AI-First Businesses are Paying an “AI Speed Tax” when Recovering from Cybersecurity Incidents, according to Fastly’s Global Security Research Report

February 25, 2026

Fast moving AI adopters are paying the price with 80 day longer recovery times, higher breach costs and expanding attack surfaces

SAN FRANCISCO--(BUSINESS WIRE)-- Fastly, Inc. (NASDAQ: FSLY), a leader in global edge cloud platforms, today published the findings from its fourth annual Global Security Research Report. It reveals that AI-first businesses – those integrating AI into key processes and offerings from the outset rather than as a secondary enhancement – are paying an AI tax by failing to modernize security in step with AI’s rapid expansion across IT infrastructure. These businesses report taking nearly seven months on average to fully recover from cybersecurity incidents, 80 days longer than businesses that do not identify as AI-first.

The implications of this AI Speed Tax are significant in today’s real-time economy. The financial toll of a cybersecurity incident for AI-first businesses exceeds that of non-AI-first businesses by more than 135%. This increased financial impact reflects both the longer recovery timelines and a higher rate of AI-specific compromise. In fact, almost half (44%) of AI-first organizations claim that AI was directly exploited in their most recent security incident, compared to just 6% for non-AI-first organizations. These findings highlight how AI-native systems expand the potential attack surface, introducing new layers like agentic workflows and decentralized data flows, all of which complicate defense.

“The speed of AI adoption is reshaping security infrastructure almost overnight. For AI-first businesses, the priority isn’t to slow down innovation — it’s to modernize security at the same rate that AI is transforming their infrastructure,” said Marshall Erwin, CISO at Fastly. “That means securing AI and inference infrastructure, monitoring and throttling unwanted AI crawler activity, anticipating the rise of shadow AI and shoring up your outer perimeter.”

Meanwhile, more than a third (34%) of AI-first organizations say that AI use led to a security oversight or blind spot that contributed to their last security incident, compared to 20% for non-AI-first organizations. This points to a growing challenge in visibility, control, and enforcing AI use policies. As AI becomes more embedded across operations, it’s getting harder for security teams to map where and how AI is being used, or to isolate its role in incident recovery.

At the same time, practices such as AI scraping are adding cost and complexity to already stretched infrastructure, driving operational disruption and pushing spend into six-figure territory.

“There is a major shift happening in terms of what organizations are responsible for defending,” continued Erwin. “The challenge is no longer confined to malicious actors and isolated security incidents. Instead, it's about managing an infrastructure footprint that is growing rapidly and, often, invisibly.”

For many businesses, these risks are no longer theoretical; they’ve become a reality. AI scraping alone has become a material cost center for nearly two-thirds (64%) of organizations, with average annual infrastructure impacts exceeding $348,000.

These costs are just the beginning. Almost half of organizations (43%) have seen infrastructure expenses increase as a direct result of AI activity, while 40% have faced operational disruption, and 29% reported issues impacting online visitors – from sluggish load times to broken functionality. For many, the reality is creeping costs and architectural complexity.

To respond, organizations are investing heavily in security tools built for this new era. Agentic discoverability (56%), API security (55%), and web application firewalls (54%) have emerged as the leading areas of investment. However, the response is far from complete; three in four (75%) respondents are concerned about Distributed Denial-of-Service (DDoS) attacks targeting AI agents, and more than half (53%) acknowledge they have an increased need for AI-specific security expertise to effectively defend their systems.

“From unmonitored agentic activity to escalating scraping costs, the risks are real, operationally and commercially. As a result, Web Application and API Protection (WAAP) tools are becoming business-critical solutions because they provide essential visibility and control organizations need to secure innovation at the edge,” noted Erwin.

To find out how to modernize your organization’s security infrastructure and implement steps to recover more quickly from cybersecurity incidents, download the report today.

About the research

This research surveyed 2,000 key IT decision-makers with an influence in cybersecurity, in large organizations spanning multiple industries across North, Central and South America, Europe, and Asia-Pacific. The interviews were conducted online by Sapio Research in Q4 2025 using an email invitation and an online survey.

About Fastly, Inc.

Fastly's powerful and programmable edge cloud platform helps the world's top brands deliver online experiences that are fast, safe, and engaging through edge compute, delivery, security, and observability offerings that improve site performance, enhance security, and empower innovation at global scale. Compared to other providers, Fastly's powerful, high-performance, and modern platform architecture empowers developers to deliver secure websites and apps with rapid time-to-market and demonstrated, industry-leading cost savings. Organizations around the world trust Fastly to help them upgrade the internet experience, including Reddit, Universal Music Group, and SeatGeek. Learn more about Fastly at https://www.fastly.com, and follow us @fastly.

Media Contact
Stacey Hurwitz
press@fastly.com

Investor Contact
Vernon Essi, Jr.
ir@fastly.com

Source: Fastly, Inc.