Salt Security Report Reveals Most CISOs Lack Full Visibility into APIs Despite Growing Threat Landscape

A new report by Salt Security found that the majority of CISOs struggle when it comes to API security, with only 17% having a fully developed strategy in place

LONDON, UNITED KINGDOM, July 22, 2025 /EINPresswire.com/ -- New research by Salt Security has revealed that the majority of CISOs do not have full visibility over their API environments, despite recognition of the growing API attack surface. The 2025 Salt Security CISO Report - API Blindspots and Breakthroughs: How CISOs are Approaching API Risk - found that while 73% of CISOs rank API security as a high or critical priority for the next 12 months, only 17% of CISOs reported having a comprehensive and implemented API security strategy, highlighting the growing gap between awareness and action when it comes to API security.

The 2025 research, conducted by Global Surveyz Research, features insights from 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. The CISOs surveyed work across a number of industries including financial services, healthcare, transportation, retail and software.

Organisations are rapidly scaling their API environments to bolster innovation, accommodate growing customer demands and boost operational efficiency. Salt Security's 2025 State of API report revealed that 30% of organisations reported a 51-100% growth in the number of APIs they manage over the past year, with 25% of respondents experiencing growth exceeding 100%. Evidently, APIs play a critical part in an organisation's ability to innovate, especially in the era of AI; however, scale and pace of adoption can strain resources and complicate security efforts. This discrepancy is further underscored by the 2025 CISO report.

Confidence and Visibility

The report also revealed that only 19% of CISOs globally have full visibility and confidence in tracking APIs across their organisation. Among large enterprises, only 27% report full oversight. For smaller organisations, the number shrinks to 12%. This general lack of visibility poses a persistent and growing security risk to organisations, with many easily exploitable shadow APIs potentially lurking within an environment.

What's more, around three-quarters (74%) of CISOs admit to constantly uncovering APIs that

they did not know existed. A further 9 in 10 CISOs can't confirm that they're free of unmanaged APIs, highlighting widespread uncertainty and visibility gaps in API environments. In smaller organisations, CISOs are nearly three times less likely to feel assured about their API inventories.

Innovation vs. Security

Similarly, the report uncovered a disparity between the pace of development, adoption and security, with modern development moving quickly. The research found that three-quarters (75%) of APIs are updated weekly or daily. However, two-thirds (66%) of organisations only audit for shadow or unmanaged APIs on a monthly or quarterly basis. This creates a dangerous window of 4 to 12 weeks of blindspots, allowing unmanaged changes to introduce risk. Only 34% of organisations globally have adopted continuous, automated auditing to close this visibility gap and match the speed of API change.

Protection and Tools

The research found that legacy tools are the primary line of defence 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 that they weren't designed to stop. These tools cannot prevent attacks that exploit legitimate, intended functionalities to access sensitive data; they only detect known signatures of malicious activity. Worryingly, only 39% of organisations are adopting best-of-breed API security solutions built for the changing threat landscape.

"There is an evident overconfidence in legacy tooling to protect against uniquely modern and complex threats," said Michael Callahan, Chief Marketing Officer of Salt Security. "These tools were not built with the threats faced by organisations today in mind, especially as the threat landscape has evolved so quickly and unpredictably in recent years. Legacy tech paired with a lack of visibility over the entire API ecosystem presents a worrying picture for CISOs aiming to secure their organisation effectively. Modern issues need modern solutions that are scalable, efficient and effective."

The Future of API Security

The data shows that a strategic shift is essential to ensuring the security of all APIs. Organisations are under-resourced, revealing that only 16% of security leaders feel they are adequately staffed to triage and respond to the volume of API-related security alerts in real-time. Increasing personnel isn't a scalable solution, rather bridging the gap requires a modern approach that addresses the core themes of speed, visibility and threat detection head-on.

Earlier this year, Salt unveiled Illuminate to revolutionise API security by providing instant, total visibility into an organisation's API landscape. The platform helps CISOs to secure business

innovation. It offers an attacker's view to find and eliminate vulnerable APIs, enforces governance and compliance automatically and uses AI to stop behavioral attacks in real-time.

To read the full report, visit: https://content.salt.security/GWEB-2675-CISO-Report-2025_LP-CISO-Report-2025.html

Methodology

The 2025 research, conducted by Global Surveyz Research, features insights from 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. The CISOs surveyed work across a number of industries including financial services, healthcare, transportation, retail and software.

About Salt Security

As the pioneer of the API security market, Salt Security protects the APIs that form the core of every modern application. Protecting some of the largest enterprises in the world, Salt's API Protection Platform is the only API security solution that combines the power of cloud-scale big data and time-tested ML/AI to detect and prevent API attacks. With its patented approach to blocking today's low-and-slow API attacks, only Salt provides the adaptive intelligence needed to protect APIs. Salt's posture governance engine also delivers operationalised API governance and threat detection across organisations at scale. Unlike other API governance solutions, Salt Security's AI-based runtime engine pulls from the largest data lake in order to continuously train the engine. Salt supports organizations through the entire API journey from discovery to posture governance and threat protection. Deployed quickly and seamlessly integrated within existing systems, the Salt platform gives customers immediate value and protection, so they can innovate with confidence and accelerate their digital transformation initiatives. For more information, visit: https://salt.security/

Charley Nash
Account Manager
charley@eskenzipr.com
Visit us on social media:
LinkedIn