SALT

API

Q1 2025 State of API Security

SALT

Table of Contents

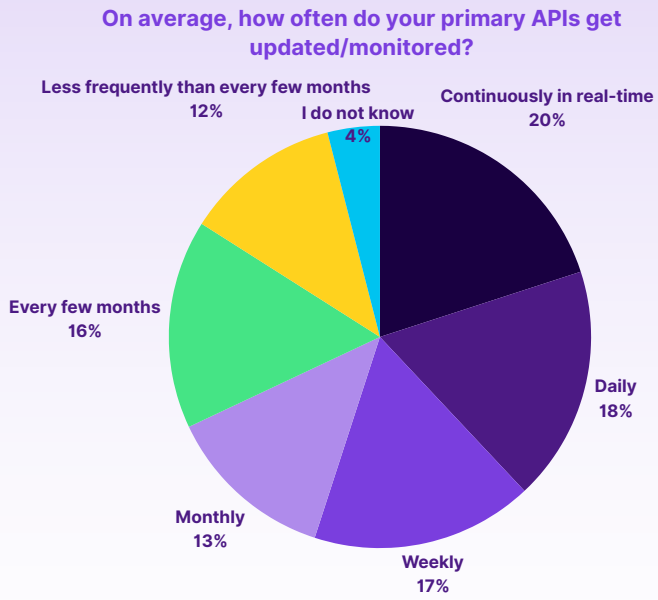
Executive Summary

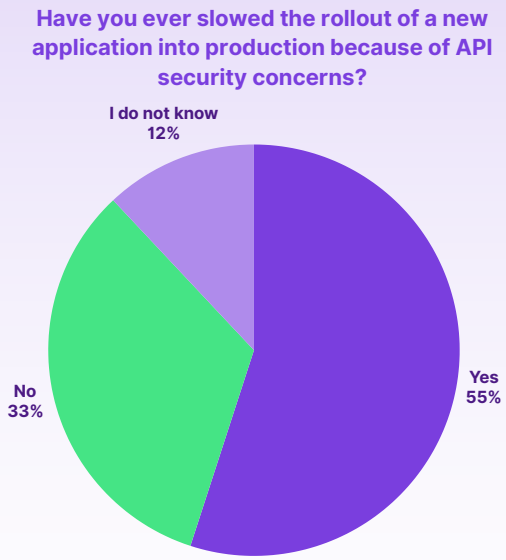
The State of API Security in Q1 2025

The Q1 2025 State of API Security Report paints a vivid picture of progress and ongoing API security challenges. API adoption has become a cornerstone of digital transformation, with rapid growth driven by cloud migration, integration efforts, and the monetization of data and functionality. This expansion, however, has created complex ecosystems that often outpace the security measures in place.

A significant challenge lies in organizations' ability to maintain accurate API inventories and monitor their usage effectively. The fact that **58% of organizations monitor their APIs less than daily and lack confidence in inventory accuracy** highlights critical vulnerabilities that adversaries could exploit. While real-time monitoring is a pressing need, only one in five organizations have achieved this level of oversight.

The prevalence of security issues, such as data exposure and authentication problems, underscores the necessity of a proactive and robust security strategy, especially considering **55% of organizations professed to slowing the rollout of a new application into production due to API security concerns**. It is concerning that nearly one in five organizations cannot identify runtime security gaps, revealing a blind spot in operational security that needs immediate attention. Organizations also face challenges in scaling their API programs, with **14% reporting that their programs are out of control or hard to manage** and **22% who said the biggest obstacle to an optimal API security strategy is people or resource shortages**.



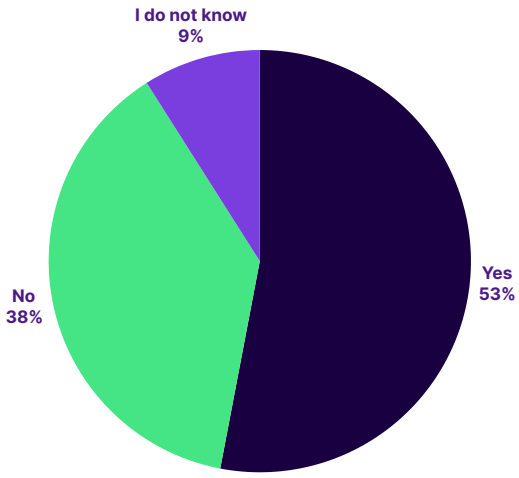


Executive Summary II

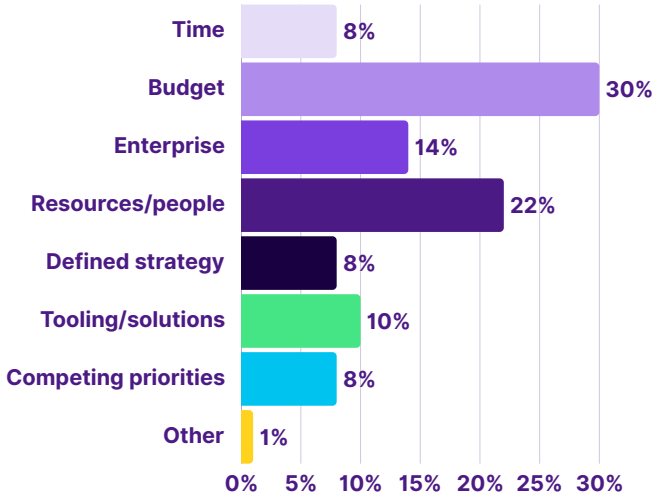
Although many organizations adopt industry frameworks and standards, adherence is inconsistent. The limited **focus on the OWASP Top Ten guidelines (highlighted by only half of respondents) showcases a missed opportunity to leverage proven practices to reduce vulnerabilities**. Additionally, posture governance is a critical yet often overlooked aspect of API security. Without strong governance, organizations struggle to enforce security policies consistently, leading to misconfigurations, excessive permissions, and weak access controls. Implementing robust posture governance ensures that API security policies are clearly defined, continuously enforced, and regularly assessed, mitigating risks before they can be exploited.

Budget and resource constraints remain a recurring theme. Despite **increased investment in API security by over half of respondents, 30% cited limited budgets, and many reported insufficient personnel (22%) or tooling (10%)**. This imbalance suggests that while awareness of API security risks has improved, organizations often struggle to translate this awareness into fully realized security programs. A well-structured posture governance framework can help optimize resource allocation, ensuring security efforts are both effective and scalable.

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



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



Executive Summary III

Generative AI (GenAI) further complicates the landscape by introducing new attack vectors and vulnerabilities. The **lack of confidence in detecting AI-driven threats, reported by one third of respondents**, and **concerns over securing the quality of AI-generated code by 31%** illustrate the need for specialized tools and training. Accurate and complete API discovery, posture governance and threat intelligence, along with developer training, governance frameworks, and advanced testing methodologies, must form the backbone of strategies to address these emerging risks.

The 2025 State of API Security Report reinforces the dual reality of progress and persistent challenges in API security. While organizations are embracing APIs as critical enablers of digital transformation, their rapid adoption has created complex ecosystems that often outpace existing security measures. Organizations must adopt proactive strategies to meet these challenges, focusing on comprehensive monitoring, adherence to established security frameworks like the OWASP Top Ten, and advanced testing practices. By prioritizing real-time monitoring, adhering to security frameworks, and investing in advanced testing and AI-specific security measures, organizations can proactively mitigate API risks and ensure continued innovation.

“Most organizations are fast-tracking digital innovation efforts, leveraging APIs to deliver positive customer experiences. As organizations scale API ecosystems, security often remains an afterthought and threat actors are actively exploiting weak authentication, misconfigurations, and gaps in runtime security to infiltrate systems and access sensitive data.” Says Roey Eliyahu, CEO and co-founder of Salt Security, “Protecting APIs requires a proactive approach—one that emphasizes continuous discovery, strong posture governance, and real-time threat detection. That’s why Salt has developed industry-leading API security solutions, empowering organizations with the visibility, intelligence, and protection needed to defend against today’s most sophisticated threats.”

Drivers for API Adoption

Organizations identified five primary drivers behind API adoption. In order, they are:

1. **Development Efficiencies and Standardization:**
   APIs streamline processes and ensure consistency across teams and projects.

2. **Platform or Systems Integration:**
   APIs enable seamless connections between disparate systems, reducing silos, and improving workflows.

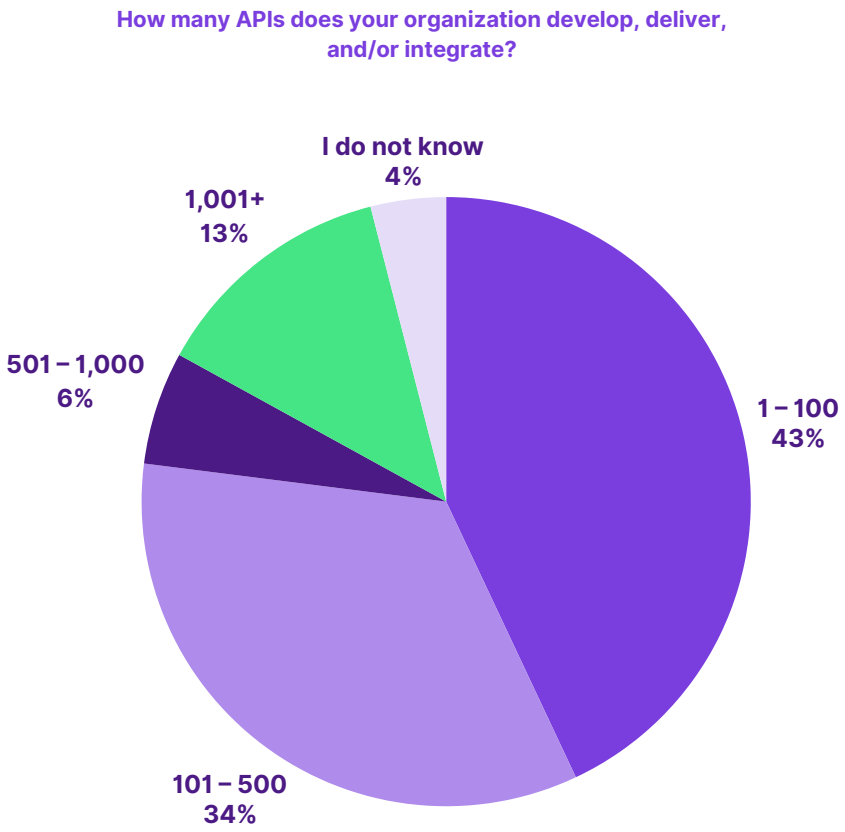
3. **Cloud Migration:**
   APIs support the transition to cloud-based environments, improving scalability, and resource utilization.

4. **Digital Transformation:**
   APIs drive modernization initiatives, enabling organizations to enhance customer experiences and stay competitive.

5. **Monetization of Functionality or Data:**
   APIs unlock new revenue streams by allowing organizations to offer data or functionality as a product.

API Development Trends

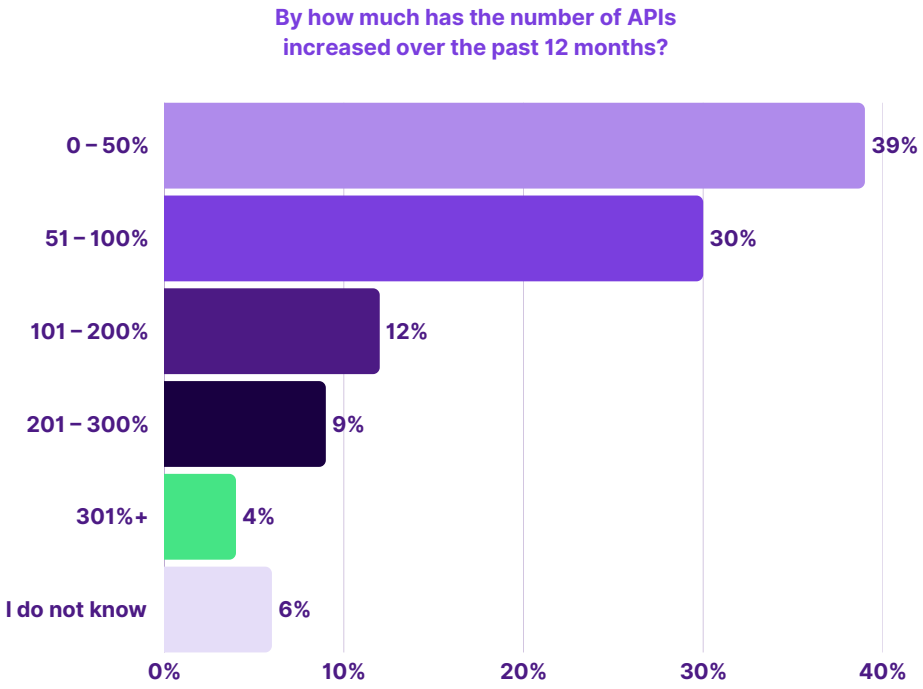
API development continues to experience rapid growth, reflecting the increasing reliance on APIs to drive digital transformation, streamline operations, and enable integration across systems. According to the data, **43% of organizations currently manage up to 100 APIs**, indicating a robust but manageable portfolio for smaller enterprises or those earlier in their API adoption journey. Meanwhile, **34% of organizations oversee between 101 and 500 APIs**, showcasing the prevalence of mid-sized API ecosystems in organizations with more complex operations. Notably, **of the 13% of respondents managing over 1,000 APIs, 53% of them are large organizations (10,000+ employees)** - demonstrating the scale at which large enterprises leverage APIs to deliver services and functionality.



API Development Trends II

The pace of API expansion is equally striking. **Thirty percent of organizations reported a 51-100% growth in the number of APIs they manage over the past year**, showing the critical role APIs play in responding to evolving business demands. Even more impressive, **one-quarter of respondents experienced growth exceeding 100%,** emphasizing the exponential demand for API-driven solutions. This surge in API adoption is driven by the need for organizations to innovate, modernize their infrastructures, and unlock new revenue streams, but it also raises concerns about the ability of security practices to keep pace.

The scale and pace of API adoption can strain resources and complicate security efforts, particularly for organizations with limited monitoring and management capabilities. As APIs continue to proliferate, it becomes imperative for organizations to adopt robust strategies for inventory management, security, posture governance and scalability to sustain this momentum and mitigate the risks associated with such rapid expansion.



API Security Challenges

API security challenges remain a pressing concern, with **nearly all organizations (99%) having encountered API issues in the past year** and **55% saying they've slowed the rollout of a new application** due to API security concerns. This near-universal prevalence, coupled with the rapid expansion of API ecosystems, highlights the growing complexity and risks associated with API-driven environments. APIs are integral to modern systems, facilitating seamless integrations and data exchange, but their widespread adoption also makes them a prime target for cyberattacks.

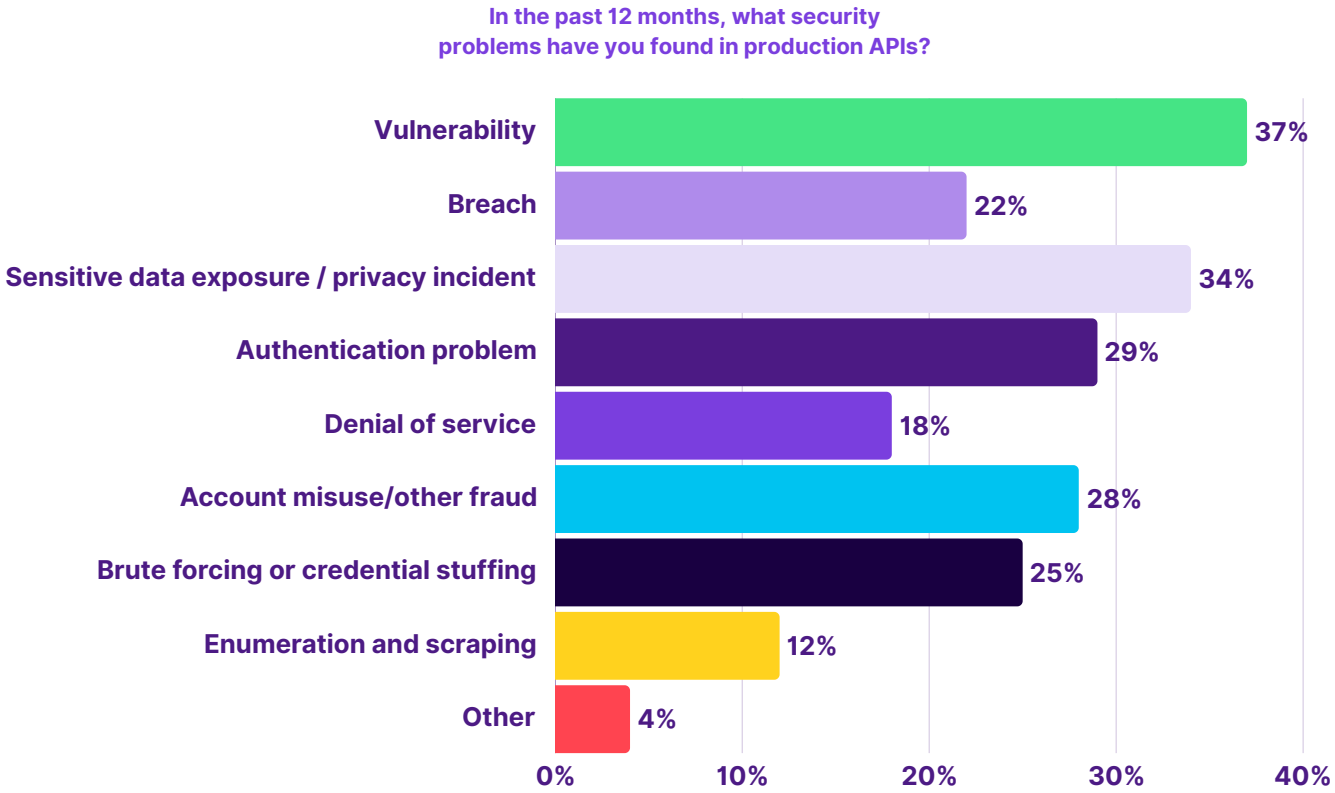
Analysis of the most frequently reported security challenges in production APIs reveals critical insecurities across multiple layers, including vulnerabilities, data exposure, and authentication.

Vulnerabilities accounted for **37% of issues**, exposing APIs to exploits such as injection attacks, misconfigurations, and broken object-level authorization. Insufficient testing, rushed deployments, and inadequate security measures during the development process are major contributing factors to these vulnerabilities.

Sensitive data exposure and privacy incidents represented **34% of issues**, and underlined the risks associated with misconfiguring, mishandling or improperly securing data exchanged through APIs. The exposure of personally identifiable information (PII) or other sensitive data can lead to compliance breaches, reputational damage, and financial penalties. This challenge is exacerbated when organizations lack visibility or have poor governance over the APIs that handle sensitive data or fail to implement robust data encryption and access controls.

API Security Challenges II

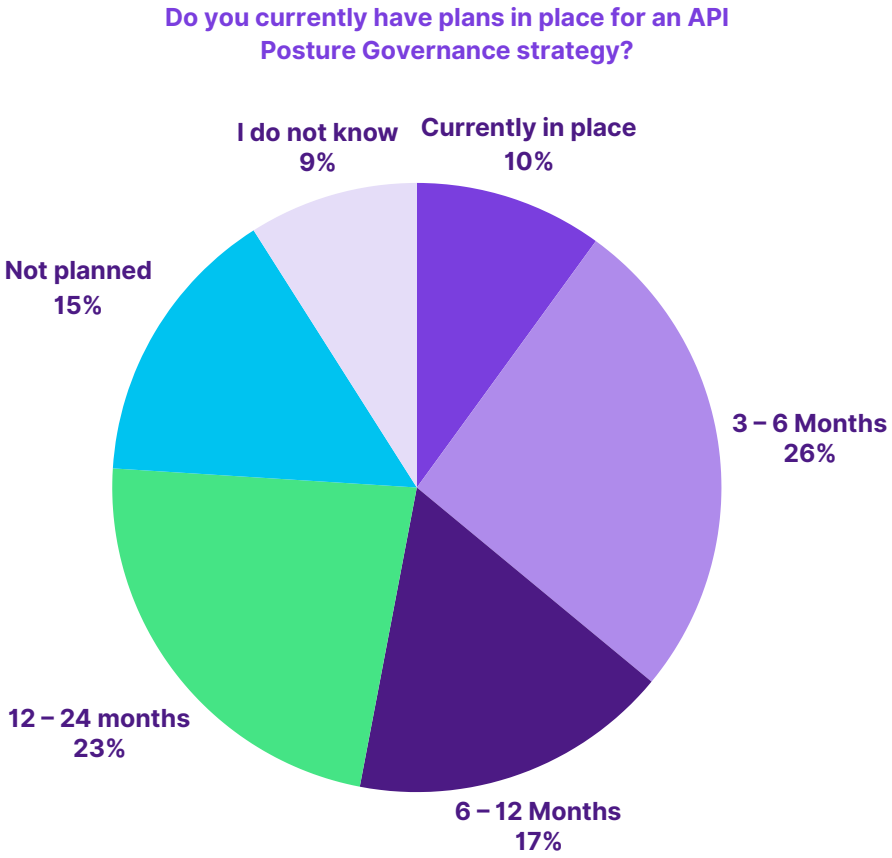
Authentication problems, responsible for **29% of issues**, highlight weaknesses in verifying user identities and enforcing access restrictions. Common vulnerabilities, such as improper session management or the use of weak authentication mechanisms, create opportunities for attackers to impersonate users or gain unauthorized access to sensitive systems. Strong posture governance is essential to mitigating these risks, ensuring that authentication policies are consistently enforced across all API endpoints. This includes implementing multi-factor authentication (MFA), enforcing least privilege access, and conducting regular audits to identify misconfigurations. A well-governed security posture helps organizations proactively address authentication weaknesses, reducing the likelihood of successful attacks.



API Security Challenges III

API posture governance strategies, which provide a structured framework for managing and securing the entire API ecosystem from design to deployment, also leave room for improvement. **Only 10% of organizations currently have an API posture governance strategy in place** - the same amount from last year's report. However, **43% plan to implement such a strategy within the next 12 months**. By deploying and implementing a robust API posture governance engine, organizations can gain complete visibility into their API landscape, eliminate blind spots, and establish corporate-wide security standards and regulations across their entire API ecosystem.

To effectively address these challenges, organizations must prioritize secure coding practices, conduct comprehensive vulnerability assessments, implement real-time monitoring solutions and take a proactive approach to API posture governance aligned with regulatory compliance to detect and mitigate threats proactively. Addressing these challenges is essential to safeguarding APIs and protecting the sensitive systems they support.

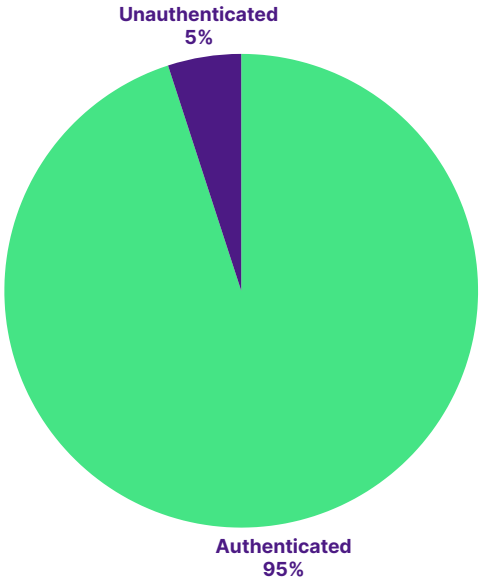


Salt Labs Analysis of Customer Data

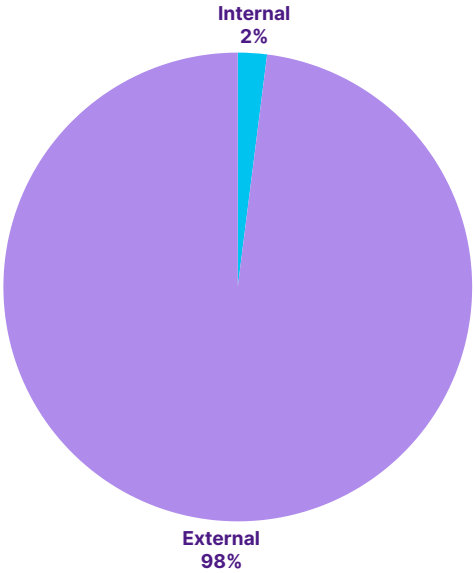
Salt Security's Salt Labs team recently performed an analysis of customer data which pointed to one extremely poignant API security issue: the overwhelming majority of attacks originate from authenticated users. With **95% of attack attempts coming from authenticated sources**, this underscores the growing risk of insider threats, compromised accounts, and attackers leveraging stolen credentials. Traditional security models that rely heavily on authentication as a primary defense are no longer sufficient—organizations must implement robust authorization checks, behavioral anomaly detection, and continuous monitoring of API usage patterns to mitigate these risks.

Additionally, the statistics show that **98% of attack attempts target external-facing APIs**, reinforcing that public APIs are the primary attack surface for malicious actors. **While internal APIs (2%) are less frequently targeted, they shouldn't be overlooked**—especially in scenarios where attackers gain internal access and attempt lateral movement. This data emphasizes the need for strong security controls on public APIs, such as strict rate limiting, input validation, and API gateway protections.

Attack attempts from authenticated vs. unauthenticated attackers



Attack attempts against internal and external facing API endpoints



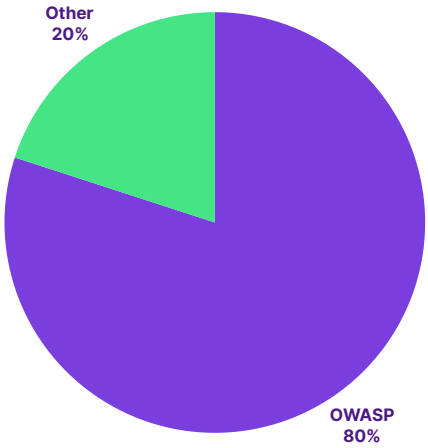
Salt Labs Analysis of Customer Data II

When examining attack techniques, **80% of attempts align with the OWASP API Security Top Ten**, indicating that attackers are actively exploiting known API vulnerabilities rather than relying on novel attack vectors. Within this framework, **API8 (Security Misconfiguration) accounts for 54% of attacks**, making it the most exploited vulnerability. This suggests that weak configurations - such as excessive permissions, exposed sensitive data, or lack of proper security headers - are a significant concern. Similarly, **API1 (Broken Object Level Authorization) contributes to 27% of attacks**, demonstrating how attackers frequently attempt to access unauthorized resources due to flawed access controls. In contrast, vulnerabilities like **API2 (Broken User Authentication) and API7 (Security Monitoring & Logging Failures) each make up just 1%**, suggesting that while these issues exist, attackers may find greater success exploiting other weaknesses.

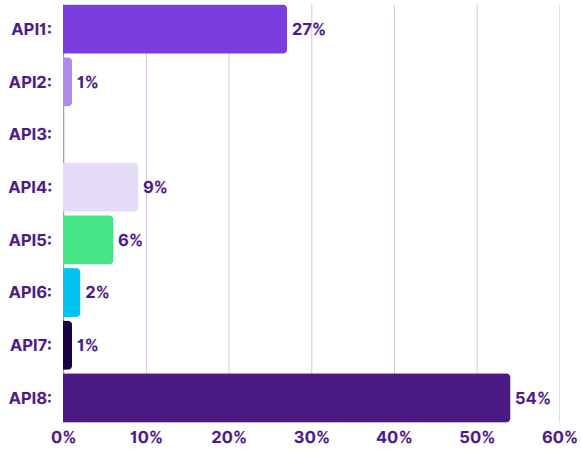
Overall, the Salt Labs analysis reinforces the urgent need for API-specific security strategies that align to the OWASP Top Ten. Organizations must go beyond traditional perimeter defenses and focus on strong authentication and authorization, proper configuration management, continuous security testing and posture governance to address the evolving API threat landscape.

“We see an increase of more sophisticated API attacks, such as BOLA, BFLA, BOPLA, and SSRF, which usually appear as a chain of events, as well as attacks aimed at abusing specific business logic—these attacks obviously pose a far bigger risk and prove to be very hard to detect by any traditional detection method,” said Yaniv Balmas, VP Security Research at Salt Security. “This aligns very well with the trend we have been seeing for the past few years, and we believe this will keep growing in the future, posing more and more risk to any business that is using APIs as part of its online service solutions.”

Attack attempts leveraging the OWASP API Security Top 10 vs other attack types



Attack attempts that map to the OWASP API Security Top 10



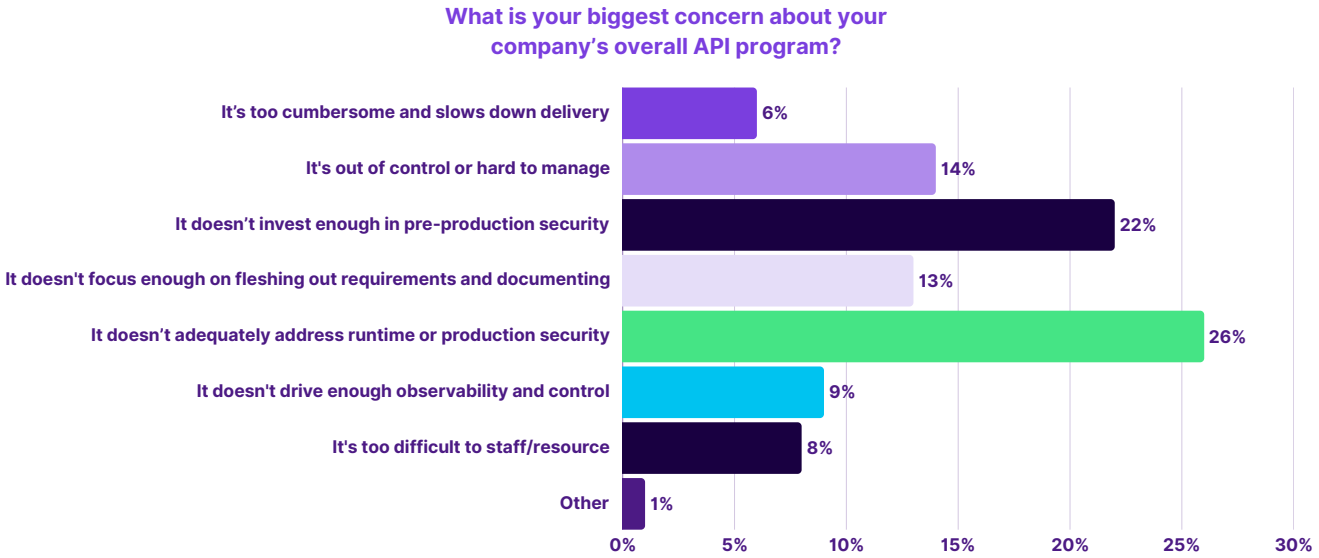
Monitoring and Securing APIs

The findings reveal critical gaps in API monitoring, inventory management, security strategies, and the effectiveness of tools, highlighting the need for greater investment and focus in these areas.

Monitoring Practices and Runtime Security

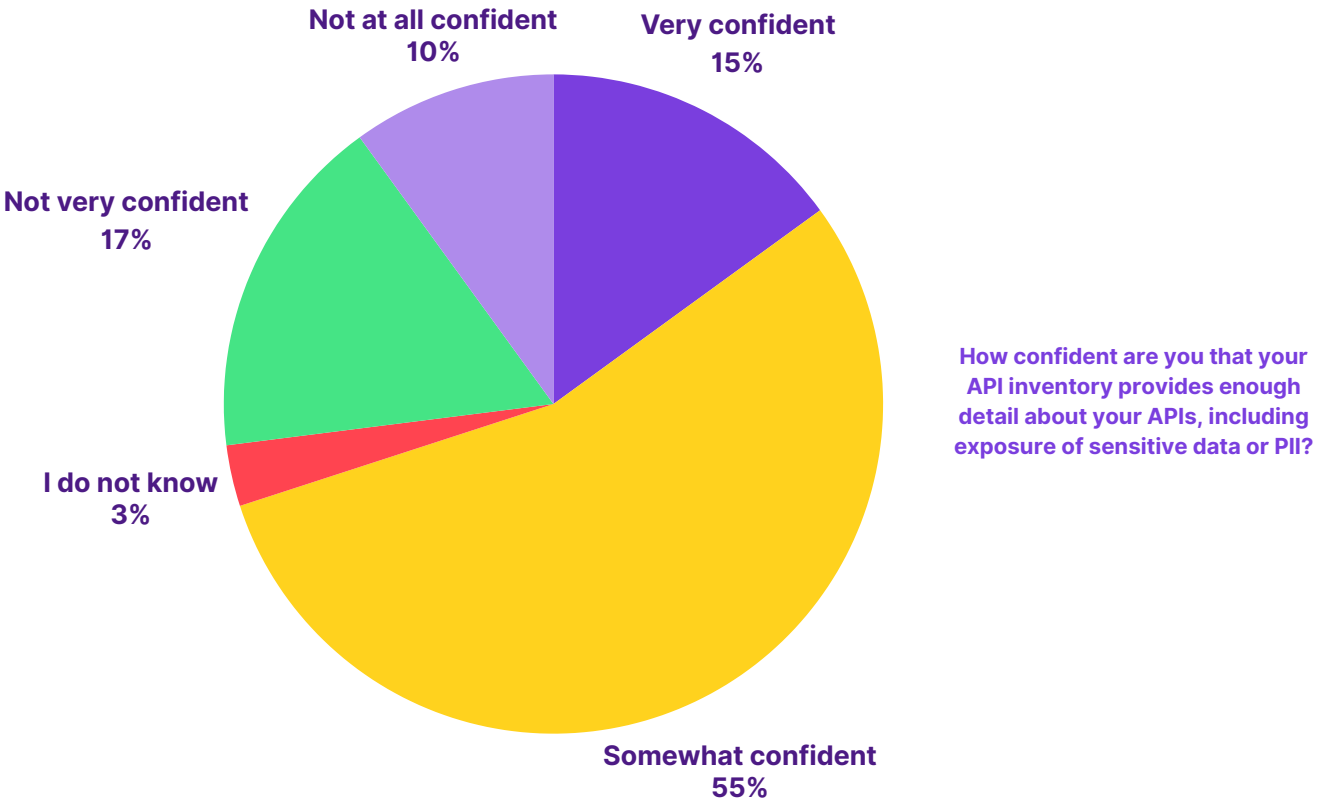
The infrequent monitoring of APIs represents a significant blind spot for many organizations. A mere **20% of organizations continuously monitor their APIs in real-time**, **leaving the majority (62%) vulnerable to attacks due to delayed threat detection**, highlighting a significant security gap. Without real-time visibility, attackers can remain undetected for extended periods, significantly increasing the risk of data breaches and system disruptions. Furthermore, **inadequate runtime security, reported by over a quarter (26%) of respondents, compounds the risks**. Real-time runtime monitoring is crucial to detect and respond to emerging threats.

The unmanageable complexity of API programs reported by **14% of organizations further highlights operational inefficiencies**. Many organizations lack the resources, expertise, or tools necessary to handle the increasing scale and complexity of their API ecosystems.



Monitoring and Securing APIs II

API Inventory and Confidence
Maintaining accurate API inventories presents a significant challenge for many organizations, further complicating security efforts. Half of the organizations rely on developer documentation to identify APIs exposing sensitive data, which is prone to human error and incompleteness. Alarmingly, **34% admitted they faced security challenges regarding lack visibility into sensitive data exposure through APIs, and only 15% expressed strong confidence in the accuracy of their API inventories**. This lack of clarity not only hampers security efforts but also exposes organizations to regulatory compliance risks.

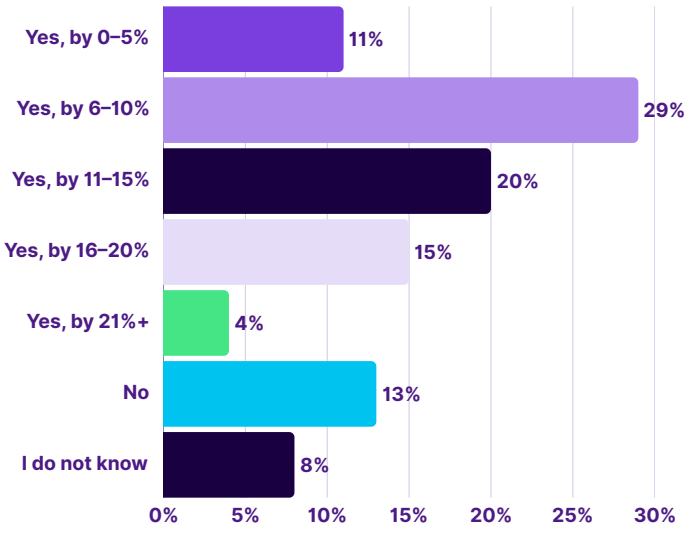


Monitoring and Securing APIs III

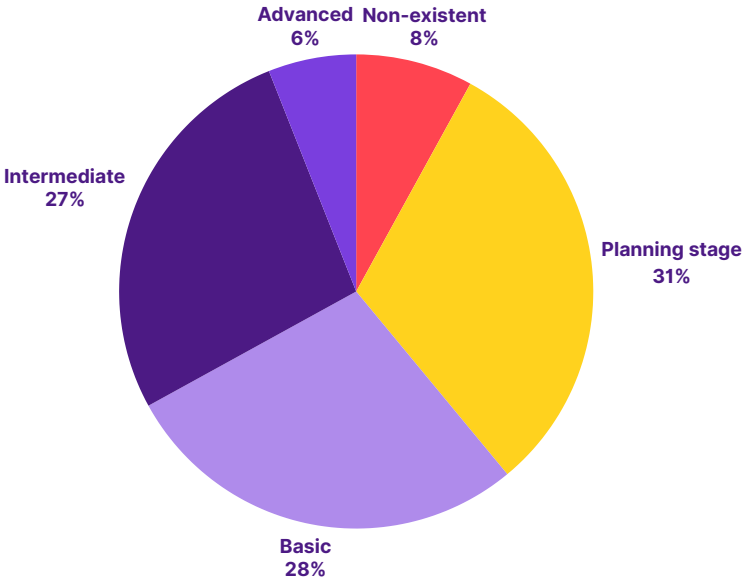
Security Strategy and Investment

Despite **69% of organizations increasing their API security budgets by more than 5%, the overall maturity of API security strategies remains disappointingly low**, indicating a gap between investment and implementation. A significant portion **(59%) are still in the planning or basic stages, with only 6% reporting advanced security programs - 8% said that their API security strategies were non-existent. Budget constraints (30%), resource limitations (22%), and inadequate tooling (10%) further hinder progress**. This clearly defines the need for better resource allocation and strategic alignment to address evolving threats effectively.

Has your organization increased their API security budget within the past 12 months? If yes, by how much?



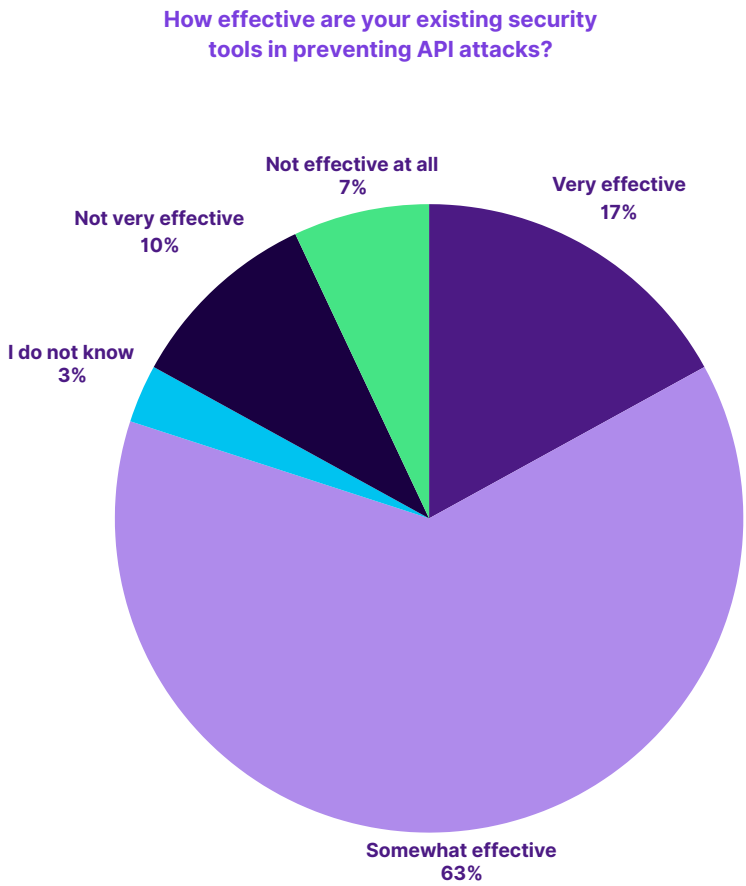
How would you describe the security strategy for your API development program?



Monitoring and Securing APIs IV

Security Gaps and Tools

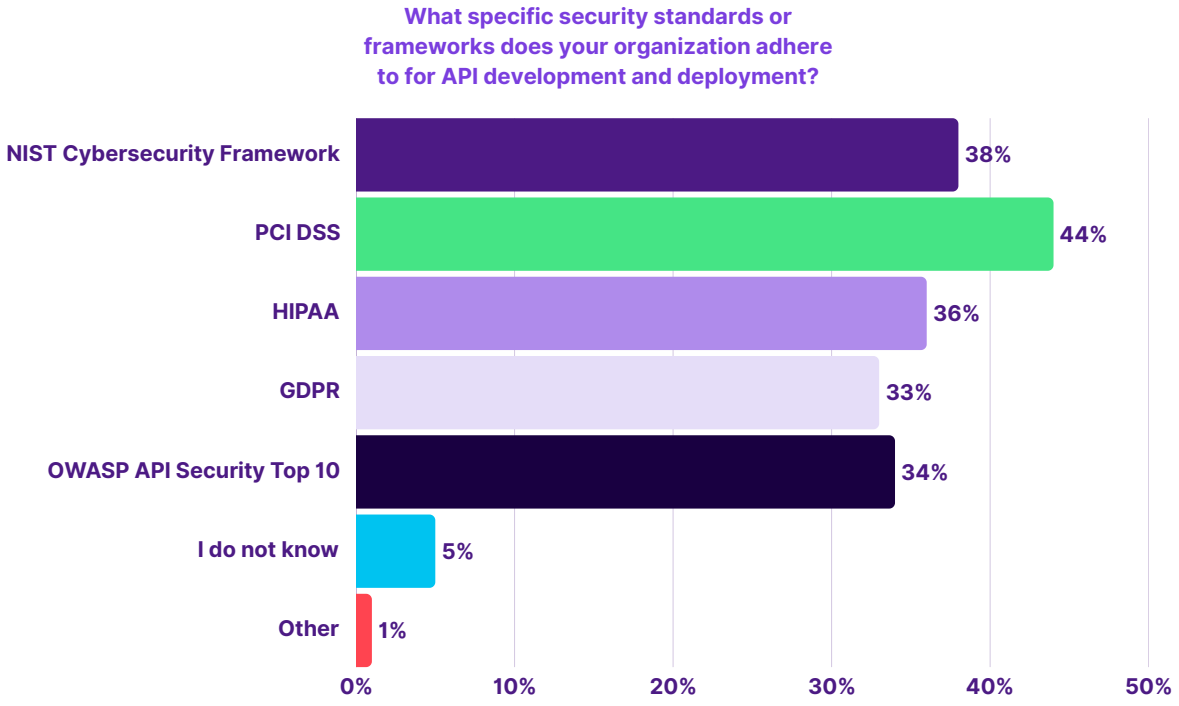
The inability to identify runtime security gaps, reported by 26% of organizations, and the **10% who lack the ability to detect API attacks altogether are alarming**. These critical gaps leave organizations highly vulnerable to sophisticated and evolving API attacks. While tools like API gateway alerts, log file analysis, and authentication error tracking are used, their effectiveness is limited. **Only 17% rated their tools as very effective in preventing API attacks, and 63% found them only somewhat effective**.



Monitoring and Securing APIs V

Frameworks and Standards
Adherence to established frameworks and standards remains inconsistent. While frameworks such as **PCI DSS (44%), NIST (38%), and HIPAA (36%) are adopted, 34% align with the OWASP Top Ten guidelines**, a critical resource for addressing API-specific security threats. This suggests a lack of awareness or prioritization of key standards that can enhance security practices.

The findings highlight the urgent need for organizations to improve API monitoring, inventory management, and adherence to security frameworks. Increased investment in advanced tools, real-time monitoring capabilities, and comprehensive security testing approaches is essential. Aligning with recognized standards like OWASP Top Ten can further strengthen security practices and posture while ensuring organizations are better equipped to manage the growing risks of API-driven ecosystems.



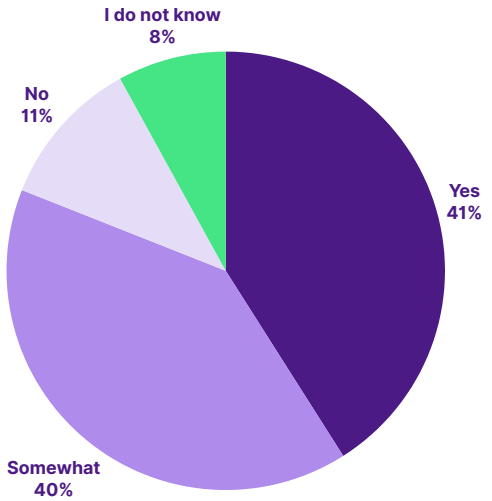
Generative AI and API Security Risks

GenAI, a rapidly evolving field of artificial intelligence with the capability to create diverse forms of content including text, images, music, and code, presents new challenges and opportunities in the realm of API security. It is based on deep learning algorithms that are trained on massive datasets. GenAI has the potential to revolutionize many industries, including healthcare, education, finance, and entertainment. Despite its potential benefits, such as developing new drugs, personalizing education, detecting fraud, and creating more realistic and engaging content, GenAI also introduces unique security challenges that organizations must address to safeguard their APIs.

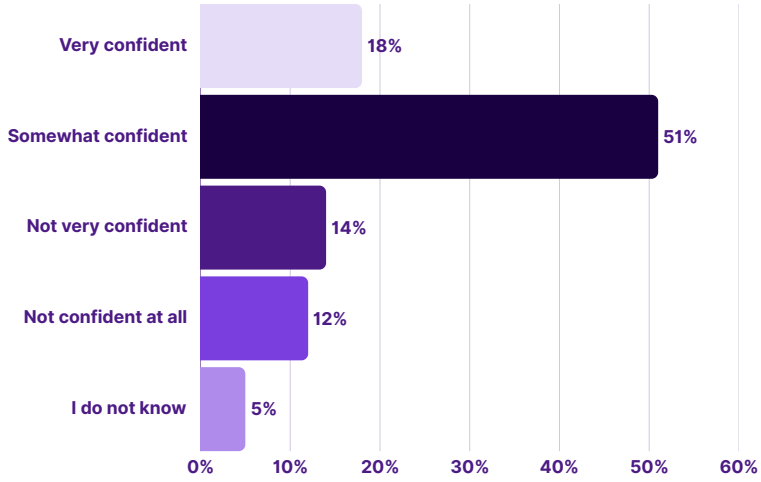
Many governments are also developing plans to integrate GenAI into their operations. For example, the UK government has launched a new AI task-force to explore the potential of GenAI for public services, such as healthcare and education.

Despite all of these potential benefits, GenAI has also introduced a new dimension of risks for organizations, particularly in the context of API security. While GenAI can enhance productivity and innovation, it also presents unique challenges that many organizations are not fully prepared to deal with.

Is Generative AI perceived as a growing security concern/risk within your organization?



How confident are you in your organization's ability to detect and respond to attacks leveraging Generative AI?



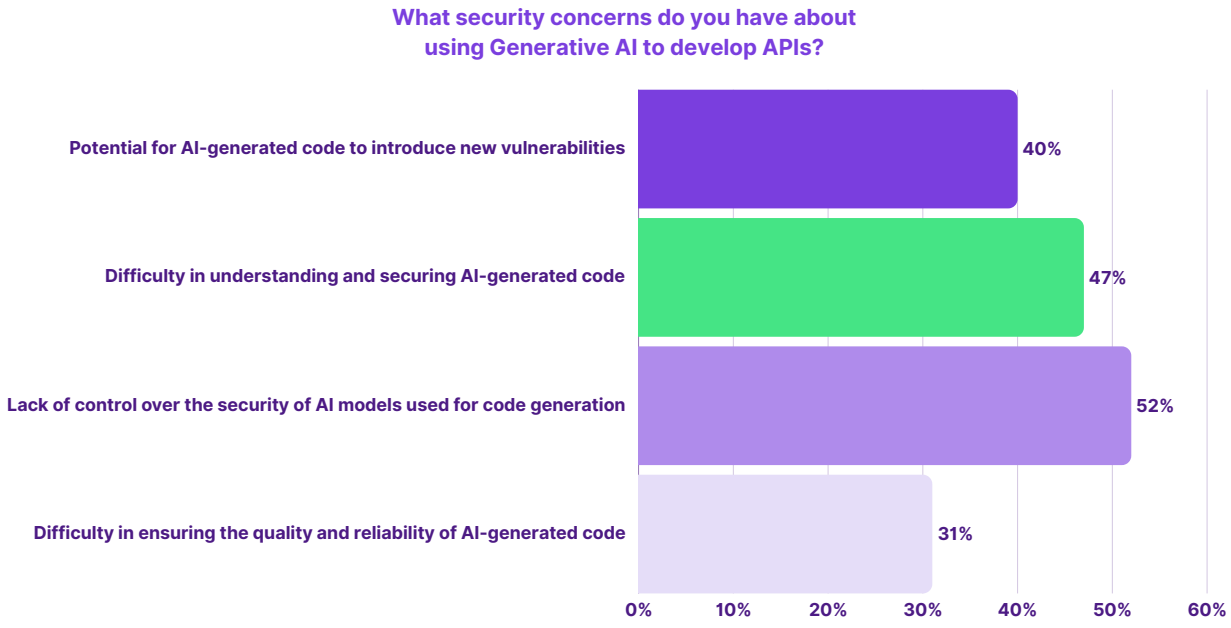
Generative AI and API Security Risks II

Confidence in Detecting AI-Driven Attacks

Only **11% of respondents do not perceive GenAI as a growing security concern within their organization**, while **51% somewhat confident in their organization's ability to detect and respond to attacks leveraging GenAI**, highlighting a significant gap in organizational preparedness for this emerging threat landscape. Attackers are increasingly leveraging AI to automate sophisticated attacks, generate realistic phishing attempts, and exploit vulnerabilities in code. Without robust mechanisms to detect these emerging threats, organizations risk falling behind in their security efforts.

Concerns with AI-Generated Code

The adoption of GenAI tools for code development introduces a range of risks. **Concerns about ensuring the quality and reliability of AI-generated code are paramount, with 31% of respondents citing this as a top concern.** This highlights the inherent challenges in verifying the accuracy and security of code generated by AI tools. **Another 47% expressed concerns about securing AI-generated code**, which often lacks the rigorous checks performed during traditional development processes. Additionally, **40% cited the potential for vulnerabilities introduced by these outputs, which may inadvertently include exploitable flaws or fail to adhere to security best practices**.

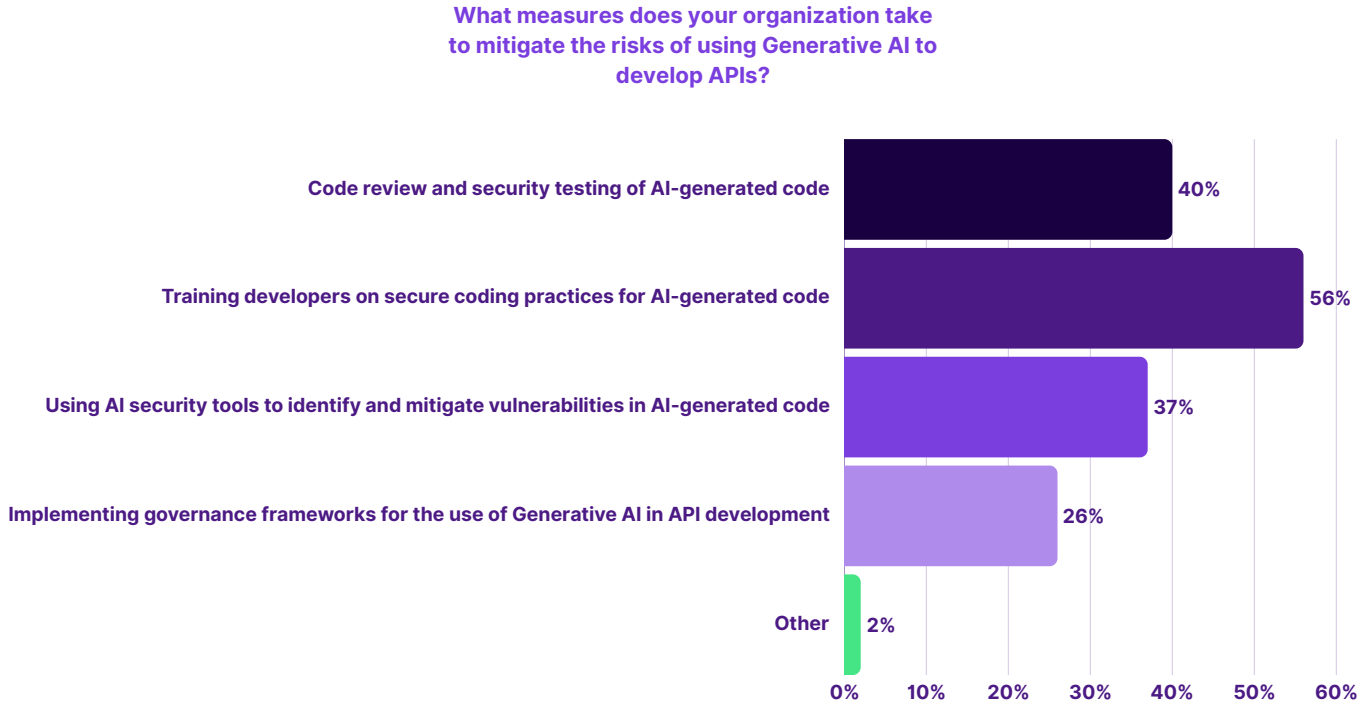


Generative AI and API Security Risks III

Mitigation Strategies

To address these risks, organizations are implementing a variety of mitigation strategies. **Developer training is a crucial element in mitigating AI-related risks, with 56% of respondents prioritizing this approach to ensure developers are equipped to handle the unique security challenges of AI-generated code**. **Code reviews and security testing, employed by 40%**, also provide an essential layer of scrutiny, ensuring that AI-generated code meets quality and security standards.

Governance frameworks were adopted by 26% of organizations to establish clear policies and procedures for managing AI-generated code. These frameworks can guide organizations in evaluating the risks associated with GenAI and enforcing security protocols. **Specialized AI security tools, used by 37%, offer a targeted approach to addressing the unique vulnerabilities introduced by AI-driven processes**.



Measuring ROI in API Security

Measuring the return on investment (ROI) in API security remains a critical aspect of justifying expenditures and optimizing resource allocation. With APIs playing a vital role in business operations, companies need to show that their investments in API security yield measurable advantages, notably in reducing risks and advancing strategic goals. The data highlights key metrics organizations use to assess the effectiveness of their API security initiatives.

Improved Compliance Posture

For **37% of organizations, improved compliance posture is the primary metric for evaluating API security ROI**. This focus reflects the rising importance of adhering to regulatory requirements and industry standards, particularly in sectors like finance, healthcare, and e-commerce, where sensitive data handling is paramount. A robust API security framework helps organizations comply with standards like GDPR, HIPAA, or PCI DSS and reduces the risk of penalties, reputational damage, and operational disruptions caused by non-compliance. Moreover, demonstrating compliance can enhance stakeholder trust, providing an indirect but significant ROI in terms of customer retention and business growth.

Cost Savings from Breach Prevention

25% of organizations measure ROI through cost savings achieved by preventing security breaches. This metric highlights the serious financial consequences of API vulnerabilities, which may lead to data breaches, system outages, and considerable expenses tied to incident response and recovery. By proactively investing in API security tools, monitoring, and training, organizations can avoid the substantial costs associated with recovering from attacks. This approach also reinforces the value of pre-emptive security measures in mitigating long-term financial risks.

Measuring ROI in API Security II

Reduction in API-Related Security Incidents

For **16% of respondents, reductions in API-related security incidents serve as a key indicator of ROI**. This metric, while it may seem little more than common sense, demonstrates that organizations are indeed starting to put emphasis on API security. The operational benefits of a well-secured API ecosystem include improved system reliability, reduced disruptions, and enhanced user experiences. A measurable reduction in security incidents indicates the success of security measures put in place, including monitoring, testing, and remediation strategies, confirming the value of a thorough API security program.

Broader Implications

While the metrics outlined provide valuable insights into API security ROI, they represent only part of the picture. Additional advantages, such as boosted developer efficiency, faster innovation, and strengthened organizational reputation, greatly add to the overall value of investments in API security. However, these benefits are harder to quantify, requiring organizations to adopt a more holistic view of ROI.

Measuring ROI in API security is essential for aligning security initiatives with organizational goals and demonstrating their value to stakeholders. While metrics like compliance improvements, cost savings, and incident reductions are critical, organizations should also consider the broader strategic advantages of robust API security. By doing so, they can build a compelling case for sustained investments in security and ensure their API ecosystems remain secure, resilient, and supportive of business growth.

Conclusion and Recommendations

The Q1 2025 State of API Security Report offers essential insights into the challenges and priorities in API development and security, and gives insight into how organizations are adjusting their strategies in response to the evolving landscape. Based on responses from over 200 professionals responsible for APIs in their organizations, the report demonstrates the growing reliance on APIs for digital transformation, the escalating pace of API adoption, and the persistent security challenges that organizations face. Even with heightened investment in API security, significant gaps persist, especially in runtime security, real-time monitoring, and the specific risks posed by emerging technologies, such as GenAI.

While the API security landscape shows signs of maturity, organizations must accelerate their efforts to close critical gaps. Real-time monitoring, enhanced runtime protection, alignment with recognized frameworks, and investments in advanced tools and training are imperative to safeguard APIs in an increasingly digital and interconnected world. By addressing these areas, organizations can turn API security from a reactive effort into a proactive enabler of innovation and growth.

"APIs are the backbone of modern applications, but their complexity and rapid evolution expose organizations to critical vulnerabilities. Salt Security empowers our customer's cybersecurity teams with unparalleled API visibility and control, combining comprehensive inventory management, robust runtime protection, effective incident response, and governance frameworks. By proactively addressing API security, we help businesses mitigate risks, ensure compliance, and build trust in their digital ecosystems," said Bill Thrash, VP Customer Operations at Salt Security.

Some recommendations based on the findings of this report include:

Prioritize Real-Time Monitoring and Runtime Security
The report highlights significant gaps in real-time API monitoring, with only **20% of organizations continuously monitoring APIs**. Prioritizing real-time monitoring tools and practices is essential to enable immediate threat detection and response, minimizing the potential damage caused by attackers.Investments in advanced runtime security solutions are also critical to address vulnerabilities during production.

Develop Comprehensive API Security Strategies and Frameworks
With **60% of organizations still in the planning or basic stages of their API security strategies**, it is essential to promote the adoption of comprehensive and advanced approaches. Aligning security practices with recognized frameworks like the OWASP API Security Top Ten and implementing robust governance policies are vital steps to ensure consistent and effective API security across the organization.

Conclusion and Recommendations II

Strengthen API Inventory Management and Visibility
The lack of confidence in API inventories is alarming, with only **15% of organizations expressing strong confidence in their accuracy**, highlighting the need for improved inventory management practices. Organizations should invest in automated tools that provide comprehensive visibility into all APIs, including shadow APIs and those exposing sensitive data. Accurate inventory management is crucial for maintaining security and compliance in dynamic, fast-growing API environments.

Mitigate Risks from Generative AI Through Targeted Strategies
GenAI introduces unique risks, including vulnerabilities in AI-generated code and AI-driven attacks. To address these risks, organizations should implement developer training, robust code review practices, and governance frameworks tailored to AI. Specialized AI security tools should be adopted to detect and mitigate threats unique to GenAI applications.

Enhance Security Tools and Testing Practices
Current tools and testing practices are insufficient for robust API security, with only **17% of organizations rating their tools as very effective**. Organizations should adopt more comprehensive security testing approaches, combining vulnerability scanning, penetration testing, and threat modeling. Investment in tools with advanced detection and prevention capabilities, particularly for runtime security and AI-driven threats, will be essential for addressing evolving risks effectively.

By implementing these recommendations, organizations can strengthen their API security posture, mitigate emerging risks, and better support the rapid growth and innovation enabled by APIs. Visit **https://salt.security** to learn more or to set up a demo.

About Salt Security

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.

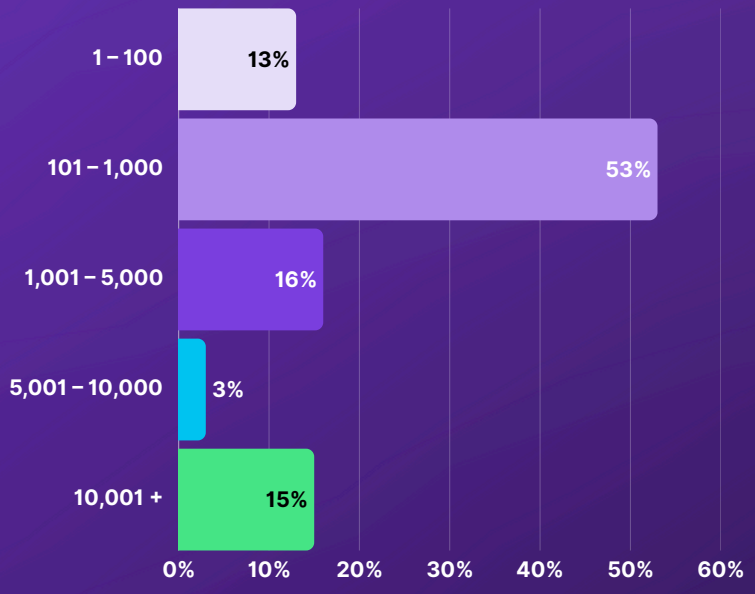
About Salt Labs

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.

Methodology

The findings of this report are based on insights from 206 professionals tasked with managing APIs in their organizations. Respondents provided detailed data on API development trends, security challenges, monitoring practices, and the adoption of frameworks and tools to address API vulnerabilities.

Size of company breakdown is as follows:



Industry breakdown: