LogicMonitor

RESEARCH REPORT

2026 Observability & AI Outlook for IT Leaders

Autonomous IT is Closer Than You Think

Based on survey data from 100 VP+ IT decision-makers with observability budget authority, conducted in mid-2025.

EXECUTIVE SUMMARY

IT operations have outgrown the model they were built on.

Enterprises now monitor tens of thousands of metrics, ingest terabytes of logs, and generate thousands of alerts daily, all while managing increasingly complex infrastructures that span on-prem data centers, multiple cloud environments, and emerging AI workloads.

Yet despite all this telemetry, too many teams still learn about outages from customers before they see them in their tools. That visibility gap is no longer acceptable.

Recent high-profile outages at CrowdStrike, Cloudflare, and others have demonstrated just how quickly a small issue can ripple across industries, interrupt daily life, and cost companies billions.

The next phase of AI-first observability requires something bigger.

It must extend beyond the data center and cloud. It must encompass the Internet itself, where applications, identity, payments, APIs, and user experience actually live. This is where business resilience is won or lost. This convergence of hybrid infrastructure observability, Internet Performance Monitoring, and Digital Experience Monitoring is the real beginning of autonomous IT.

Leaders need to think bigger.

Figure 1. Each force builds momentum for the other.

The answer is not another tool or more humans chasing alerts. The real shift requires a new operating model that moves IT from reacting to predicting and from patching to self-healing. This is autonomous IT, and it's no longer theoretical.

Survey data from 100 VP+ IT decision-makers reveals **five forces** converging to accelerate this shift. Each one reinforces the others (figure 1). We explore each of these forces in further detail in the following sections.

Cost pressure drives consolidation. Consolidation creates unified data.

Unified data allows AI to work. AI delivers autonomous capabilities that reduce incidents and justify continued investment. This cycle is already forming inside the highest-performing organizations.

The companies that recognize this pattern and act decisively will transition from reactive to predictive, and ultimately, to autonomous operations. Those who treat these trends as isolated projects will fall behind as the gap between reactive and autonomous operations widens–quickly.

Five Forces Converging Toward Autonomous IT

1 Observability budgets are protected infrastructure

Cost pressure is real. Organizations are being asked to do more with less. Yet observability budgets aren't following the typical pattern. 96% of IT leaders expect observability spending to hold steady or grow over the next 12-24 months, with 62% anticipating increases.

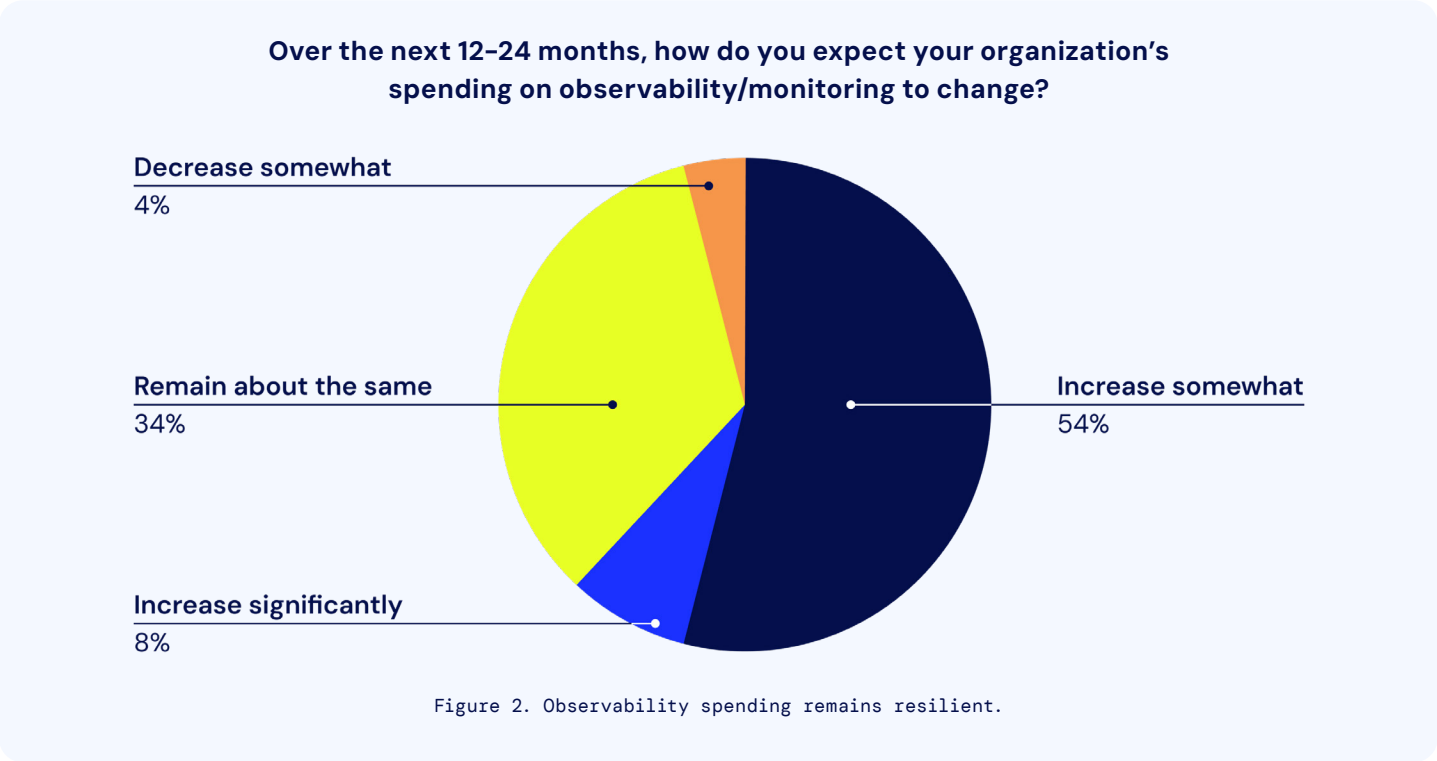


Figure 2. Observability spending remains resilient.

This isn't immunity from budget scrutiny; it's evidence that observability has become foundational, strategic infrastructure that leaders protect. Every company now has IT at its operational core—whether retail, banking, healthcare, or manufacturing—and protecting uptime has become non-negotiable for business delivery.

As enterprises adopt distributed architectures and AI-powered services, observability now extends from internal systems to the Internet and customer-facing layers. This makes comprehensive visibility critical—performance issues at any point directly impact revenue, customer retention, and service delivery. Investments increasingly cover Internet performance and end-user monitoring, beyond core infrastructure.

Which IT initiative is currently receiving the highest level of strategic focus and attention within your organization (e.g., top priority initiatives, executive attention, resource allocation? (up to 3)

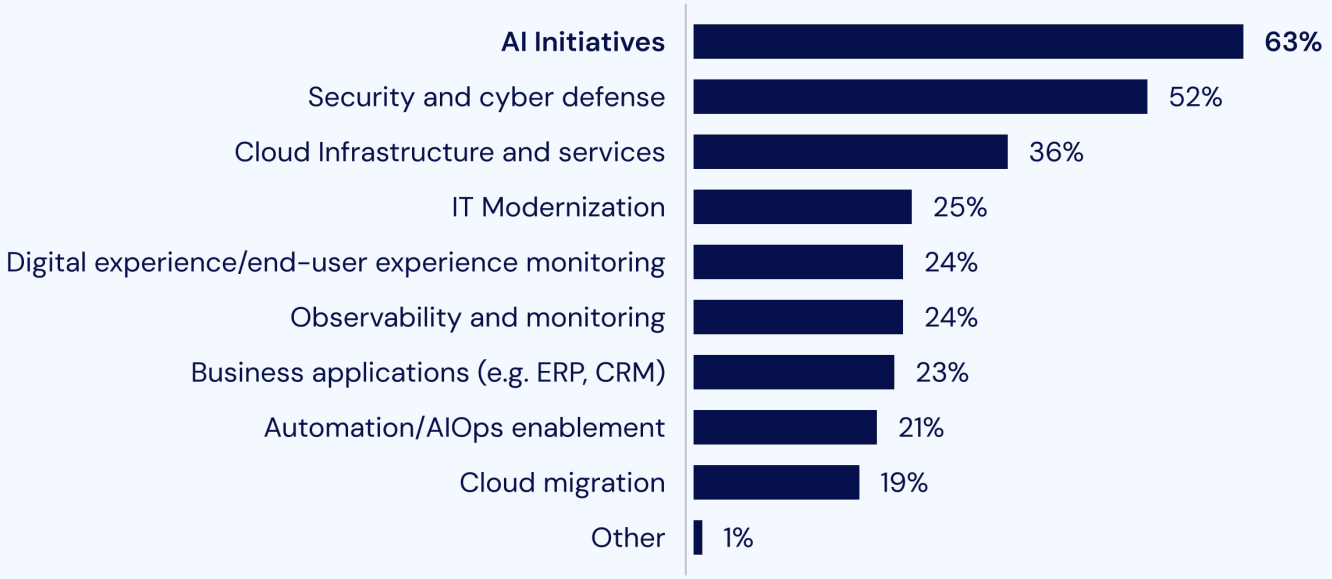


Figure 3. AI initiatives top strategic priorities.

While AI initiatives command the highest share of strategic focus (cited by 63% of leaders as a top priority), cost savings are coming from other areas, not the systems that keep infrastructure visible and operational. Tool sprawl and rising telemetry costs create pressure to optimize. Yet, observability spending remains stable or grows because it underpins everything else: application performance, user experience, security monitoring, and increasingly, the AI initiatives receiving all that executive attention.

Protected budgets don't mean static spending. Organizations are actively reallocating spending toward outcomes rather than tools. The next trend shows where that redirection leads.

96%

of IT leaders expect observability budgets to **hold steady or grow** through 2026.

2 Consolidation is the optimization strategy

84% of organizations are pursuing or considering tool consolidation. 41% are actively consolidating, while another 43% are evaluating it. Leaders now view consolidation as the most effective way to reduce cost, improve service delivery, and unlock the unified data foundation that AI requires. Consolidation is no longer just a cost-saving measure. It is a strategic accelerator.

Is your organization currently looking to consolidate or reduce the number of observability/monitoring tools in use?

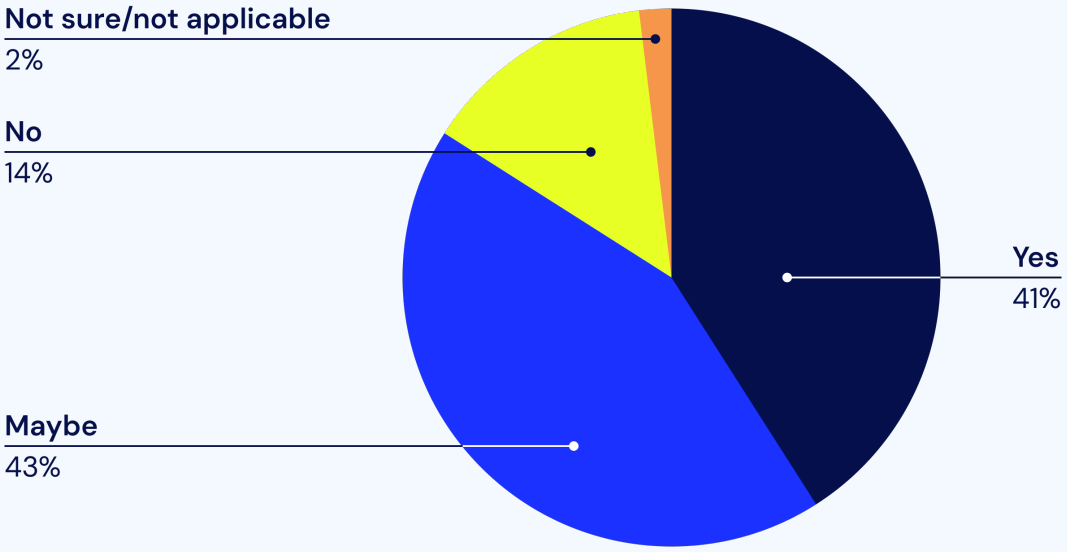


Figure 4. Consolidation is the dominant optimization strategy.

84%

of organizations are **consolidating or considering consolidating** to **reduce costs and improve visibility**.

The math is straightforward. Organizations running 2-3 observability platforms (66% of respondents) or 4-5 platforms (18%) pay for overlapping capabilities, duplicate data pipelines, integration maintenance, plus bear the operational overhead of context-switching during incidents. Only 10% currently operate from a single unified platform, but they represent the most future-ready organizations, already positioned to harness AI and automation effectively.

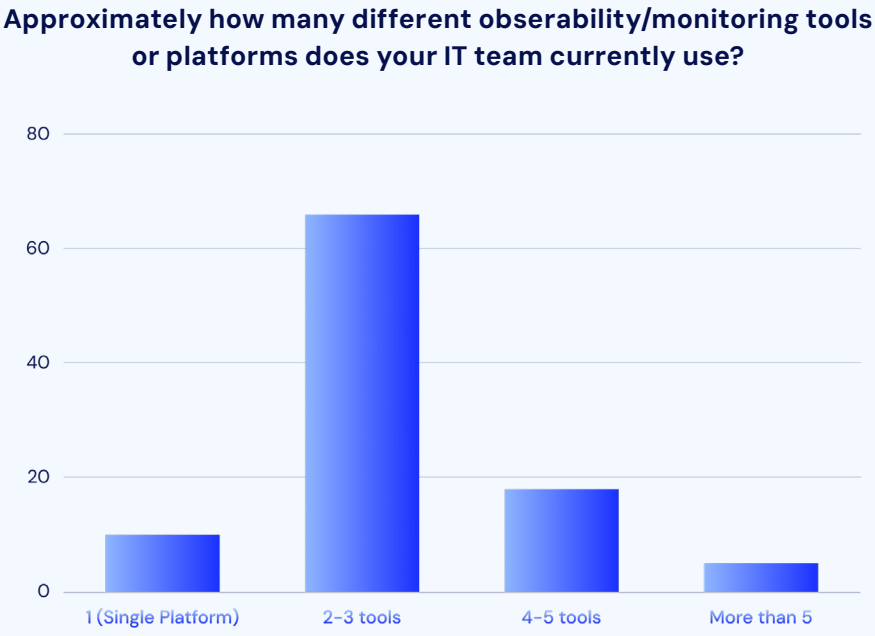


Figure 5. Most IT teams still manage multiple observability platforms and tools.

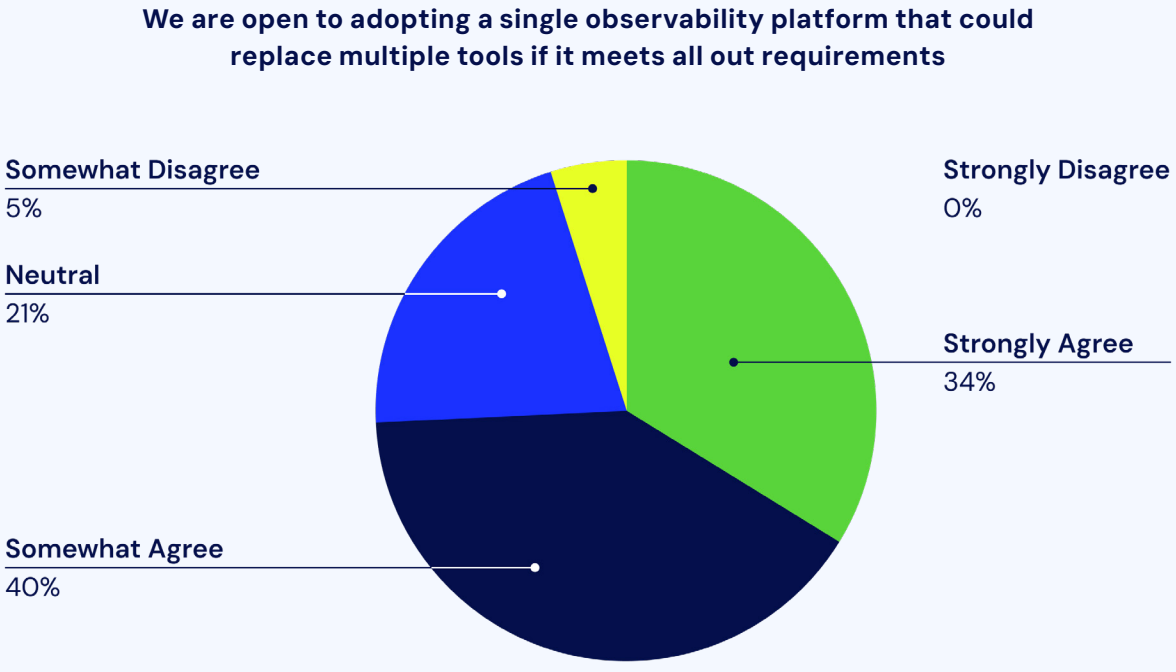


Figure 6. Most organizations would consolidate to a single platform if it meets requirements.

Which of the following challenges do you face with your current obserability/monitoring tools or practice?

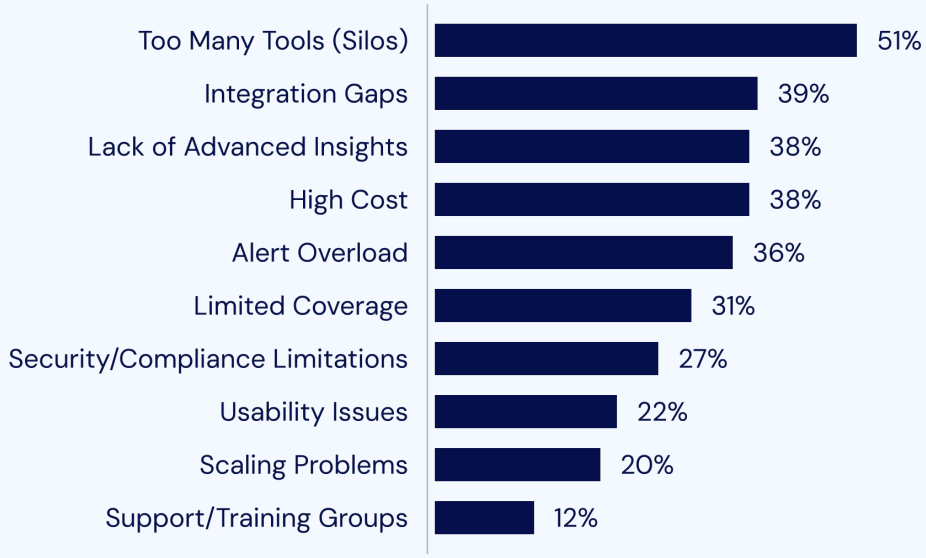


Figure 7. Too many silos, integration gaps, and a lack of advanced insights top the list of challenges holding back observability maturity.

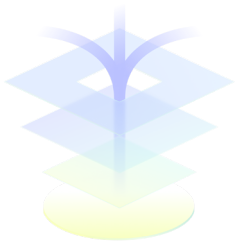
The gap between the current state and the desired state is massive. 74% indicate openness to a single platform if it meets requirements—a remarkable willingness to consolidate in an industry historically resistant to vendor concentration.

During production incidents, engineers context-switch between platforms, manually correlate data across systems, and waste critical minutes assembling the complete picture. The cost of tool fragmentation goes beyond redundant licensing and consumption fees. When incidents do occur—whether from faulty updates, misconfigurations, or system failures—every minute of downtime erodes customer trust and costs millions in lost revenue. A prime example of this operational and financial impact is the 2024 CrowdStrike outage, which is estimated to have cost Fortune 500 companies over $5 billion. Not a single industry was spared.

Two-thirds of organizations use 2–3 tools, while just

10%

operate from a single platform today.



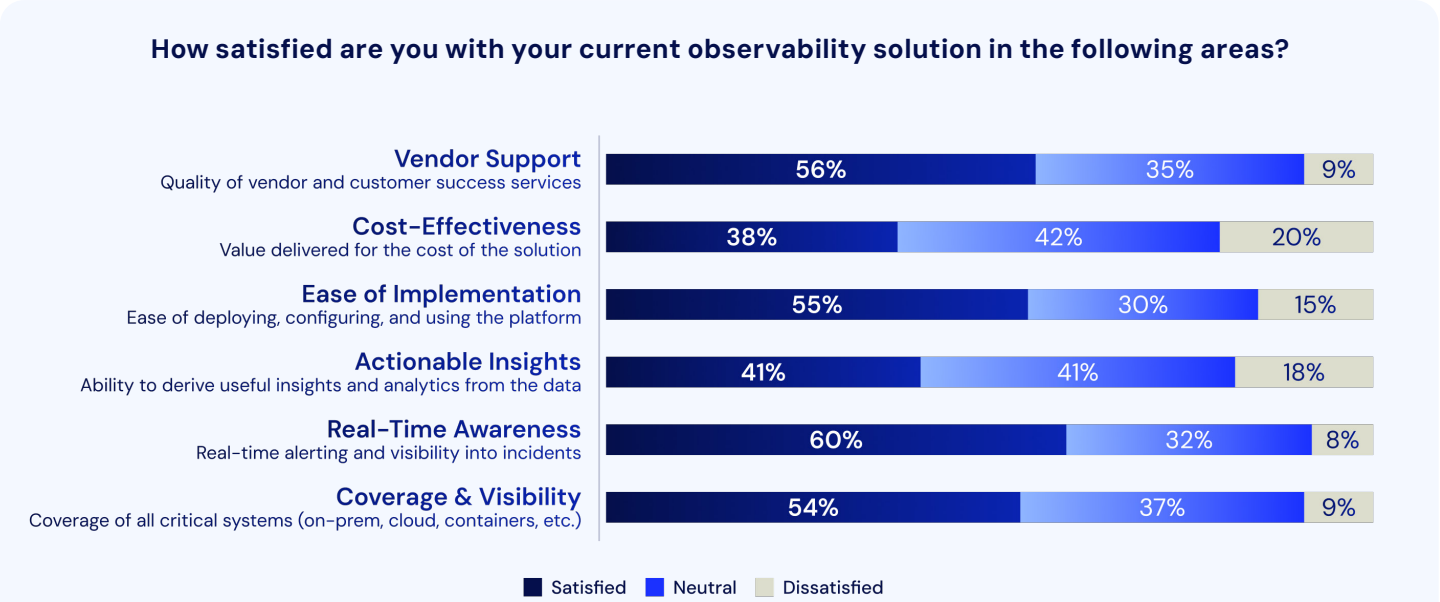


Figure 8. Fragmented tools limit insight generation.

Forward-looking organizations are collapsing separate domains (e.g., APM, NPM, IPM, and DEM) into unified platforms that offer full-path visibility from user to code. This reduces telemetry silos and accelerates correlation across internal and external environments.

The consolidation wave creates two outcomes that enable autonomous IT: it generates budget savings that can be reinvested in AI capabilities, and it establishes the unified data foundation that AI requires to work effectively. You can't build autonomous operations on fragmented telemetry.

Satisfaction with cost-effectiveness and actionable insights trails other dimensions of observability performance.

3 Platform loyalty is giving way to agility

67% of IT leaders say their organization is likely to switch observability platforms within 1–2 years. This represents a fundamental shift in enterprise software buying behavior. Platform decisions that once took years to revisit are now being reconsidered on 12–24 month cycles.

How likely is your organization to consider switching to a new observabiity/monitoring platform in the next 1–2 years?

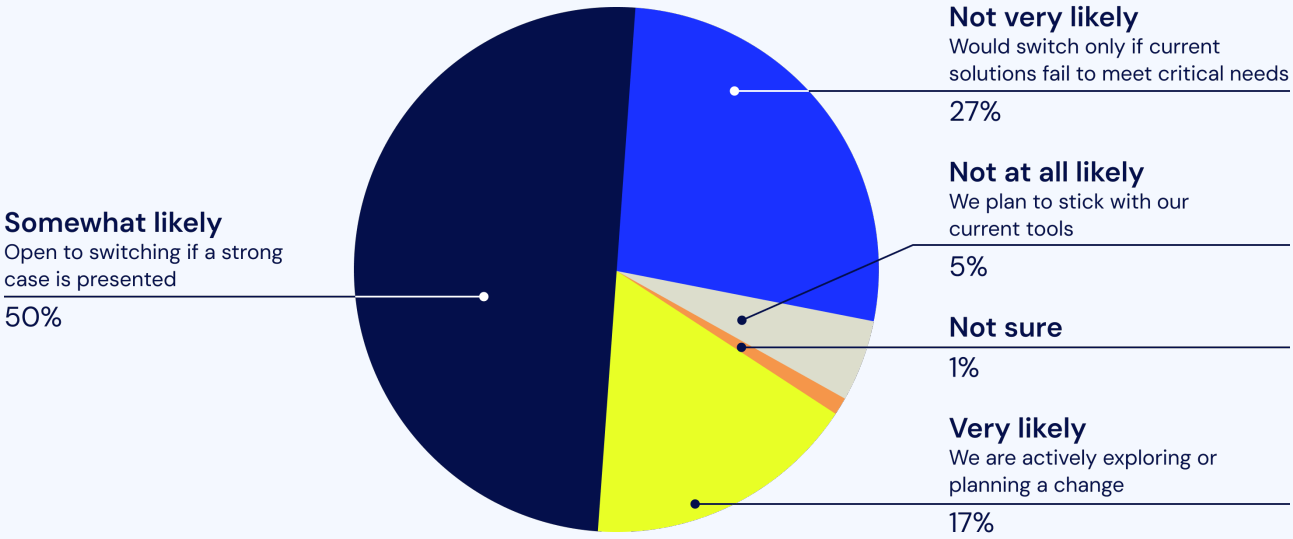


Figure 9. Platform loyalty is fading fast.

67%

of organizations are very likely or somewhat likely to switch observability platforms within **1–2 years**.

The likelihood of switching breaks down as follows: 17% very likely (actively exploring or planning changes), 50% somewhat likely (open to switching if a strong case emerges), 27% not very likely, and 5% not at all likely. The 67% combined likelihood suggests a genuine willingness to make changes.

But what triggers platform switches? Top reasons include new company initiatives requiring better monitoring (27%), security and compliance mandates (22%), a need to replace outdated tools (19%), that major outages have highlighted monitoring gaps (13%), and regular technology refresh cycles (11%) all create catalysts for change.

But what triggers platform switches? Top reasons include new company initiatives requiring better monitoring (27%), security and compliance mandates (22%), a need to replace outdated tools (19%), that major outages have highlighted monitoring gaps (13%), and regular technology refresh cycles (11%) all create catalysts for change.

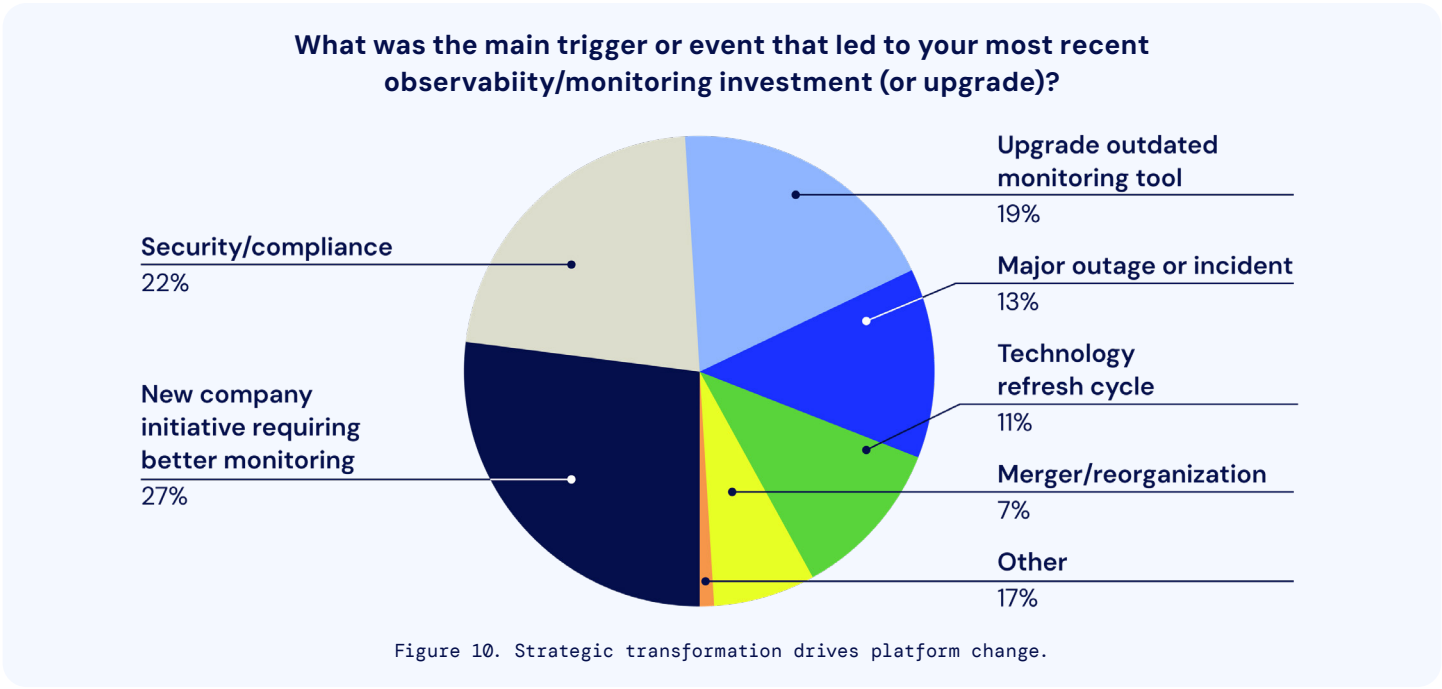


Figure 10. Strategic transformation drives platform change.

Notably, cost efficiency means value for spend, not just cheaper alternatives—IT leaders want platforms that justify their price through measurable outcomes.

What's more, the barriers to switching are operational rather than strategic: integration complexity, migration risk, training requirements, and budget approval processes are the most cited reasons that prompt switching. With the rise of OpenTelemetry and API-based integrations, switching costs are lower, and IT leaders now prioritize openness and Internet-aware visibility over ever-increasing ingest costs or complexity in monitoring tools. These are execution challenges, not fundamental objections to technology upgrades.

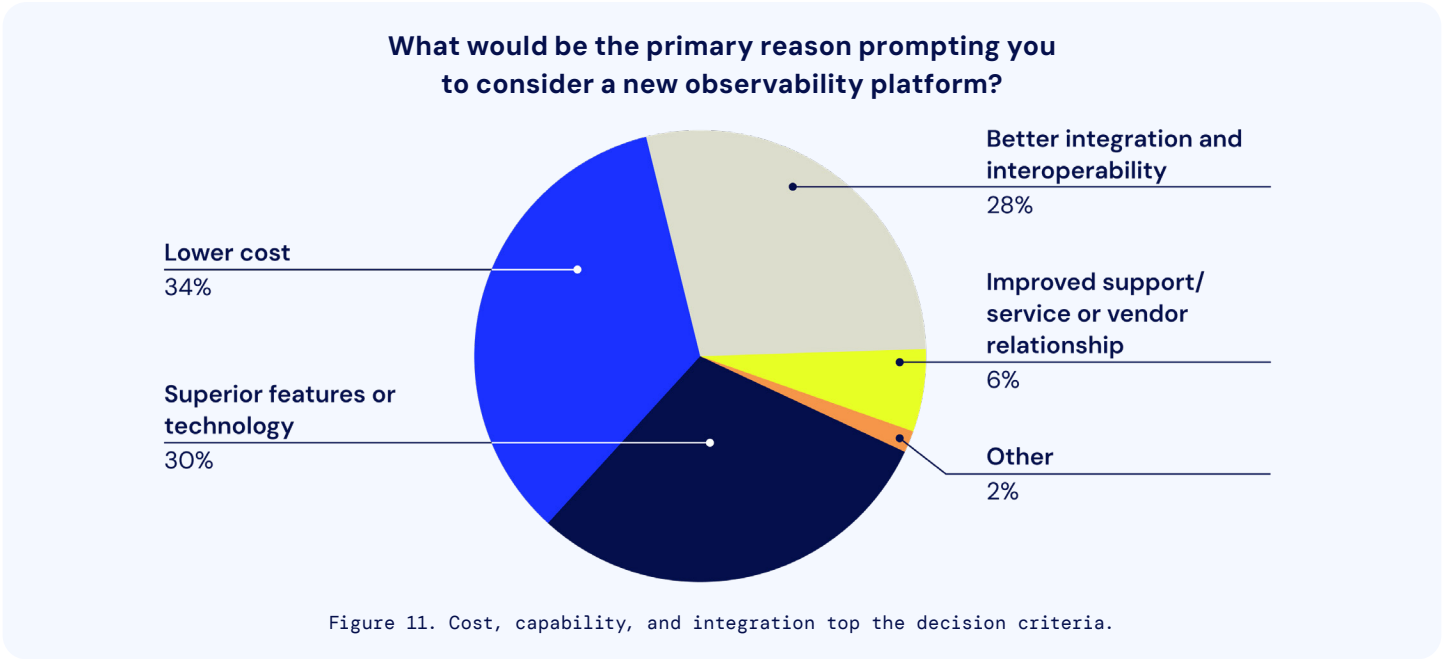


Figure 11. Cost, capability, and integration top the decision criteria.

4 Current tools aren't delivering actionable insights

Only 41% of IT leaders report satisfaction with their platform's ability to derive useful insights from collected data.

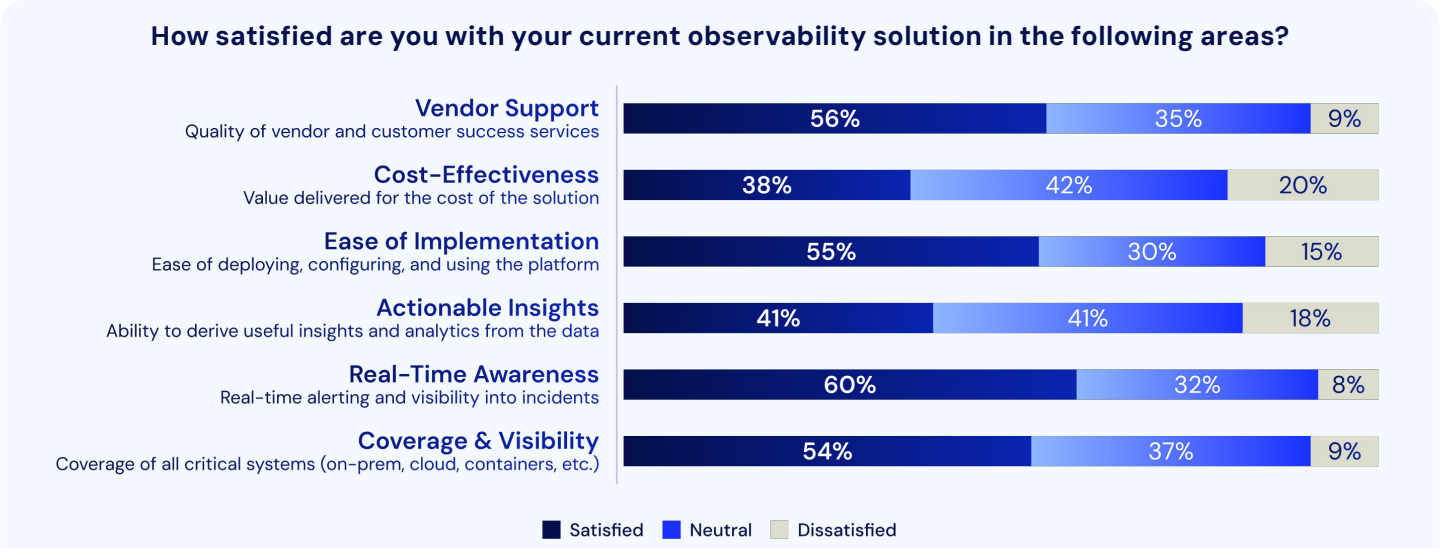


Figure 12. Few IT leaders are satisfied with their observability platform's ability to deliver actionable insights.

This means 59% are sitting on mountains of telemetry without the tools to turn data into action and prevention. IT teams can see that something broke. But, they can't quickly determine what, why, or how to fix it–or better yet, prevent the incident altogether.

The satisfaction gap reveals itself in specific pain points. 38% cite a lack of advanced insights as a top barrier to achieving observability goals. 36% struggle with alert fatigue, receiving hundreds or thousands of notifications daily while missing critical issues in the noise. 39% report integration gaps that prevent their monitoring tools from working seamlessly with ITSM systems and DevOps workflows.

Teams struggle to connect internal infrastructure telemetry with external Internet dependencies, user experience data, and application delivery metrics. The result is partial visibility: great insight inside the firewall, but blind spots where customers and employees actually experience issues.

Which of the following challenges do you face with your current obserability/monitoring tools or practice?

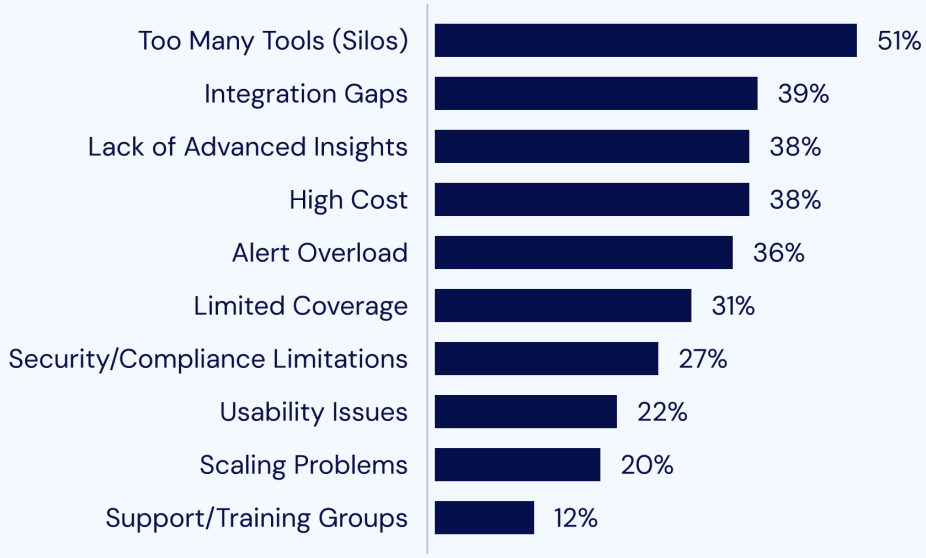


Figure 7. Too many silos, integration gaps, and a lack of advanced insights top the list of challenges holding back observability maturity.

The problem isn't data collection—it's correlation, context, and causality. Traditional observability tools were built for simpler architectures and smaller data volumes. They struggle with high-cardinality data from containerized environments, correlating metrics, logs, and traces across systems, identifying root causes in distributed architectures where failures cascade between services, and reducing alert noise to distinguish genuine issues from normal variation.

This dissatisfaction creates demand for AI-powered capabilities that deliver measurable outcomes: automated correlation and root cause analysis, predictive capabilities that identify issues before they impact users, and intelligent alerting that reduces false positives. The gap between what current tools provide and what teams need is the opening for platforms that can actually deliver insight that drives action and prevention at scale.

Without **correlation and causality**, observability stops at visibility.

5 AI adoption is maturing, but most organizations have significant runway

Just 4% of organizations have reached full operational maturity, fully leveraging AI across IT operations. Another 12% are using AI to automate root cause analysis and remediation, while 13% rely on AIOps mainly for anomaly detection and incident response. The majority—49%—are still piloting or experimenting with AI in limited environments, and 22% haven't adopted it yet.

What best describes your organization's current use of AI or AIOps capabilities in observability and IT Operations?

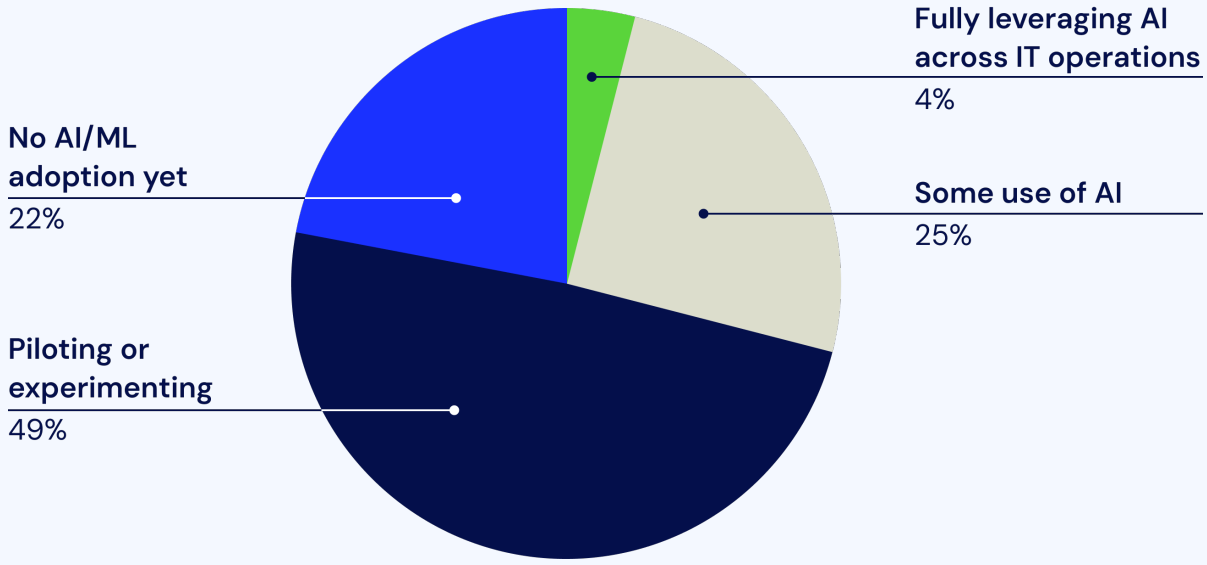


Figure 14. AI adoption in observability remains early-stage

AI adoption has clearly begun, but scaling it is where progress stalls. 62% of organizations have started implementing AI—piloting, testing, or using it in limited ways—but haven't yet operationalized it across IT. This friction from pilot to production suggests most teams are still fine-tuning models, integrating data, and learning how to translate AI insights into trusted action. It's not a failure of ambition; it's a signal that real operational maturity requires unified data, contextual understanding, and automation that teams can actually trust.

When asked what they most want from AI in observability, IT leaders pointed toward action-oriented automation rather than diagnostic capabilities. 52% selected accelerating root cause analysis and incident response, followed by 47% seeking predictive analytics to prevent incidents, and 44% aiming to automate remediation and enable self-healing systems.

Others cited cost optimization (40%), reducing alert fatigue (39%), and improving security detection (31%) as key priorities.

But leaders want automation with guardrails. They need policy-driven actions with approval workflows, integration with existing governance processes, and explainability that shows why AI flagged an issue and which data contributed to the determination. Black-box systems that can't explain their reasoning erode trust and limit adoption.

What are the top benefits or capabiliites you are seeking from AI in observability?

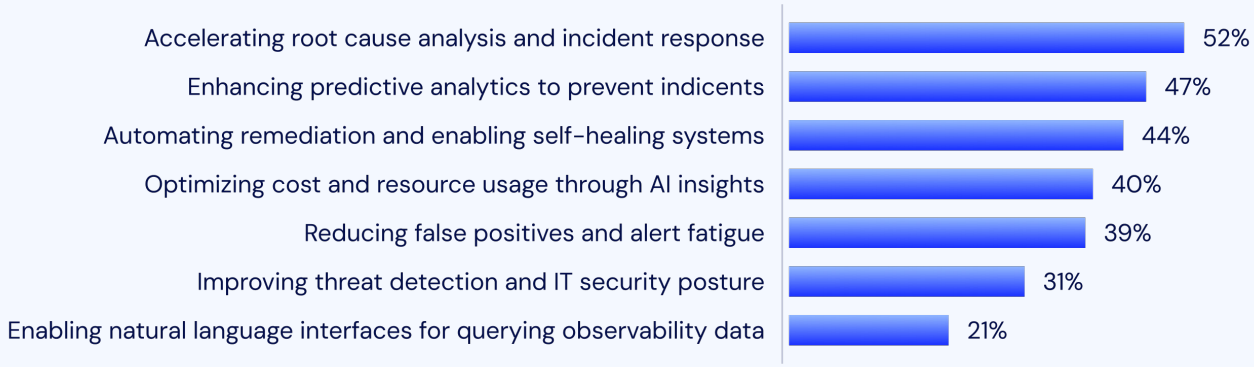


Figure 15. IT leaders are prioritizing action-oriented AI.

The maturity gap represents opportunity, but more importantly, the conditions to close it finally exist. The 78% that haven't reached full operationalization aren't stuck because AI doesn't work. They're stuck because they've been trying to run AI on fragmented data, disconnected tools, and platforms that can't explain their reasoning.

But IT leaders' survey responses show that those sticking points are temporary. Observability spending remains resilient, giving IT leaders the resources to keep investing. Consolidation creates the unified data foundation AI needs to work effectively. And with greater flexibility to replace underperforming tools, organizations are finally able to turn pilot projects into real, scalable results.

AI maturity is accelerating, but the next wave applies intelligence across the entire delivery chain—from infrastructure to Internet to user. Synthetic data from global vantage points, combined with telemetry from production environments, feeds models that not only detect but also validate and self-correct digital experience issues.

AI earns trust only when it **explains itself.**

Why Autonomous IT is Closer Than You Think

These five behavior shifts don't exist in isolation. They form a reinforcing cycle that accelerates the shift toward autonomous IT.

The cycle begins with cost pressure. While observability budgets are protected within IT organizations, there is a rationalization of total spend with consolidation as the optimization strategy—reducing vendor count, eliminating duplicate capabilities, and cutting integration overhead. But consolidation delivers more than cost repurposing. It creates the unified data foundation that effective AI requires. You can't train models on fragmented, inconsistent telemetry scattered across disconnected tools.

That unified foundation enables AI capabilities that actually work: automated correlation, root cause analysis, predictive alerting, and eventually autonomous remediation. These capabilities deliver measurable outcomes, like reduced MTTR, less alert fatigue, and fewer incidents reaching production. And measurable outcomes justify continued investment, which protects observability budgets even when other spending gets cut.

When **data, decisions, and action connect**, autonomy follows.

Protected budgets restart the cycle. Organizations with stable funding can pursue the next round of optimization and capability building, widening their advantage over competitors still stuck in reactive operations.

Organizations that recognize this as an integrated system will move faster than those treating each trend as an independent initiative.

IT leaders report two additional accelerators of this cycle: dissatisfaction with current tools creates urgency to move, and declining platform loyalty removes the friction that once kept organizations locked into underperforming solutions. The 59% unsatisfied with their platform's insight generation aren't waiting for contract renewals—67% are likely to switch within 1-2 years.

The Mandate for IT Leaders

This convergence creates a clear mandate: autonomous IT is no longer a future-state vision. It's the 2026 operational requirement. Organizations face a decision point. Continue managing observability as a collection of disconnected tools and manual processes, or move decisively toward unified platforms that enable AI-powered autonomous operations. The window to act is open now—but it won't stay open indefinitely. The path forward requires three sequential moves:

1

Unify Visibility Across All Layers

First, establish the foundation through platform consolidation. Unified visibility is the prerequisite for everything else. Organizations running 3-5 fragmented tools cannot effectively implement AI because their data lacks consistency. Consolidation both optimizes costs by reducing vendors and creates the data foundation AI requires. Leaders must consolidate tools not only across infrastructure but across the whole delivery path: combining infrastructure observability, Internet performance monitoring, and digital experience monitoring.

2

Operationalize AI Across the Delivery Chain

Second, implement AI capabilities that deliver measurable outcomes. Start with incident response automation and root cause analysis—the capabilities leaders respectively identify as top priorities. Focus on systems that increase business resilience, reduce MTTR, decrease alert noise, and provide explainability. Avoid black-box AI that teams won't trust. Apply AI to correlate telemetry across infrastructure and Internet layers to predict and prevent disruptions to customers' and employees' digital experiences.

3

Adopt Autonomous Operations with Guardrails

Third, scale autonomous operations with governance. Introduce agentic AI that can act and proactively resolve issues across internal and external systems while maintaining policy-based governance and explainability. Deploy predictive capabilities that prevent issues before they impact users. Implement auto-remediation with policy-driven controls and approval workflows, where teams can see exactly why an action was triggered and roll it back if needed. Integrate with existing ITSM and change management systems to maintain compliance.

The organizations that execute this path will gain a competitive advantage through improved reliability, faster innovation cycles, and reduced operational overhead. Those who delay will find themselves managing increasingly complex infrastructure with insufficient tooling while competitors operate autonomously.

The technology exists. The budgets are available. The switching windows are open. The market is ready. The question for IT leaders isn't whether autonomous operations will become standard. It's whether you'll be among those who define that standard or those scrambling to adapt to it.

By combining infrastructure intelligence with Internet performance and customer experience insights, forward-thinking leaders can close the visibility gap that still separates operational excellence from customer outcomes and establish their organizations as infrastructure innovators rather than followers.

Autonomous IT is closer than you think.

ABOUT THIS RESEARCH

This report draws on survey data from 100 VP+ IT decision-makers with observability budget authority, conducted in Q2 2025. Respondents represent organizations across diverse industries and geographies. Organization sizes range from under 500 employees to more than 20,000, with 67% representing enterprises with 1,000 or more employees. 75% of respondents have final decision-making authority for observability platform selection and budgeting, while 25% are key influencers. All respondents currently use or plan to implement observability solutions within the next 12 months.

About LogicMonitor®

LogicMonitor® is the AI-first hybrid observability platform powering the next generation of digital infrastructure. Powered by Edwin AI, our SaaS-based solution gives organizations complete visibility and actionable intelligence across on-premises, cloud, and edge environments. By anticipating issues before they strike, optimizing resources in real time, and enabling faster, smarter decisions, LogicMonitor helps IT and business leaders protect margins, accelerate innovation, and deliver exceptional digital experiences without compromise. For more information, visit www.logicmonitor.com and our blog, or follow us on LinkedIn, X, Facebook, and YouTube.