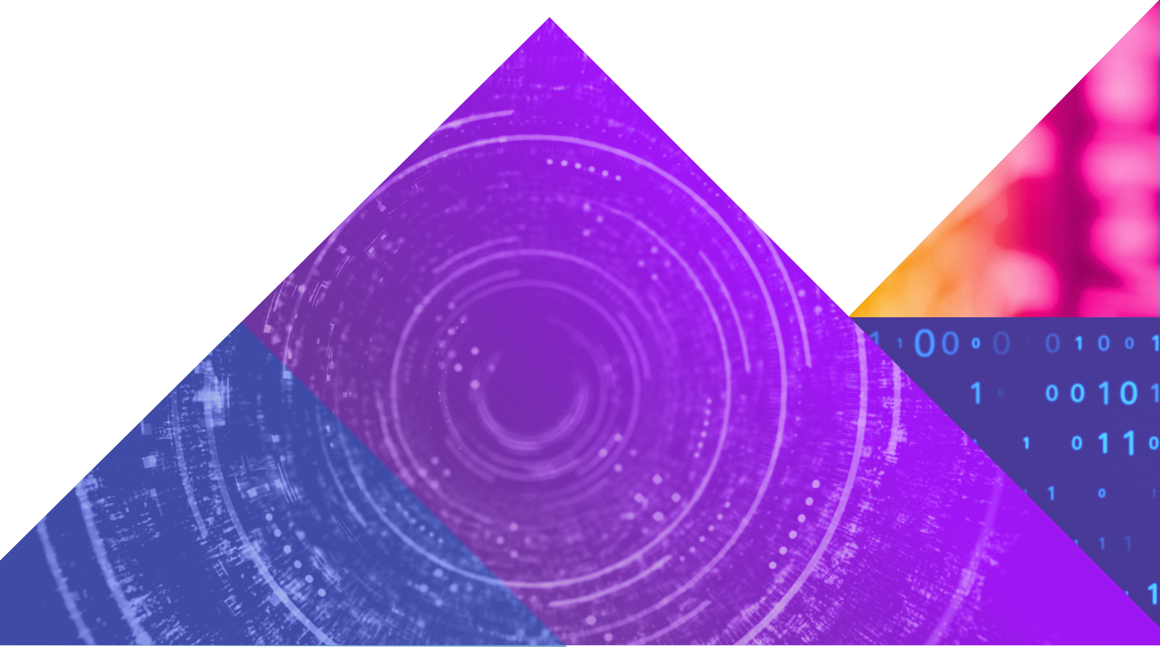
The State of **Observability 2023**

Global research: Amid rising complexity, leading orgs are ensuring visibility, driving resilience and realizing off-the-charts ROI



splunk>

Observability Has Arrived

Observability used to be on the cutting edge. Now it's commonplace. Once only adopted by visionary organizations, observability has become foundational to modern enterprises, providing a way to see into the stunningly complex web of systems that characterizes today's IT environments.

In the two years since our inaugural State of Observability report, we've seen the number of organizations getting started with observability rise substantially, and a whopping 87% of respondents now employ specialists who work exclusively on observability projects. There are plenty of good reasons so many businesses are jumping on the observability bandwagon.

The State of Observability 2023

We surveyed 1,750 observability practitioners, managers and experts to examine the state of observability — from the success of today to the ambitions of tomorrow. The brightest highlights:

- Observability leaders are 7.9x as likely as beginners to say that their ROI on observability tools far exceeded expectations.
- An extraordinary 89% of leaders are completely confident in their ability to meet availability and performance requirements for their applications, 3.9x the rate of beginners.
- Leaders are 4x as likely to resolve instances of unplanned downtime or serious service issues in just minutes, versus hours or days.

Organizations that build a rich observability practice have more visibility into their interwoven environments, which translates into fewer outages, faster issue resolution, greater confidence in their apps' reliability — and, ultimately, more revenue and happier customers. We'll get into the nuances of what defines a leader and beginner later, but first, let's look at the factors defining observability today.

A mature observability practice paves the way for greater reliability, better performance, higher revenue and happier customers.

Resilience as North Star

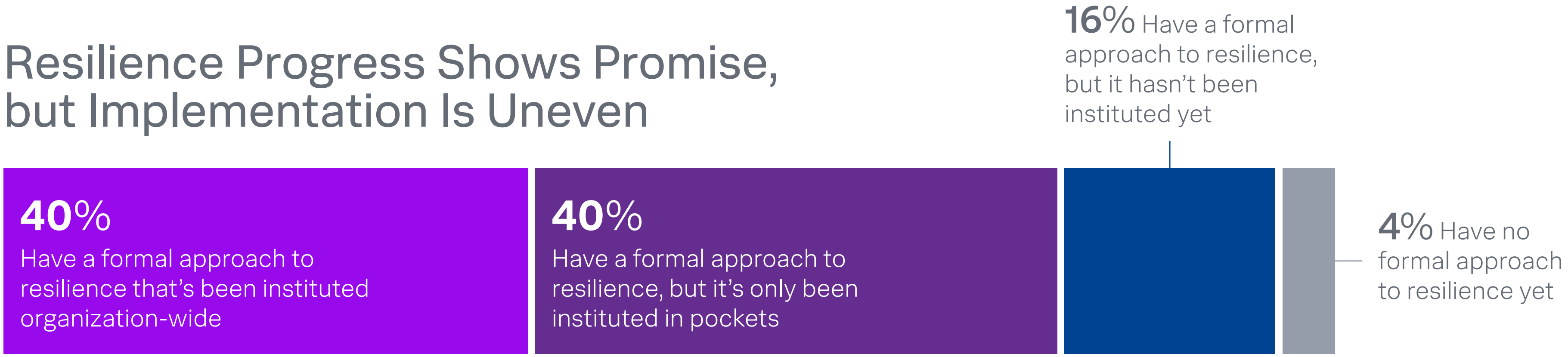
Businesses are investing more in resilience, fearing that failure to do so will cause them to lose customers due to an outage (according to 73% of respondents) or be out-innovated due to lost productivity (74%). It's no wonder then that 95% of respondents say that their observability leaders are actively collaborating more with line-of-business leaders on resilience strategies, priorities and investments than just a year ago. This number reaches 100% among leading observability orgs, which represent the strongest performers on six measures — but comprise only 10% of respondents. The least advanced group, beginners, represent 33% of respondents. We'll detail what defines the four levels of maturity in section two.

When asked about their resilience strategies in the coming year, organizations report definitive plans to invest in solutions that achieve a range of goals. About half of respondents say they'll invest in solutions to:

- **Recover customer and user services faster**
- **Respond and remediate security incidents quicker**
- **Gain visibility throughout the entire technology environment**
- **Combine resilience efforts with traditional business continuity preparation**
- **Understand the downstream impact of security incidents**

These abilities are fundamental for businesses to keep operations smooth, systems secure and customers happy. And if the tumultuous last few years are any indication of the years ahead, orgs will need resilience strategies in place to withstand the next storm on the horizon — whatever it may be.

Resilience Progress Shows Promise, but Implementation Is Uneven



Observability rises as complexity increases

All things trend toward disorder. It's a law of nature — and observability ecosystems are no exception. Mirroring the rising complexity of broader IT environments, 81% of respondents say the number of observability tools and capabilities they use has been increasing recently, with 32% saying the increase is significant.

It's a natural progression: Orgs add more tools, scale their systems, create more apps and launch more revenue streams. In turn, their environments can become sprawling and unwieldy, precipitating the need for greater visibility and, as a result, observability.

But even though the number of tools is surging, that doesn't always mean an equal influx of vendors. While 44% report an uptick in vendor count (and 12% significantly so), 40% report consolidation. But even then, that's a lot of vendors and tools to manage, which makes the single-pane-of-glass nirvana that IT professionals have always strived toward a destination that's harder to both attain and maintain.

Methodology

Between December 12, 2022, and January 19, 2023, researchers from the Enterprise Strategy Group surveyed 1,750 IT operations, application development and DevOps leaders from organizations with 500 or more full-time employees and who are knowledgeable about their organization's observability practice.

10 countries

Australia, Canada, France, Germany, India, Japan, New Zealand, Singapore, the United Kingdom and the United States

16 industries

Aerospace and defense, consumer packaged goods, education, energy, financial services (banking, securities, insurance), government (federal/national and state/local), healthcare, technology, life sciences, manufacturing, media, oil/gas, retail/wholesale, telecom, transportation/logistics, utilities

Speaking of complexity, organizations report operating and maintaining, on average, 165 internally developed business applications, with about half in the public cloud (51%) and half on-premises (49%). Fifty-six percent of these apps at least partly use cloud-native architecture, while 44% rely entirely on legacy/monolithic architectures.

After years of hearing that cloud will soon be the only architecture type that matters, these numbers are surprising. With a significant swath of apps still running on monoliths, and the complexity of refactoring legacy apps for the cloud, it's clear that hybrid architectures will persist.

Looking ahead, cloud is clearly here to stay, but slightly fewer orgs are still aggressively refactoring legacy apps to cloud-native architecture.

- **58% say that cloud-native apps will make up a larger proportion of their internally developed apps a year from now, down from 67% last year.**
- **40% say cloud-native apps will make up the same percentage going forward, compared to 32% last year.**
- **2% say cloud-native apps will make up a smaller percentage, up from 1% last year.**

With cloud so deeply ingrained, and hybrid a continued certainty, observability will remain vital to cut through the complexity and unify monitoring across different environments.

A cloud-only reality isn't inevitable — at least not yet. Hybrid still reigns supreme.

44% of internally developed applications are still built on monolithic architectures (on average).

86% say it's important to have flexible observability solutions that cover hybrid architectures, though half identify this as an area of improvement.

Getting by with a little help from some friends

Observability tools have become more common in organizations' arsenals, with 73% of respondents reporting they've been using observability tools for over a year. But they're still pretty new: Only 14% have been using them for more than three years.

Peeking into the tool chest more closely, organizations noted these tools as the most prevalent:

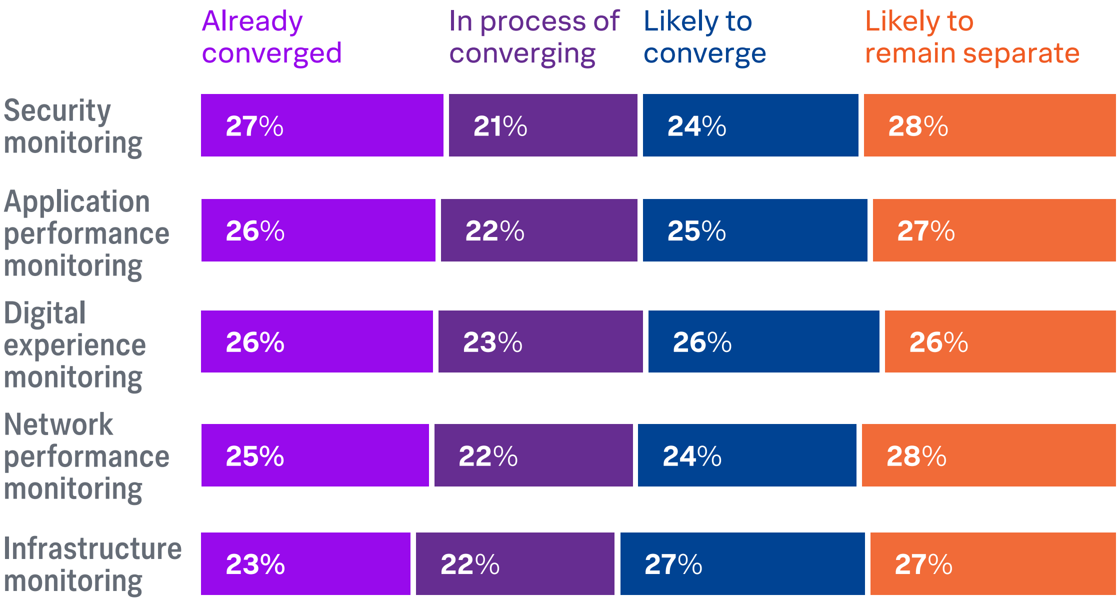
- **Network performance monitoring (79%)**
- **Security monitoring (78%)**
- **Application performance monitoring (78%)**
- **Digital experience monitoring (72%)**
- **Infrastructure monitoring (70%)**

Across the board, respondents are more likely than last year to report using every tool listed, which squares with the fact that 81% say their tools and capabilities are increasing. Yet bringing these tools together is also becoming more common. More respondents report converging aspects of observability with other monitoring practices. This percentage has increased from last year, and we'll see later that leaders are always more likely to converge their tools.

But all tools aren't created equal. Eighty percent of respondents report having seen vendors position solutions as observability tools but felt that in reality this was just rebranding, without any specific observability functionality being added. This sneaky practice — called o11y-washing — has surfaced as a clear danger when organizations evaluate new tooling.

Better Together

Nearly 75% of respondents report that tools and teams will eventually unite under one observability umbrella — but progress toward this end goal is mixed.



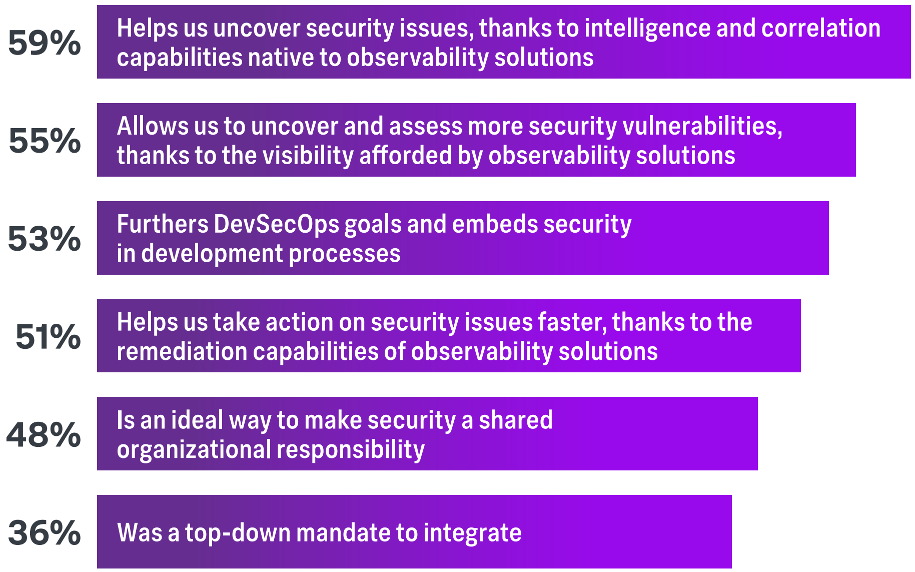
Observability and security monitoring are the most common disciplines to merge. And when compared to last year, more and more organizations are unifying security and observability for a dynamic duo that can increase visibility — providing greater context around incidents and accelerating resolution.

We asked respondents why they brought security and observability together in the first place. Orgs note that the visibility afforded by observability solutions also helps them better uncover and evaluate security vulnerabilities — and once these issues are found, they're also acted on and fixed faster. The least common reason for integration? A top-down mandate, which suggests that unifying security and observability has happened organically, instead of just due to orders from on high.

As observability tools continue to become more sophisticated, the visibility they provide grows deeper and more granular. This rising tide will no doubt lift both boats — security and observability — as more teams maximize these benefits to proactively prevent issues, pinpoint problems and keep systems running smoothly and securely around the clock.

It Takes Two

Respondents cite reasons for converging observability and security monitoring.



AI/ML also has a home in the observability toolset. Long before ChatGPT brought AI to the masses, observability teams were relying on AI/ML to enrich their tools. Sixty-six percent already use AI/ML, while 26% are in the process of deploying. A paltry 1% have no interest in those newfangled technologies.

Respondents say AIOps tools outperform legacy solutions in a number of ways — from automatically determining the technical root cause of an issue (34%) to predicting potential problems before they turn into customer-impacting incidents (31%), to better assessing how severe the impact of an issue really is (30%).

These benefits go a long way in helping organizations fix issues faster and become more efficient. But rampant rebranding is still a hazard here, too: 76% of respondents tell us they've seen AIOps-washing, nearly as many as o11y-washing.

91% say AIOps is an important enabler of their observability goals.

64% report that ROI on their AIOps tools has exceeded expectations.

AIOps acceleration: Orgs report that the top benefits of AIOps are faster mean time to detection and faster root cause diagnosis.

Changing tides of the talent pool

As observability has proven its staying power, the talent landscape has evolved. More organizations report bringing their observability experts together as a centralized team working across standardized tooling (58%), versus orgs that embed them within app development teams (42%).

Last year's report revealed significant challenges across hiring observability talent in both quantity and quality. Overall, the vast majority of orgs are still finding it hard to find ITOps team members (85%), as well as SRE and DevOps engineers (86%).

But this year is already looking up for employers — in some ways, but not others:

- **Respondents are less likely to say it's challenging to find enough ITOps candidates (22% in 2023, versus 36% in 2022), though more likely to say it's challenging to find the right candidates (21% in 2023, versus 13% in 2022).**
- **71% report teams have been left short-staffed due to workforce reductions or layoffs (with about a third saying this has happened multiple times).**
- **Yet by the same token, these layoffs could also mean an expanding talent pool, which might explain why more organizations are reporting zero challenges with sourcing the quantity or quality of staff they need (15% in 2023, versus just 5% in 2022).**

And 35% of leaders say they don't have challenges at all, underscoring that orgs further along in their observability journey recruit top talent.

> As specialized talent becomes more prolific, it's clear that observability isn't just a flash in the pan.

87% of respondents employ people who work exclusively and entirely on observability projects.

Full visibility lies ahead. ROI is already here.

Less than half of all orgs are completely confident in their teams' ability to meet its application reliability and performance objectives (according to 43%). Another 48% are mostly confident but harbor some reservations. Not very assuring, is it? This "completely confident" number, though, explodes to 89% among observability leaders, which may suggest this lack of confidence could be related to issues with adoption or mindset within the organization, instead of tool immaturity.

Orgs say they have "excellent visibility" into each component of their environment — such as on-prem legacy infrastructure, private cloud infrastructure, security posture or containers — no more than 52% of the time. That's alarming, considering that gaining visibility is the primary reason for observability. These numbers underscore a major area of improvement, and may shed light on why so many teams don't feel that they can meet their performance objectives.

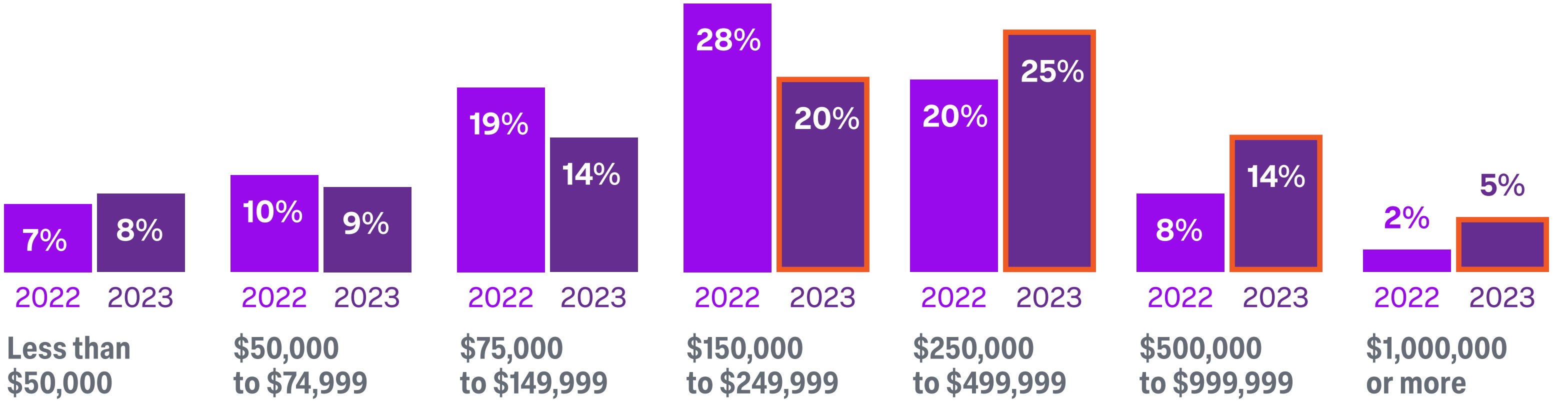
The harsh reality is that costly critical incidents like downtime still plague many organizations. When we asked orgs about service-impacting issues among their internally developed apps in the last one to two years, they outline these business ramifications:

- **49% report lower customer satisfaction**
- **45% report loss of revenue**
- **38% report loss of customers**
- **36% report reputation loss**
- **Only 12% report no business ramifications**

Respondents note internal consequences of these issues as well, the highest of which are increased turnover on their team and increased outsourcing of the observability function — both at 38%.

Downtime Is Getting More Expensive

Nearly two-thirds of orgs report that every hour of downtime costs more than $150,000.

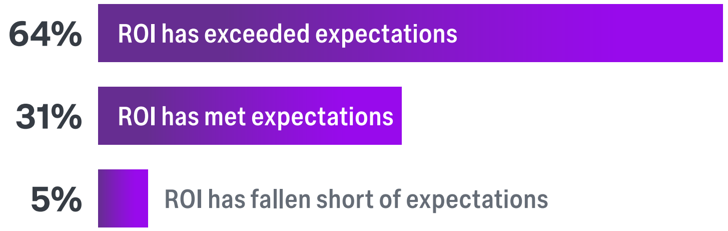


On the flip side, observability efforts are also paying high dividends, helping organizations find and fix problems faster (83% and 82%, respectively), see into hybrid ecosystems (81%) and secure applications better (81%).

These vital benefits seem to outweigh the cost of the tools themselves. Respondents tell us that their observability investments are both positive and transformative: 64% report that their ROI has exceeded expectations — and among leaders, this number jumps to 86%. In total, just 5% of respondents say ROI has fallen short of expectations.

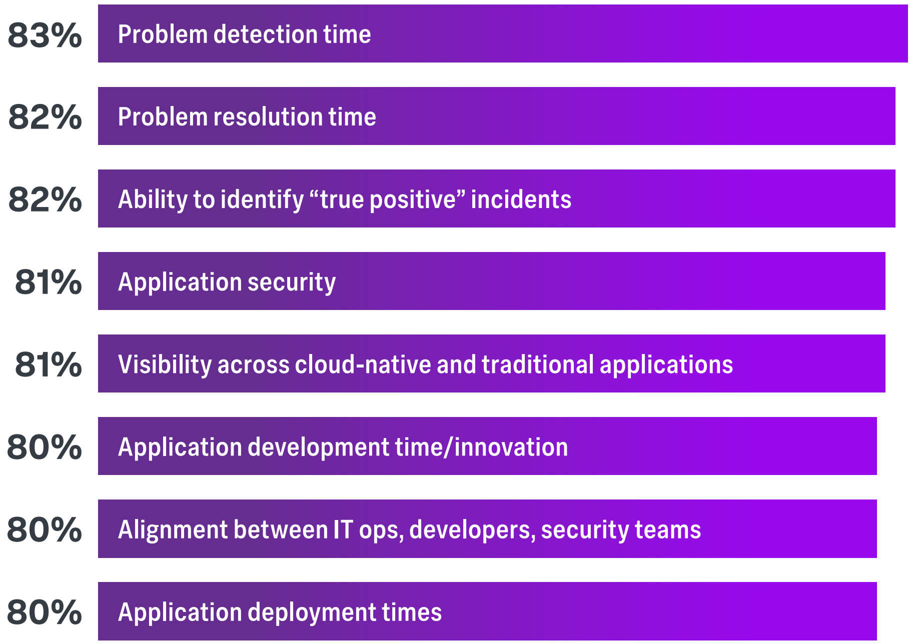
At right, respondents paint a clearer picture of how observability is benefitting their organization — ranging from greater visibility into hybrid apps to faster app development time. Of these benefits, respondents identify two standout areas in which observability solutions are having a significant positive impact: app security and MTTR — two critical priorities for today's modern IT and engineering teams.

An Eye on ROI



Observability's Benefits Extend Far and Wide

Respondents report that observability solutions are having a positive impact across the board.



Being A Leader Pays Off

As observability becomes more prolific, beginner-level organizations heavily outweigh leaders — yet leaders have blazed a trail for success that includes higher ROI, faster innovation and far greater confidence that they'll deliver on their performance promises.

Being an observability leader matters — and translates into real-world benefits ranging from reputation to revenue. (Bonus points for bragging rights, too.)

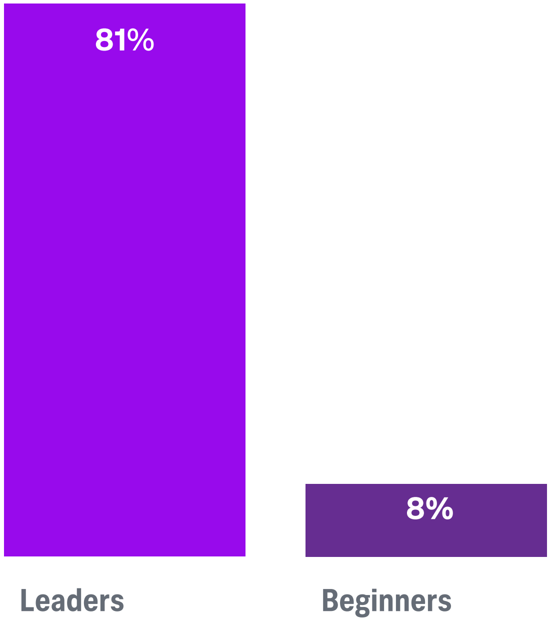
For leaders, observability — and the visibility it affords — is entrenched in their organizations, resulting in a richer picture of interwoven ecosystems, fewer outages, faster issue resolution, greater innovation and an easier time recruiting top talent.

Leaders stand out from the pack in a variety of noteworthy ways. As we've mentioned, nearly 90% are confident that they can meet their reliability and performance goals (and that's up from 71% last year, and 48% in 2021), and nearly the same percentage say their observability ROI has exceeded expectations. Three more measures of satisfaction:

- **Leaders report, on average, one-third the number of outages per year as beginners.**
- **Those leaders are 4x as likely to resolve instances of unplanned downtime or serious service issues in just minutes, versus hours or days.**
- **Leaders have launched, on average, 34% more products/revenue streams.**

Those are impressive benefits, especially as expectations for performance and innovation climb with each passing year. Organizations that build a rich observability practice into everything they do can expect to see a sizable advantage over the competition.

Leaders Prioritize Resilience More Than Everyone Else



Leaders report that they have a formal approach to resilience that has been instituted organization-wide across critical systems.

Observability leadership defined

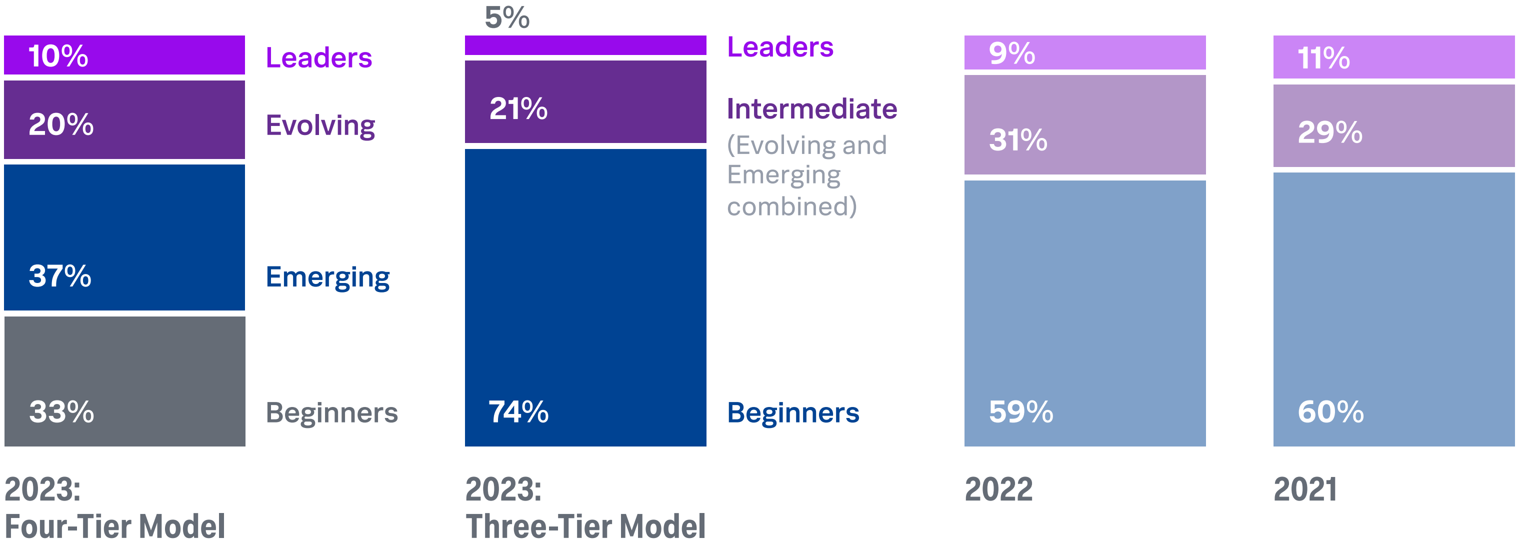
Given that we have more data than last year (1,750 respondents versus 1,250), we were able to generate a view of maturity with greater resolution, refining 2022's framework of beginners-intermediate-leaders to beginners-emerging-evolving-leaders in 2023.

We define the maturity of an organization's observability practice by six factors, three of which are the same as last year: experience (at least 24 months defines a leader, fewer than 12 marks a beginner), ability to correlate data across all observability tools, and adoption of AI/ML technology within their observability toolset. The other three factors are new: skills specialization (individuals working exclusively on observability), ability to cover both cloud-native and traditional application architectures, and adoption of AIOps. We also removed vendor consolidation as a factor this year.

Leaders achieved the highest tier in all six categories; any five define evolving organizations; emerging organizations possess three or four; and beginners reached the highest level in two or fewer categories.

A more granular maturity model reveals that most organizations are still nascent in their observability journeys — 33% are beginners and another 37% are still emerging. If using the same three-tier model as last year, beginners represent 74% of respondents. This large uptick in beginners underscores that observability adoption is rising quickly — and that it's never too late to join.

For the purposes of this report, we'll mostly compare leaders to beginners. The two intermediary groups are always in between, with evolving orgs outperforming emerging orgs in nearly every category.

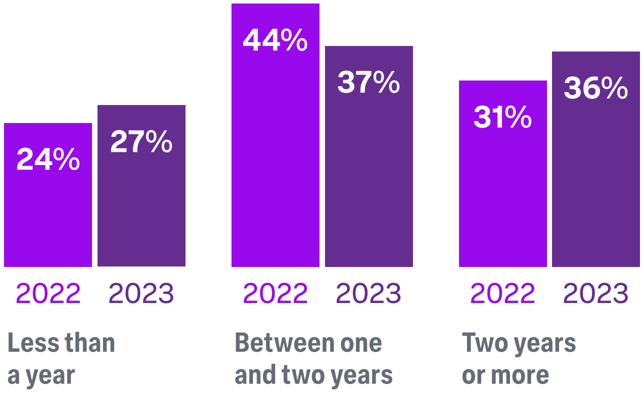


As we examine the six factors more closely, we see mixed effects from the increase in new entrants.

- **Data correlation: How much data can be correlated across IT systems**
  - Beginner: Limited to none (14% of all respondents versus 19% in 2022 versus 15% in 2021)
  - Emerging and Evolving: Moderate (45% versus 44% classed as intermediate in 2022 versus 51% in 2021)
  - Leader: Extensive (39% versus 36% in 2022 versus 33% in 2021)
- **AI/ML functionality: Use of AI/ML within observability tools**
  - Beginner: "Not currently planning/deploying" (8% versus 11% in 2022 versus 13% in 2021)
  - Emerging and Evolving: "In process of deploying" (26% versus 26% in 2022 versus 33% in 2021)
  - Leader: "Use to a limited/extensive degree" (66% versus 62% in 2022 versus 52% in 2021)
- **Skills specialization: Individuals that work exclusively/entirely on observability projects**
  - Beginner/Emerging: Less likely to have this level of specialization (12% say "no" or "don't know")
  - Evolving and Leader: Almost universally have this level of specialization (87% say "yes")
- **Extensible solutions: Importance and use of observability tools that can cover both cloud-native and traditional application architectures**
  - Beginner: Do not see this as important (14%)
  - Emerging and Evolving: Recognize the importance, but need improvements to their tooling (49%)
  - Leader: See this as important and have effective tooling in place (37%)
- **AIOps implementation: Use of AIOps tools within the observability practice**
  - Beginner: Have no plans for, or interest in, AIOps tools (7%)
  - Emerging and Evolving: Are in the process of deploying AIOps tools or use them in a limited fashion (60%)
  - Leader: Use AIOps tools extensively (32%)

The Age Gap

When asked how long they'd been maintaining an observability practice, orgs say:



Visibility breeds confidence

Leaders have better eyes into their environments. When things go wrong, they know about it sooner and can fix the issue faster — and are more likely to prevent an issue from ever happening in the first place.

As a stark contrast to beginners' cloudier vision, most leaders report excellent visibility into every area we asked about:

- **Containers (71% of leaders versus 32% of beginners)**
- **Public cloud IaaS (71% versus 38%)**
- **Security posture (70% versus 37%)**
- **On-prem infrastructure (66% versus 34%)**
- **Applications at the code level (66% versus 31%)**

This visibility means that when things are going right, leaders can hum along more smoothly, releasing more products while hitting their performance goals more confidently.

- **The vast majority of leaders (89%) say that they have complete confidence in their ability to meet application performance requirements, up from 71% last year and 48% in 2021.**
- **Most leaders say their ROI on observability tools to date has far exceeded expectations (55%), compared to just 7% of beginners.**
- **On average, leaders have launched 34% more products/revenue streams from their software engineering teams, than beginners.**

Teams that are hitting their targets and efficiently adding value by way of new revenue streams tend to be happier. As we mentioned earlier, 35% of leaders say they've had no challenges hiring enough observability talent or finding individuals with the right skills, which suggests that success does indeed breed success.

89% of leaders are completely confident in their ability to meet their application availability and performance requirements.

86% of leaders report ROI on their observability tools has exceeded their expectations.

Lower risk, faster fixes, fewer outages

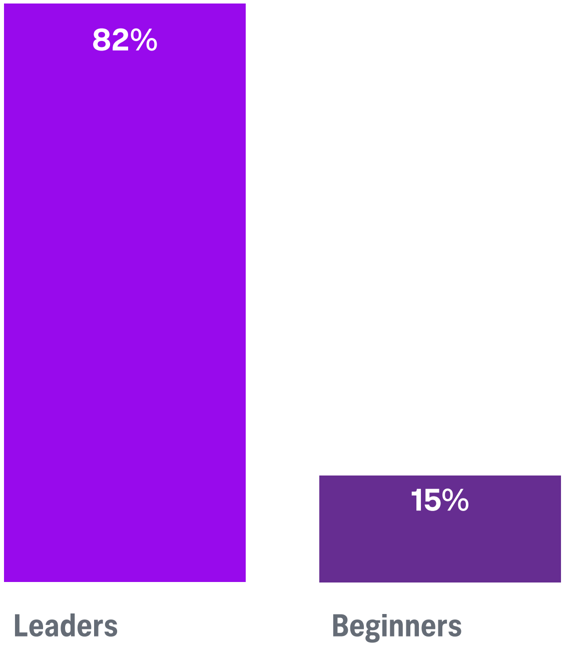
Observability leaders outperform beginner organizations across several application development and reliability KPIs, including:

- **3.8x as many leaders (47% versus 15% of beginners) can push code to production on demand for most internally developed applications.**
- **6.3x as many leaders report root cause identification has gotten significantly faster (63% versus 10%).**
- **Leaders report more actionable alerts, and 62% say that half or more of these alerts are triaged by automated remediation systems.**
- **Though leaders push code to production more frequently, they report that downtime is less common; 57% say that business-critical internally developed applications go down once every few quarters or less.**
  - **Median number of such outages per year: Leaders: 2; Beginners: 6.**
- **Resolution is faster, too: 4x as many leaders say that they resolve instances of unplanned downtime or serious application degradation to business-critical internally developed applications in just minutes. By contrast, beginners are 2x as likely to report resolution takes days.**

These KPIs comprise nearly all the DevOps Research and Assessment (DORA) metrics, which are used to measure high-quality software development and delivery.

Leaders Reap the Benefits of Security and Observability Convergence

Leaders report that bringing together aspects of observability and security monitoring tools and teams has had "significant positive impact" on risk management and incident response.



Leaders are also more likely than beginners to report that observability solutions have:

- **Accelerated development times: 59% say they've seen a significant improvement versus 25%**
- **Accelerated deployment times: 63% say they've seen a significant improvement versus 25%**
- **Increased visibility across cloud-native and traditional apps: 60% say they've seen a significant improvement versus 25%**
- **Accelerated problem detection: 59% say they've seen a significant improvement versus 24%**
- **Accelerated problem resolution: 65% say they've seen a significant improvement versus 25%**

These differences, especially that 35-point gap in visibility across traditional and cloud-native apps, are noteworthy — and the gap has widened across all categories compared to last year. Certainly the data shows that every organization is heading toward this hybrid, multicloud reality and will need true visibility across all of it.

They've also seen that observability solutions are helping promote cross-functional alignment. Sixty percent of leaders attribute improved alignment among ITOps, developers and security teams to their use of observability solutions, compared to just 26% of beginners. Also, 55% of leaders say they've seen an improvement in hiring efforts versus 23% of beginners.

More than ever, leaders are using observability solutions to significantly improve their visibility into hybrid architectures — while also accelerating development, deployment, incident detection and problem resolution.

Lessons From the Leaderboard

It’s hard to argue with the advantages of being a leader. So what are the secrets to their success? Aside from just length of time running maturing their practice, leaders consistently favor a few key factors that help set them apart from the competition.

Expect the unexpected

No business has been immune from the rollercoaster of the last several years — demand spikes, increasing cyberthreats, geopolitical tensions and natural disasters, just to name a few. But there has been a big difference in how organizations have reacted.

For leaders, resilience is foundational. Not only do 97% of observability leaders cite having a formal approach to resilience, a significant 81% have instituted that strategy across the organization to protect critical systems. This formal, organization-wide approach to resilience is only 8% for beginners, illuminating a key area of improvement moving forward.

Looking ahead, observability leaders are also more apt to have definitive plans to invest in solutions that further increase resilience over the next year — but their top priorities don't line up with those of beginners. Chief among them?

- **Gaining more visibility throughout the entire technology environment, which is the no. 1 priority for leaders and outweighs beginners' plans by 15 points.**
- **A close second: Examining non-technical business processes for vulnerabilities and mitigating risk, which is an 18-point spread compared to beginners.**

We don't know what the future holds for business or observability. But by investing more in key resilience strategies and solutions, leaders are more likely to react quickly while preventing any issues from becoming major incidents.

It's a team effort: **100% of leaders** collaborate with other line-of-business leaders (security, finance, marketing, operations, etc.) on resilience strategies, investments and identification of critical business systems to protect.

Come together. Right now. Over observability.

Things are getting harder. Environments and apps are becoming more complex, and modern delivery methods like microservices are harder to understand. At the same time, 45% of leaders report a significant uptick in the number of observability vendors they're working with. This reality translates to thornier problems as teams try to sort through the noise to pinpoint the root cause of an incident or fix a performance degradation.

To combat complexity creep, observability leaders are collaborating more with teams across the organization, using the same tools and datasets to better see into systems, share information, diagnose problems and optimize performance. When asked whether they had already converged various tools and teams with observability, leaders say yes more often across all six categories we inquired about: AIOps, application performance monitoring, infrastructure monitoring, digital experience monitoring, log management and network performance monitoring.

In integrating these functionalities, teams can work together more efficiently and reduce duplicate efforts while banding together for proactive monitoring.

Leaders are 75% more likely to report some level of convergence with observability tools and teams has taken place.

Think for yourself

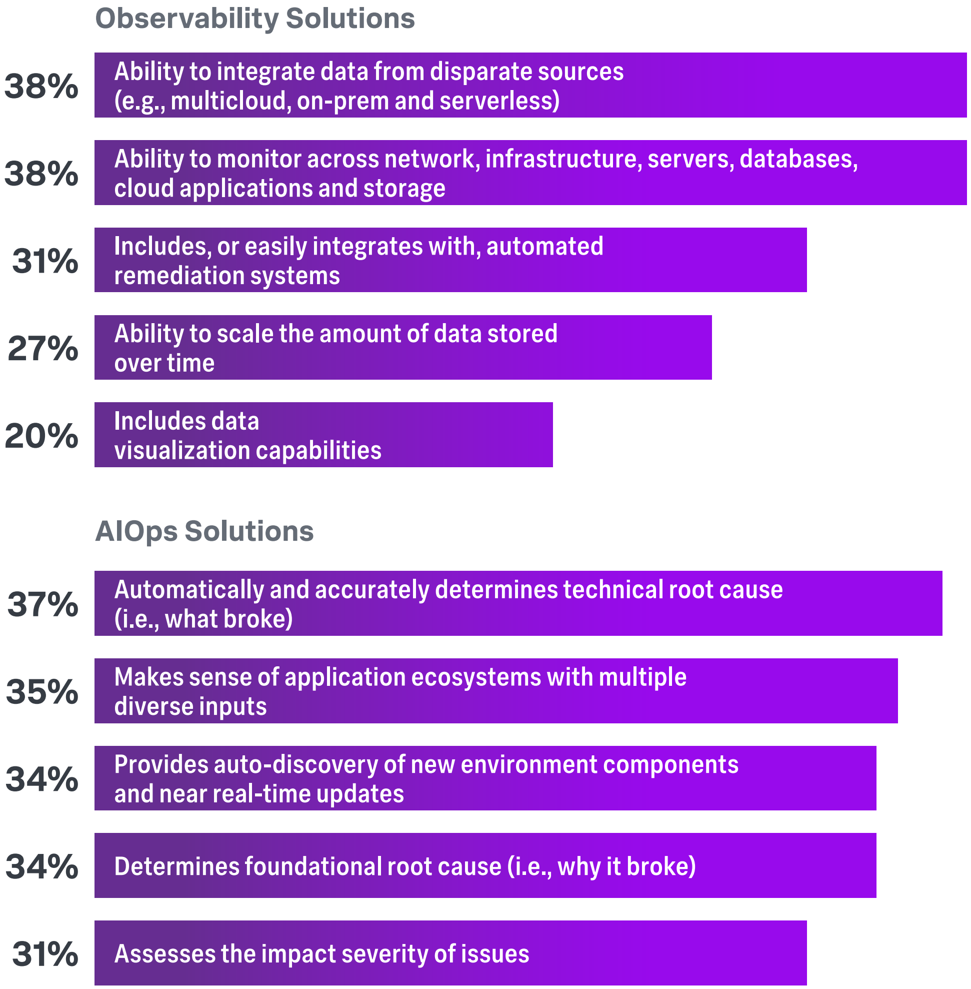
Observability leaders approach purchasing with more skepticism. They are far more likely to report seeing frequent o11y-washing than beginners (68% versus 29%), and cite similar levels of AI Ops-washing as well (56% versus 25%).

When we asked leaders what organizations should look for when evaluating observability tools, two responses tied for first, standing out above other options by several percentage points: ability to integrate data from disparate sources; and ability to monitor across network, infrastructure, servers, databases, cloud applications and storage.

These frontrunners both boil down to consolidation and visibility. With most orgs charting a decidedly hybrid course for the foreseeable future, observability teams require tools with the ability to monitor multiple cloud environments, on-premises deployments, hybrid apps and everything in between. Organizations should take a page from leaders' playbooks, assessing any observability solution with a critical eye to ensure it aligns with their visibility objectives.

Leaders' Advice When Evaluating Tools

When it comes to selecting both observability and AIOps solutions, leaders recommend emphasizing the following capabilities.



Build a strong foundation

Implementing an observability practice in any organization can feel daunting. How can you achieve optimal visibility? How can you detect — and resolve — problems faster? Where do you even start?

When we asked this question, leaders and beginners have similar priorities: Begin by building observability pipelines based on standardized metrics, logs and traces. Hint: OpenTelemetry is perfect for this. With this as a first step, the rest can fall into place more easily, and standardization can help ensure consistency and enable scalability over time.

One answer that ranked very highly among leaders, but not beginners: the importance of implementing feedback loops when beginning an observability practice. While feedback loops — including post-incident reviews that assess why an incident occurred — are a principal part of any effective operations discipline, they may be less vital than other foundational capabilities. This begs the question: Are some observability leaders too far removed from the beginning stages of implementing an observability practice to provide advice for newbies?

Leaders and beginners agree that one of the most vital first steps to implement an observability practice is to build observability pipelines based on standardized metrics, logs and traces across the org.

Key Recommendations

1. Prioritize resilience

Bad things are bound to happen — outages, system stressors, adverse events. Creating and implementing a resilience strategy is vital to your organization's ability to proactively get ahead of major issues while staying secure and reliable in the face of the next disruption. Your customers demand it.

Leaders illustrate the importance of not just having a formal resilience strategy, but also having it implemented organization-wide, versus just in pockets. By baking resilience into all they do, leading organizations are more prepared to respond rapidly when incidents occur, and pivot quickly when the macro environment calls for it.

2. Have standards

Whether just getting started with observability or evolving your practice, respondents across all maturity levels report that standardized metrics, logs and traces are an essential first step. They help ensure data is consistent across systems while increasing efficiency and promoting interoperability.

Leaders also more often have a centralized observability team that works together across standardized tooling. That approach may not work for everyone, but it's an important consideration when mapping out how observability professionals fit into your overall organizational structure.

Regardless of whether you have a centralized observability team or specialists distributed across app development teams, set your standards now and build the right data pipelines. When built correctly on standardized metrics, these data pipelines will help you have the flexibility to scale with your needs and adopt any observability tool as your practice matures.

3. Look under the hood

With the prevalence of both o11y- and AIOps-washing, it's imperative to pick the right product from your vendor and scrutinize every solution before purchase. Respondents across all maturity levels — and especially leaders — emphasize the importance of selecting observability solutions that integrate data from disparate sources, and monitor across everything from infrastructure to cloud applications. Hybrid is here to stay, so finding observability solutions that give you eyes into all your systems is paramount.

When evaluating a new solution, ask your vendor to show you the unique capabilities of their product. What differentiates it from legacy monitoring solutions? Does it give you visibility into both cloud and on-prem environments? Does it also monitor across networks, infrastructure and databases? Don't be afraid to ask questions — you'll be glad you did before making a purchase.

4. Build feedback loops

Things will go wrong. It's a fact of life. A robust observability practice, of course, helps to mitigate those risks and fix issues before they turn into failures or outages. But even the most sophisticated observability practice won't be able to prevent every single incident. What distinguishes observability leaders from beginners, however, is their ability to learn from their mistakes — a reason why leaders ranked feedback loops so highly in their advice when building an observability practice.

After an incident is resolved, schedule a post-incident review to examine the root cause of the problem, so you can answer what went wrong, why and how you can prevent it next time. This extra step can help you improve systems and tune alerts to reduce superfluous noise while preventing similar incidents from happening in the future.

This practice also builds a culture of continuous improvement across the observability team — a key quality that will set your team up for success as observability continues to evolve.

Country highlights

Snapshots of the global state of observability

Australia and New Zealand

In Australia and New Zealand (ANZ), organizations tend to be more mature in their observability journey: Just 25% of respondents are beginners (versus 34% in the rest of the world) and significantly more are classified as “evolving” (36% versus 19%).

Orgs in Australia and New Zealand focus more on resilience. Fifty-five percent report having a formal approach to resilience, instituted organization-wide across critical systems (versus 39% in other countries). ANZ organizations are also more likely to invest in resilience solutions that examine non-technical business processes to detect vulnerabilities and mitigate risk (55% versus 44%).

From a process standpoint, organizations in ANZ are more likely to drive observability tool adoption from their centralized IT team (48% versus 26% in other countries) and less likely to rely on a platform engineering team to provide tooling to developers and operations teams (19% versus 35%).

Orgs in Australia and New Zealand seem to value observability subject matter expertise and specialization more than their peers. When asked how they would advise a colleague trying to implement an observability practice, they more often suggest “staffing a dedicated observability team whose task is to take ownership of observability” than respondents in other countries (40% versus 30%).

ANZ respondents are also more likely to take a platform approach to observability. While most are increasing the number of capabilities in their observability toolsets (53% versus 31%), they’re also significantly consolidating the number of observability vendors (34% versus 13%).

Canada

Respondents in Canada are more mixed in terms of observability maturity: While less likely to be leaders (5% versus 10% in the rest of the world), they are also less likely to be beginners (25% versus 34%). This leaves a predominant 70% in either the “emerging” or “evolving” categories.

Canadians, like their peers in ANZ, emphasize resilience, with 50% reporting a formal approach instituted organization-wide across critical systems (versus 39% across other countries). And they strongly agree that failing to advance resilience may lead to losing customers (50% versus 33%) and falling behind on innovation (54% versus 33%).

Canadian orgs are more likely to employ cloud-native architecture for their internally developed applications, with 70% expecting that a larger proportion of these apps will be built on cloud-native architectures in the coming year (versus 57% in the rest of the world).

Canadians are aggressively increasing the capabilities in their toolsets while also rationalizing vendors. Though 42% report that they have been significantly increasing the number of functional capabilities in their observability environment (versus 32% in the rest of the world), 51% have been consolidating vendors (compared to 39%).

Staffing observability teams seems particularly challenging in Canada today, which may explain why so many orgs are rationalizing vendors to drive simplicity. Fifty-three percent of Canadian respondents report hiring challenges related to both the quantity and quality of IT operations staff (versus 42% in the rest of the world), and 56% report hiring challenges related to both the quantity and quality of application development staff.

France

Organizations in France are just a tad below the global mean in terms of observability maturity: Beginners account for 39% versus 33% in the rest of the world, while a near-identical proportion are leaders (9% versus 10% in the rest of the world) and evolving (19% versus 20%).

French organizations lag in a couple key areas:

- Using AI and ML within their observability toolsets (23% versus 31%).
- Having an observability solution that spans both cloud-native and traditional application architectures (25% versus 38%).

On the bright side, French organizations are also ahead of the pack when it comes to a few best practices. For starters, French respondents are more likely to have open standards for data formats used for observability (46% versus 35% across other countries), which improves data integration, visibility and correlation.

French orgs are also more likely to have observability tools that span the full application stack, enabling them to monitor across everything from networks and infrastructure to servers, databases and cloud apps. This visibility helps eliminate blind spots while allowing teams to gain insights faster.

To alleviate the challenges that accompany rising complexity and data silos, organizations in France rationalize their observability vendors — or at least keep the number of vendors flat (67% versus 54% in the rest of the world).

Germany

Organizations in Germany are significantly below the global mean in terms of observability maturity: 42% are beginners versus 32% in the rest of the world, while just 19% have progressed to an evolving or leading state (compared to 31% in the rest of the world).

While not a determining factor in maturity, German organizations have made less progress than their peers on resilience. Only 32% report having a formal approach to resilience that has been instituted organization-wide across critical systems (versus 41%). And German respondents are less likely to plan investments in resilience solutions that increase visibility throughout the entire technology environment (39% versus 50%) or improve the ability to recover to a “known good” copy of data (35% versus 45%).

One key impediment to German orgs’ maturity? They’re less likely to be able to extensively correlate the data collected by their observability and monitoring tools (31% versus 39%). Complexity is a probable culprit given that Germans are more likely to be adding observability vendors to their environments (64% versus 42%), which can exacerbate complexity and integration challenges.

Reduced alert accuracy is a likely outcome of German orgs' lower observability maturity. For 78%, less than half of the alerts from observability and monitoring solutions are true positives (versus 44% in other countries).

However, many German organizations have identified the need for more comprehensive, extensible observability solutions to overcome the challenges they face. Fifty-nine percent of German organizations acknowledge that having a single observability solution that can cover both cloud-native and traditional app architectures is both important and necessary (versus 48%).

India

Respondents in India are on the leading edge of observability maturity: 23% of represented orgs are classified as leaders (versus 9% in the rest of the world), and just 18% are beginners (versus 34% in the rest of the world).

Perhaps as a result of their observability maturity, Indian organizations are more aggressively transforming their internally developed application portfolios. Eighty-two percent expect that substantially more of these apps will be cloud-native within the next 12 months (versus 56% in the rest of the world).

Indian orgs also prioritize resilience — 52% say they have a formal approach to resilience that has been instituted organization-wide across critical systems (versus 39%). And they're not slowing down. Indian organizations are more likely to plan to invest in resilience solutions that will accelerate incident response and remediation (65% versus 49%) and improve the recovery of customer/user services (62% versus 50%).

Indian organizations approach observability tools with greater skepticism — and for good reason. Sixty-six percent report having seen o11y-washing (versus 42% in the rest of the world). When asked what they look for in observability tools, teams in India focus on the ability to integrate data from disparate sources, such as multiple cloud environments, on-premise deployments and serverless functions (45% versus 35%). They also look for tools with integrated visualization capabilities (27% versus 19%).

Japan

Organizations in Japan are quite behind in terms of observability maturity: 48% are beginners, compared to 31% in the rest of the world. And only 1% classify as leaders (versus 11% in other markets).

Japanese organizations lag in a few specific areas:

- Using observability solutions for at least two years (18% versus 38%)
- Correlating data collected from the bulk of their observability and monitoring tools (11% versus 42%)
- Using AI and/or ML technologies within their observability toolsets (15% versus 33%)
- Having an observability solution that spans both cloud-native and traditional application architectures (12% versus 40%)

Nonetheless, the Japanese are aggressively modernizing their internally developed applications. These orgs anticipate that more of these apps will be cloud-native over the next year (67% versus 57%), and 41% say that the majority of their apps are updated on demand (versus 29% across other countries).

Although Japanese organizations do not always have the tools and processes in place to monitor and triage their applications, they are forging ahead — at least on the application development front.

Singapore

Observability maturity among organizations in Singapore is behind the global mean: 41% are beginners versus 33% in the rest of the world, while just 6% are leaders (compared to 10% elsewhere).

As observed among beginners, and other countries with a high concentration of beginners, organizations in Singapore are more likely to have siloed monitoring tools and teams. They are less likely to report convergence between observability and other functions, including infrastructure monitoring (9% versus 24%), digital experience monitoring (14% versus 36%), network performance monitoring (10% versus 26%), and security monitoring (13% versus 28%).

Singaporean teams especially struggle with hiring, with 57% reporting challenges related to both the quantity and quality of IT operations staff (versus 41% across other countries). On top of that, their teams are experiencing lower efficiency as more staff "quiet quit" (45% versus 31%).

These issues are likely contributing to poorer application performance KPIs and outcomes:

- Singaporean organizations have less confidence in their ability to meet application reliability and performance objectives (30% versus 44%).
- More than half (54%) of Singaporean respondents say their change failure rate for new code is more than 30%. In the rest of the world, only 36% of respondents report failure rates this high.

On the upside, organizations in Singapore are aggressively adopting AIOps tools to help. Thirty-six percent say they are in the process of deploying AIOps solutions (versus 24%). And among early adopters of AIOps, 64% say they're getting faster at diagnosing the root cause of issues (versus 50%).

United Kingdom

In the U.K., organizations are just a tick below the global mean in terms of observability maturity: Beginners account for 38% (versus 32% in the rest of the world), while the proportions of leaders (10%) and evolving organizations (20%) are the same as the international average.

Compared to other countries, U.K. orgs are more likely to have already converged monitoring tools and teams with their observability practices. This is true across infrastructure monitoring (30% versus 22%), log management (35% versus 23%) and network performance monitoring (33% versus 23%).

U.K. respondents are more likely to have a platform engineering team that provides self-service observability and other software delivery tooling to developer teams and SREs/DevOps engineers (42% versus 32%). Conversely, it's less common for these orgs to embed SREs and DevOps engineers in development teams that select and use observability tools (12% versus 20%).

U.K. organizations are likely to reskill individuals outside of the observability team to help fill gaps (45% versus 38%). They also cite investing more in observability training for IT/development staff as key to overcoming staffing challenges (52% versus 44%). Why the emphasis on reskilling? Those in the U.K. expect resourcing positions to get harder as macroeconomic conditions potentially worsen (anticipated by 49% of respondents in the U.K., versus 37% across the rest of the world).

United States

U.S. organizations are further along in their observability journey than their global counterparts. Thirteen percent are classified as leaders (versus 9% in the rest of the world), while just 25% are beginners (versus 36%).

For starters, orgs in the U.S. are more focused on resilience, with 50% reporting a formal approach that has been instituted organization-wide across critical systems (versus 36% across the rest of the world). These orgs also report better alerting capabilities. Close to a third tell us their monitoring systems have an alert accuracy of 75% or more, compared to 22% of their peers globally.

U.S. orgs are also more apt to have their observability tools and teams already unified, at least to some degree, with tools and teams in other functions, including application performance monitoring (32% versus 24%), network performance monitoring (30% versus 23%) and infrastructure monitoring (28% versus 22%)

When it comes to purchasing, U.S. respondents more often state their buying process is centralized within ITOps (32% versus 26%) or driven by top-down directives from executives (18% versus 9%).

U.S. organizations are less likely to update their applications on demand:

- 24% say they update less than 10% of their internally developed apps via pushing code to production on demand (versus 15% in the rest of the world).
- Just 25% say the majority of internal apps are updated on demand (versus 33%).

However, updates to applications are less likely to cause service-impacting issues that require remediation: 31% of U.S. organizations report more than 30% of code changes degrade application performance, compared to 39% of non-U.S. respondents.

Industry highlights

Standout data points for four select industries

Financial Services

Organizations in financial services tend to be less mature in observability. Just 8% were categorized as leaders, while 43% are beginners. Two trends emerged among those surveyed:

1. Let's start with the bad news first: Financial institutions are less likely to have "excellent visibility" into several aspects of their environments, including legacy infrastructure (41% versus 49% among other verticals), private clouds (42% versus 52%), public cloud infrastructure (53% versus 44%), and their overall security posture (38% versus 53%). This may explain their lower level of confidence as well — just 26% of respondents at financial institutions are completely confident in their ability to meet application reliability and performance objectives (versus 45%).
2. On the bright side, organizations in the financial services sector are more likely to use a robust set of monitoring tools. Compared to 30% in other verticals, 45% of financial institutions report using all of the tools presented in the survey (AIOps, APM, NPM, infrastructure monitoring, digital experience monitoring, log management and security monitoring). Additionally, these organizations are embracing convergence at higher rates — reporting observability tools and teams have already begun converging with AIOPs (36% versus 23%), infrastructure monitoring (33% versus 22%), digital experience monitoring (36% versus 24%), log management (37% versus 23%), and NPM (33% versus 24%).

One drawback to the variety of monitoring tools (that doesn't appear to be offset by tool and team convergence) is that financial service organizations struggle with siloed data. Thirty-two percent report that correlating data from multiple sources is one of their primary observability challenges (versus 24% in other verticals).

Manufacturing

Manufacturing organizations are right in the middle of the pack in terms of observability maturity: 8% are leaders and 38% are beginners. Three noteworthy trends:

1. Manufacturers are less likely than their peers to use all of the monitoring tools covered in the survey (24% versus 33%). In particular, they're less likely to report using AIOps tools (51% versus 59%) and NPM tools (72% versus 80%).
2. Manufacturers are more likely to centralize both data and teams in their observability practice.
    - When asked what they would recommend to a peer building out an observability practice, 34% cite data centralization as one of their top three recommendations (versus 27% of peers in other industries).
    - As for team structure, individuals working on observability are more likely to be part of a centralized team focused on standardizing software delivery tooling across the organization (65% versus 57%), as opposed to being distributed among individual app development teams that organically adopt observability tools to suit their specific needs (35% versus 43%).
3. Finally, manufacturers are slower in issue detection. When asked how long it takes for the right teams to detect a problem with an internally developed app, 40% said the mean time is measured in days (versus 30% across other verticals). But manufacturers seem aware of the issue. Forty-one percent strongly agree that their org needs to increase resilience, fearing they'll lose customers due to outages and downtime (versus 33% of their peers in other industries). And 95% report observability leaders are collaborating more with business leaders on the topic of resilience.

Communications and Media

Communications and media companies are leading the way on observability maturity, with 13% qualifying as leaders and just 26% as beginners. The industry's relative strength on observability seems to stem from:

1. Early adoption of observability. An impressive 28% have been using observability solutions for more than three years (versus 12% in other verticals). They're also more aggressively building out their toolsets, with 40% reporting that they've been significantly increasing the number of tools and capabilities in use (versus 31%). Communications and media organizations have also been focused on breaking down data silos, with 46% reporting that all or almost all of their collected observability data can be correlated across tools (versus 38%).
2. Convergence of monitoring teams. Twenty-eight percent say that they are in the process of converging AIOps with observability (versus 18% in other industries). This convergence is also happening across APM, digital experience monitoring and NPM. And 37% say security monitoring is already converged with observability (versus 26%).

The payoffs from observability maturity are evident across this sector. Two areas that stand out: more accurate alerts and greater automation. When asked to estimate the accuracy of monitoring alerts, 35% reported a 75% and above accuracy (versus 24% of their peers). Additionally, 55% of these alerts are triaged and remediated via automation (versus 48% among their peers).

Public Sector

Organizations in the public sector lag in terms of observability maturity. Just 4% were categorized as leaders, while a majority (53%) are beginners. Some challenges this vertical faces:

1. Siloed monitoring tools and teams. Right now, only 14% of public sector orgs report that their APM tools and teams are unified with their observability practice, versus 27% in other verticals. This is even truer for AIOps (3% report convergence versus 26%).

   Although they are lagging, public sector organizations are more likely to report there will be functional convergence in the future across APM and observability (37% versus 25%), as well as AIOps and observability (40% versus 24%). This suggests that the public sector recognizes the importance of functional convergence and is making efforts to catch up to its private sector counterparts.
2. Lack of a formal approach to resilience. Public sector organizations also trail the private sector when it comes to their stance on resilience — i.e., the ability to prevent, respond and quickly recover from events that have the potential to disrupt key business processes, service delivery and access to technology. While 40% in the private sector have instituted a formal approach to resilience, only 26% in the public sector have done the same.
3. Staff attrition. The public sector reports more instances of “brain drain,” where critical staff on the observability team are poached and leave for other positions. Forty-nine percent report multiple occurrences of brain drain in the past 12 months (versus 34%). And with a possible recession looming, public sector organizations are more pessimistic: 59% expect that hiring staff with the necessary observability skills will be harder in the event of a recession (versus 43%).

These issues have consequences. While 77% of private sector organizations report faster root cause analysis for internally developed applications in the last 12 months, 48% in the public sector report that it takes the same amount of time or longer than it did 12 months ago.

On a more hopeful note, 74% of public sector orgs report an increase in functional observability capabilities — without creating a more complex vendor landscape, since 77% report that they haven’t added new observability vendors to their ecosystem (versus 55% of private sector organizations). Being able to do more — without the burden of complexity challenges — will be especially handy if skill shortages worsen.

Make your organization more resilient with the unified security and observability platform. Go from holistic visibility to effective action, fast and at scale. See how Splunk can help you keep your organization securely up and running, no matter what digital disruptions come your way.

Learn More

splunk>