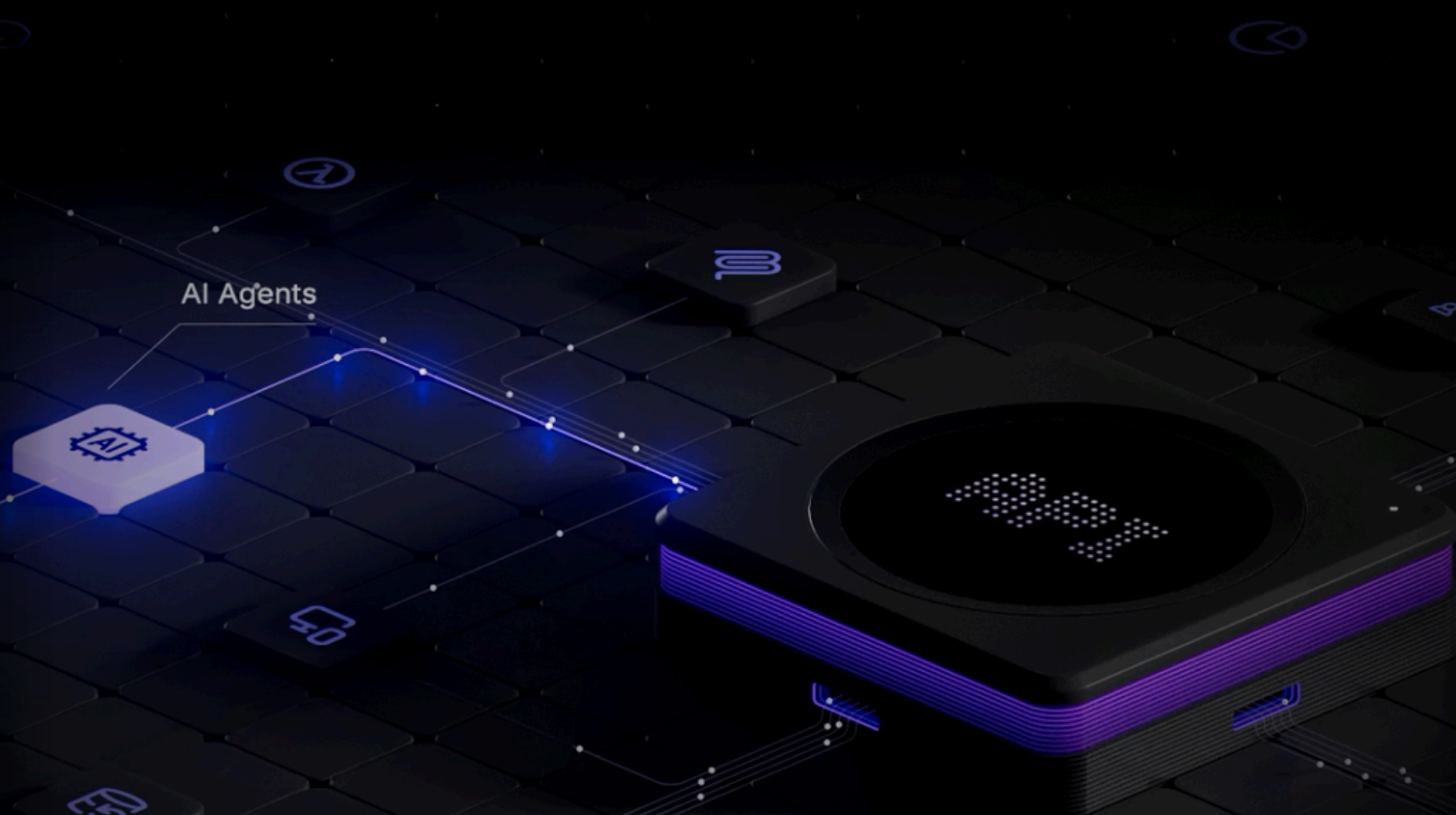
SALT

H2 2025 State of API Security



SALT

1

Table of Contents

2 Executive Summary

The State of API Security in H2 2025

AI adoption has turned APIs into the action plane for autonomous systems; every LLM workflow, agent, and MCP tool call rides on APIs. That exposes a critical truth: **you cannot secure AI without securing APIs.** In H2 2025, this dependency is outpacing today's API security practice. Our survey of 386 security leaders reveals that 80% lack continuous, real-time API monitoring, 33% have suffered an API incident in the past year, and 50% have slowed a release due to API risk; evidence that visibility gaps and weak posture governance are already throttling AI velocity.

Agents + MCP intensify exposure. As MCP accelerates agent-to-tool orchestration, its early design lacks embedded security controls. Without API-level guardrails, prompt-injection, data exfiltration, and over-permissioned tools can become system-level failures. KuppingerCole summarizes the market shift succinctly: APIs are the backbone of AI, and legacy, gateway-only models are giving way to policy-driven controls from design and build through deploy and runtime.

What the attackers are actually doing. Salt Labs research found that 96% of attack attempts originate from authenticated entities (compromised users, insiders, or rogue agents) and 98% target external-facing APIs. The dominant vectors map to OWASP: API8 Security Misconfiguration (78%) and API1 BOLA (10%), issues that automation amplifies from "serious bugs" into systemic agent abuse. Authentication alone won't save you; orgs need continuous discovery, posture governance, runtime anomaly detection, and authorization depth.

What leaders are doing now. Leaders are **prioritizing continuous API discovery**, improving **inventory accuracy** and **sensitive-data mapping**, and expanding **real-time monitoring and runtime protection**. They are also establishing **GenAI governance** and **guardrails** to prevent sensitive-data exposure to and from AI models via APIs.

Outcome: Treat API security as the foundation for AI agent security. Done right, it transitions from cost-avoidance to innovation enablement, measured by faster AI releases, fewer rollbacks, lower enterprise risk, and better audit readiness.

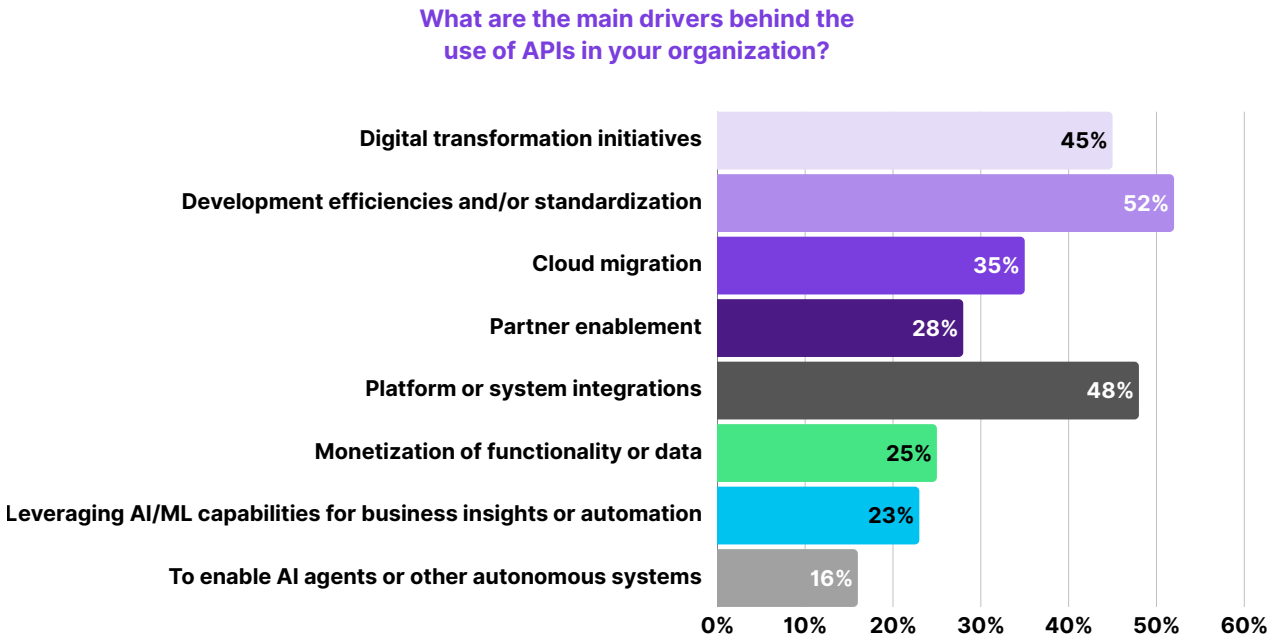
Key Findings

The AI Action Plane is Here, But Security is Lagging

Our survey of 386 security leaders reveals that API security gaps are directly throttling business and AI velocity.

- **Business Velocity at Risk**
  - 50% have slowed a new application rollout due to API security concerns.
  - 33% reported an API security incident in the past year.
- **Critical Visibility & Governance Gaps**
  - 80% lack continuous, real-time API monitoring.
  - Only 19% are “very confident” in their API inventory accuracy.
- **AI Fuels Adoption and New Risk**
  - AI/ML (23%) and AI Agents (16%) are now key API drivers.
  - 62% use GenAI for development, while 56% see it as a growing security concern.
- **The New Attacker Playbook (Salt Labs)**
  - 96% of attacks come from authenticated sources.
  - 78% exploit Security Misconfiguration (API8).
- **Investment and Maturity Are Misaligned**
  - Most budget increases are modest (≤15% for 61% of orgs).
  - 51% of organizations are still in planning or basic stages of API security maturity.

These findings highlight that APIs are indispensable to business strategy, yet security remains inconsistent and reactive. Closing this gap is essential for transforming API security from a bottleneck into an enabler of AI innovation.



4 Drivers for API Adoption

While APIs have long been the foundation of digital business, their primary purpose is undergoing a fundamental shift. The core drivers of integration and efficiency now serve a new, urgent imperative: powering the AI-driven enterprise. This year's survey reveals how organizations are building the API infrastructure for this new reality by prioritizing both emerging AI-specific needs and the foundational drivers that support them.

The New Imperative: Powering the AI-Driven Enterprise

A significant and growing number of organizations now cite AI and automation as key drivers for API adoption, creating the channels through which autonomous systems will operate:

- **AI/ML Enablement:** 23% of respondents indicated APIs are enabling advanced analytics, automation, and business insights powered by machine learning.
- **Support for AI Agents:** 16% cited APIs as critical for enabling autonomous systems such as AI agents, which rely on APIs for communication and orchestration.
- **Foundational Drivers:** These new AI initiatives are built upon a bedrock of traditional, yet essential, drivers that continue to fuel API growth.
- **Development Efficiencies and Standardization:** 52% of organizations selected this as a leading driver to reduce duplication and accelerate delivery cycles.
- **Platform and Systems Integration:** 48% of respondents cited this as a top reason for connecting disparate applications and streamlining workflows.
- **Digital Transformation:** 45% pointed to digital transformation initiatives as a primary driver for modernizing legacy systems and accelerating new services.
- **Cloud Migration:** 35% are using APIs to support migration to modern cloud architectures.
- **Partner Enablement:** 28% identified this as an important factor to expand ecosystems and integrate with third-party services.
- **Monetization of Functionality and Data:** 25% of respondents said APIs are used to create new revenue streams.

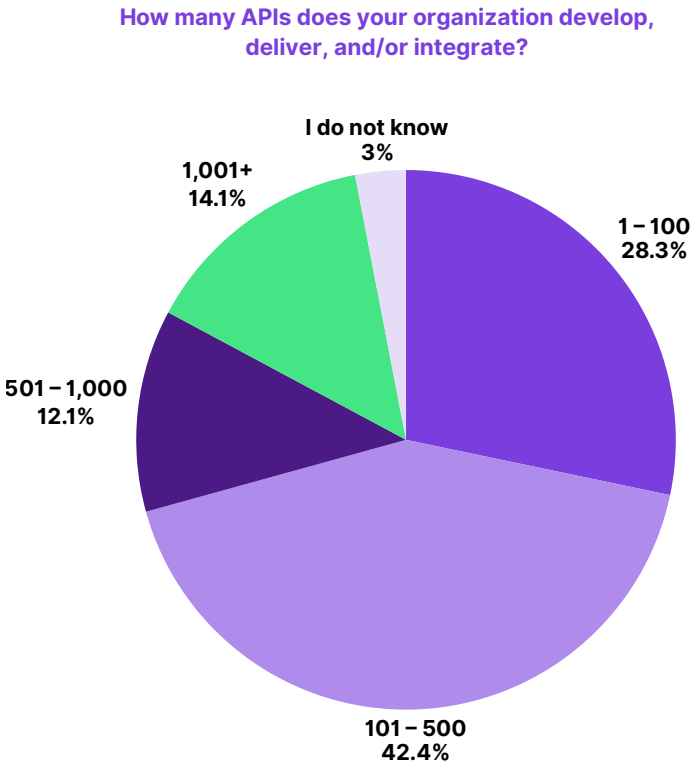
This dual focus underscores the growing reliance on APIs as the core of digital strategy. As organizations build the infrastructure for AI, the need for robust and scalable API security becomes inseparable from the success of these strategic initiatives.

API Development Trends

The reliance on APIs continues to grow, reflecting their role as the backbone of digital operations, integrations, and innovation. The 2025 survey data reveal that organizations are managing increasingly complex API portfolios, with scale varying widely across industries and companies.

- **Portfolio Size**
  - 28% of organizations manage between 1 and 100 APIs, a figure that reflects smaller organizations or those still in the earlier stages of their API journey.
  - The largest group, 42%, reported managing 101–500 APIs, signaling that mid-sized API ecosystems are the most common across enterprises today.
  - 12% manage 501–1,000 APIs, while 14% said they oversee 1,001 or more APIs.
  - Only 3% indicated they do not know how many APIs they are responsible for.

These findings illustrate that APIs are no longer limited to niche use cases. Even among organizations with modest digital footprints, the API landscape is expanding rapidly—and in large enterprises, API portfolios routinely span into the thousands.

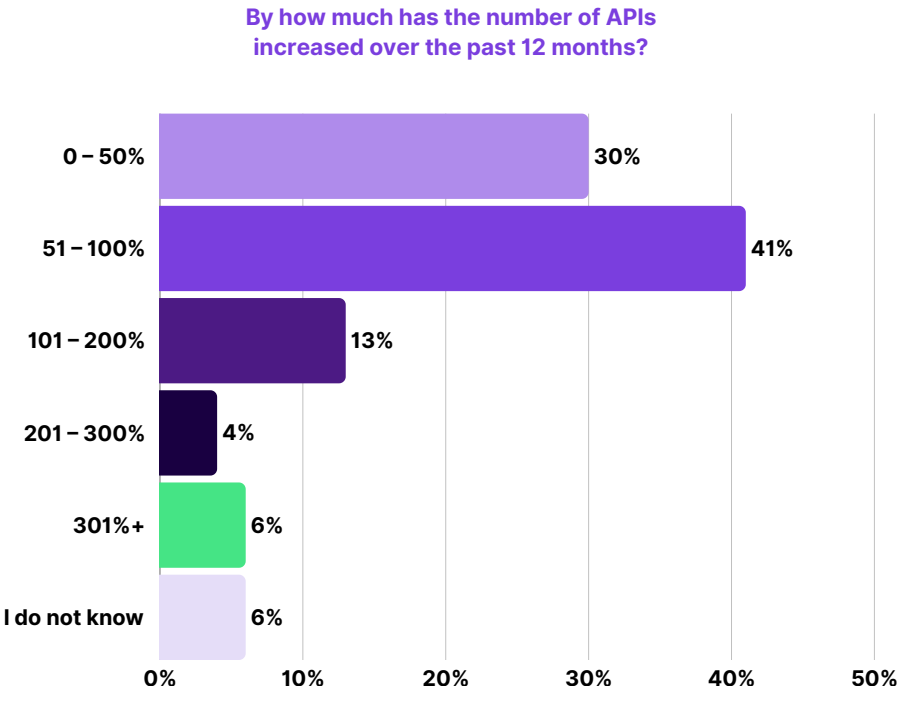


API Development Trends II

- **API Growth Rates: The pace of growth is equally striking**
  - 30% of organizations reported a 0–50% increase, indicating steady but controlled expansion.
  - 41% reported API growth of 51–100% over the past year.
  - Another 13% experienced explosive growth of 101–200%, while 4% reported increases of 201–300%.
  - A small but notable 6% indicated their API volume more than tripled (301%+) in just 12 months.

This rapid proliferation is being fueled by modernization initiatives, AI adoption, and the need to enable new digital services. However, it also raises the stakes for security and governance. As APIs multiply across hybrid and multi-cloud environments, organizations face mounting challenges in maintaining visibility, scaling protections, and ensuring that development velocity does not outpace security maturity.

APIs have become central not only to application delivery but also to the adoption of advanced technologies such as AI and automation. This means the risks tied to rapid API expansion now extend beyond technical vulnerabilities, shaping business resilience, regulatory compliance, and customer trust.



API Security Challenges

API security challenges remain a critical concern for nearly all organizations, with 33% reporting they experienced at least one API security incident in the past 12 months. As API ecosystems expand, so do the attack surfaces and the risks associated with misconfigurations, poor visibility, and insufficient runtime protections.

Types of Security Problems Found

As organizations enable AI agents, common API security flaws are transformed from serious issues into systemic risks. The speed and scale of automation amplify the potential damage from these problems:

- **Vulnerabilities** were the most common, cited by 41% of respondents. When exploited by automated tools or AI agents, common flaws allow attackers to rapidly discover and compromise the full API attack surface, rather than targeting one endpoint at a time.
- **Sensitive data exposure and privacy incidents** were reported by 34% of respondents. This risk is magnified when APIs grant access to AI models and agents. A single API misconfiguration could allow an agent to access and exfiltrate entire datasets at machine speed.
- **Authentication problems** were flagged by 33%. In an automated ecosystem, this is no longer just about user logins; it is a fundamental flaw in machine identity that can grant an autonomous AI agent dangerous levels of access.
- **Account misuse or other fraud** was identified in 29% of cases. This threat evolves when AI agents are involved, enabling fraudulent transactions or data manipulation to occur at a scale and speed that is impossible for human attackers to replicate.
- **Breaches** were reported by 28% of organizations. This is the ultimate outcome of the preceding failures. In an AI-driven environment, the time from initial compromise to a full-scale breach can shrink from weeks or days to mere minutes.
- **Denial-of-service attempts** were reported by 20%. APIs that power critical AI and automation workflows become high-value targets. A successful DoS attack can halt automated business processes, resulting in significant operational disruption.
- **Brute forcing or credential stuffing** was found in 18% of cases. Attackers are now using these automated techniques to target not just user accounts, but also the machine identities of AI agents and services, seeking to compromise the core of an organization's automation fabric.
- **Enumeration and scraping** were found by 13%. Malicious AI can use this reconnaissance technique at an unprecedented scale, mapping an organization's entire API attack surface to find the weakest point of entry for a larger attack.

These statistics demonstrate that API attacks are not just theoretical risks; they are operational realities impacting organizations across industries.

API Security Challenges II

Biggest Concerns About API Programs

Beyond specific incidents, organizations highlighted structural concerns in managing their API programs:

- 15% said their programs do not adequately address runtime or production security.
- 14% reported their programs are out of control or hard to manage.
- 12% cited a lack of investment in pre-production security.
- Others highlighted challenges with staffing, observability, compliance, and prioritization.

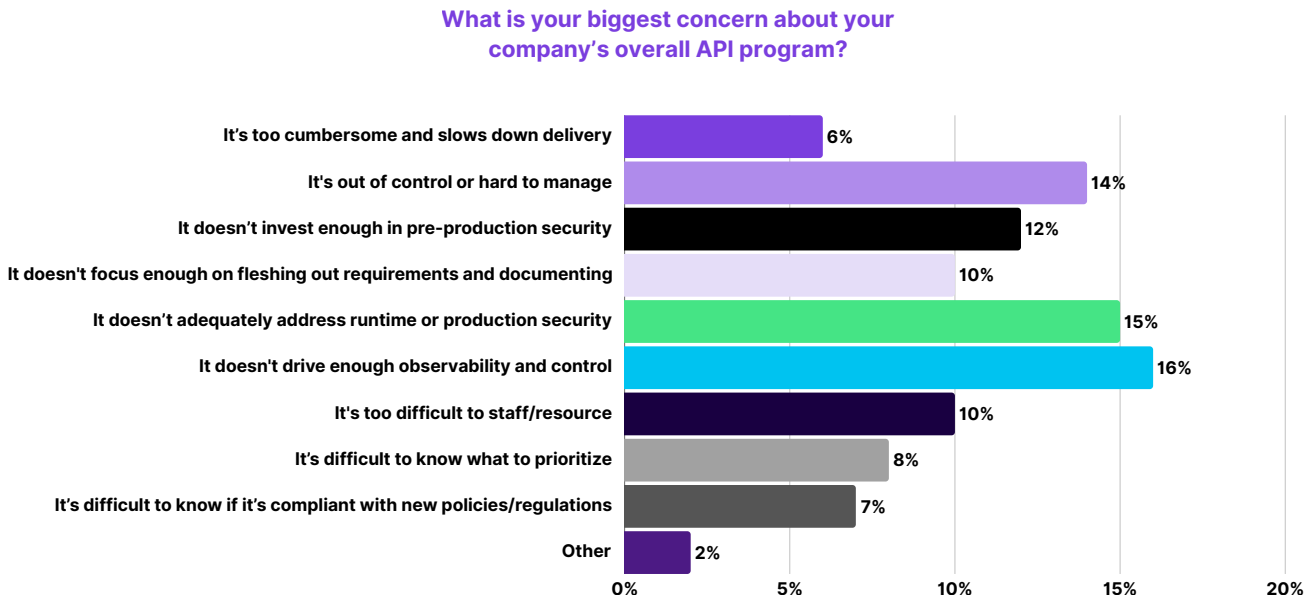
These concerns suggest that as API environments grow, organizations often struggle with both security maturity and operational efficiency.

Obstacles to an Optimal API Security Strategy

When asked about the primary barrier to implementing a strong API security program, respondents pointed to:

- Budget limitations (25%)
- Resource or staffing shortages (16%)
- Time constraints (7%)
- Competing priorities (11%)
- Tooling/solutions gaps (11%)

Together, these findings reveal a fundamental tension: while APIs are essential to business growth, many organizations lack the resources, processes, or governance to secure them effectively.

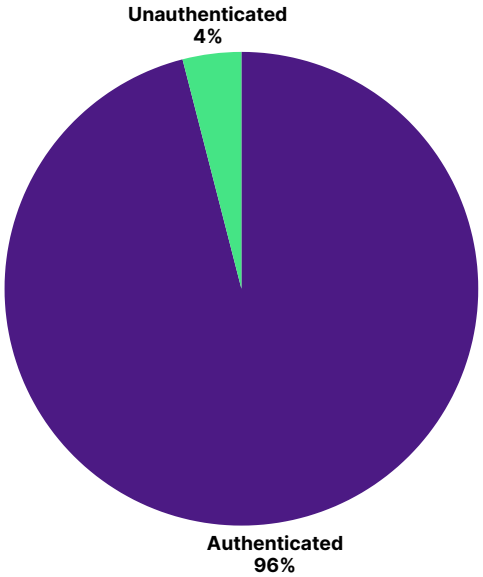


Salt Labs Analysis of Customer Data

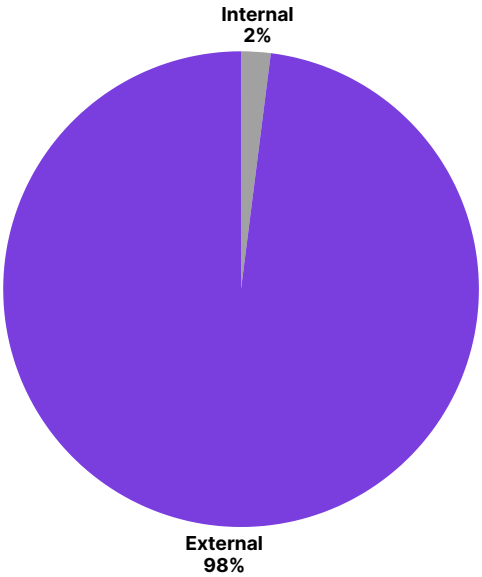
Insight from the Front Lines: The New Attacker Playbook
Our analysis of real-world attack data reveals the playbook attackers will use in the AI Agent Economy, and it confirms that perimeter security is becoming irrelevant. The primary threat is no longer an unauthenticated outsider trying to break in, but an authenticated entity, whether it's a compromised user account, an insider threat, or a rogue AI agent abusing its legitimate access. This represents a paradigm shift that legacy security tools are not equipped to handle.

The data shows that a staggering 96% of attack attempts originate from authenticated sources, while 98% target external-facing APIs. This proves that traditional security models focused on authentication are insufficient. Organizations must evolve to a model based on continuous monitoring, behavioral anomaly detection, and robust authorization checks to mitigate these modern risks.

Attack attempts from authenticated vs. unauthenticated attackers



Attack attempts against internal and external facing API endpoints



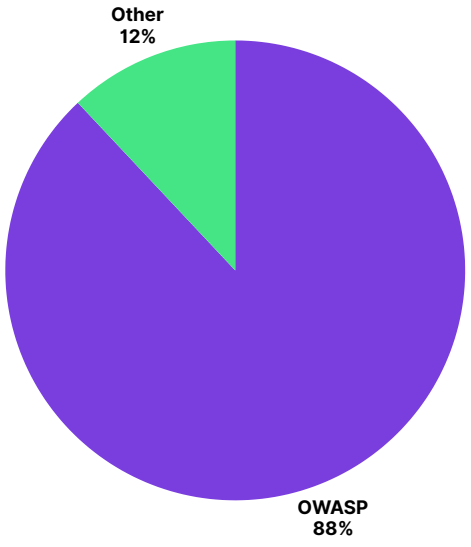
Salt Labs Analysis of Customer Data II

When examining attack techniques, we found that 88% of attempts align with the OWASP API Security Top Ten, confirming that attackers are exploiting known, common vulnerabilities. The two most dominant vectors are governance and authorization failures:

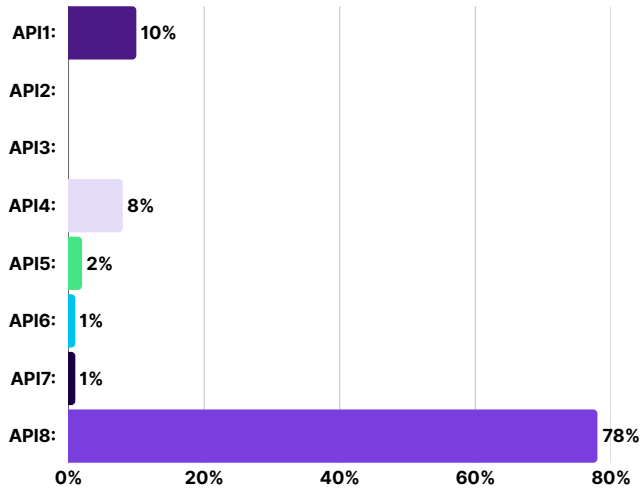
- **The Dominant Threat - API8 (Security Misconfiguration):** This accounts for the vast majority of attacks at 78%. This suggests that simple weaknesses like excessive permissions and improper security headers are the most common entry points.
- **The Authorization Gap - API1 (Broken Object Level Authorization):** This contributes to 10% of attacks, as adversaries frequently attempt to access unauthorized resources due to flawed access controls.
- **Less Common Exploits:** In contrast, other issues like **API2 (Broken User Authentication)** and **API7 (Security Monitoring & Logging Failures)** account for just 1% of attempts, indicating that attackers are finding far more success exploiting misconfigurations and authorization flaws.

Overall, the Salt Labs analysis reinforces the urgent need for API-specific security strategies that align with 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.

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

Monitoring Practices

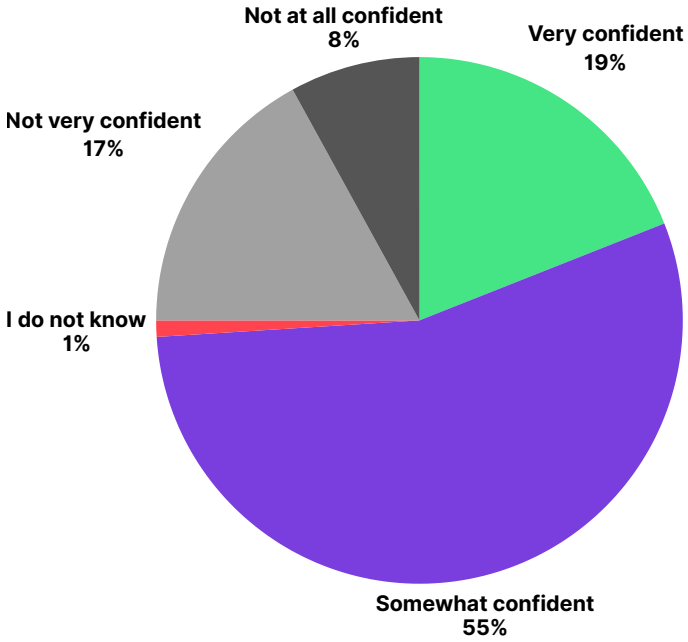
The survey shows persistent challenges in API monitoring and runtime visibility. While 20% of organizations monitor their APIs continuously in real-time, the majority rely on less frequent checks—daily (20%), weekly (23%), or monthly (10%). Another 12% monitor only every few months, and 10% said they monitor even less frequently. These gaps create significant blind spots, giving attackers extended opportunities to exploit vulnerabilities before detection.

API Inventory and Confidence

Accurate API inventories remain elusive for many organizations. More than half (54%) rely on developer documentation to identify which APIs expose sensitive data or PII, while 51% use API management tools. Alarmingly, 15% admitted they do not know which APIs expose PII. When asked about inventory confidence:

- Only 19% were “very confident” in the accuracy of their inventories.
- 55% were only “somewhat confident.”
- 25% said they were “not very” or “not at all confident.”

This lack of clarity creates compliance risks and weakens overall security posture, especially as shadow and undocumented APIs proliferate.



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

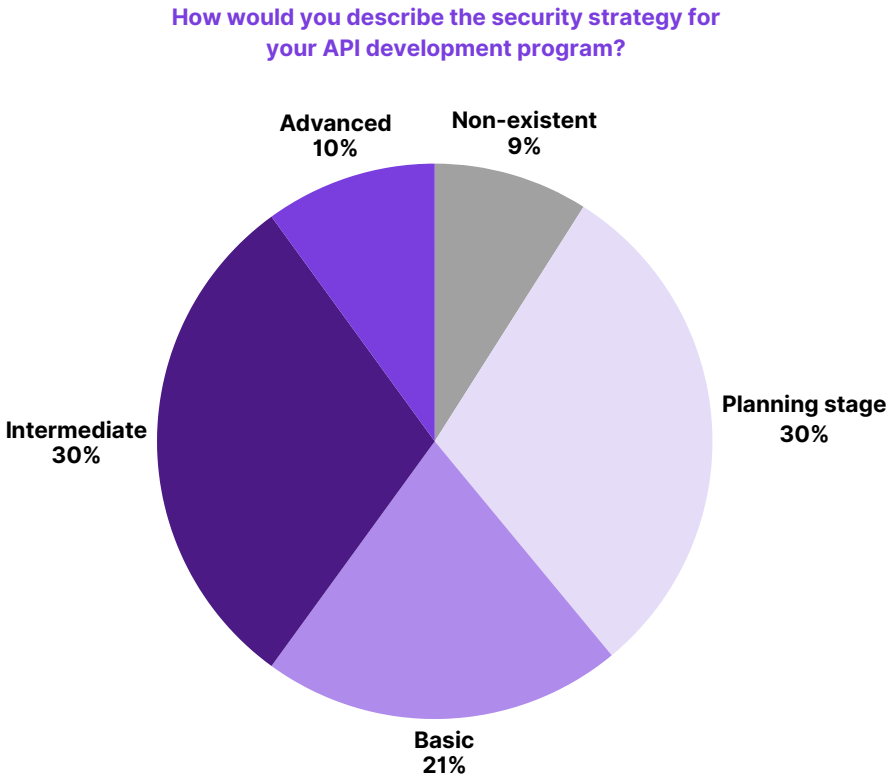
Monitoring and Securing APIs II

Security Strategy Maturity

Organizations' API security programs are still maturing:

- 9% said they have no formal strategy in place.
- 30% are in the planning stage.
- 21% have basic programs focused on risk assessments or manual reviews.
- 30% reported intermediate maturity, with app sec testing and API gateways in place.
- Just 10% said they have advanced strategies that include dedicated API testing and protection.

This distribution highlights that while awareness of API risks is high, comprehensive strategies remain rare.



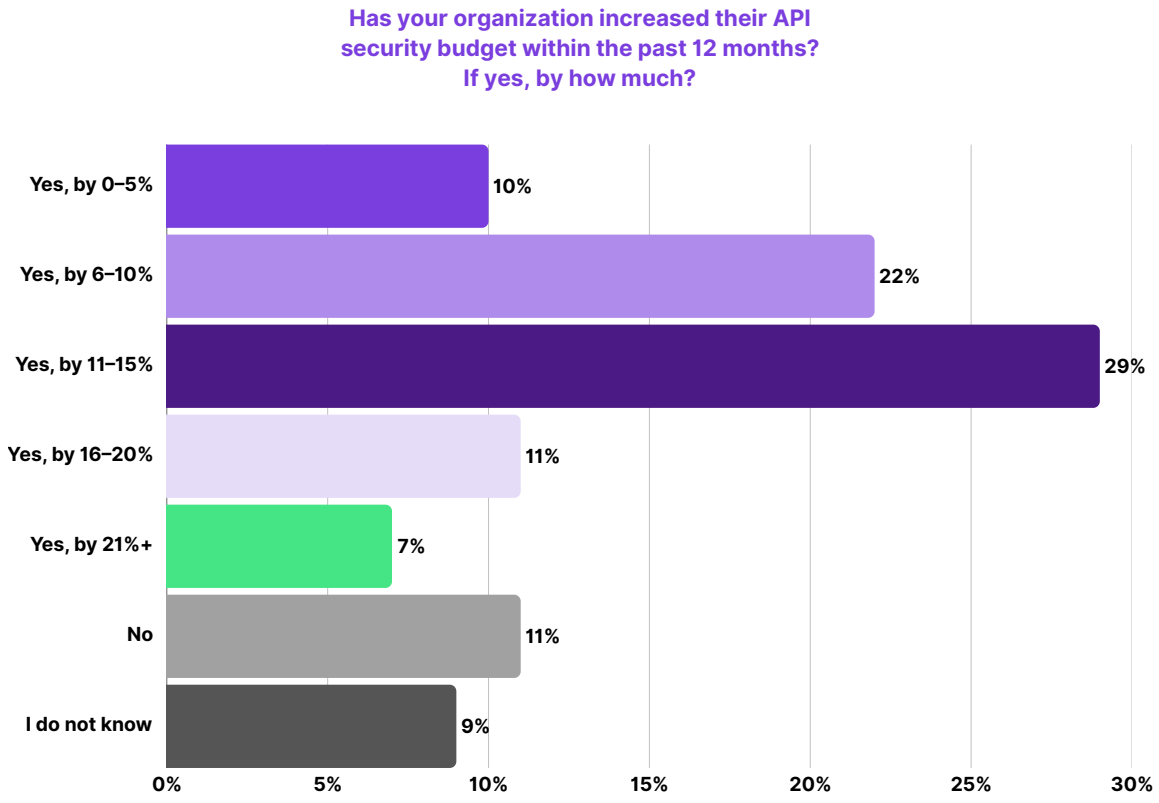
Monitoring and Securing APIs III

Budget and Investment

Nearly 80% of organizations increased their API security budgets in the past year; 61% of all respondents reported modest increases (≤15%):

- 10% raised budgets by 0–5%.
- 22% by 6–10%.
- 29% by 11–15%.
- 11% by 16–20%.
- Only 7% reported increases greater than 21%.
- Meanwhile, 11% said their budget did not increase, and 9% were unsure.

Budget growth demonstrates progress, but modest increases often lag behind the pace of API adoption and the escalating threat landscape.



Monitoring and Securing APIs IV

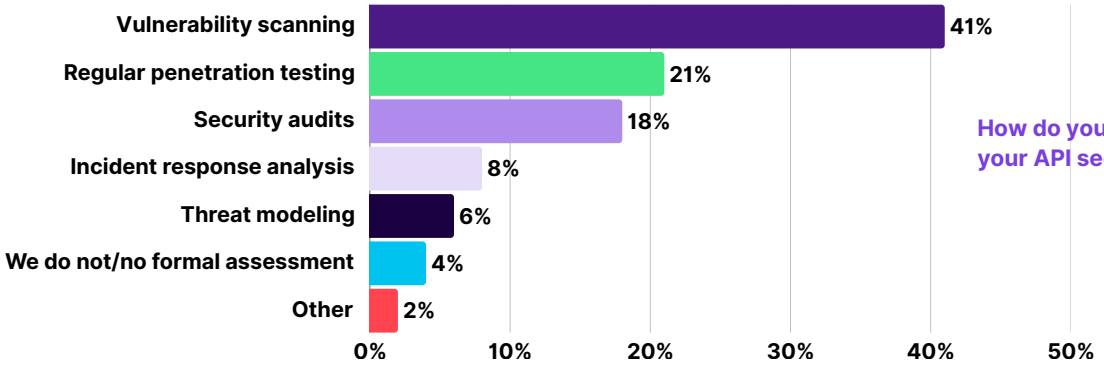
Tools and Effectiveness

Organizations rely on a mix of tools and methods to detect and prevent attacks:

- 41% use vulnerability scanning.
- 21% rely on regular penetration testing.
- 18% perform security audits.
- 6% conduct threat modeling, and 8% conduct incident response analysis.

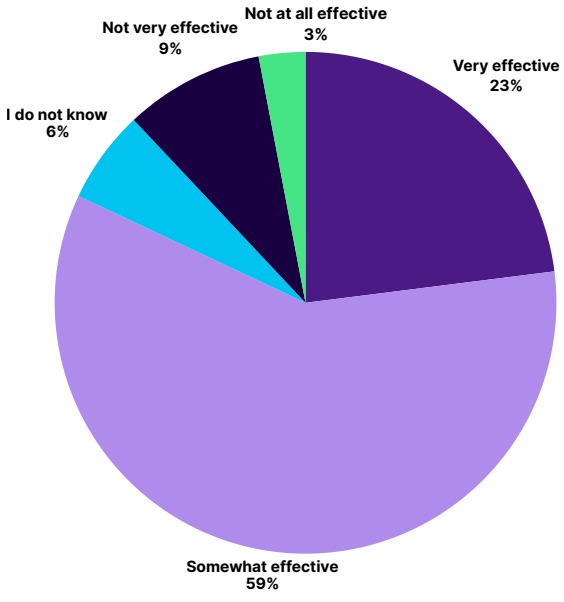
However, the effectiveness of these measures is limited:

- Only 23% rated their tools as very effective.
- 59% said their tools are only somewhat effective.
- 9% rated them as not very effective, and 3% as not effective at all.



How do you assess the effectiveness of your API security measures?

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



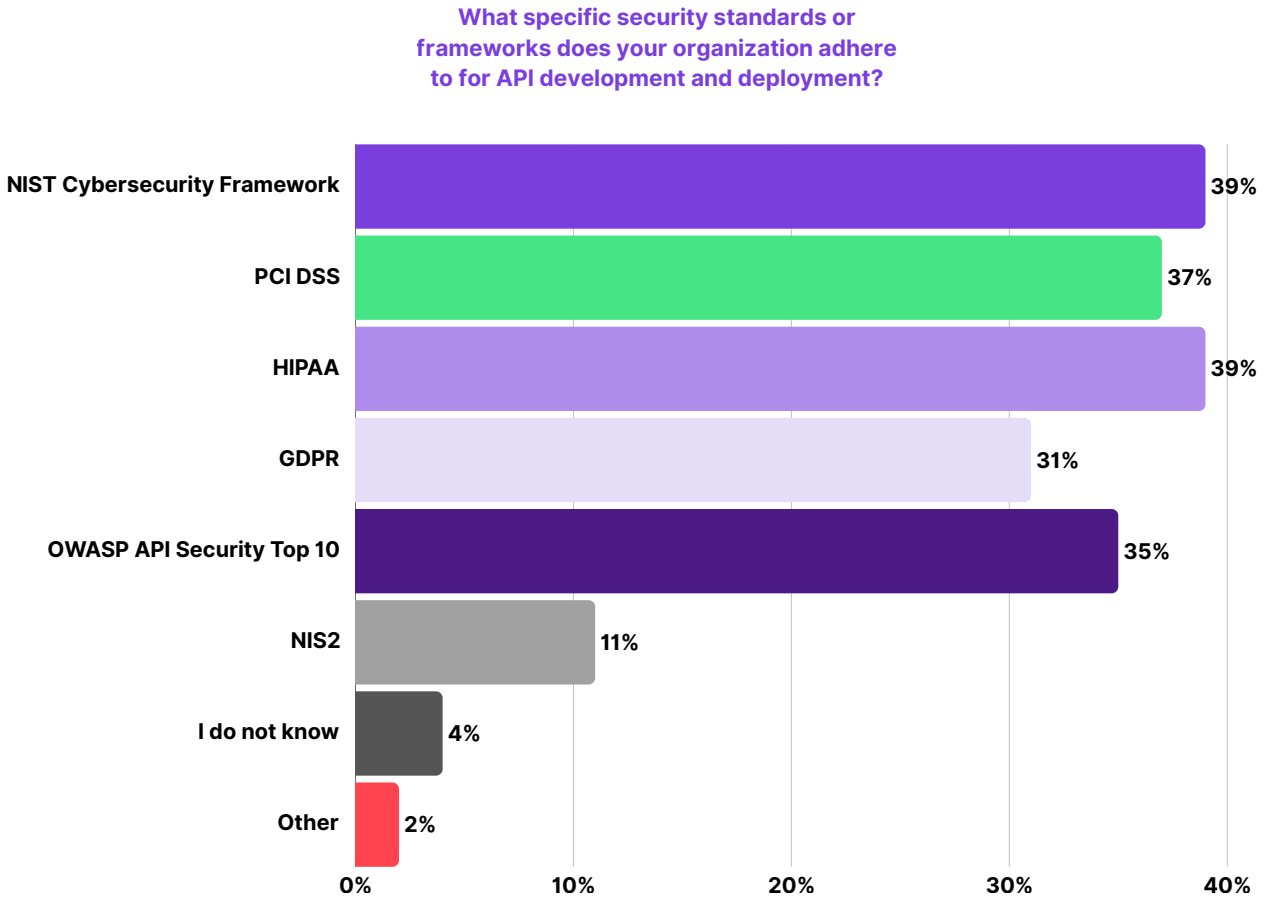
Monitoring and Securing APIs V

Framework Adoption

Adoption of formal standards and frameworks remains inconsistent:

- NIST Cybersecurity Framework (39%)
- PCI DSS (37%)
- HIPAA (39%)
- GDPR (31%)
- OWASP API Security Top 10 (35%)
- NIS2 (11%)

While many organizations are adopting broad compliance frameworks, alignment with API-specific guidelines, such as the OWASP Top 10, remains lower than expected, leaving critical gaps unaddressed.



Generative AI and API Security Risks

Generative AI (GenAI) is rapidly transforming both development practices and security operations—and with it, the threat landscape for APIs. This year's survey reveals that most organizations are now grappling with how GenAI introduces new risks, while also experimenting with GenAI as a defensive tool.

Perceived Risk

A clear majority (56% of organizations) perceive GenAI as a growing security concern, while 36% say it is somewhat concerning. Only 5% reported that it is not a concern at all. This highlights the increasing awareness that AI-driven code generation, automated agents, and large-scale automation create unique attack surfaces.

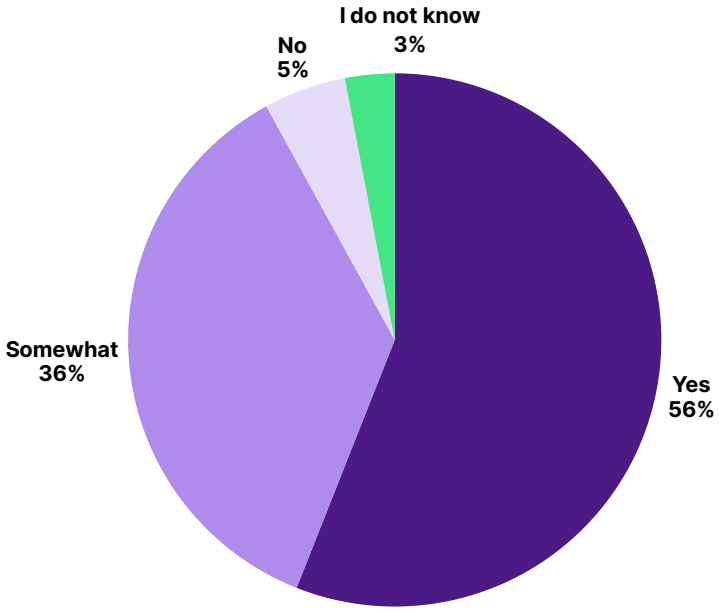
Use of GenAI in Development

Adoption is already widespread:

- 13% of organizations reported using GenAI for all API development.
- 49% are using it for some development.
- 23% plan to adopt it within the next 6–12 months.
- Only 9% said they have no plans to use GenAI in development.

This momentum underscores the inevitability of GenAI in the software lifecycle, but it also raises urgent security concerns.

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



Generative AI and API Security Risks II

Key Security Concerns

Respondents cited several risks tied to AI-generated code:

- Potential for new vulnerabilities (45%).
- Difficulty understanding and securing AI-generated code (47%).
- Difficulty ensuring quality and reliability (35%).
- Lack of control over AI model security used for code generation (56%).

These findings suggest that while GenAI accelerates development, it often bypasses traditional safeguards and quality checks, introducing new weaknesses into production systems.

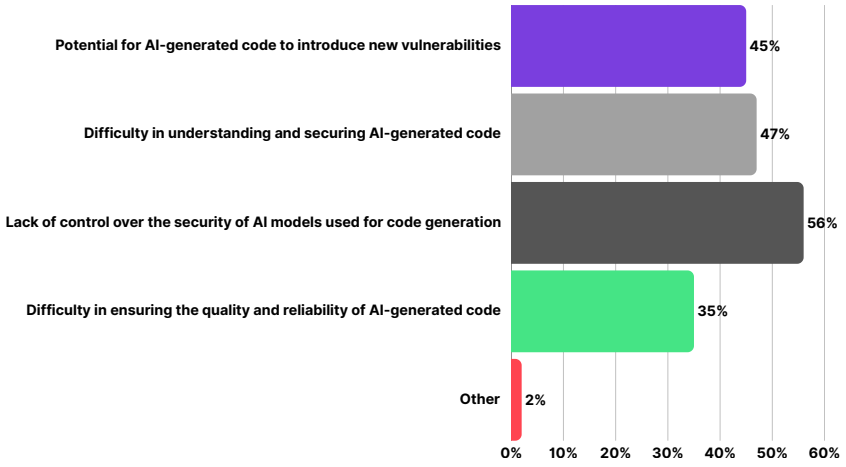
Confidence in Defending Against AI-Driven Attacks

Organizations also expressed uncertainty about their ability to defend against AI-driven threats:

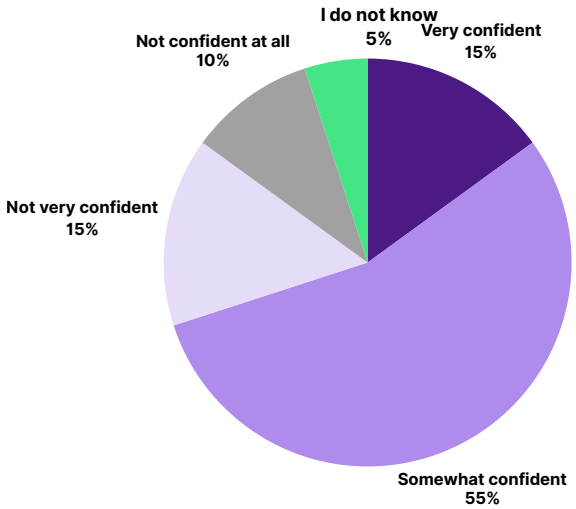
- Only 15% said they are very confident in detecting and responding to attacks leveraging GenAI.
- 55% were somewhat confident.
- 25% admitted they were not confident or not confident at all.

This lack of confidence highlights a readiness gap as attackers increasingly use AI to scale reconnaissance, generate exploits, and automate malicious activity.

What security concerns do you have about using Generative AI to develop APIs?



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



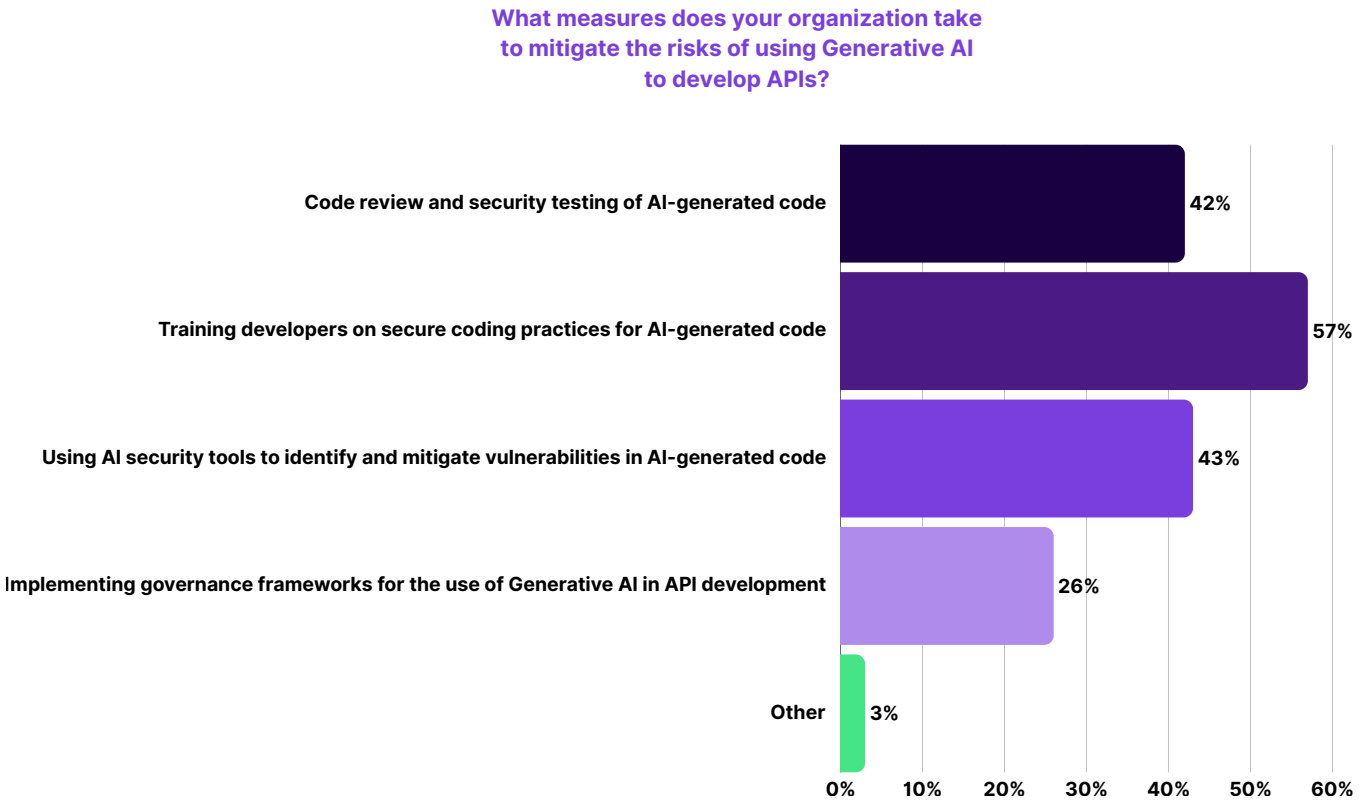
Generative AI and API Security Risks III

Mitigation Strategies

To address these challenges, organizations are beginning to implement GenAI-specific safeguards:

- 42% conduct code reviews and security testing.
- 57% train developers on secure coding practices for AI-generated code.
- 43% are using specialized AI security tools.
- 26% are adopting governance frameworks to establish rules for AI use in development.

Encouragingly, more than half (59%) are also leveraging GenAI within their own security operations to streamline threat detection and risk mitigation. This dual role of GenAI, both as a risk and as a defensive tool, is reshaping how organizations must think about API security.



19

Measuring ROI in API Security

As API ecosystems grow more complex, measuring the return on investment (ROI) in API security has become essential for justifying expenditures and aligning initiatives with business priorities. The 2025 survey highlights how organizations are quantifying the value of their security programs and where gaps exist.

Top ROI Metrics

In the AI era, the ROI of API security is shifting from a defensive calculation of "cost avoidance" to a strategic measure of "innovation enablement." While traditional metrics remain important, leading organizations now justify security investments by their ability to accelerate the development and deployment of new AI-driven services safely.

The top metrics for measuring API security ROI now reflect this dual focus:

- **Accelerating Secure Innovation:** The primary value of a mature API security program is the ability to say "yes" to the business. This is measured directly by increased developer productivity (18%), as robust security practices reduce rework and accelerate development timelines. This allows organizations to seize new market opportunities with AI-powered applications safely.
- **Strengthening Business Resilience:** A strong security posture provides the stable and trusted foundation required for innovation.
- **Improved Risk and Compliance Posture:** A lower enterprise risk score, cited by 18% of organizations, and a strong compliance posture, cited by 26%, are direct outcomes of a proactive security strategy that builds trust and audit readiness.
- **Financial and Operational Stability:** The most direct financial returns are measured by cost savings from breach prevention (18%) and the reduction in API security incidents (9%), which improve system reliability and prevent business disruptions.

The Bigger Picture

Although these metrics provide clear business justification, they represent only part of the value equation. Strong API security also delivers harder-to-measure benefits such as accelerated innovation, improved customer trust, and resilience against emerging AI-driven threats.

To maximize ROI, organizations must ensure that investments in tools, processes, and training translate into measurable improvements in compliance, cost avoidance, and risk reduction. By aligning API security programs with these outcomes, security leaders can demonstrate value to stakeholders while strengthening overall business resilience.

Conclusion and Recommendations

The H2 2025 State of API Security Report highlights both progress and persistent gaps in how organizations approach API security. While APIs have become indispensable for digital transformation, cloud migration, partner enablement, and AI adoption, the rapid pace of growth continues to outstrip the maturity of most security strategies.
Organizations face several recurring challenges: limited visibility into API inventories, inconsistent monitoring practices, resource and budget constraints, and uncertainty around emerging risks such as generative AI. Half of respondents slowed the rollout of a new application due to API security concerns, and one in three experienced a security incident in the past year. These findings underscore the urgent need for more proactive and holistic security strategies.

To close these gaps, organizations should prioritize the following actions:

1. Prioritize Real-Time Monitoring and Runtime Security
Only 20% of organizations monitor APIs continuously in real time. Investments in advanced runtime security and continuous monitoring tools are critical for detecting and stopping attacks before they escalate.

2. Mandate a Real-Time "API Bill of Materials" to Govern AI-Driven Development
You cannot govern what you cannot see. As this report highlights, only 19% of organizations are "very confident" in the accuracy of their API inventories. With GenAI tools poised to dramatically increase the speed and scale of API creation, this visibility gap represents a systemic risk. Security leaders must mandate the use of automated discovery to establish and maintain a dynamic inventory of all APIs, a foundational control for mitigating "shadow APIs" created by new AI-powered workflows.

3. Mature API Security Strategies and Governance
51% of organizations remain in the planning or basic stages of their API security programs. Adopting structured frameworks, such as the OWASP API Security Top 10, NIST, and API posture governance models, provides consistency and resilience.

Conclusion and Recommendations II

4. Shift from Reacting to GenAI Risks to Governing GenAI Usage
With 85% of organizations already using or planning to use GenAI for development, the risks are now embedded in the software lifecycle. Instead of merely reacting to code reviews, leaders should establish a formal governance framework for secure AI/GenAI adoption. This includes setting policies on acceptable model usage, mandating specialized AI security testing tools, and implementing guardrails to prevent the exposure of sensitive data to and from AI models via APIs.

5. Optimize Resource Allocation for ROI
Budget growth has been modest, but leaders are measuring ROI through compliance improvements, breach prevention cost savings, and incident reduction. Demonstrating value requires aligning security investments with these outcomes while also considering long-term benefits such as innovation enablement and customer trust.

Final Note
APIs are now at the heart of digital business. But without stronger visibility, governance, and real-time protections, organizations remain vulnerable to breaches, compliance failures, and reputational damage. By investing in proactive monitoring, advanced security frameworks, and GenAI-specific safeguards, enterprises can transform API security from a reactive burden into a strategic enabler of growth, resilience, and innovation.

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.

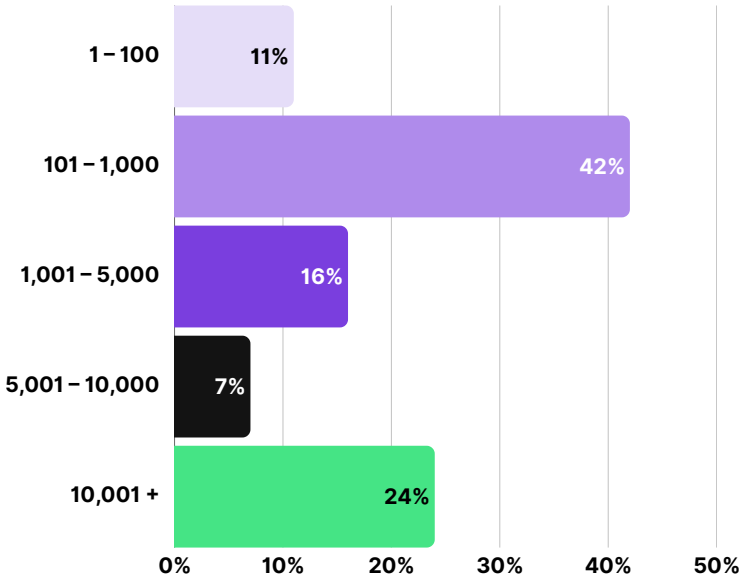
Improves your API security posture – Salt proactively identifies vulnerabilities in your APIs even before they serve production traffic. The platform also uses attackers like pen testers, capturing their minor successes to provide insights for dev teams while stopping attackers before they reach their 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 386 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: