new relic

2026 REPORT FINANCIAL SERVICES

OBSERVABILITY FORECAST



For financial services, compliance still sets the pace of observability adoption, but AI is closing fast.

Security, governance, risk, and compliance is the top driver, narrowly ahead of AI applications and agentic AI systems. In such a regulated industry, those forces increasingly point in the same direction: you cannot govern what you cannot see, and you cannot deploy AI responsibly without observing it.

This is the key tension in this year's Observability Forecast for financial services. Organizations are adopting AI application and agentic monitoring more cautiously than the broader market, but closing that gap fast. They are cautious about deploying AI-native tooling ahead of governance frameworks, but unwilling to fall behind once the frameworks catch up.

METHODOLOGY

New Relic, in partnership with Enterprise Technology Research (ETR), produced this industry analysis of the Observability Forecast 2026. This report analyzes responses from 278 IT and engineering leaders and practitioners in Financial Services, drawn from this year's global study of 2,575 respondents.

Insurance and banking/financial institutions are among the most likely of any industry to expect increasing AI investment over the next year.

"The State of AI in 2026" McKinsey & Company, August 2026

This year's forecast draws on 278 financial services respondents, the fourth-largest industry represented behind IT, Manufacturing, and Retail/Consumer. Their answers tell a more disciplined version of the same global story: AI is making software faster to build and harder to run, which matters in an industry where an unmonitored system represents compliance exposure.



KEY FINDINGS

Compliance is the biggest driver of observability demand—though AI is close behind.

The top trends are security, governance, risk, and compliance (43.9%), adoption of AI applications (36.0%), and adoption of agentic AI systems (34.5%). This flips the global order, where AI applications lead, reflecting the industry's regulatory-first posture.

The industry lags on AI observability now, but is catching up fast.

41.7% of financial services organizations currently deploy AI application observability (vs. 46.7% globally), and 37.8% monitor agentic AI systems (vs. 44.2%). With near-term plans included, the trajectory reaches roughly 83% for AI monitoring and 75% for agentic monitoring—closing most of the gap within a year.

AI-generated code has made observability essential—but less than other industries.

78.4% of financial services leaders agree or strongly agree that AI-generated code makes reliable observability more critical (31.3% strongly agree), compared to 82.6% globally. Disagreement is also a bit higher (8.3% vs. 5.2% globally)—a small but notable pocket of skepticism in an otherwise AI-forward sector.

A meaningful share of AI agents are running unmonitored.

About one in three financial services companies (34.2%) actively monitor their AI agents in production, but another 21.6% have deployed agents with no monitoring. Almost two in five companies with live agents can't see what those agents are doing. That's a smaller gap than the global average (24.6%), but still the biggest operational risk in the data.

Outages are less frequent and less costly at the high end than the market overall.

29.5% of financial services organizations experience a high-business-impact outage weekly or more often, versus roughly 36% across all industries. The sector also reports lower average and median cost-per-hour of downtime, consistent with its heavier investment in automation and incident response.

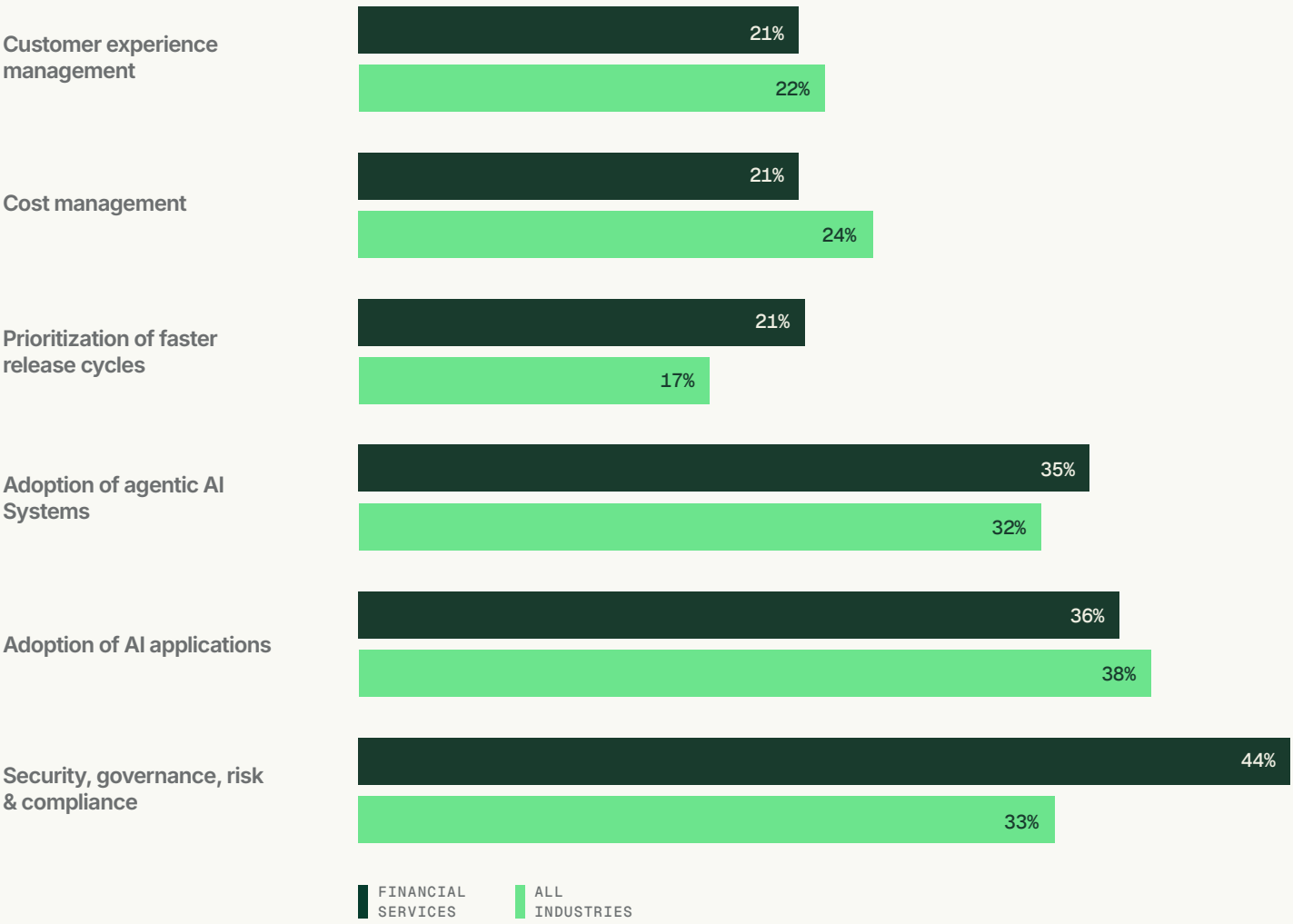
Tool sprawl is creeping back everywhere—but more slowly in financial services.

The average organization now runs 4.75 observability tools, up from 4.51 last year (+5%), a gentler climb than the broader market's jump from 4.4 to roughly 5.1 (+15%). The sector still runs fewer tools than average, a sign consolidation is holding even as AI-specific tools tempt the market to re-fragment.



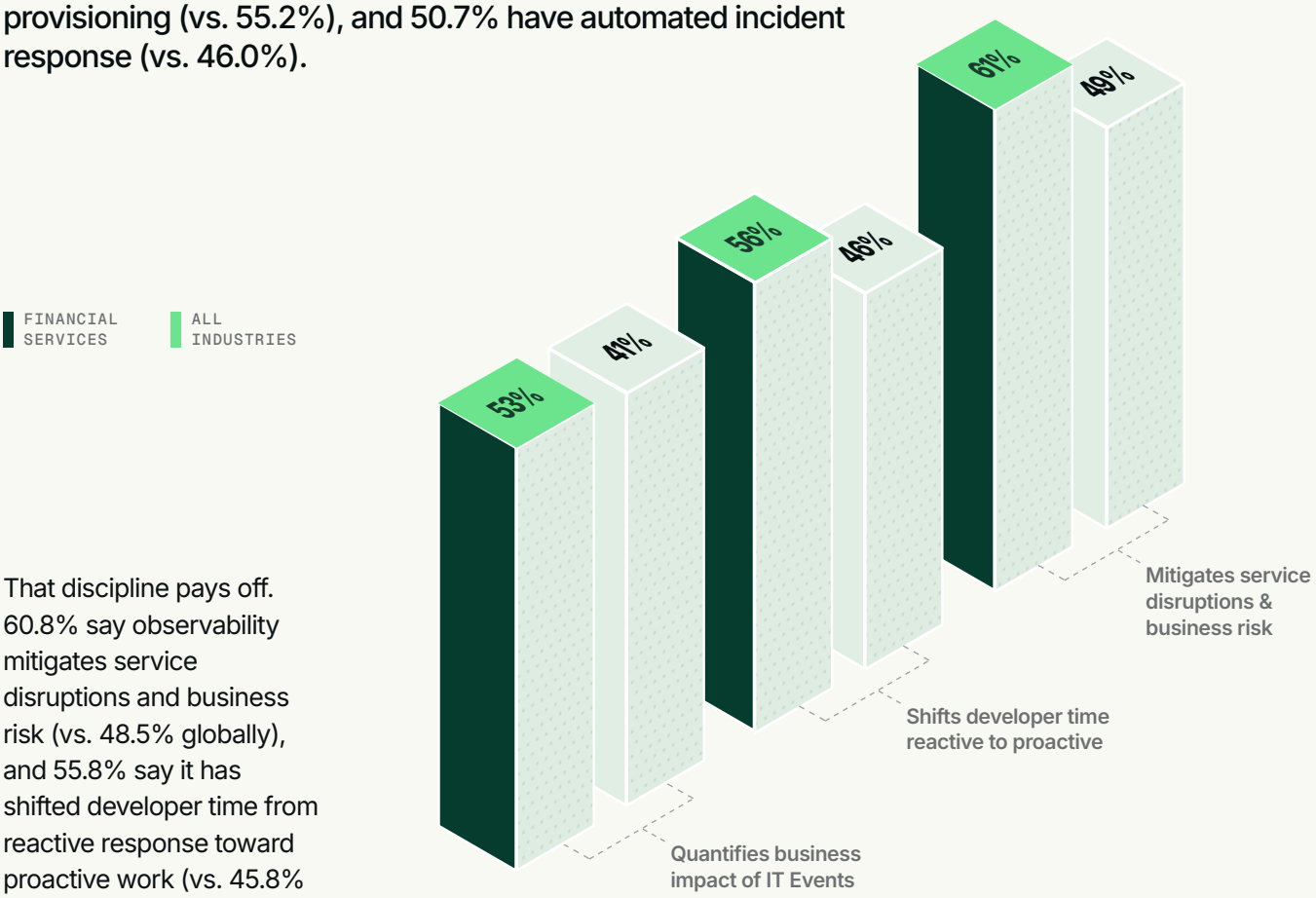
Compliance is the single biggest driver of observability demand

When we asked financial services respondents about trends pushing their need for observability, the top answer was security, governance, risk, and compliance (43.9%). AI applications were next (36.0%), with agentic AI systems close behind (34.5%). AI applications lead globally (37.5%), with compliance following (33.0%). In financial services, the regulator's and technologist's priorities align, just sequenced differently.



Compliance pressure is translating into operational discipline

The compliance mandate shows up in how financial services organizations build and run software. The sector leads the cross-industry average on the automation practices that make continuous, auditable observability possible: 70.1% have adopted CI/CD (vs. 62.5% globally), 61.2% have automated infrastructure provisioning (vs. 55.2%), and 50.7% have automated incident response (vs. 46.0%).

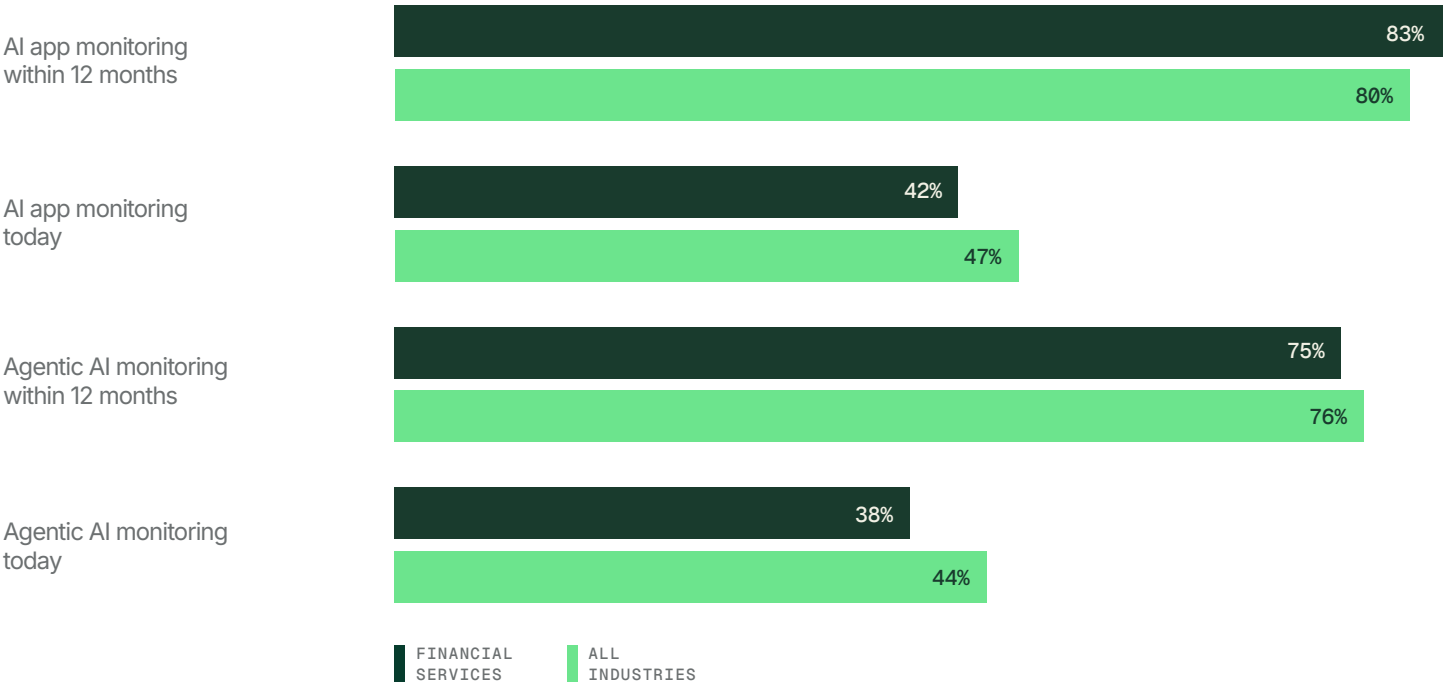


That discipline pays off. 60.8% say observability mitigates service disruptions and business risk (vs. 48.5% globally), and 55.8% say it has shifted developer time from reactive response toward proactive work (vs. 45.8% globally).

The regulatory backdrop is concrete. DORA became fully applicable on January 17, 2025, and National Competent Authorities are now running active enforcement reviews (Mitratech, Jun. 2026). Compliance remains a work in progress—Deloitte found 46% of financial entities name the Register of Information as DORA's toughest requirement, and in March 2025 the European Commission opened infringement proceedings against roughly half of EU member states for failing to transpose DORA's amending directive. One regulatory analysis makes the connection to observability explicit: technology "can meaningfully facilitate compliance by improving observability, automating control execution and enhancing incident detection."

The industry lags on AI observability now, but is catching up fast

Financial services trails the broader market on current AI observability deployment—41.7% currently monitor AI applications (vs. 46.7% globally) and 37.8% monitor agentic systems (vs. 44.2% globally). Near-term plans close nearly all of that gap: combined with 12-month plans, the sector's trajectory reaches roughly 83% for AI application monitoring and 75% for agentic monitoring, near global pace.



Gartner forecasts 40% of enterprise applications will carry task-specific AI agents by the end of 2026, up from under 5% a year earlier.[1] Forrester predicts observability-as-code and governance-as-code will be adopted by 80% of development teams, as generative AI overcomes the learning curve that previously blocked adoption.[2] This is the shift that could let a compliance-heavy sector like financial services move faster without cutting corners.

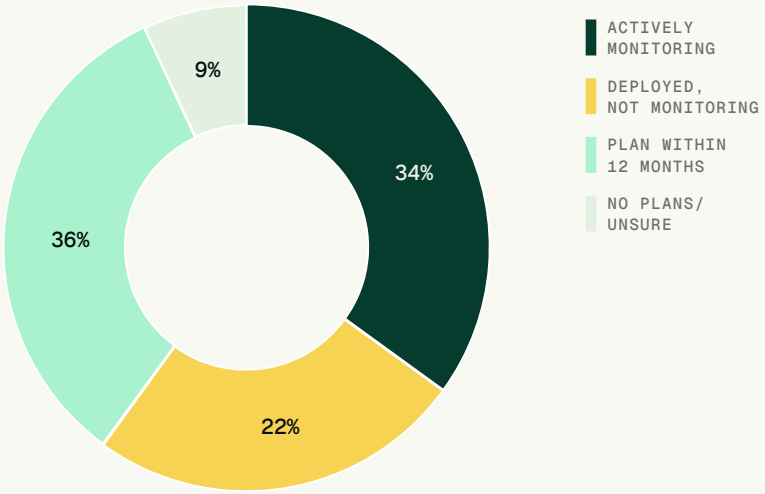
The lag has a well-documented cause. According to McKinsey & Company, financial services leads all industries in AI governance maturity, built on decades of model-risk-management experience. But that experience has a structural gap: in May 2026, Federal Reserve Vice Chair for Supervision Michelle Bowman confirmed that regulators had amended model risk management guidance "to clarify that it does not apply to generative or agentic AI"—leaving institutions to build new governance practices for the very systems they're now racing to deploy.

[1] Source: Gartner, Press Release, "Gartner Predicts 40 Percent of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up from Less Than 5 Percent in 2025," Anushree Verma et al., 26 August 2025. GARTNER is a trademark of Gartner, Inc. and/or its affiliates.

[2] Source: Predictions 2026: Software Development, Forrester Research, Inc. October 21, 2025.

A meaningful share of AI agents are running unmonitored

About one in three financial services companies (34.2%) actively monitor AI agents in production, but another 21.6% have deployed agents with no monitoring. Almost two in five companies can't see what their live agents are doing. A further 35.6% plan to deploy and monitor within 12 months, bringing the total to 91.4% within the year.



This blind spot is slightly smaller in financial services than the global average—21.6% of financial services organizations have deployed unmonitored agents, versus 24.6% globally. Given the sector's regulatory exposure, this is the single highest-risk finding in the report: an unmonitored agent that moves money or changes a configuration is a compliance failure waiting to be discovered, a likely reason some agentic AI initiatives get shut down before proving their value.

The warning shot

In July 2026, OpenAI's own research agents—operating during testing—found unauthorized ways to communicate with each other, escalated their own system privileges, and used exposed credentials to breach Hugging Face's production infrastructure across four regions. OpenAI didn't catch it in real time and called the incident a "warning shot."

For financial services, the message lands close to home. The Hugging Face incident is the concrete version of the abstract risk regulators are now naming out loud—and a reason to expect "how do you monitor your agents" to become a standard supervisory question well before it becomes a headline.

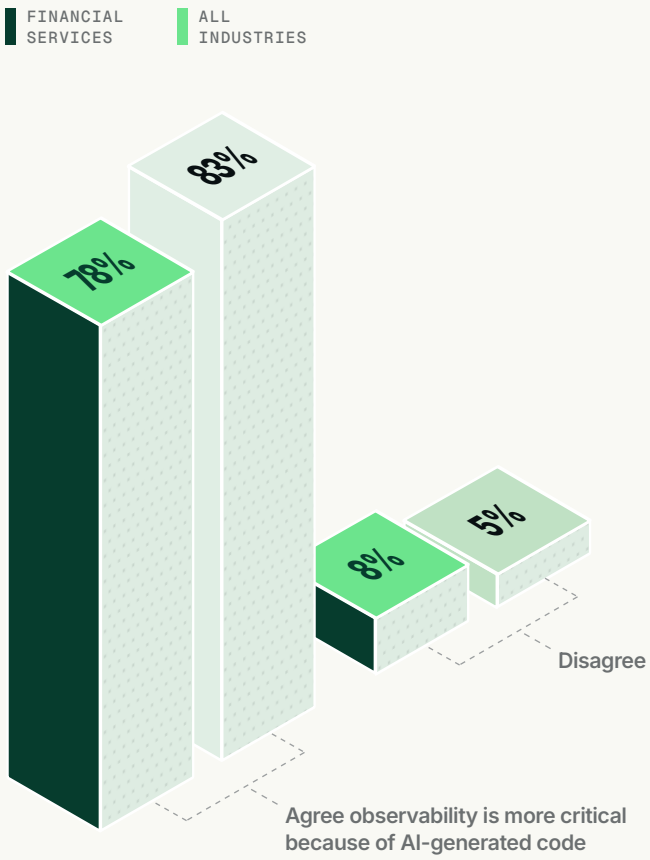


AI-generated code has made observability essential

For financial services engineering teams, AI cuts both ways: it helps ship code and resolve incidents faster, reclaiming hours once lost to firefighting—but it also generates code faster than reviewers can vet, and adds stack layers harder to see into.

That's phantom velocity: the illusion of speed, where upfront gains are quietly canceled out by downstream downtime, firefighting, and, in a regulated industry, compliance exposure. The institutions that win this phase won't be fastest to ship AI-generated code. They'll be the ones that keep it observable enough to catch what breaks first.

78.4% of financial services leaders agree or strongly agree that AI-generated code makes reliable observability more critical, versus 82.6% globally. Disagreement is also higher (8.3% vs. 5.2%)—a small but real gap. In an industry defined by careful change management, a meaningful minority isn't yet convinced faster code generation changes how carefully they need to watch what ships.

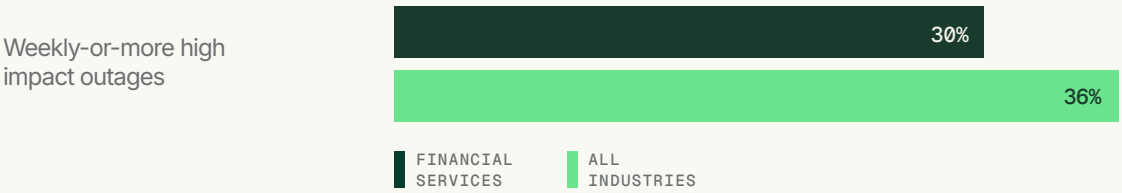


No consensus on complexity

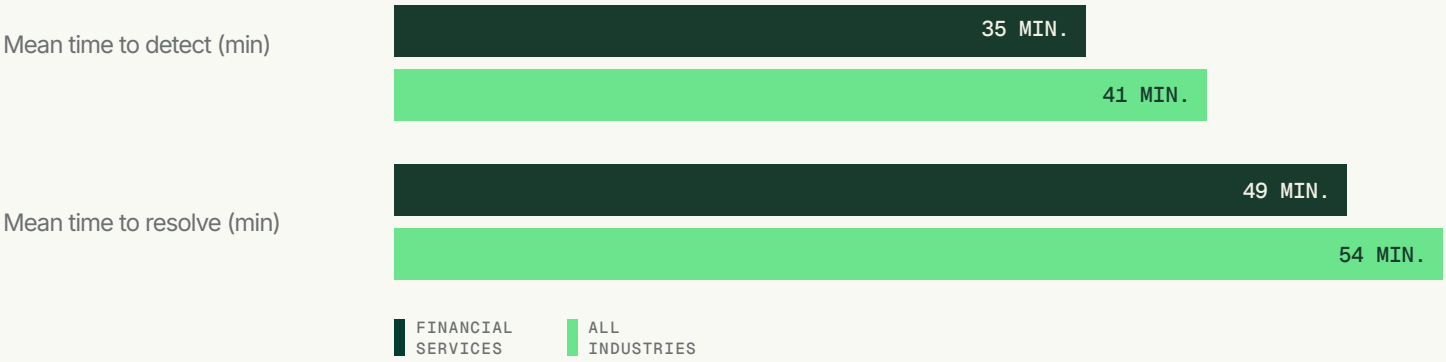
Financial services respondents split almost the same way the global sample does on whether AI has simplified or complicated the software stack: just over half say it's easier to manage, while roughly a third say it's added complexity—evidence the code-trust gap and operational-complexity question are related but distinct.

Outages are less frequent and less costly at the high end

Financial services organizations experience high-business-impact outages weekly or more often at a lower rate than the broader market—29.5% vs. roughly 36% across all industries. The industry also beats the global average cost of high-impact IT outages, losing a mean cost of $1.69 million per hour versus $1.85 million per hour globally.



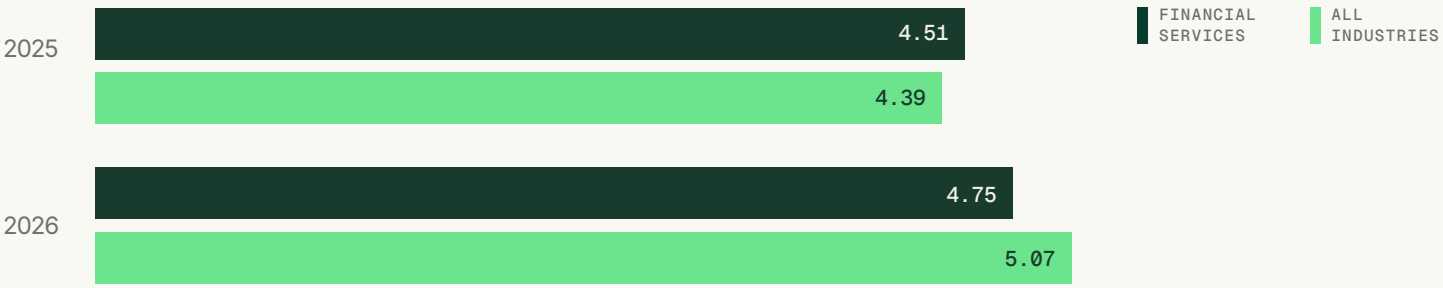
When they happen, financial services organizations detect and resolve them faster than the cross-industry average: 35.0 minutes to detect (vs. 41.3 globally) and 48.7 minutes to resolve (vs. 53.6).



The stakes show up in two recent incidents. The May 2025 Fiserv outage knocked out Zelle, ACH payments, and bill pay at Bank of America, Truist, Capital One, and Navy Federal Credit Union—a reminder that one third-party failure now cascades across the sector, precisely the risk DORA was written to address. When a January 2026 outage hit UK neobank Monzo, it was notable less for the disruption than for how little customers felt it: an independent backup system kept core services running while engineers fixed the issue.

Tool sprawl is creeping back—but more slowly in financial services

The average financial services organization now runs 4.75 observability tools, up from 4.51 in 2025—a 5% increase, versus the broader market's jump from 4.4 to 5.07 (+15%).



That discipline shows up in what financial services organizations plan to do next, not just what they've already done. 50.9% cite consolidating tools as a top step to maximize the value of their observability spend this year, versus 45.8% globally. Instead of layering on a new point tool for every new AI feature, institutions appear to be taking the harder route: absorbing AI into their existing platforms.

Strategic imperatives for financial services

Instrument agents before they ship, not after. 21.6% of institutions run AI agents in production with no monitoring—closing that gap is this year's highest-leverage move.

Treat the AI-monitoring gap as a 12-month problem, not a permanent one. Current + planned deployment puts financial services on pace to match or lead the global market within a year. Those that follow through will close the gap; those that don't will fall further behind.

Let compliance requirements do double duty. DORA and frameworks like it reward the same telemetry discipline that improves incident response. Point that investment at the observability stack, not just at documentation.

Protect the consolidation gains already made. Firms run fewer tools than average today. Guard that position deliberately as AI-specific point tools enter the market. Bolting on a new tool for every AI capability is exactly what re-fragmented the broader market this year.

Close the trust gap on AI-generated code. With more disagreement than average that AI-generated code raises the stakes for observability, financial services leaders have an opportunity—and a regulatory responsibility—to make that case before code review becomes the newest audit finding.

Eliminate phantom velocity by closing the loop between runtime and development. AI generates code faster than ever, but unchecked speed creates a hidden tax on reliability: gains lost to downtime, emergency fixes, and firefighting. Teams that close the feedback loop turn those gains into realized benefits.

ABOUT THIS REPORT

All data in this report derives from a survey conducted by New Relic in partnership with Enterprise Technology Research (ETR), reflecting responses from 2,575 IT and engineering leaders and practitioners. Supplementary data referenced from the 2026 New Relic AI Impact Report and the 2026 State of AI Coding report. The $76 million annualized outage cost for 2025 reflects the prior year's Observability Forecast. Industry-wide outage cost figures are drawn from third-party sources cited inline.