API security is creating changes in how security professionals do their jobs?



Implications for API security

The results from the Q3 2022 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 protocols and attack trends. API traffic and customer usage trends from the customer base further confirm these 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 across teams. Here are some tips to consider as you build a more robust and manageable API security program:

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 attacks based on the OWASP API Security Top 10 list and see whether your WAF or API gateway can detect them. Emulate the tactics of well-known API security incidents of 2021 and 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 applications running 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.

Tap the power of cloud-scale big data, AI, and ML to pinpoint the subtle probing of API attackers

Since every API is unique, bad actors must perform extensive reconnaissance to understand how each API works and identify vulnerabilities or gaps in business logic they can exploit. Attackers know how to probe your systems with subtlety, to avoid tripping coarse security protections such as rate limiting on WAFs. To see these nefarious but quiet activities, an API security platform must be able to capture millions of data points over a long period of time, since API attacks can take weeks and months to unfold. Then, the platform must tap AI and ML to process all that data in near real time, so they can discern the recon activities of a bad actor and correlate them into a single attacker profile to avoid alerting on each bad action. Such robust analysis requires cloud-scale big data and mature AI algorithms – it cannot be achieved using VM-based collection and AI and ML of limited experience.

Don't over-rotate on shift-left tactics

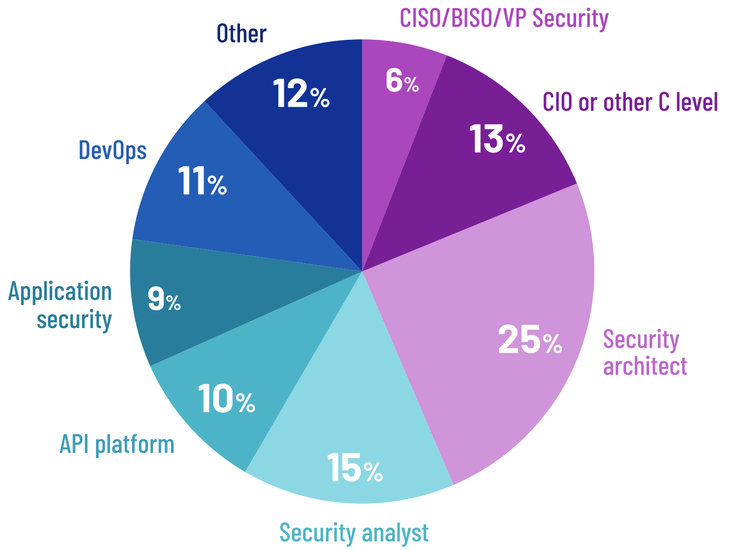
Shift-left and secure build pipeline approaches have their merits. But many API security gaps can't be detected as part of code review – they can be detected only in runtime. Look for an API security platform that complements pipeline testing and analysis with robust runtime protection. Shift-left tactics take much longer to deliver value and ultimately offer limited value as they identify only a fraction of API security risk and leave your security teams dependent on developers to work through a backlog of vulnerability fixes. Get your APIs protected today with runtime security – then you can make hardening APIs over time a realistic goal.

Get a Salt Security demo »

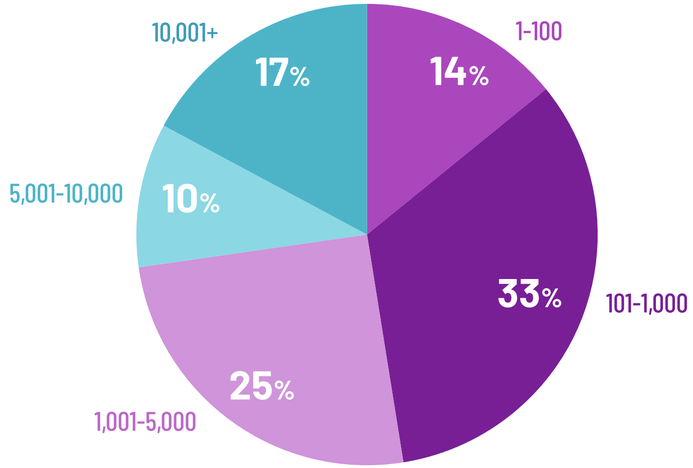
Demographics

These report findings are a combination of live Salt customer data and the survey responses of more than 350 respondents. The survey respondents are well distributed across a range of job responsibilities, industries, and company sizes. Nearly half (49%) hold roles in security, 19% are executive-level security or IT leaders, and another 21% sit within platform, DevOps, or product teams. Technology and financial services companies – widely viewed as at the forefront of API use – make up 47% of respondents. Companies large and small are evenly represented.

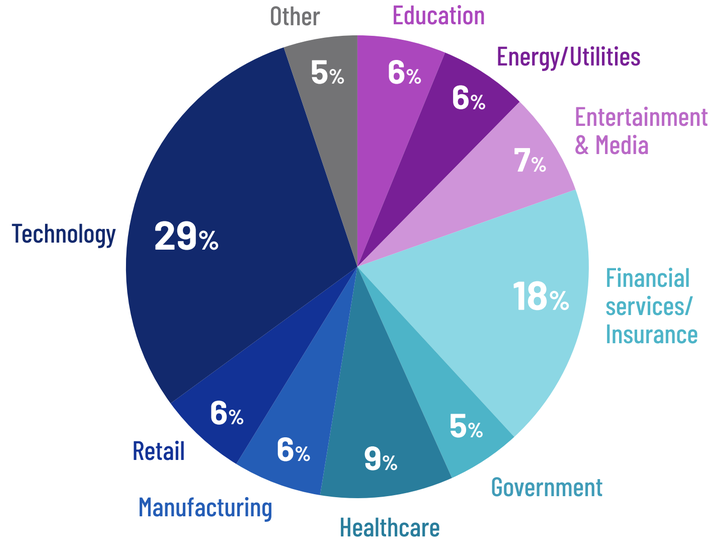
What area best represents your functional role?



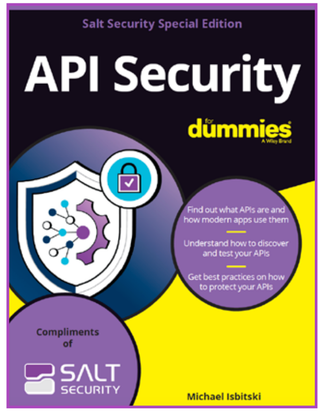
Size of company (employee count)



Industry

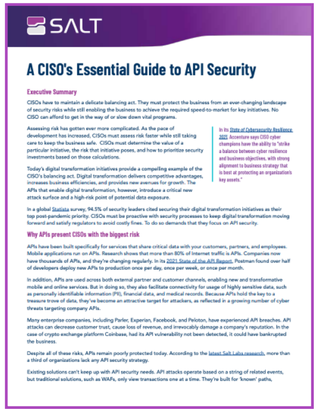


Resources to help you get started securing your APIs



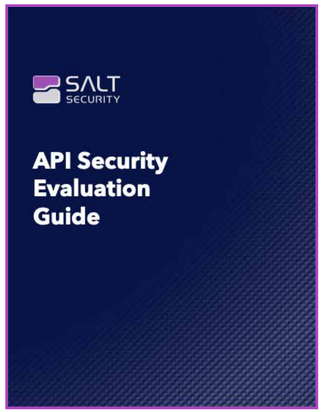
[Salt Security Special Edition API Security for Dummies eBook »]

[The Top Five Myths in API Security »]



[A CISO's Essential Guide to API Security »]

[API Security Best Practices Guide »]



[API Security Evaluation Guide »]

About Salt Security

Salt Security protects the APIs that form the heart of every modern application.

The Salt Security API Protection Platform is the industry's first patented solution to prevent the next generation of API attacks. Only Salt harnesses the power of AI and big data at cloud scale to detect and prevent API attacks, providing unrivaled end-to-end API security so businesses can innovate with confidence. Deployed in minutes, the Salt platform learns the granular behavior of your APIs and requires no agents, configuration, or customization to pinpoint and stop API attackers.

Salt provides a number of technical and business advantages that set us apart as the leader in API security, including:

- **Pioneering expertise** – Salt was the first company to recognize the risk of APIs and the first to develop a dedicated API security platform. We have the biggest customer base, with the greatest penetration of Fortune and Global 500 companies, and we're the only company with a security research team dedicated to API security.
- **Transformative impact** – Our breadth of deployments means our algorithms are unparalleled in their exposure and learning. Only Salt brings cloud-scale big data to solve this very thorny challenge of detecting today's sophisticated low-and-slow API attacks that unfold over days and weeks. We help you move faster by taking API risk off the table.
- **Unwavering integrity** – Our research, our technical innovation, and our track record of follow-through make us an ideal partner. Listening to your needs and priorities helps shape our development, and collaboration with our customers as innovation partners helps us stay out in front.

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 becoming 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 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.

SALT
SECURITY