SALT

2025 API Blindspots and Breakthroughs: How CISOs Are Approaching API Risk Survey Report

May 2025

Table of Contents

Introduction and Key Findings

Introduction & Methodology

APIs are at the heart of digital transformation. Whether organizations are launching new customer experiences, streamlining partner integrations, engaging with prospects, or improving internal workflows for employees, they're doing it through APIs. From payroll systems to customer portals, APIs are the connective tissue enabling access to data and functionality at scale. As AI adoption accelerates, and particularly with the rise of agentic AI, API traffic is set to go through the roof.

But while API usage is skyrocketing, is API security keeping pace? Many organizations are only beginning to grapple with the reality that traditional security controls, built for web applications not APIs, are falling short in protecting against today's threats. APIs expose business logic, sensitive data, and core operations. That makes them both a prime target and a strategic vulnerability.

This report captures the voice of the global CISO. It's a peer-driven snapshot of how security leaders are thinking about API risk today. From visibility gaps and auditing delays to overreliance on legacy tools and the slow adoption of purpose-built solutions, the findings paint a picture of an evolving challenge and a security discipline in transition.

We know that you don't have time for hypothetical questions. Instead, we asked CISOs what they're actually doing: how they discover APIs, how often they audit them, whether they have the resources to respond to API alerts in real time, and how confident they really are in their current defenses.

If you're a CISO, this is your opportunity to benchmark yourself against your peers across industries. To see where the gaps are, where maturity is emerging, and where priorities are shifting, so that you can lead your organization with sharper insight and stronger defenses in the API-first era.

Methodology

To get more insight into these important business drivers, we commissioned a survey of 300 CISOs from France, Germany, Italy, the United Kingdom and the United States, all of whom work at companies with more than 1,000 employees. CISOs work across various industries including Financial services, Healthcare, Transportation, Retail and Software.

This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during April 2025. The average amount of time spent on the survey was 5 minutes and 8 seconds. The order of the answers in the majority of the non-numerical questions was randomized, to prevent order bias.

01 | API Security Is a Top Priority — But Only 17% of CISOs Have a Fully Developed Strategy in Place

While 73% of CISOs rank API security as a high or critical priority for the next 12 months, just 17% report having a fully developed and implemented API security strategy. Despite recognition of the growing API attack surface, most organizations remain in early or incomplete stages of securing it, revealing a significant gap between urgency and execution.

02 | Just 19% of CISOs Have Full Visibility Into Their API Landscape

Only 19% of CISOs cite complete visibility and confidence in tracking APIs across their organization. Even among large enterprises, just 27% report full oversight. For smaller organizations, that number drops to 12%. Close to three-quarters (74%) admit to ongoing surprises, constantly uncovering APIs they didn't know existed. This lack of visibility poses a persistent and growing security risk.

03 | Nearly 9 in 10 CISOs Can't Confirm They're Free of Unmanaged APIs

Only 11% of CISOs are confident they have no unknown, unmanaged, or deprecated APIs in production. Nearly half (48%) believe they probably do, highlighting widespread uncertainty and visibility gaps in API environments. Confidence drops further in smaller organizations, where CISOs are nearly three times less likely to feel assured about their API inventory.

04 | Most Companies have a 4-12 Week Visibility Gap in their API Auditing Processes

Despite industry research citing 75% of APIs being updated weekly or even daily, most organizations aren't auditing at the same pace. Two-thirds of CISOs report API audits occur only monthly or quarterly, creating a 4–12 week window of potential blind spots. During this time, unmanaged or shadow APIs can emerge, increasing risk. Only 34% of organizations have adopted continuous, automated auditing to close this visibility gap and match the speed of API change.

05 | Legacy Tools Are the Primary Line of Defense for Most CISOs

To secure APIs, 76% of CISOs rely on WAFs and 72% on API Gateways. Despite their limitations, 85% express confidence that these tools can block business logic attacks—threats they weren't designed to stop. Nearly half (48%) also use them as their primary method for API discovery and inventory. This overreliance creates a false sense of security and leaves critical blind spots, while only 39% of organizations are adopting best-of-breed API security solutions built for today's complex threat landscape.

Survey Report Findings

Is API Security a Priority in CISOs' Cybersecurity Strategy?

As organizations accelerate their digital transformation and increasingly rely on APIs to power everything from mobile apps to interconnected cloud services, the attack surface continues to expand, making API security not just a technical concern, but a strategic business imperative.

As a result, close to three-quarters of CISOs (73%) consider API security a high or a critical priority for the next 12 months. Only 1% of CISOs say that API security is not a priority for the next 12 months, and just 3% extend that view over the next 24 months.

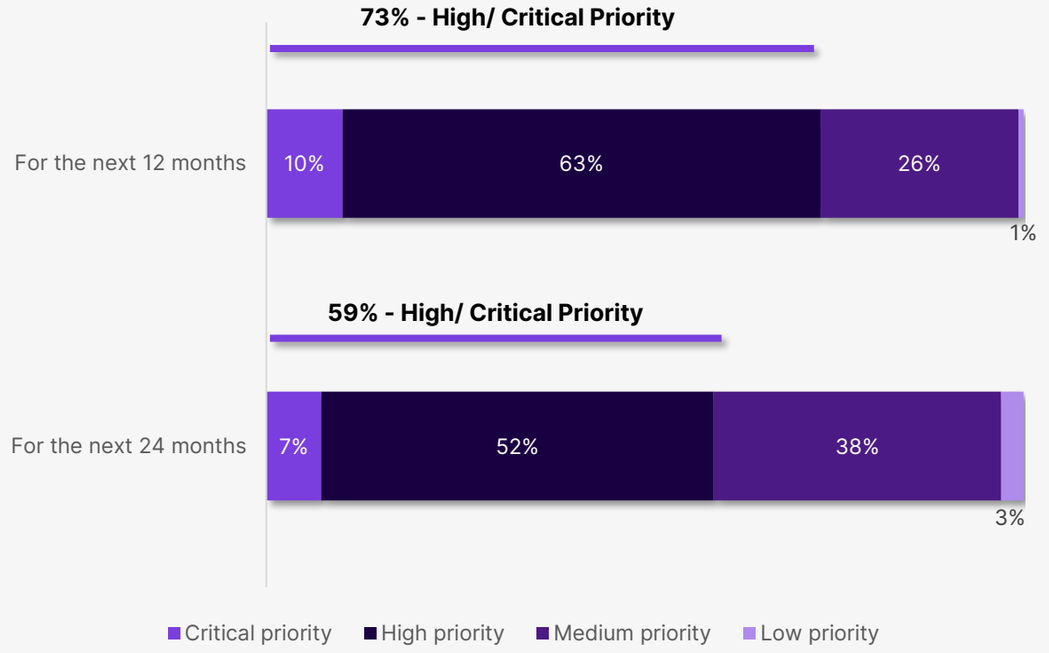

Figure 1: API Security Priority in Cybersecurity Strategy, Next 12 vs. 24 Months

Do CISOs Have a Dedicated API Security Strategy?

The vast majority of CISOs are actively prioritizing API security, with only 1% reporting no current plans to develop a dedicated strategy. Most organizations are still maturing in this area, highlighted by the majority (57%) of CISOs who define their API security strategy as either in progress or just partially developed. However, 17% of CISOs report having a fully developed and implemented strategy in place.

What sets these mature organizations apart? A closer look reveals a clear correlation between company size and API security maturity. Among enterprises with over 10,000 employees, 25% have a fully rolled-out API security strategy, compared with just 8% of companies with fewer than 5,000 employees. This data suggests that scale, complexity, and risk exposure are driving more comprehensive API security efforts in larger organizations.

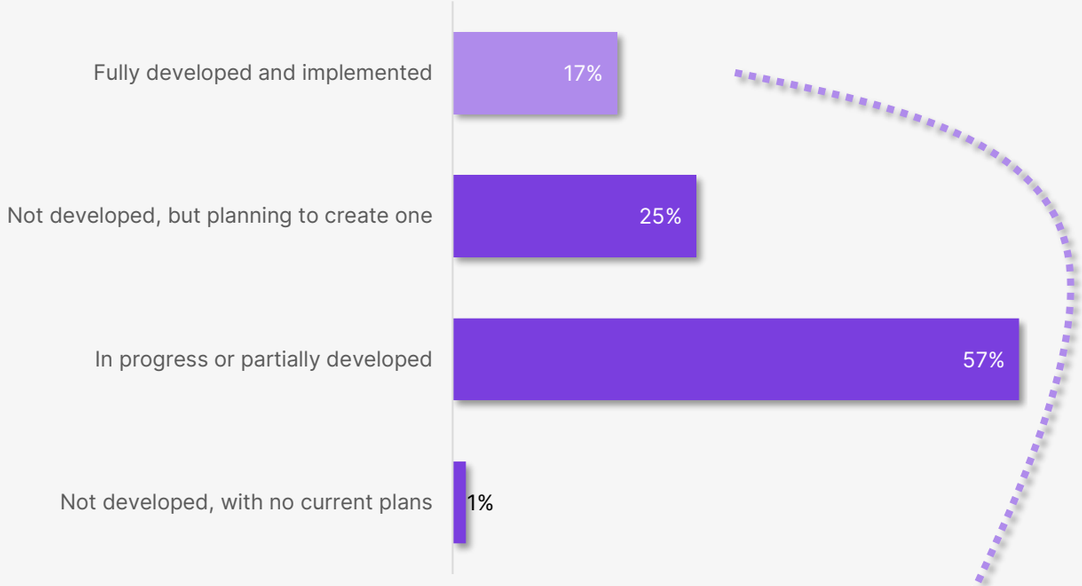

Figure 2: Current Status of Dedicated API Security Strategy

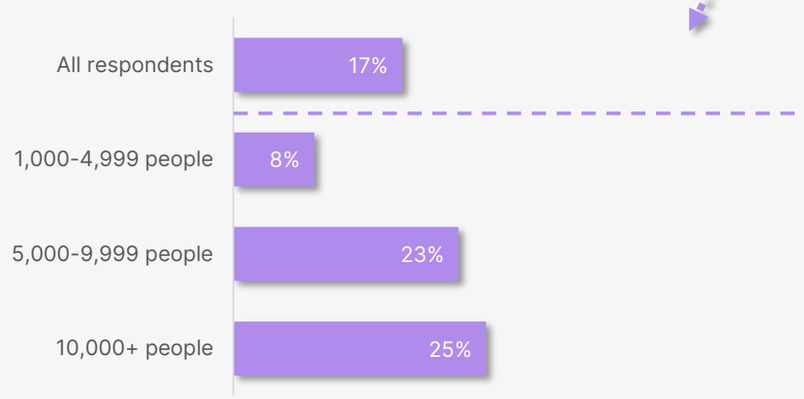

Figure 3: "Fully Developed and Implemented" by Company Size

How Visible is an Organization's API Landscape to its CISO?

We asked CISOs, *"How much visibility do you have into your organization's API landscape, including knowing where all APIs are, how well they're documented, and whether they comply with internal policies?"*

Just 19% of respondents have complete visibility and confidence in tracking all their APIs, while at the other end of the scale, 7% indicate very little to no visibility into their current API landscape.

Notable, 74% of global CISO leaders report having some visibility into their APIs, but that they are frequently surprised to discover new APIs they were previously unaware of. This is a tremendous risk, and one which organizations need to take control over.

When we look in greater detail at the 19% of respondents that have full visibility and confidence, we can see that this is more prevalent in larger companies. 27% of CISOs from enterprises with 10,000+ employees have full visibility, compared with 12% in companies with fewer than 5,000 employees.

It's important to remember that even for large enterprises, we're still finding that more than two-thirds of CISOs cannot claim confidence and oversight over their API landscape. While the problem is more acute for smaller businesses — a lack of API visibility is everyone's concern.

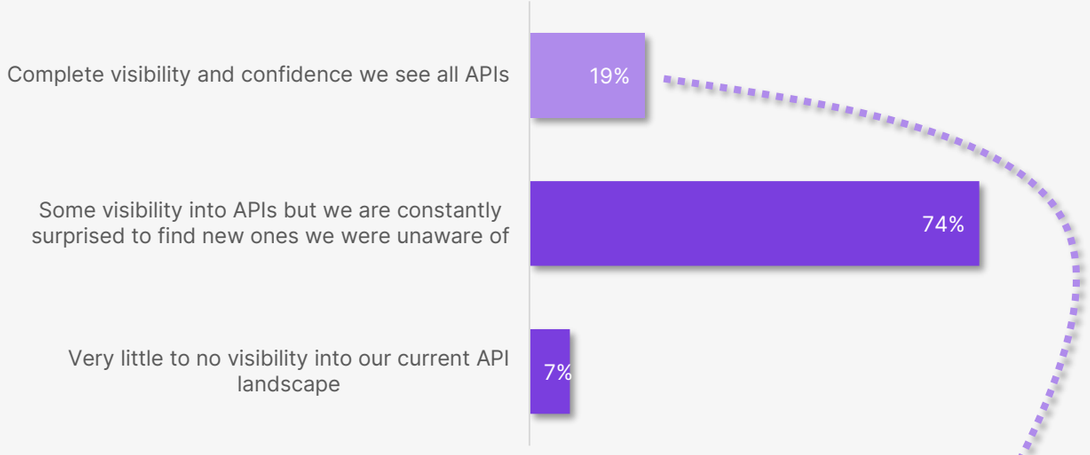

Figure 4: Visibility into Organization's API Landscape

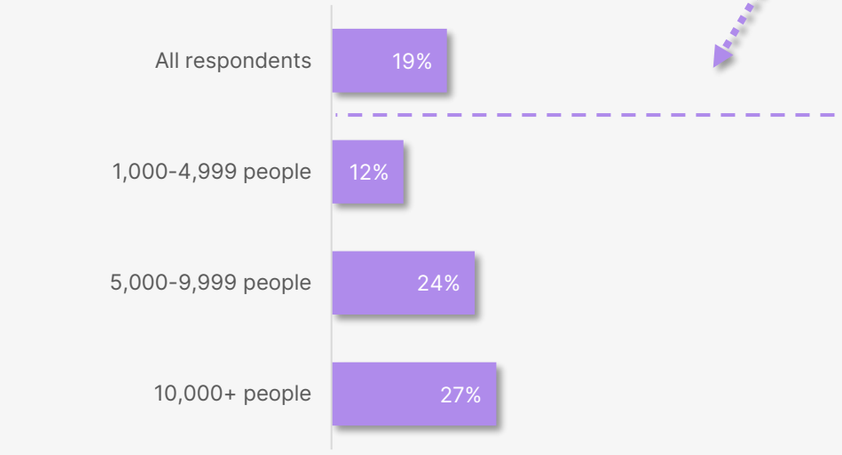

Figure 5: "Complete Visibility" by Company Size

How Organizations Discover and Inventory APIs

All CISOs believe they have a reliable API inventory in place.

However, 48% say API data is pulled from API gateways and WAF logs. While API gateways and WAFs play crucial roles in managing and securing APIs, they may not provide complete visibility into all API endpoints, especially undocumented or "shadow" APIs. This leaves CISOs with gaps which open the business up to risk.

Close to half of enterprises are relying on these traditional and somewhat ineffective methods and as we saw in Figure 4, not getting a full picture of their API landscape as a result.

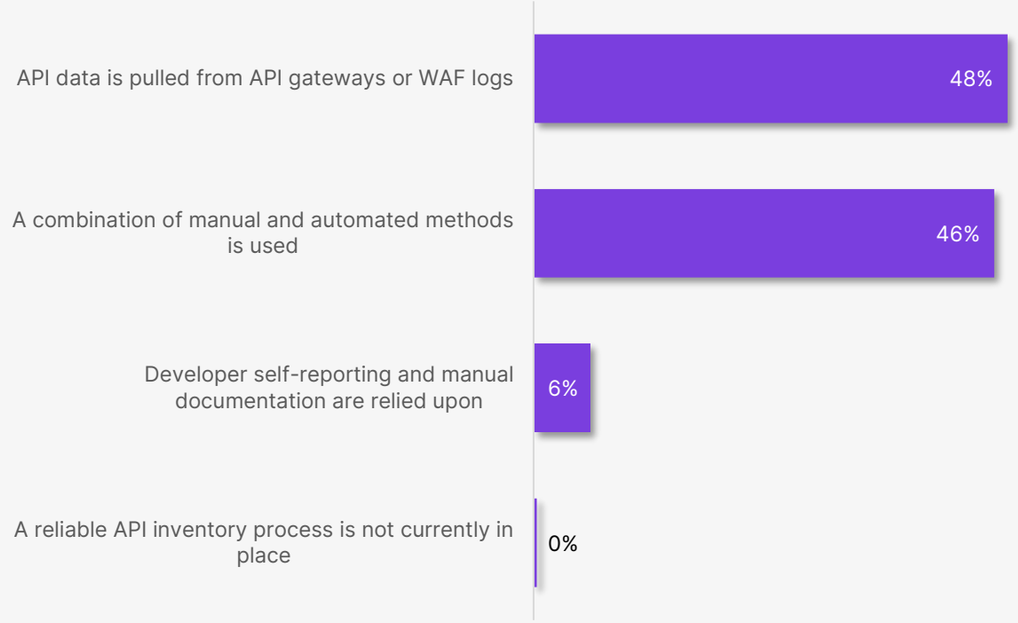

Figure 6: How Organization Discovers and Inventories APIs

Presence of Unknown, Unmanaged, or Deprecated APIs in Production

We asked global CISO leaders whether they believe unknown, unmanaged, or deprecated APIs exist in their production environments. Only 11% expressed confidence that they don't — leaving 89% either unsure or suspecting these risks exist. Close to half of CISOs (48%) admit they probably do.

Unsurprisingly, confidence declines in smaller organizations. CISOs at companies with fewer than 5,000 employees are nearly three times *less* likely to feel confident about the absence of unmanaged or unknown APIs compared to those at larger enterprises. This data suggests that limited resources or visibility may compound the challenge of maintaining full API oversight

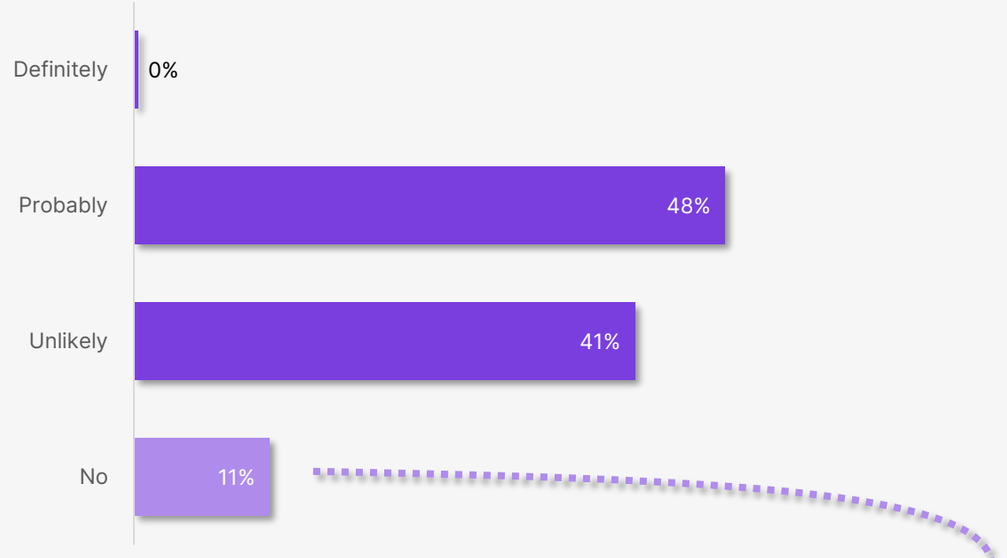

Figure 7: Presence of Unknown, Unmanaged, or Deprecated APIs in Production

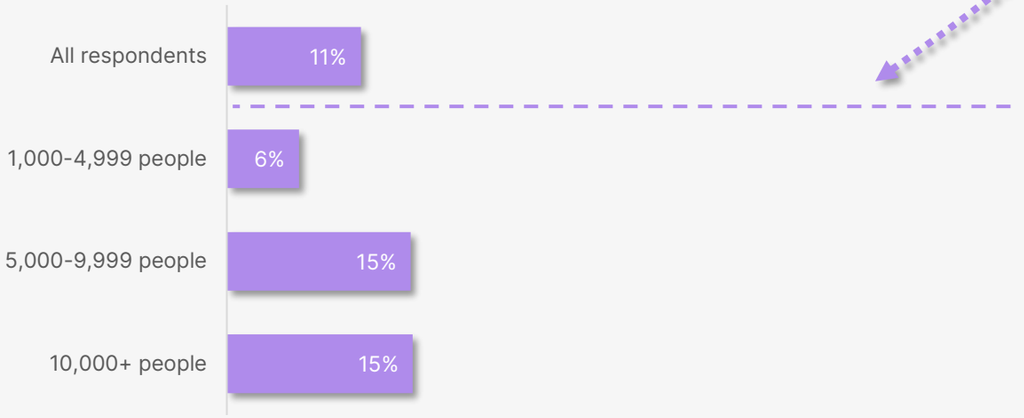

Figure 8: "No" by Company Size

How Frequent are API Inventory Audits for Shadow or Zombie APIs?

All organizations report having some form of auditing process in place to detect shadow or zombie APIs, signaling a strong intent to maintain oversight. However, a significant gap exists between intent and execution.

Industry research shows that 75% of APIs are updated on a weekly or even daily basis, yet our data here uncovers that two-thirds of organizations audit APIs only monthly or quarterly. This creates a visibility gap of 4-12 weeks during which unmanaged changes can introduce risk. Only 34% of organizations have implemented continuous, automated auditing to close this exposure window and keep pace with the rapid rate of API change.

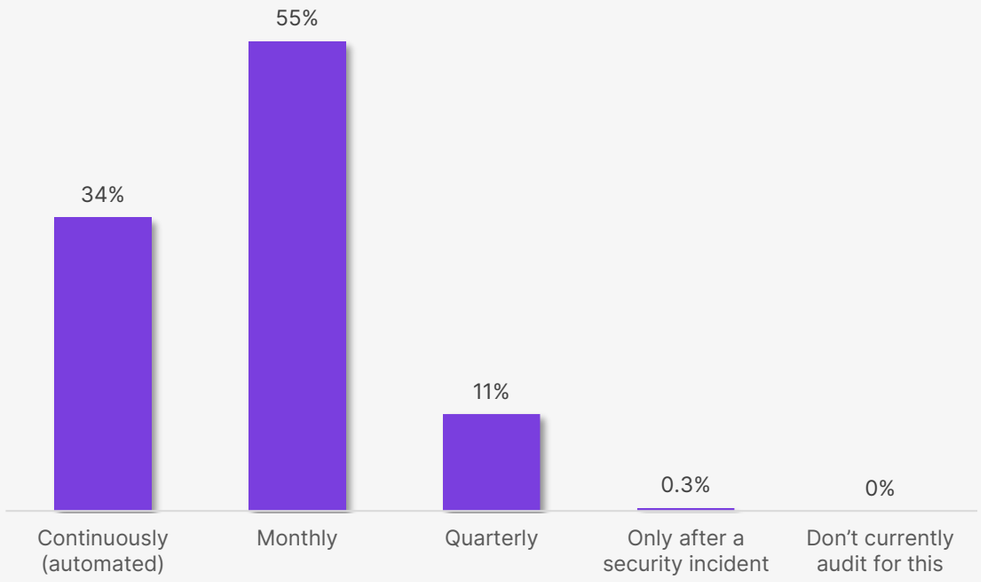

Figure 9: Frequency of API Inventory Audits for Shadow or Zombie APIs

Do CISOs Have the Resources to Respond to API-related Security Alerts in Real Time?

When asked whether they have sufficient tools, personnel, and budget to triage and respond to API-related security alerts in real time, most CISOs indicated they are under-resourced across the board.

Only 26% say they have the right tools in place, just 16% feel adequately staffed, and 26% report having sufficient budget. This shortfall highlights a critical gap between the urgency of API threats and the operational capacity available to respond effectively.

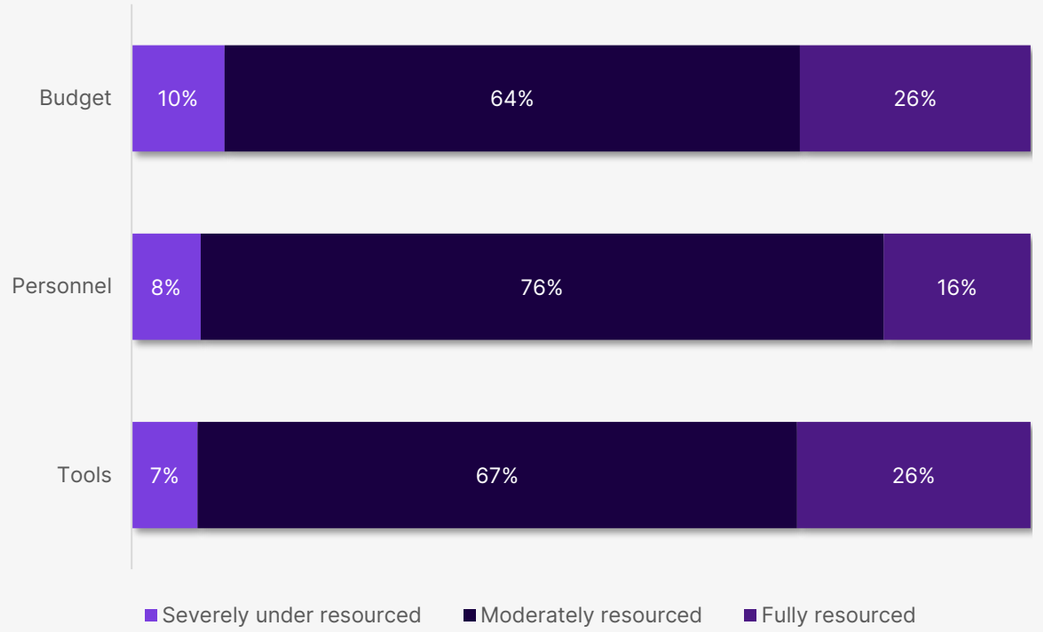

Figure 10: Resources Available for Real-time Response to API-related Security Alerts

Which Controls Are Used by the Organization to Secure APIs?

By asking CISOs which controls are currently in place in their organization, we can get a wide view of how enterprises are protecting themselves from API risk.

The data shows that most organizations are leaning on incumbent technologies to secure their APIs. 76% use Web Application Firewalls (WAFs) and 72% rely on API Gateways. While these tools offer a level of protection, they were not originally designed to address the unique threats APIs face today, they only detect North-South traffic, and they don't pull detailed API payload information that helps organizations to understand posture and risk. As a result, many organizations may assume they have adequate coverage, when in reality, critical gaps remain.

Encouragingly, 39% of respondents are turning to best-of-breed API security solutions. This signals a growing recognition that traditional controls alone are not sufficient for securing modern API environments.

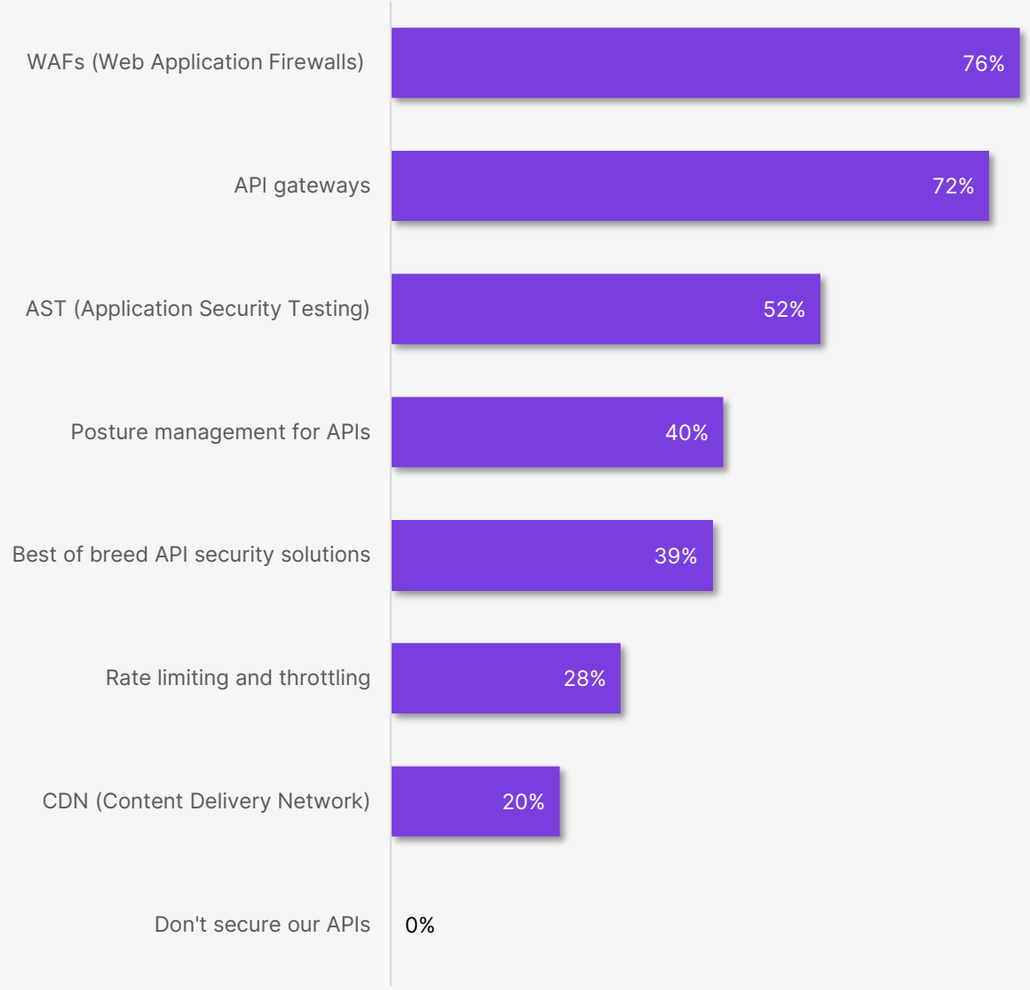

Figure 11: Controls Used by the Organization to Secure APIs

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Confidence in WAFs and API Gateways to Block Business Logic Attacks

85% of global CISOs express confidence that Web Application Firewalls (WAFs) and API Gateways can block business logic attacks. However, this confidence may be misplaced.

These tools were not designed to detect or mitigate the complex, context-aware threats that business logic attacks represent. These attacks exploit the intended functionality of an API rather than leveraging known vulnerabilities. When enterprises rely on legacy perimeter tools as their primary defense, they risk operating under a false sense of security. The result is a dangerous blind spot that leaves critical business processes exposed to sophisticated, targeted exploitation.

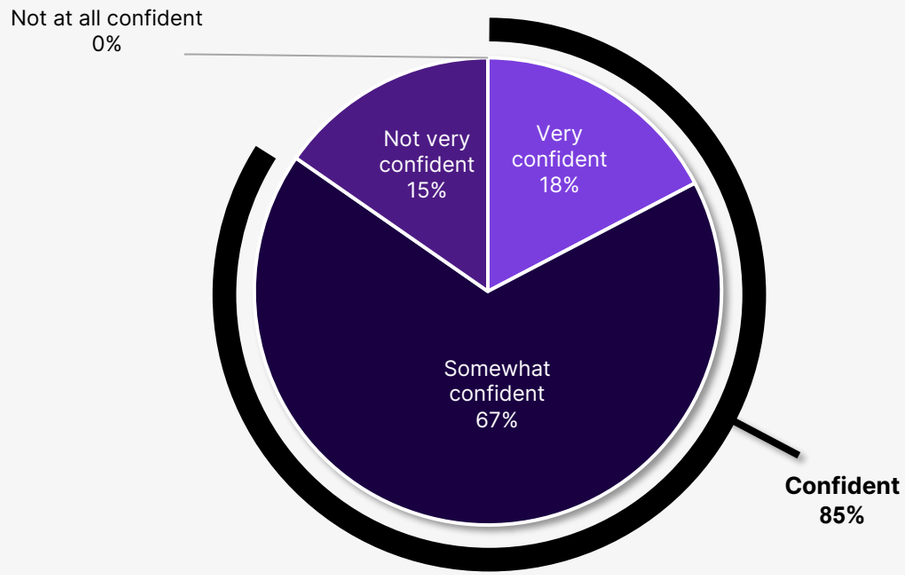

Figure 12: Confidence in WAFs and API Gateways to Block Business Logic Attacks

Demographics

Country, Industry, Company size

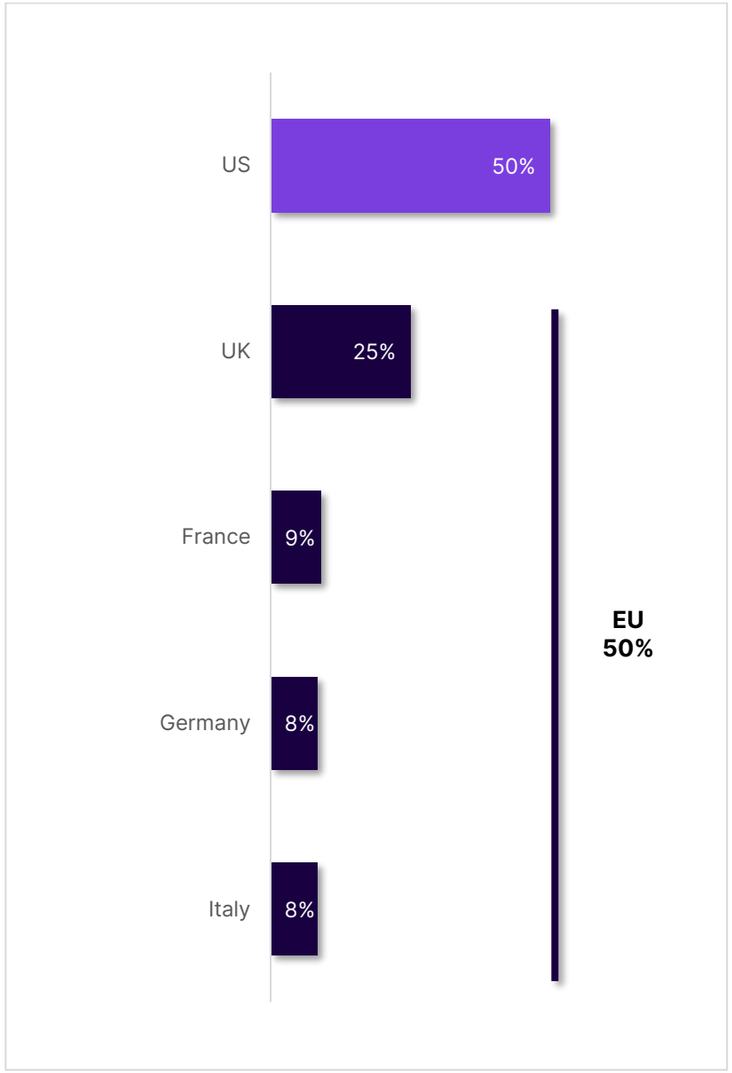

Figure 13: Country

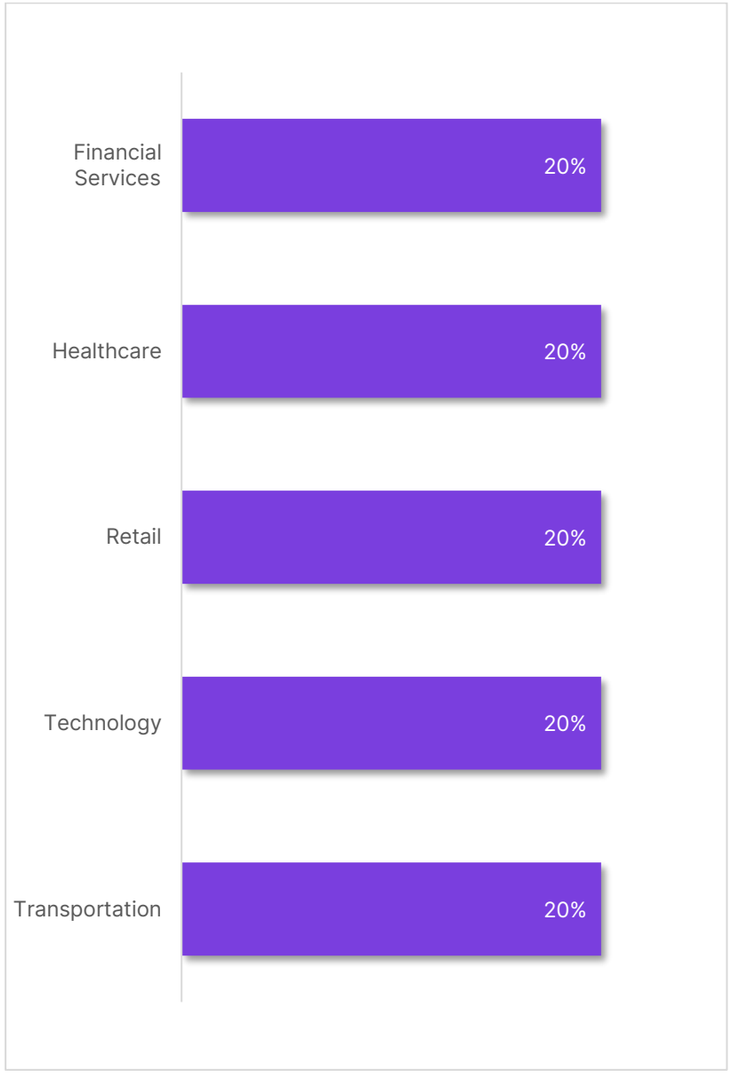

Figure 14: Industry

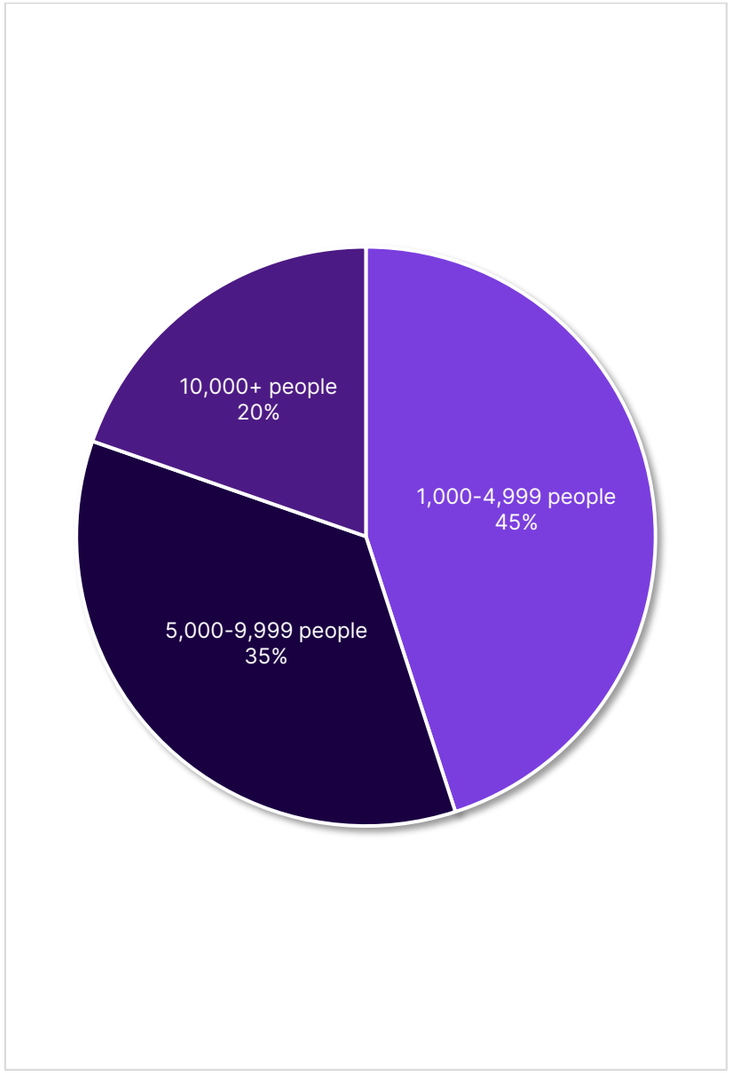

Figure 15: Company size

About Salt Security

Salt Security secures the APIs that power today's digital businesses. Salt delivers the fastest API discovery in the industry—surfacing shadow, zombie, and unknown APIs before attackers find them. The company's posture governance engine and centralized Policy Hub automate security checks and enforce safe API development at scale. With built-in rules and customizable policies, Salt makes it easy to stay ahead of compliance and reduce API risk. Salt also uses machine learning and AI to detect threats early, giving companies a critical advantage against today's sophisticated API attacks. The world's leading organizations trust Salt to find API gaps fast, shut down risks, and keep their businesses moving

Request a Demo

Visit us at:

StateofCISO@salt.security
Phone: +1 214-435-5394