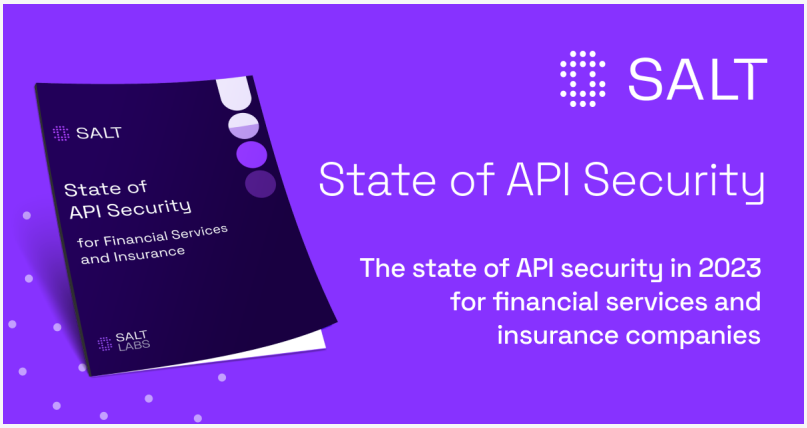
Salt Security Report Identifies API Vulnerabilities and Attacker Activity in Financial Services and Insurance Companies

Industry-focused report shows nearly 70% of financial services and insurance companies have suffered rollout delays due to API security.



The Salt Security State of API Security in 2023 for Financial Services and Insurance Companies report

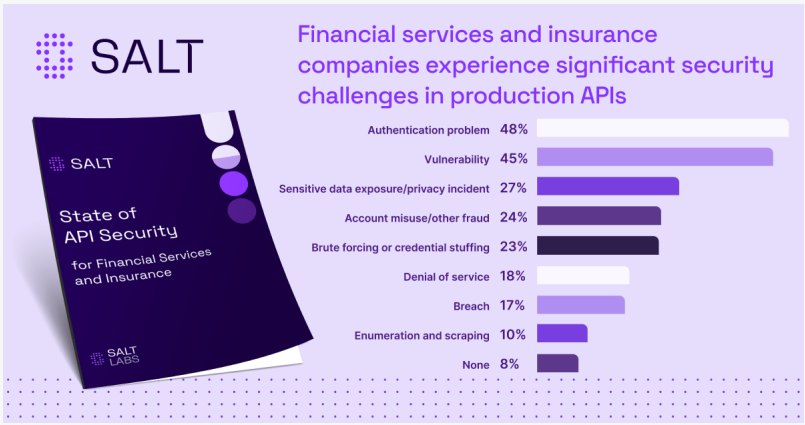
LONDON, UNITED KINGDOM, July 19, 2023 /EINPresswire.com/ -- Salt Security, the leading API security company, today released findings from its first industry-focused report on API security, the 2023 "State of API Security for Financial Services and Insurance." The report combines empirical data from Salt customers and findings from two separate surveys to provide an in-depth analysis of the impact of API security threats and vulnerabilities on these industries.

> APIs are essential for the innovative digital services being delivered today by financial and insurance organisations."
>
> *Roey Eliyahu, CEO and co-founder of Salt Security*

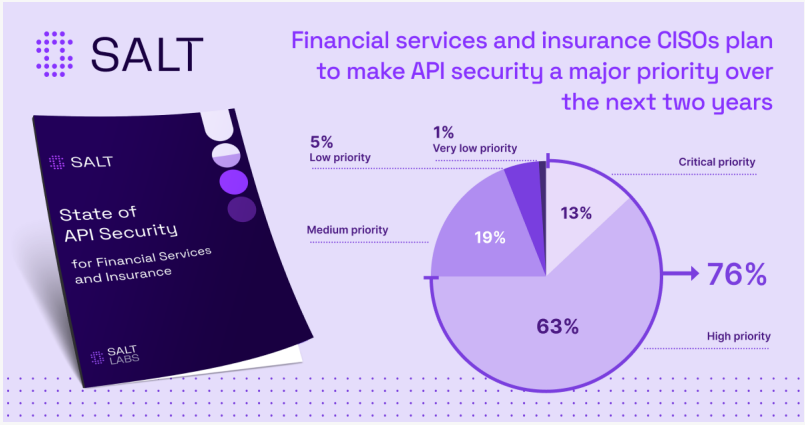
The results found API attackers targeting financial services and insurance APIs have become increasingly active, with a 244% increase in unique attackers between the first and second halves of last year. In addition, 92% of financial/insurance respondents say they have experienced a significant security issue in production APIs over the past year, and nearly one out of five have suffered an API security breach. Top findings include:

- 69% of financial services/insurance respondents say they have experienced rollout delays due to API security issues – 11% higher than the overall response average
- 17% of respondents have experienced an API-related security breach
- 84% of attacks against financial services/insurance sectors came from "authenticated" users who appeared legitimate but were actually attackers

• 71% of financial/insurance respondents say their existing tools are not very effective in preventing API attacks
• More than 25% of respondents say they have no current API strategy



The Salt Security State of API Security in 2023 for Financial Services and Insurance Companies report



The Salt Security State of API Security in 2023 for Financial Services and Insurance Companies report

"APIs are essential for the innovative digital services being delivered today by financial and insurance organisations," said Roey Eliyahu, CEO and co-founder of Salt Security. "However, because these APIs transport sensitive customer and financial information, cyber criminals also know they share a wealth of data that can be leveraged for theft or fraud. The findings show these companies are suffering significant increases in attackers and other security issues, increasing their vulnerability to API-related incidents."

Securing APIs to protect new digital services is a business priority
API security breaches can cost businesses in fines, loss of customer trust, and reputational damage. Also costly are delays in application rollouts or rollbacks of new applications. Given the importance of digital services as a business driver in these industries, API security has become a critical issue, as highlighted by the following findings:

• 56% of financial services/insurance respondents say API security is now a C-level issue (8% higher versus the overall response average at 48%)
• 79% of financial services/insurance CISOs say that API security is a higher priority today than two years ago
• 76% of financial services/insurance CISOs say their organisations have made API security a planned priority over the next two years, with 13% saying it will be a critical priority

"Given the growing importance of APIs over the last several years for enabling modern businesses, it is surprising that API security has become mainstream only recently," said Jeff Farinich, SVP technology and CISO at New American Funding. "The fact that security frameworks and regulations are slow to evolve is partly to blame, but I see hope on the horizon. The Federal Financial Institutions Examination Council (FFIEC), which usually takes years to issue a new

mandate, in just one year explicitly called out APIs as a separate attack surface, requiring financial institutions to inventory, remediate, and secure API connections."

Despite rising attacks, financial services/insurance lack adequate protection for APIs
Financial services/insurance respondents say they are not prepared or taking the right measures to protect APIs from threats:

- 28% of respondents – all with APIs running in production – say they have no current API strategy
- 42% of respondents have little confidence in understanding which APIs expose PII
- Just 13% of respondents consider their API security programs advanced
- 25% of respondents say their current API security strategy doesn't focus enough time on documenting APIs
- Only 42% of respondents identify API security gaps during production/runtime, which is where actual attack activity occurs

Financial services/insurance respondents also cited outdated/zombie APIs as their number one API security concern at 48% – nearly 35% higher than second top API security concern cited, account takeover (ATO).

Other notable findings from the State of API Security for Financial Services and Insurance include:

- 9% of API attacks against financial/insurance institutions targeted internal APIs, representing a 613% increase between the first and second halves of last year
- 61% of financial/insurance respondents manage more than 100 APIs, and 36% manage more than 500
- 27% say they have more than doubled their APIs over the past year
- Respondents most value the ability to stop attacks (49%) in an API security platform, followed closely by meeting compliance/regulatory requirements (48%)
- While 36% of respondents update their APIs at least weekly, only 10% update documentation at the same pace

Methodology
"The State of API Security for Financial Services and Insurance" report was compiled using data obtained from the "Q1 2023 State of API Security Report," empirical customer data from the Salt Security API Protection Platform cloud-based data lake, the independent "State of the CISO 2023" survey, and vulnerability research from Salt Labs, the research arm of Salt Security. A full copy of the report can be downloaded here.

About Salt Security
Salt Security protects the APIs that form the core of every modern application. Its patented 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. By correlating activities across millions of APIs and users over time, Salt delivers deep context with real-time analysis and continuous insights for API discovery, attack prevention, and hardening APIs. 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
Eskenzi PR
+44 7881202324
email us here