Rampant API Growth Causing Cybersecurity Risks for Businesses

March 20, 2024

- *Fastly survey reveals that 9 out of 10 decision-makers know that APIs are a trojan horse for cyber-attacks - but most don't invest in advanced security*
- *UK is marginally ahead of the pack - but financial services sector shows a lack of urgency over the risk of reputationally-damaging cyber breaches*
- *Single provider security solutions and AI could provide answers*

LONDON--(BUSINESS WIRE)-- A recent survey of 235 IT and cybersecurity decision-makers commissioned by Fastly, Inc. (NYSE: FSLY), one of the world's fastest edge cloud platforms, has found that - despite the critical role of APIs - the vast majority of commercial decision-makers are ignoring the burgeoning security risk for businesses. Application Programming Interfaces (APIs) have long been recognised as a bedrock of the digital economy and recent figures suggest that the majority of all internet traffic is now directed via APIs.

Lack of advanced API security endemic

The ubiquity of APIs means they have become one of cybercriminals' favourite gateways for account takeover attacks. In a recent survey by Fastly, 84% of respondents admitted to not having advanced API security in place.

The lack of action on API breaches comes despite the vast majority of decision-makers knowing there is a problem. 95% of respondents surveyed by Fastly said they had experienced API security problems in the last twelve months. Over three quarters (79%) had delayed the rollout or integration of a new application due to API security concerns. In addition, 79% claim to place a 'high or very high' level of importance on API security. Asked why none of this has translated into action, 'insufficient budget' and a 'lack of expertise' were the most commonly stated reasons.

Risk of operational and reputational damage

Jay Coley, Senior Security Architect at Fastly, said: "The results of our survey show that decision-makers know that increased reliance on APIs creates a risk of serious cyberattacks. But so far they are not doing enough about it. This is surprising given that the operational and reputational cost of a breach far outweighs the price of deploying a consolidated web application and API security solution from a single provider."

Key areas of concern

Asked which attributes of an API security platform would be the most important to their company, respondents said number one would be identifying which APIs expose personal or sensitive data (43%). Other top concerns included identifying all APIs, including those that are undocumented (40%) and logging and monitoring (28%). However, companies are increasingly struggling to identify API attacks because of the sheer volume of notifications that they receive using legacy security solutions.

In Fastly's experience, credential stuffing, business logic abuse, and DDoS attacks are just a few of the malicious automated bot attacks that are being deployed to take over accounts and perpetrate identity theft and fraud. Readily available scripts and tools make orchestrating API attacks easier than ever, and legacy bot defence techniques struggle to detect these potentially devastating incursions.

AI security solutions untapped – but coming

One solution to the complexity of the API landscape could be a new generation of AI-powered cybersecurity systems, but Fastly found there is currently little enthusiasm for this. Only 14% of companies surveyed regarded the use of AI technologies in API security as a priority. That said, 58% anticipate that generative AI will have a 'large or very large' impact on API security over a window of approximately 2-3 years.

Sector-based and regional variations

One concerning aspect of Fastly's survey is that heavily-regulated sectors dealing with sensitive data are some of the worst culprits when it comes to API inaction. Only 80% of respondents in financial services placed a high or very high level of importance on API security. This compares with 89% in wholesale, retail and e-commerce.

In terms of regional variations, the importance of API security was rated highly in the UK (86%) compared to a cross-border average of 79%. Zombie APIs and data scraping were cited by UK firms as priorities. Despite this, there was still a tendency in

the UK not to translate thoughts into actions. “79% of UK participants said their API security was not advanced,” notes Coley, “compared with 84% across the board. This represents a huge target for increasingly sophisticated cyber criminals to aim at.”

One intriguing insight is the gulf in attitudes within company hierarchies. 91% of C-suite and compliance experts place ‘a high or very high’ level of importance on API security but only 74% of in-house security specialists feel the same way. The implication, perhaps, is that the security cohort is underestimating the scale of the threat – either that or they are exposed to a wider pool of threats on a day to day basis.

To read the full report and understand how businesses can help establish a secure digital environment, visit https://learn.fastly.com/api-security-study-24.html.

About the research

This research surveyed 235 key IT and cybersecurity decision-makers in large organisations spanning multiple industries across the UK, France, Spain, the Nordics and DACH region.

About Fastly

Fastly’s powerful and programmable edge cloud platform helps the world’s top brands deliver some of the best online experiences possible through edge compute, delivery, security, and observability offerings improving site performance, enhancing security, and empowering innovation at global scale. Compared to legacy providers, Fastly’s powerful and modern network architecture is one of the fastest on the planet, empowering developers to deliver secure websites and apps with rapid time-to-market and industry-leading cost savings. Organisations around the world trust Fastly to help them upgrade the internet experience, including Reddit, Wendy’s, Stripe, Neiman Marcus, Universal Music Group, SeatGeek, and Advance Publications. Learn more about Fastly at https://www.fastly.com, and follow us @fastly.

Source: Fastly, Inc.

Media Contact:

Alex Klepel

press@fastly.com

Investor Contact:

Vernon Essi, Jr.

ir@fastly.com

Source: Fastly, Inc.