Salt Security Report Reveals 95% of Respondents Experienced API Security Problems Driven by Accelerated API Usage

Research highlights rapidly growing API ecosystems, rising attack activity, and lack of API security maturity

LONDON, UNITED KINGDOM, June 18, 2024 /EINPresswire.com/ -- Salt Security, the leading API security company, today unveiled the findings from the Salt Labs State of API Security Report, 2024. The research, which Salt Security, the leading API security company, today unveiled the findings from the Salt Labs State of API Security Report, 2024. The research, which analysed survey responses from 250 IT and security professionals, combined with anonymised empirical data from Salt customers, highlights a lack of API security maturity and posture governance across organisations, leading to a rise in API security incidents and attack traffic.

> The volume of APIs within organisations are showing no sign of decline, and security teams are struggling to keep pace with the sheer breadth and depth of modern API ecosystems."
>
> *Roey Eliyahu, co-founder and CEO, Salt Security*

The research found that almost all (95%) survey respondents experienced security problems in production APIs, with 23% suffering breaches as a result of API security inadequacies. The volume of APIs within organisations is also accelerating, with Salt customer data showing a 167% increase in API counts over the past 12 months, and nearly two-thirds (66%) of survey respondents indicating that they are managing more than 100 APIs. With increased API usage, comes an expanded API attack surface putting malicious activity on the rise.

The 2024 report also highlights the ongoing lack of API security maturity. Only 7.5% of organisations consider their API security programs to be 'advanced' and alarmingly, over one-third (37%) of the respondents, who have APIs running in production, do not have an active API security strategy in place. Despite this, nearly half (46%) of

respondents stated that API security is a c-level discussion within their organisation.

According to the research, API posture governance strategies, which provide a structured framework for managing and securing the entire API ecosystem from design to deployment, also remain a relatively new phenomenon. Only 10% of organisations currently have an API posture governance strategy in place. However, realising its critical importance, almost half (47%) plan to implement such a strategy within the next 12 months. By deploying and implementing a robust API posture governance engine, organisations can gain complete visibility into their API landscape, eliminate blind spots, and establish corporate-wide security standards and regulations across their entire API ecosystem.

“The volume of APIs within organisations are showing no sign of decline, and security teams are struggling to keep pace with the sheer breadth and depth of modern API ecosystems,” said Roey Eliyahu, co-founder and CEO, Salt Security. “As illustrated by the findings of our research, attackers are continuing to take advantage of this, leveraging weak spots within APIs to execute malicious attacks and gain access to company and customer data. With bad actors constantly refining their tactics to discreetly launch API attacks, often through legitimate means, it requires organisations to take a more sophisticated approach to securing APIs. One that encompasses strong API discovery capabilities, a posture governance strategy, and the ability to quickly and efficiently detect active threats and malicious API traffic.”

Additional key findings from the 2024 State of API Security Report include:

The threat of API attacks is growing
- The research revealed that API security incidents are on the rise.
- API security incidents more than doubled within the past 12 months, with 37% of respondents experiencing an incident, compared to just 17% in 2023.
- Salt Labs analysis of customer data found that attackers are using a diverse range of tactics, with a significant portion bypassing authentication protocols. - Almost two-thirds (61%) of attacks are unauthenticated.
- Internal APIs are also vulnerable, with 13% of attack attempts explicitly targeting them.

Zombie APIs remain a top concern amongst respondents
- Respondents expressed high levels of concern about the potential risks associated with "Zombie" APIs -he outdated, forgotten APIs within ecosystems.
- An alarming 70% highlight Zombie APIs as a great or strong concern, up from 54% in 2023.
- Account takeover and denial of service top the second and third concern, respectively.

API discovery remains a challenge
- API discovery was highlighted as an ongoing hurdle for many organisations.
- Only 58% of organisations have processes in place to discover APIs across their infrastructure.
- Less than 15% of respondents are very confident that they understand which APIs expose personal identifiable information (PII).

Traditional methods are insufficient for protecting against modern attacks
- Only 21% of respondents believe that their current API security approaches are effective in protecting against API attacks, signalling issues with existing methods.
- API gateways (54%), analysing log files (45%) and web application firewalls (WAFs) (42%) are the most common tools organisations are leveraging to detect and prevent malicious API activity but remain insufficient and lack user confidence.

API updates take place more frequently and organisations struggle to keep pace with documentation
- The rapid change of APIs, combined with the increasing use of AI-generated APIs, has rendered traditional documentation methods obsolete.
- Over a third of organisations update their APIs at least once a week (38%), and a significant portion (13%) make daily updates.
- Only 12% of respondents feel very confident in the accuracy of their API inventory, highlighting a widespread lack of trust in security posture.

Attackers are following OWASP Top 10
A large percentage of API attacks target well-known security weaknesses outlined in the OWASP API Security Top 10 list.
- 80% of attack attempts leverage one or more of the Top 10 methods outlined on the list.
- Despite this established knowledge base, only 58% of organisations prioritise protection against the API threats outlined by OWASP.

The State of API Security Report, 2024, was compiled by researchers from Salt Labs, the research division of Salt Security, utilising survey data from nearly 250 respondents across a range of job responsibilities, industries, and company sizes, globally. 20% of respondents were executive-level security or IT leaders, and another 18% within platform or DevOps teams. Technology and financial services companies—widely viewed as the forefront of API usage —comprised 37% of respondents. Companies large and small were evenly represented. The report also includes real-world API attack attempt data from the Salt Security API Protection Platform. This customer data is anonymised, aggregated, and then analysed by Salt's researchers to identify critical trends that can help educate the broader security industry.

To download a copy of the full report, please visit: https://content.salt.security/state-api-report.html

A comprehensive blog exploring the findings also be found here: https://salt.security/blog/increasing-api-traffic-proliferating-attack-activity-and-lack-of-maturity-key-findings-from-salt-securitys-2024-state-of-api-security-report

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 organisations 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
charley@eskenzipr.com
Eskenzi PR
