# new relic | ETR

o11y

Alerting Groups_

[Info]

2022

# 2022 Observability Forecast

Research into the current use of and future investment in observability

Annual report / September 2022

AUTHOR:

**Alicia Basteri,** Senior Technical Content Marketing Manager, New Relic in

COAUTHOR:

**Daren Brabham,** PhD, Senior Director Analyst, ETR in

# Contents

# List of tables and figures

# About this report

Find quantifiable data points and an in-depth analysis of the state and future of observability.

# Executive summary
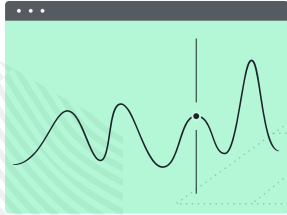
To capture new insights into observability, New Relic partnered with Enterprise Technology Research (ETR) to conduct a survey and analysis for this second annual *Observability Forecast* report.

Last year, the *2021 Observability Forecast* report focused on how, driven by digital transformation, full-stack observability (o11y) has become mission-critical to the success of every modern business. The report provided compelling reasons why it's time for organizations to shift to full-stack observability so that they can plan, build, deploy, and run great software that powers optimal digital experiences for their customers, employees, partners, and suppliers.

This year, the *2022 Observability Forecast* report focuses on the next chapter in the story—it looks at what's driving observability practices today, how organizations are transforming those practices, and how observability impacts the lives of technical professionals. The report also includes a snapshot of emerging technologies that will potentially drive a further need for observability over the next three years.

Today, many organizations make do with a patchwork of tools to monitor their technology stacks, requiring extensive manual effort for fragmented views of their information technology (IT) systems and overall businesses. At the same time, survey respondents longed for—planned for—simplicity, integration, seamlessness, and more efficient ways to complete high-value projects.

## Challenges

Monitoring is fragmented. Most organizations do not currently monitor their full tech stacks.

**82%** [+]
used 4+ observability tools

**33%** [+]
still detected outages manually or from complaints

**27%** [+]
had achieved full-stack observability

**5%** [+]
had a mature observability practice

**<2%** [+]
used a single observability tool
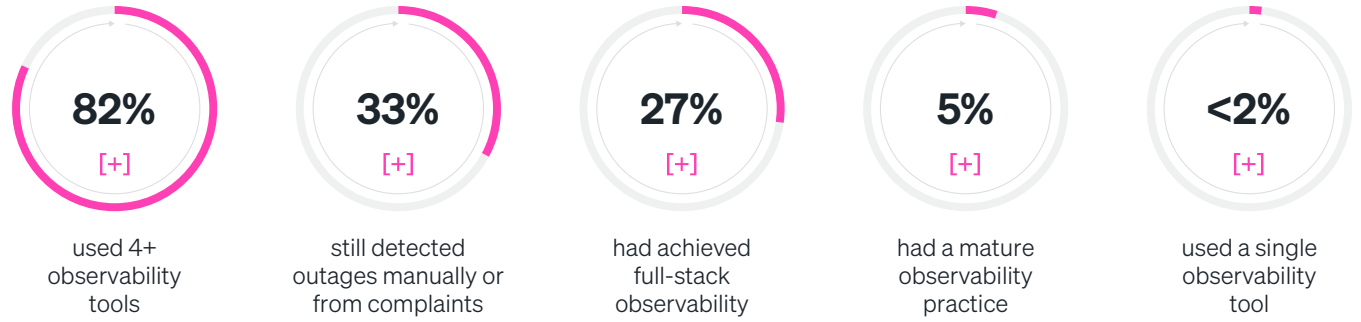
**Figure 01.** Summary of observability challenges

## Opportunities

Observability improves service-level metrics. Organizations see its value—and expect to invest more in it.

**88–97%** [+]
of 17 different observability capabilities should be deployed by 2025

**73%** [+]
said C-suite execs are advocates of observability

**72%** [+]
expected to increase or maintain observability budgets next year

**50+%** [+]
said observability enables core business goals

**47%** [+]
preferred a single, consolidated observability platform

**Figure 02.** Summary of observability opportunities

## Prioritizing/achieving full-stack observability

[+]

**fewer outages**

**faster MTTD**

**faster MTTR**
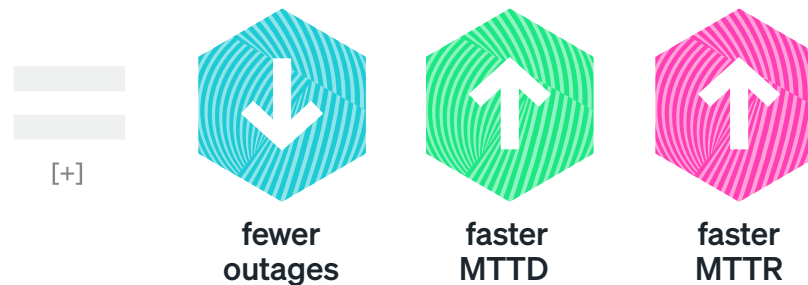
**Figure 03.** Summary of how observability helps improve service-level metrics

# Definitions

We've defined some common terms and concepts used throughout this report.

## Observability

Note that to avoid bias, we did not define observability in the survey.

Observability is the ability to measure how a system is performing and identify issues and errors based on its external outputs. These external outputs are telemetry data (metrics, events, logs, and traces). Data-driven engineering puts telemetry data to work to drive action. Observability requires instrumenting systems to secure actionable data that identifies an error and details when, why, and how an error occurs. Observability also involves collecting, analyzing, altering, and correlating that data for improved uptime and performance. Achieving observability brings a connected, real-time view of all data from different sources—ideally in one place—where teams can collaborate to troubleshoot and resolve issues faster, ensure operational efficiency, and produce high-quality software that ensures an optimal customer/user experience.

Software engineering, development, site reliability engineering, operations, and other teams use observability to understand the behavior of complex digital systems and turn data into tailored insights. Observability helps them pinpoint issues more quickly, understand root causes for faster, simpler incident response, and proactively align data with business outcomes.

A subset of observability, monitoring is reactive and reveals *what* is wrong (an error) and *when* an error happened. Observability is proactive in how it determines *why* and *how* an error happened (in addition to the what and when). Monitoring tools alone can lead to data silos and data sampling, while an observability platform provides the ability to instrument an entire technology stack and correlates the telemetry data drawn from it in a single location for one unified, actionable view.

| Monitoring | Observability |
|---|---|
| Reactive | Proactive |
| Situational | Predictive |
| Speculative | Data-driven |
| What + when | What + when + why + how |
| Data silos | Data in one place |
| Data sampling | Instrument everything |

**Table 01.** Key differences between monitoring and observability

Many tools are purpose-built for observability and include capabilities such as:

- ⌬ AIOps  (artificial intelligence for IT operations)
- ⚠ Alerts
- 🖼 Application performance monitoring (APM)
- 🖼 Browser monitoring
- 🖥 Custom dashboards
- 🗄 Database monitoring
- 🔗 Distributed tracing
- ⚙ Error tracking
- ⬓ Infrastructure monitoring
- ✦ Kubernetes monitoring
- 🗐 Log management
- ◈ Machine learning (ML) model performance monitoring (MLOps)
- 📈 Mobile monitoring
- ⇄ Network performance monitoring
- 🛡 Security monitoring
- λ Serverless monitoring
- ✛ Synthetic monitoring

Real-user monitoring (RUM) includes browser monitoring and mobile monitoring. Digital experience monitoring (DEM) includes RUM plus synthetic monitoring.

# Full-stack observability

The ability to see everything in the tech stack that could affect the customer experience is called full-stack observability or end-to-end observability. It is based on a complete view of all telemetry data.

With full-stack observability, engineers and developers don't have to sample data, compromise their visibility into the tech stack, or waste time stitching together siloed data. Instead, they can focus on the higher-priority, business-impacting, and creative coding they love.

Full-stack observability, as used in this report, is achieved by organizations that deploy specific combinations of observability capabilities, including customer experience monitoring/ DEM (front-end), services monitoring, log management, and environment monitoring (back-end).

See how many respondents had achieved full-stack observability.



**Environment monitoring**
› Database monitoring AND/OR
› Infrastructure monitoring AND/OR
› Network monitoring

**Services monitoring**
› Application performance monitoring AND/OR
› Serverless monitoring

**Log management**

**Customer experience monitoring/DEM**
› Browser monitoring AND/OR
› Mobile monitoring AND/OR
› Synthetic monitoring

**Full-stack observability**
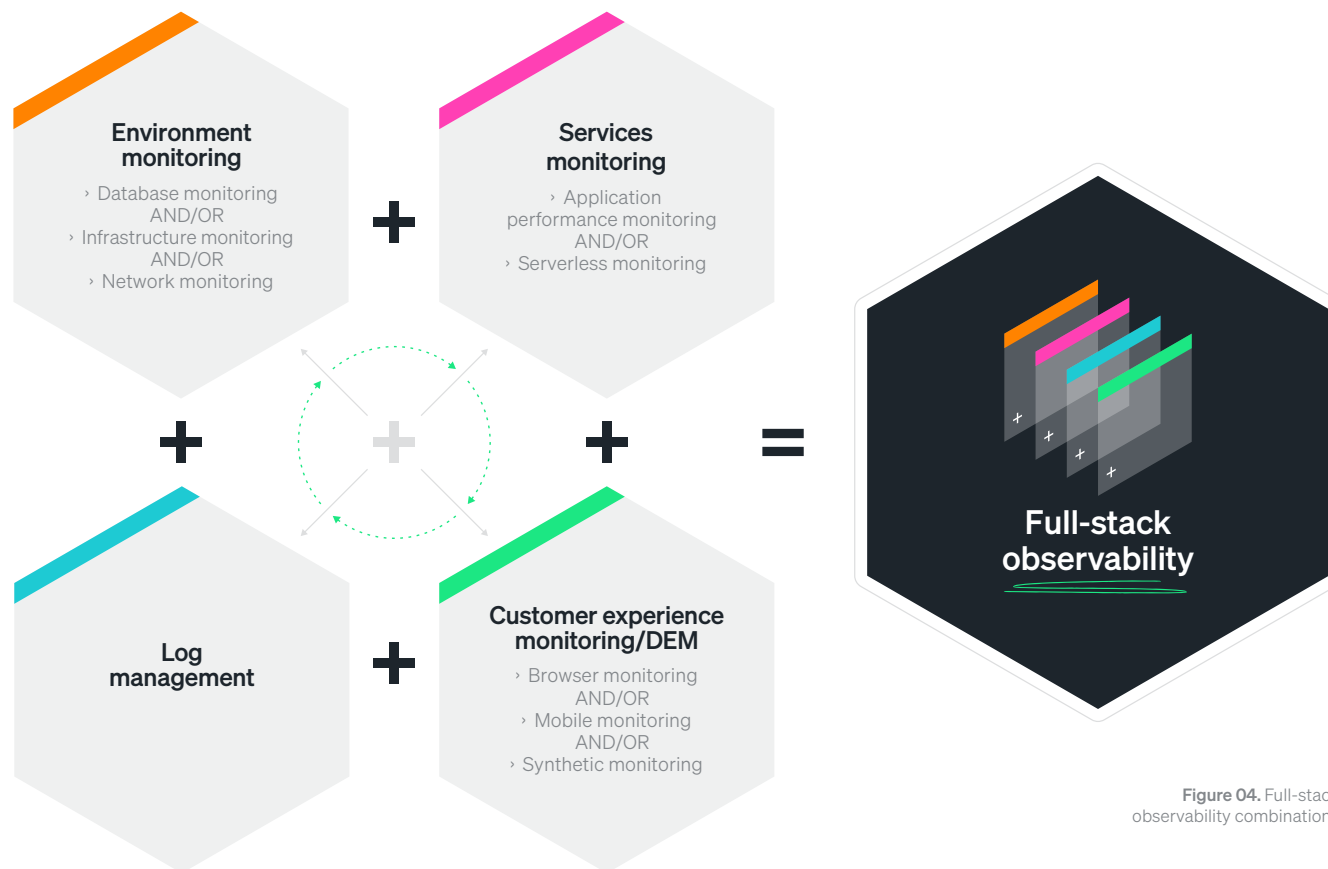
**Figure 04.** Full-stack observability combinations

# Mature observability practice

What constitutes a mature observability practice is somewhat subjective. In this report, we define a mature observability practice as one that follows best practices and delivers specific outcomes.

## Best practices

- Instrumentation is automated
- Portions of incident response are automated
- Infrastructure is provisioned and orchestrated using automation tooling
- Telemetry is captured across the full stack
- Telemetry (metrics, events, logs, traces) is unified in a single pane for consumption across teams
- Users broadly have access to telemetry data and visualization
- Software deployment uses CI/CD (continuous integration, development, and deployment) practices
- Ingestion of high-cardinality data
- Ability to query data on the fly

## Outcomes

- Developer [and engineer] time is shifted from incident response (reactive) towards higher-value work (proactive)
- Improved collaboration across teams to make decisions related to the software stack
- Observability mitigates service disruptions and business risk
- Telemetry data includes business context to quantify the business impact of events and incidents
- Observability improves revenue retention by deepening understanding of customer behaviors
- Observability creates revenue-generating use cases

**For the purpose of this report, a mature observability practice employs at least these five characteristics:**

- ✓ Unifies telemetry (metrics, events, logs, traces) in a single pane for consumption across teams
- ✓ Shifts developer and engineer time from incident response (reactive) towards higher-value work (proactive)
- ✓ Improves collaboration across teams to make decisions related to the software stack
- ✓ Mitigates service disruptions and business risk
- ✓ Improves revenue retention by deepening understanding of customer behaviors

Learn about the maturity of survey respondents' observability practices.
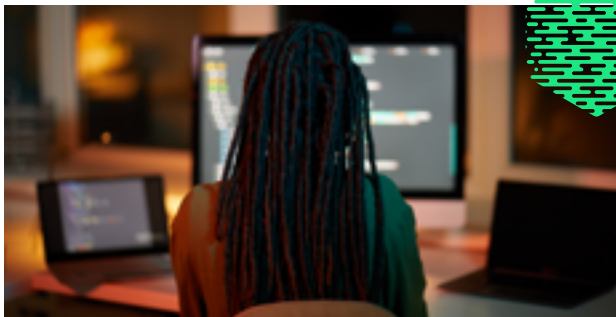
# Roles

Study participants consisted of practitioners and IT decision-makers (ITDMs).
Practitioners are typically the day-to-day users of observability tools.

| | Roles | Job titles | Descriptions | Common KPIs |
|---|---|---|---|---|
| **Practitioners** | Developers | Application developers, software engineers, architects, and their frontline managers | Members of a technical team who design, build, and deploy code, optimizing and automating processes where possible<br><br>Enjoy taking on new coding challenges, adopting new technologies, and being up to date on the latest and greatest tools | • Cycle time (speed of making changes)<br>• Endpoint security incidents<br>• Error rates<br>• Lead time (speed from idea to deployment)<br>• Mean time between incidents (MTBI)<br>• Speed of software performance<br>• Uptime percentage |
| | Operations professionals | IT operations engineers, network operations engineers, DevOps engineers, DevSecOps engineers, SecOps engineers, site reliability engineers (SREs), infrastructure operations engineers, cloud operations engineers, platform engineers, system administrators, architects, and their frontline managers | Members of a technical team who are responsible for the overall health and stability of infrastructure and applications<br><br>Detect and resolve incidents using monitoring tools, build and improve code pipeline, and lead optimization and scaling efforts | • Availability<br>• Deploy speed and frequency<br>• Error budgets<br>• Error rates<br>• Mean time to detection (MTTD)<br>• Mean time to resolution (MTTR)<br>• Service level agreements (SLAs)<br>• Service level indicators (SLIs)<br>• Service level objectives (SLOs)<br>• Uptime percentage |
| **ITDMs** | Non-executive managers | Directors, senior directors, vice presidents (VPs), and senior vice presidents (SVPs) of engineering, operations, DevOps, DevSecOps, SecOps, site reliability, and analytics | Leaders of practitioner teams that build, launch, and maintain customer-facing and internal products and platforms<br><br>Own the projects that operationalize high-level business initiatives and translate technology strategy into tactical execution<br><br>Constantly looking to increase velocity and scale services | • Customer satisfaction<br>• MTBI<br>• MTTR<br>• On-time project completion<br>• Software development and efficiency<br>• Speed of deployment<br>• Uptime percentage |
| | Executives (C-suite) | More technical focused: Chief information officers (CIOs), chief information security officers (CISOs), chief technology officers (CTOs), chief data officers (CDOs), chief analytics officers (CAOs), and chief architects<br><br>Less technical focused: Chief executive officers (CEOs), chief operating officers (COOs), chief financial officers (CFOs), chief marketing officers (CMOs), chief revenue officers (CROs), and chief product officers (CPOs) | Managers of overall technology infrastructure and cost who are responsible for business impact, technology strategy, organizational culture, company reputation, and cost management<br><br>Define the organization's technology vision and roadmap to deliver on business objectives<br><br>Use digital to improve customer experience and profitability, enhancing company reputation as a result | • Conversion rates<br>• Cost-effectiveness<br>• Customer satisfaction<br>• Return on investment (ROI)<br>• Speed of deployment<br>• Speed of innovation<br>• Total cost of ownership (TCO)<br>• Uptime percentage |

**Table 02.** Roles, job titles, descriptions, and common key performance indicators (KPIs) for practitioners and ITDMs

## Organization size

In this report, organization size is determined by employee count.



**Small**
1–100

**Midsize**
101–1,200

**Large**
1,201+

**Figure 05.** Organization size by employee count

# Methodology

ETR sent survey respondents a questionnaire and compensated them for completing the survey.

All data in this report are derived from the survey, which was in the field from March to April 2022.

ETR qualified survey respondents on the basis of relevant expertise. ETR performed a non-probability sampling type called quota sampling to target sample sizes of respondents based on their country

of residence and role type in their organizations (in other words, practitioners and ITDMs). Geographic representation quotas targeted 14 key countries.

All dollar amounts in this report are in USD.

Download the survey results.

# Respondent demographics

n=1,614

In 2022, ETR polled 1,614 technology professionals—more than any other observability report and 25% more than the 1,295 we polled in 2021—in the same 14 countries across Asia Pacific, Europe, and North America. France, Germany, Ireland, and the United Kingdom represented 44% of respondents. Approximately 31% of respondents were from Canada and the United States. The remaining 25% were from the broader Asia Pacific region including Australia, India, Indonesia, Japan, Malaysia, New Zealand, Singapore, and Thailand. View regional highlights.
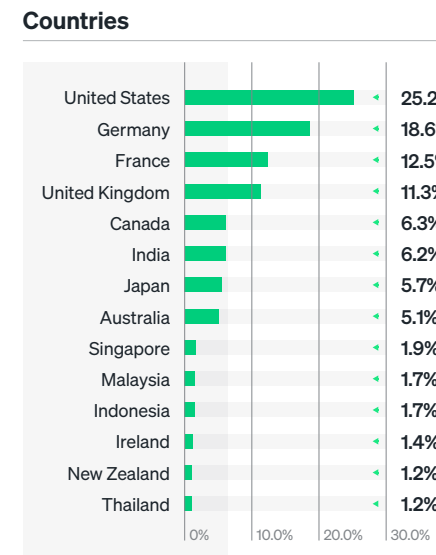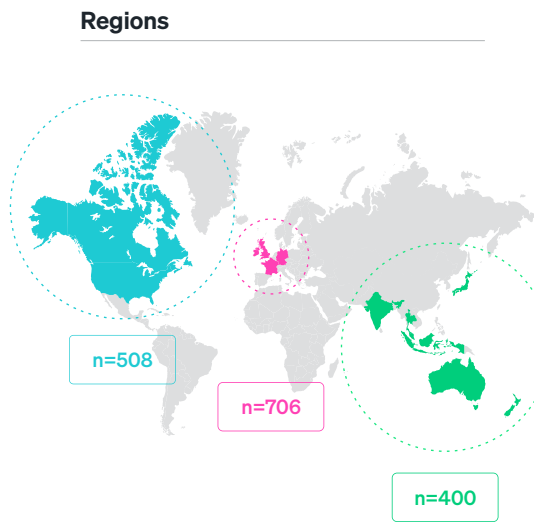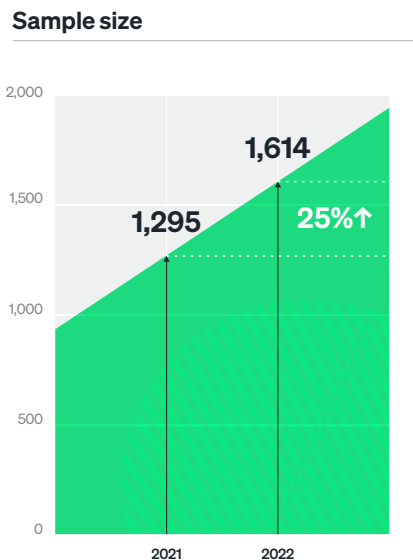
The survey respondent mix was about the same as last year—65% practitioners and 35% ITDMs. A running theme in the data is a split between what practitioners value and perceive and what ITDMs value and perceive regarding observability.
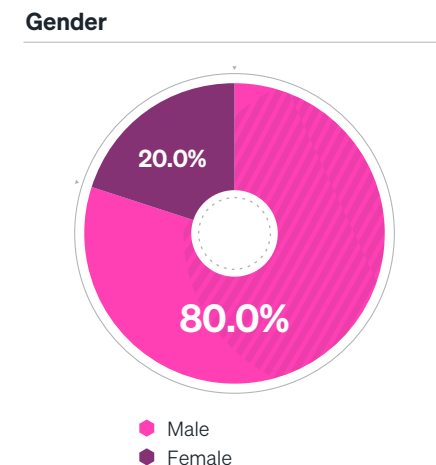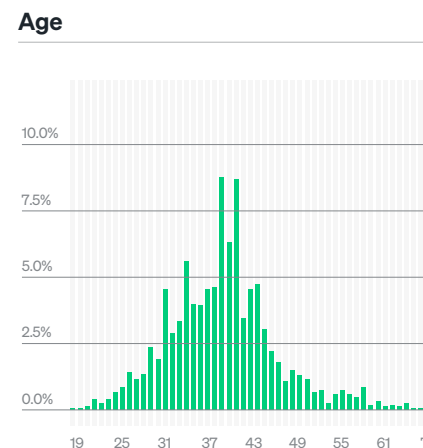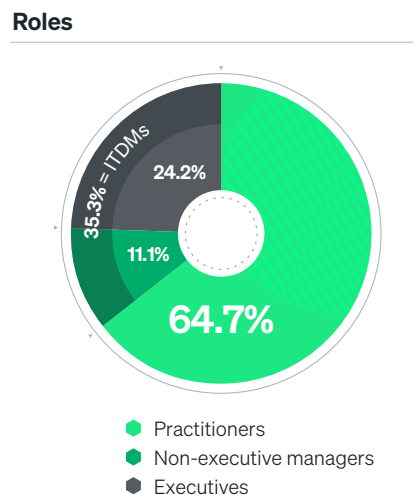
Respondents' age ranged from 19–72 with 80% identifying as male and 20% identifying as female, which (unfortunately) reflects the gender imbalance among technology professionals today.

**Sample size**



**Regions**



n=508

n=706

n=400

**Countries**

| United States | 25.2% |
| Germany | 18.6% |
| France | 12.5% |
| United Kingdom | 11.3% |
| Canada | 6.3% |
| India | 6.2% |
| Japan | 5.7% |
| Australia | 5.1% |
| Singapore | 1.9% |
| Malaysia | 1.7% |
| Indonesia | 1.7% |
| Ireland | 1.4% |
| New Zealand | 1.2% |
| Thailand | 1.2% |

**Roles**



24.2%

35.3% = ITDMs

11.1%

64.7%

● Practitioners
● Non-executive managers
● Executives

**Age**



**Gender**



20.0%

80.0%

● Male
● Female

**Figure 06.** Respondent demographics, including sample size, regions, countries, roles, age, and gender

# Respondent firmographics

More than half of survey respondents (56%) worked for midsize organizations, followed by 35% for large organizations, and 8% for small organizations.

For organization annual revenue, 17% had $1 million to $9.99 million (35% of those were small organizations and 55% were midsize), 43% had $10 million to $99.99 million (76% of those were midsize organizations), and 40% had $100 million or more (63% of those were large organizations).

The respondent pool represented a wide range of industries, including IT/telecommunications (telco), financial/insurance, industrials/materials/manufacturing, retail/consumer, healthcare/pharmaceutical (pharma), energy/utilities, services/consulting, education, nonprofit/unspecified, and government.

View industry highlights.

### Organization size



8.4%
35.3%
56.3%

- ● Small
- ● Midsize
- ● Large

### Annual revenue



$1M–$9.99M    $10M–$99.9M    $100M+

17.1%    40.1%    42.8%

- ● Small
- ● Midsize
- ● Large

### Industries



| | |
|---|---|
| IT/telco | 38.0% |
| Financial/insurance | 20.0% |
| Industrials/materials/manufacturing | 13.4% |
| Retail/consumer | 11.0% |
| Healthcare/pharma | 6.2% |
| Energy/utilities | 3.0% |
| Services/consulting | 2.9% |
| Education | 2.2% |
| Nonprofit/unspecified | 1.7% |
| Government | 1.6% |
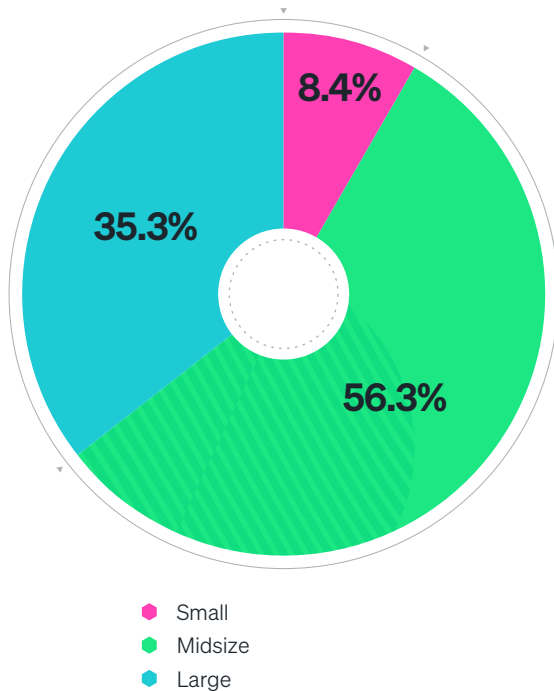
**Figure 07.** Respondent firmographics, including organization size, annual revenue, and industries

# State of observability

## Monitoring is fragmented. Most organizations do not currently monitor their full tech stacks.

# Current deployment

First, we look at the observability characteristics employed and capabilities deployed at the time of the survey, how those capabilities were deployed, strategy and organization, the benefits they experienced, the percent of their IT budgets allocated for observability, their pricing and billing preferences, and the challenges to prioritizing/achieving full-stack observability.

## Mature observability practice characteristics

We asked survey respondents which mature observability practice characteristics they think are the most important and—in a separate question later in the survey—which they had employed. We found that:

- Only 2% indicated that their organizations had all 15 observability characteristics employed
- Just 1% indicated that they had none employed
- More than half (53%) had three to five employed (52% had one to four employed, 48% had five or more employed, and 10% had 10 or more employed)

Based on our definition of a mature observability practice, only 5% of survey respondents had a mature observability practice.

Those with mature observability practices also tended to have more observability practice characteristics employed: 97% had nine or more and 40% had all 15.

Of those who had mature observability practices, 100% indicated that observability improves revenue retention by deepening their understanding of customer behaviors compared to the 34% whose practices were less mature.
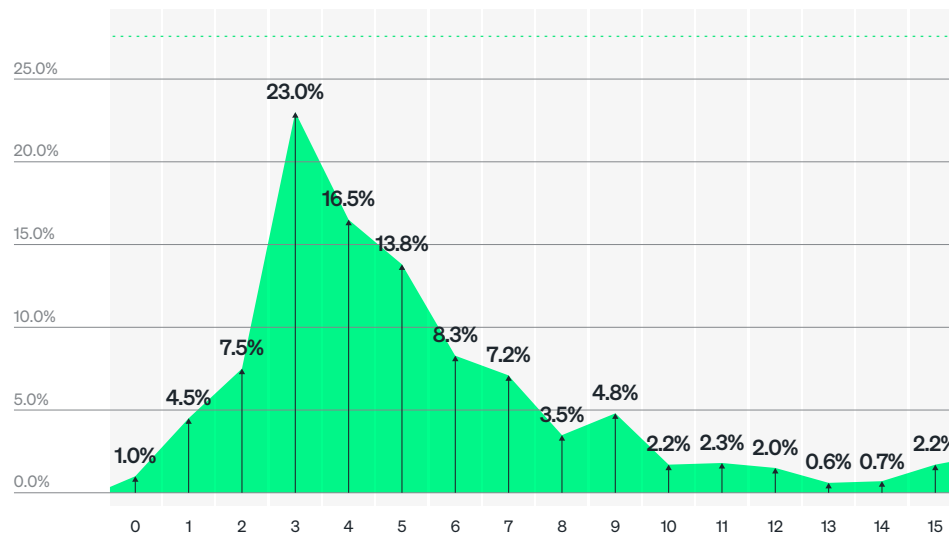


**Figure 08.** Number of mature observability practice characteristics employed

⚡ **Regional insight**

North American organizations were the most likely to have a mature observability practice (7%), while European organizations were the least likely (4%).
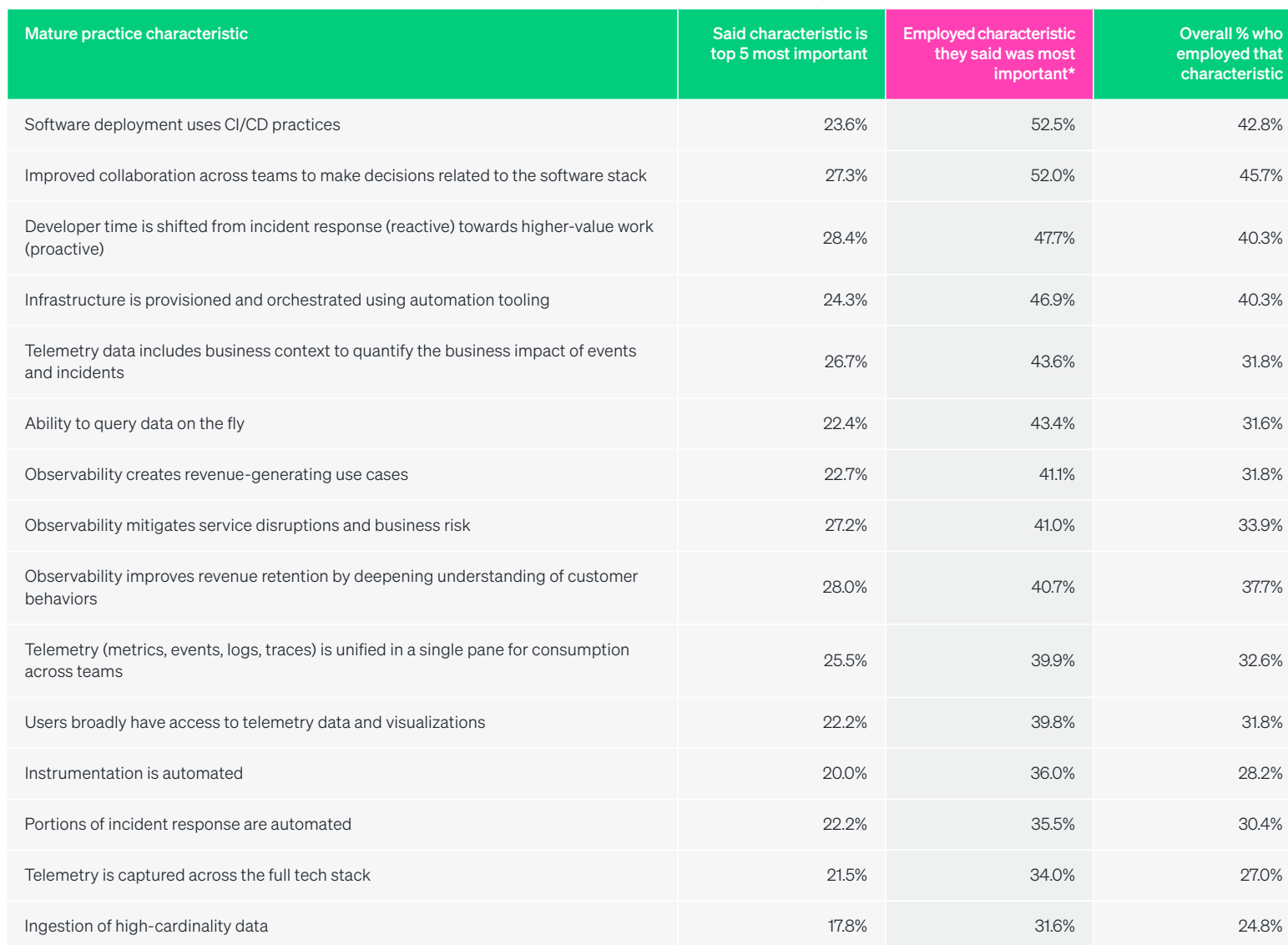
👤 **Role insight**

Unsurprisingly, executives felt that observability improves revenue retention by deepening their understanding of customer behaviors (top pick). In contrast, this did not strike a chord with others—revenue retention placed a distant tenth for non-executive managers and sixth for practitioners.

# 5%
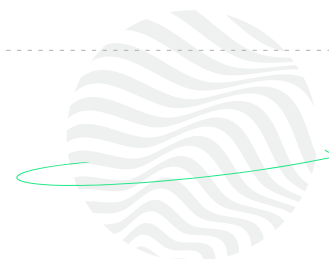
had a mature observability practice

There was a gap between what respondents thought were the most important characteristics of a mature observability practice and what characteristics they actually were employing.

**This column should be read as,** for example, "Of the 23.6% of respondents who thought software deployment using CI/CD practices is one of the five most important characteristics of a mature observability practice, only 52.5% actually were employing that characteristic."

| Mature practice characteristic | Said characteristic is top 5 most important | Employed characteristic they said was most important* | Overall % who employed that characteristic |
|---|---|---|---|
| Software deployment uses CI/CD practices | 23.6% | 52.5% | 42.8% |
| Improved collaboration across teams to make decisions related to the software stack | 27.3% | 52.0% | 45.7% |
| Developer time is shifted from incident response (reactive) towards higher-value work (proactive) | 28.4% | 47.7% | 40.3% |
| Infrastructure is provisioned and orchestrated using automation tooling | 24.3% | 46.9% | 40.3% |
| Telemetry data includes business context to quantify the business impact of events and incidents | 26.7% | 43.6% | 31.8% |
| Ability to query data on the fly | 22.4% | 43.4% | 31.6% |
| Observability creates revenue-generating use cases | 22.7% | 41.1% | 31.8% |
| Observability mitigates service disruptions and business risk | 27.2% | 41.0% | 33.9% |
| Observability improves revenue retention by deepening understanding of customer behaviors | 28.0% | 40.7% | 37.7% |
| Telemetry (metrics, events, logs, traces) is unified in a single pane for consumption across teams | 25.5% | 39.9% | 32.6% |
| Users broadly have access to telemetry data and visualizations | 22.2% | 39.8% | 31.8% |
| Instrumentation is automated | 20.0% | 36.0% | 28.2% |
| Portions of incident response are automated | 22.2% | 35.5% | 30.4% |
| Telemetry is captured across the full tech stack | 21.5% | 34.0% | 27.0% |
| Ingestion of high-cardinality data | 17.8% | 31.6% | 24.8% |

**Table 03.** Comparison of the most important characteristics of a mature observability practice and characteristics employed

# Capabilities deployed

Capabilities, not to be confused with characteristics, are specific components of observability. We asked survey respondents to tell us which of 17 different observability capabilities they deployed. Below we review the results by capability and by the number of capabilities.

## By capability

The survey respondents indicated their organizations deploy observability capabilities by as much as 57% (network monitoring) and as little as 34% (Kubernetes monitoring). We found that:

- Just over half said they deploy environment monitoring capabilities and log management
- DEM and services-monitoring capabilities were in the 40% range
- Monitoring capabilities for emerging technologies were among the least deployed, with each hovering in the low-30% range

View highlights for each capability.

| Capability | % |
|---|---|
| Network monitoring | 56.6% |
| Security monitoring | 55.7% |
| Database monitoring | 53.8% |
| Alerts | 51.5% |
| Infrastructure monitoring | 51.0% |
| Log management | 50.3% |
| Browser monitoring | 48.6% |
| Error tracking | 48.5% |
| Custom dashboards | 46.7% |
| APM | 45.4% |
| Mobile monitoring | 43.3% |
| Serverless monitoring | 38.2% |
| AIOps | 37.3% |
| Distributed tracing | 36.3% |
| Synthetic monitoring | 34.2% |
| ML model performance monitoring | 34.1% |
| Kubernetes monitoring | 33.7% |

**Figure 09.** Deployed capabilities

## By number of capabilities

When we looked at how many capabilities the survey respondents said their organizations deploy, we found:

- Only 3% indicated that their organizations have all 17 observability capabilities deployed
- Just (3%) indicated that they had none deployed
- Most (61%) had four to nine deployed (9% had one to three, 80% had five or more, and 28% had 10 or more)

These results show that most organizations do not currently monitor their full tech stacks. However, this is changing. View future deployment plans.
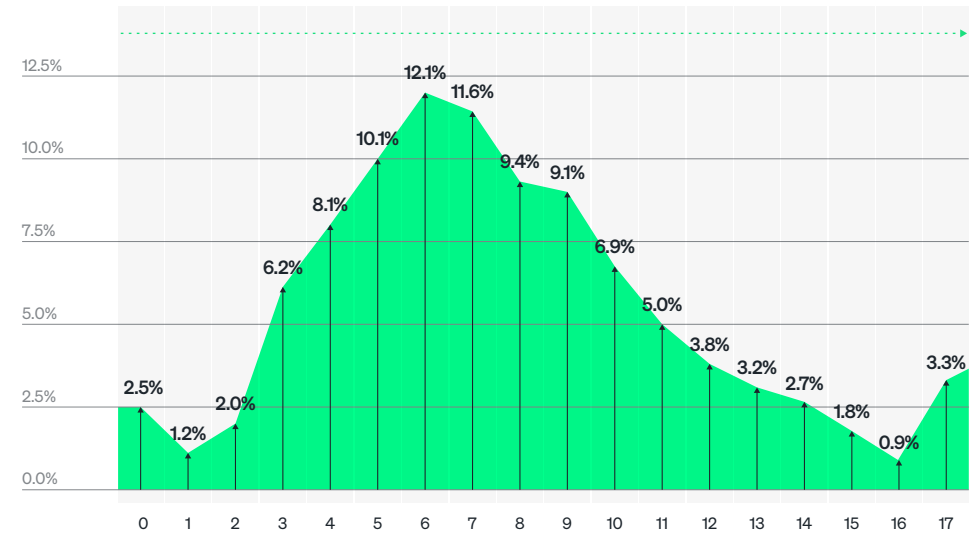


**Figure 10.** Number of deployed capabilities

Regional insight

In general, Asia Pacific organizations had the most capabilities deployed, while European organizations had the least.

Role insight

Executives were more likely to state that all observability capabilities are deployed (6%, compared to 2% for non-executive managers and 3% for practitioners), suggesting a gap in knowledge of what is deployed versus what will be deployed.

# Full-stack observability prevalence

Based on our definition of full-stack observability, only 27% of survey respondents' organizations have achieved it. And an even smaller percentage—3%—said that their organization has already prioritized/achieved full-stack observability.

These results indicate that large parts of organizations' tech stacks are not being monitored or fully observed today, creating ample opportunities to make rapid progress in achieving full-stack observability.

Notably, 84% of organizations that have achieved full-stack observability allocated at least 5% of their total IT budget for observability tools.
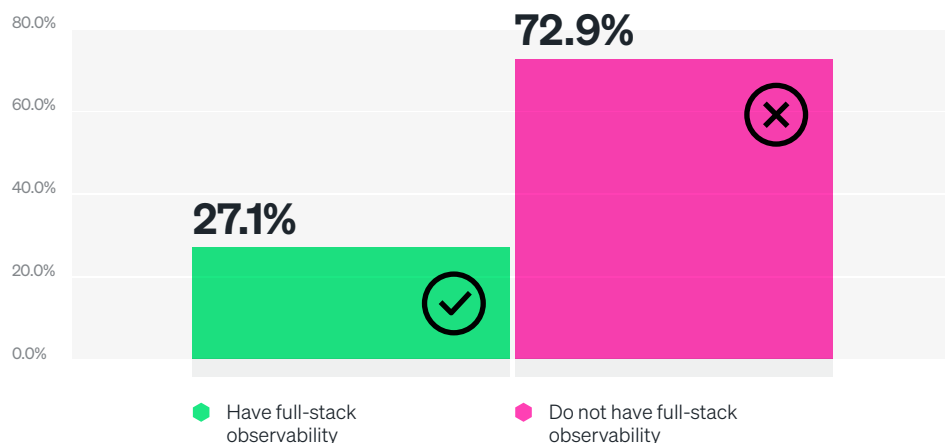


**Figure 11.** Percentage of organizations that do and don't have full-stack observability

**Regional insight**

Asia Pacific organizations were the most likely to have achieved full-stack observability (33%), while European organizations were the least likely (21%).

**Organization size insight**

Of those organizations that had achieved full-stack observability, only 7% were small, while 52% were midsize, and 42% were large.

"On any given day, 33–35% of our infrastructure and our platform compute and storage cycles are in multiple cloud locations. Most of that is unmonitored because our application space is decentralized, which is very common in academia. From a security risk management angle, it represents one of our biggest areas of security risk."

CISO, LARGE EDUCATION ENTERPRISE
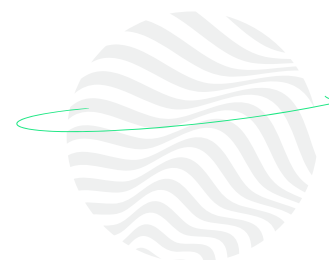
**73%**

had NOT achieved full-stack observability

# Number of monitoring tools

When asked about the number of tools they use to monitor the health of their systems, survey respondents overwhelmingly reported using more than one.

- Most (82%) used four or more tools (94% used two or more)
- One in five used seven tools, the most common number reported
- Only 2% used just one tool to satisfy their observability needs

tool fragmentation

So, the state of observability today is most often multi-tool—and therefore fragmented—and likely inherently complex to handle. In fact, 25% of survey respondents noted that too many monitoring tools are a primary challenge that prevents them from prioritizing/achieving full-stack observability.
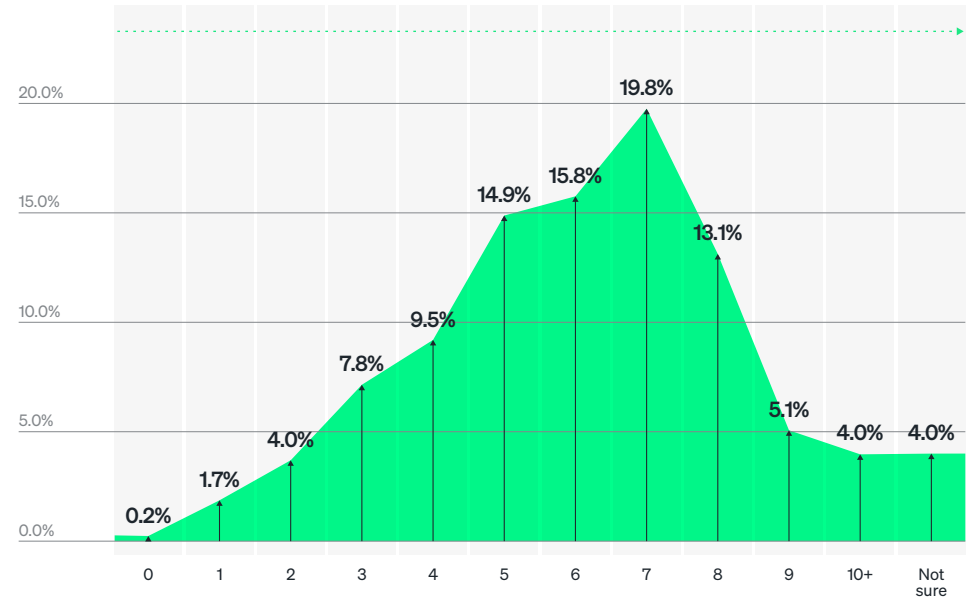
**Figure 12.** Number of tools used for observability capabilities

⬏ **Organization size insight**

Small organizations were the most likely to use only one monitoring tool (6%, compared to 2% for midsize and only 1% for large).

"Observability monitoring and information security can draw closer together and leverage common platforms—there's a lot of overlap. To the extent that you can use one tool to provide everything, that's going to become more important."

SVP AND CTO, LARGE RETAIL ENTERPRISE
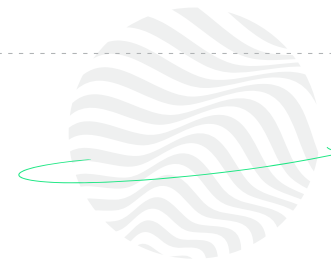
# 82%
toggle between 4+ observability tools

# Unified telemetry, visualization, and dashboarding

When it comes to telemetry data and the visualization and dashboarding of that data, how unified or siloed/disparate are they?

## Unified telemetry

When survey respondents were asked about how unified or siloed their organizations' telemetry data is:

- Almost half (49%) said more unified (they unify telemetry data in one place), but only 7% said entirely unified
- A third said more siloed (they silo telemetry data in discrete data stores), including 8% who said entirely siloed
- Less than one-fifth (17%) said roughly equally unified and siloed

data fragmentation
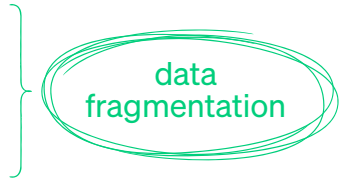
Interestingly, among the 51% who had more siloed data, 47% indicated that they actually strongly prefer a single, consolidated platform. And 77% of those who had entirely siloed data indicated that they prefer a single, consolidated platform.

Given the use of disparate monitoring tools and open-source solutions—only 2% of respondents used a single tool for observability—these findings are not surprising. Because siloed and fragmented data make for a painful user experience (expensive, lack of context, slow to troubleshoot), the more silos an organization has, the more preference to consolidate. Perhaps the respondents who seemingly feel the most pain from juggling data from different silos long for more simplicity in their observability solutions.

● Entirely    ● Mostly    ● Somewhat

**More unified**
7.3%
23.0%
19.0%
**49.3%**

**More siloed**
7.9%
12.8%
11.9%
**32.5%**

**Equally unified and siloed**
**17.1%**

**I'm not sure**
**1.1%**

0.0%    20.0%    40.0%    60.0%
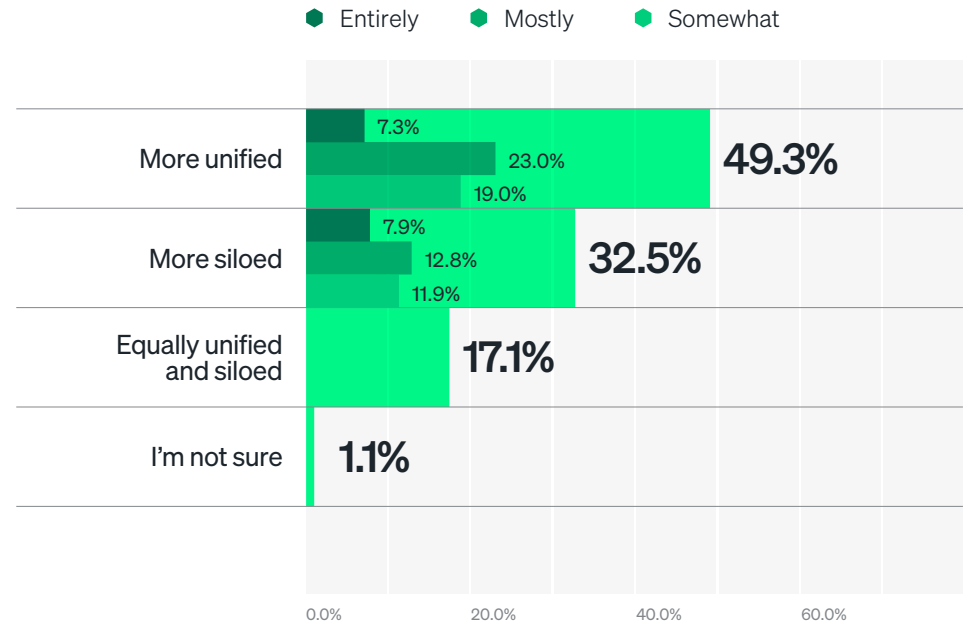
**Figure 13.** Unified versus siloed telemetry data

⚡ **Regional insight**

Organizations in Europe and North America were more likely to have unified telemetry data (51% and 56% respectively) and less likely to have siloed data (31% and 25% respectively). While organizations in Asia Pacific were the least likely to have unified telemetry data (38%) and the most likely to have siloed data (45%)—in fact, 15% were entirely siloed.

⬈ **Organization size insight**

Large organizations were slightly more likely to have more unified telemetry data (54%) and less likely to have siloed data (30%). Conversely, small organizations were less likely to have unified telemetry data (40%) and more likely to have siloed data (45%).

## Unified visualization and dashboarding

For the visualization and dashboarding of that data, it's a similar story. When survey respondents were asked how unified or disparate the visualization/dashboarding of their organizations' telemetry data is:

- More than two-thirds (68%) said it is more unified (telemetry data is visualized in a single dashboarding solution)
- Almost a quarter (23%) said it is more disparate (multiple visualization solutions are used without cross-communication)
- Less than one-tenth (8%) said it is neither unified nor disparate

Despite the reality of multiple tools to capture observability needs, it appears that respondents mostly managed to unify and visualize the data from their many tools. These findings seem to point to the desire for a unified observability experience.



● Entirely  ● Mostly  ● Somewhat

| | |
|---|---|
| More unified | 12.9% / 30.4% / 24.4% — 67.7% |
| More disparate | 5.5% / 7.2% / 10.3% — 22.9% |
| Neither unified nor disparate | 8.3% |
| I'm not sure | 1.1% |
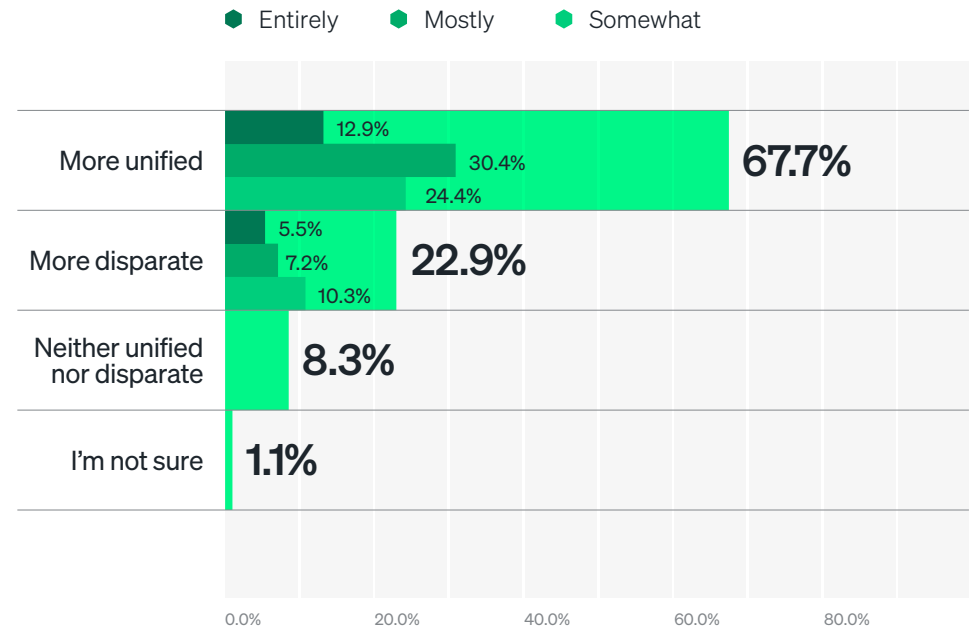
**Figure 14.** Unified versus disparate visualization/dashboarding of telemetry data

---

⚡ **Regional insight**

Respondents surveyed in North America were more likely to have telemetry data visualized in a single dashboarding solution (74%) and less likely to have multiple visualization solutions without cross-communication (18%). While those surveyed in Asia Pacific were the least likely to have telemetry data visualized in a single dashboarding solution (61%) and the most likely to have multiple visualization solutions without cross-communication (33%)—in fact, 11% were entirely disparate.

👤 **Role insight**

ITDMs were more likely to think that their visualization and dashboarding of telemetry data was more unified (71%), while practitioners were less likely (66%).

⬚ **Organization size insight**

Respondents from midsize organizations were the most likely to think that their visualization and dashboarding of telemetry data is more unified (70%), while those from small organizations were the least likely (62%).

## 23%

used multiple visualization solutions without cross-communication (disparate telemetry data)

# Strategy and organization

Next, we looked at the observability strategies and team organization of the survey respondents, including their preference for a single platform or multiple point solutions, how they learn about software and system interruptions, trends driving the need for observability, advocacy for observability by role, the perceived purpose of observability, in which stages of the software development lifecycle they are using observability, and what teams are responsible for observability when.

## Single platform or multiple point solutions

For the past decade, observability vendors have created purpose-built tools to help specialty engineering teams monitor their part of the stack. For example, New Relic created and led the APM category for application developers. Others chose different specialty roles and created best-in-class tools that served those teams well. However, this practice increased complexity as each tool brings a disparate experience and data store.

To achieve the full power of observability, organizations require a unified, underlying data store for all types and sources of telemetry (like New Relic now offers with its observability platform). With a unified experience, engineering teams can see all their entities and their dependencies in one place and collaborate more closely together while eliminating team, tool, and data silos.

But what are the strategic preferences of organizations when it comes to the number of tools they use for observability? Do they prefer a single, consolidated observability platform or multiple point/best-in-class solutions that are often cobbled together or used only for specific monitoring capabilities? We found that:

- Almost half (47%) preferred a single, consolidated observability platform
- A third preferred multiple point solutions
- One in five had no preference



● Strongly    ● Somewhat

Prefer a single, consolidated platform: 19.0% / 27.6% — **46.6%**
Prefer multiple point solutions: 11.2% / 21.8% — **33.0%**
No preference: **19.9%**
I'm not sure: **0.9%**

0.0%    20.0%    40.0%    60.0%    80.0%
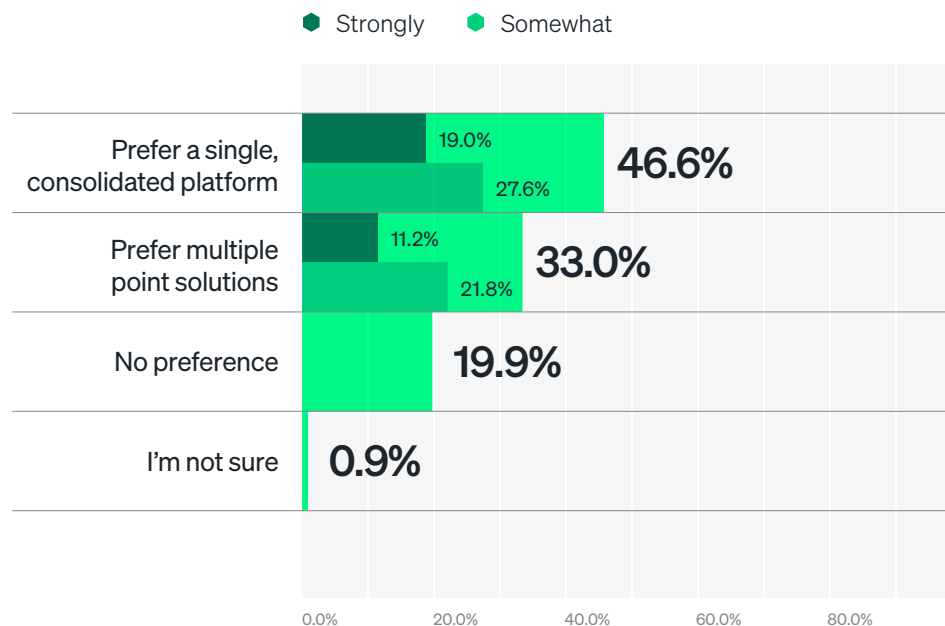
**Figure 15.** Preference for a single, consolidated platform versus multiple point solutions

# 47%

preferred a single, consolidated observability platform (all-in-one)

These results imply that many organizations desire a single-tool, all-in-one approach to their observability needs.

However, even though more respondents claimed that they prefer a single, consolidated platform, 94% used two or more monitoring tools—just 2% used a single tool for observability and only 7% indicated their organizations' telemetry data is entirely unified.

What's more, when asked what the primary challenges are that prevent prioritizing/achieving full-stack observability, a quarter said it was that they have too many monitoring tools.

Taken together, we see the current state of observability as multi-tool and fragmented, yet we see an increasing strategic preference for a single, consolidated observability platform with the knowledge that tool fragmentation is a significant hindrance to full-stack observability.

"Our stated strategy and the vision that we have is to use fewer providers and cover more territory. Where appropriate, we try to use one vendor to do many things as opposed to many vendors to do only one thing each."

SVP AND CTO, LARGE RETAIL ENTERPRISE

⚡ **Regional insight**

In the Asia Pacific region, 55% of respondents claimed that they prefer a single, consolidated platform.

👤 **Role insight**

About a third (32%) of non-executive managers said that they strongly prefer a single, consolidated platform, compared to 17% of executives and practitioners.

📊 **Industry insight**

In the financial/insurance and industrials/materials/manufacturing industries, more than half of respondents claimed that they prefer a single, consolidated platform (60% and 54% respectively).

# Detection of software and system interruptions

How does observability impact performance in the organization? The survey results showed that:

- Almost half (46%) primarily learn about interruptions through multiple monitoring tools
- Only about one in five (21%) primarily learn about interruptions through one tool

So, about two-thirds of respondents (67%) indicated that they primarily learn about interruptions through one or more monitoring tools. That a higher percentage primarily learn about interruptions through multiple monitoring tools makes sense given what we know about the large number of monitoring tools respondents deployed for observability purposes.

But what is remarkable is how manual the process remains for so many organizations. We found that:

- Almost a quarter (22%) primarily learn about interruptions through manual checks/tests that are performed on systems at specific times
- About one in 10 (11%) primarily learn about interruptions through incident tickets and complaints from customers and employees

In sum, a third of respondents still primarily learned about interruptions and outages through manual checks/tests or through incident tickets and complaints.

What's more, there is a clear connection between how respondents primarily learned about interruptions and how unified their telemetry data was. Generally, when telemetry data was more unified, notice of interruptions came through one observability tool.



**20.6%**
**45.9%**
**9.1%**
**22.3%**
**32.8% = manual/complaints**
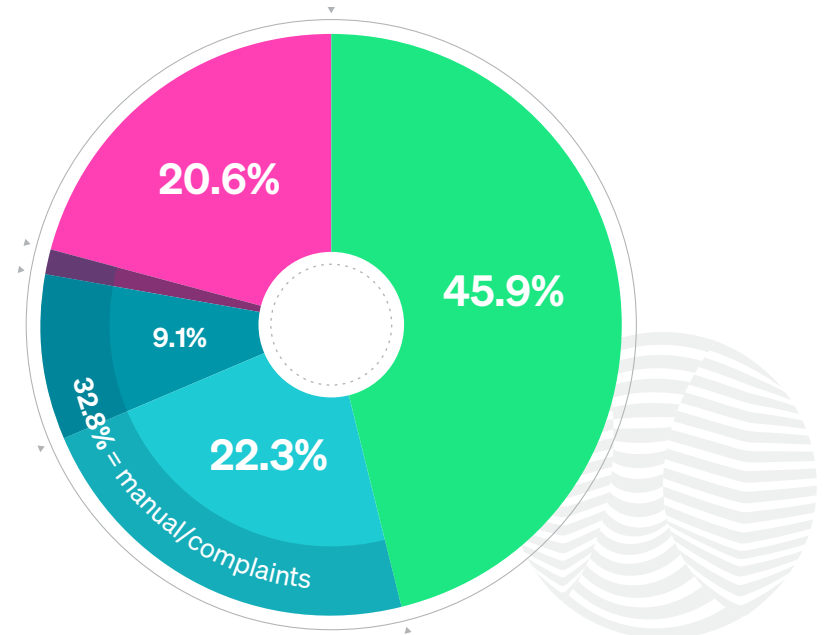
- With multiple monitoring tools
- With manual checks/tests that are performed on systems at specific times
- With complaints or incident tickets from external customers
- With complaints from internal customers
- With one observability platform

**Figure 16.** How respondents detected software and system interruptions

⬈ **Organization size insight**

Large organizations were more likely to detect interruptions through multiple tools, while small organizations were more likely to use manual checks/tests and multiple tools.

# 33%
still primarily learned about interruptions through manual checks/ tests and complaints

# Trends driving observability

So, what technology strategies and trends are driving the need for observability?

Modern applications typically run in the cloud and depend on hundreds of components, each introducing additional monitoring challenges and security risks. With cloud adoption, cloud-native application architectures, and cybersecurity threats on the rise, it's not surprising that an increased focus on security, governance, risk, and compliance was the most frequently cited strategy or trend driving the need for observability at the organizations surveyed (49%).

Development of cloud-native front-end application architectures, an increased focus on customer experience management, and migration to a multi-cloud back-end environment were all mentioned more than 40% of the time as well.

While not the top responses, 39% of respondents said that they are adopting open-source technologies such as OpenTelemetry, 36% are adopting serverless computing, and 36% are containerizing applications and workloads—all trends where observability requires a unified approach.

| | |
|---|---|
| Increased focus on security, governance, risk, and compliance | 49.1% |
| Development of cloud-native application architectures (front-end) | 46.8% |
| Increased focus on customer experience management | 44.8% |
| Migration to a multi-cloud environment (back-end) | 42.2% |
| Adoption of open-source technologies (such as OpenTelemetry) | 39.0% |
| Prioritization of faster software release cycles | 38.2% |
| Adoption of serverless computing | 36.4% |
| Containerization of applications and workloads | 36.2% |
| I'm not sure | 0.9% |

**Figure 17.** Technology strategies and trends driving the need for observability

**Regional insight**

The development of cloud-native application architectures (front-end) was the number one strategy driving the need for observability in the Asia Pacific region (53%).

**Role insight**

The development of cloud-native application architectures (front-end) was the number one driver for executives (50%) and the second driver for non-executive managers and practitioners (47% total).

**Industry insight**

Respondents from the energy/utilities and nonprofit industries were more likely to say that migration to a multi-cloud environment is their top driver, while those in government were more likely to say development of cloud-native application architectures, and those in healthcare/pharma were more likely to say adoption of serverless computing. Those from the services/consulting industry were equally torn between security, cloud-native, and multi-cloud for their top driver.

"As we've gone to the cloud, there's a lot more we have to monitor and a lot of additional needs. Observability has come to encompass more than just standard premise monitoring and become the way we look at all the different aspects and view all of them."

SENIOR ENGINEER, LARGE FINANCIAL ENTERPRISE

# Advocates of observability

Who were the biggest advocates of observability in respondent organizations? We asked survey participants to rate the varying levels of advocacy among several roles in their organizations.

In general, survey respondents indicated that all roles advocate for observability more than resist it. At first glance, there seems to be little pattern in the varying levels of advocacy. But it's intriguing that survey-takers thought the less technical-focused C-suite executives have the highest levels of strong observability advocacy (39%), even higher generally than more technical-focused C-suite execs (31%). Other notable findings include:

- There was low resistance to observability overall (less than 10%)
- Those with full-stack observability or a mature observability practice by our definitions were notably more likely to have strong observability advocates than those without those two things
- Respondents whose organizations saw observability completely as an enabler of core business goals indicated notably higher levels of strong advocacy for observability in nearly every role

These findings tend to support future observability deployment plans and budget plans as organizations are more likely to expand deployment and increase budgets if individual roles and teams see the value in and advocate for observability.
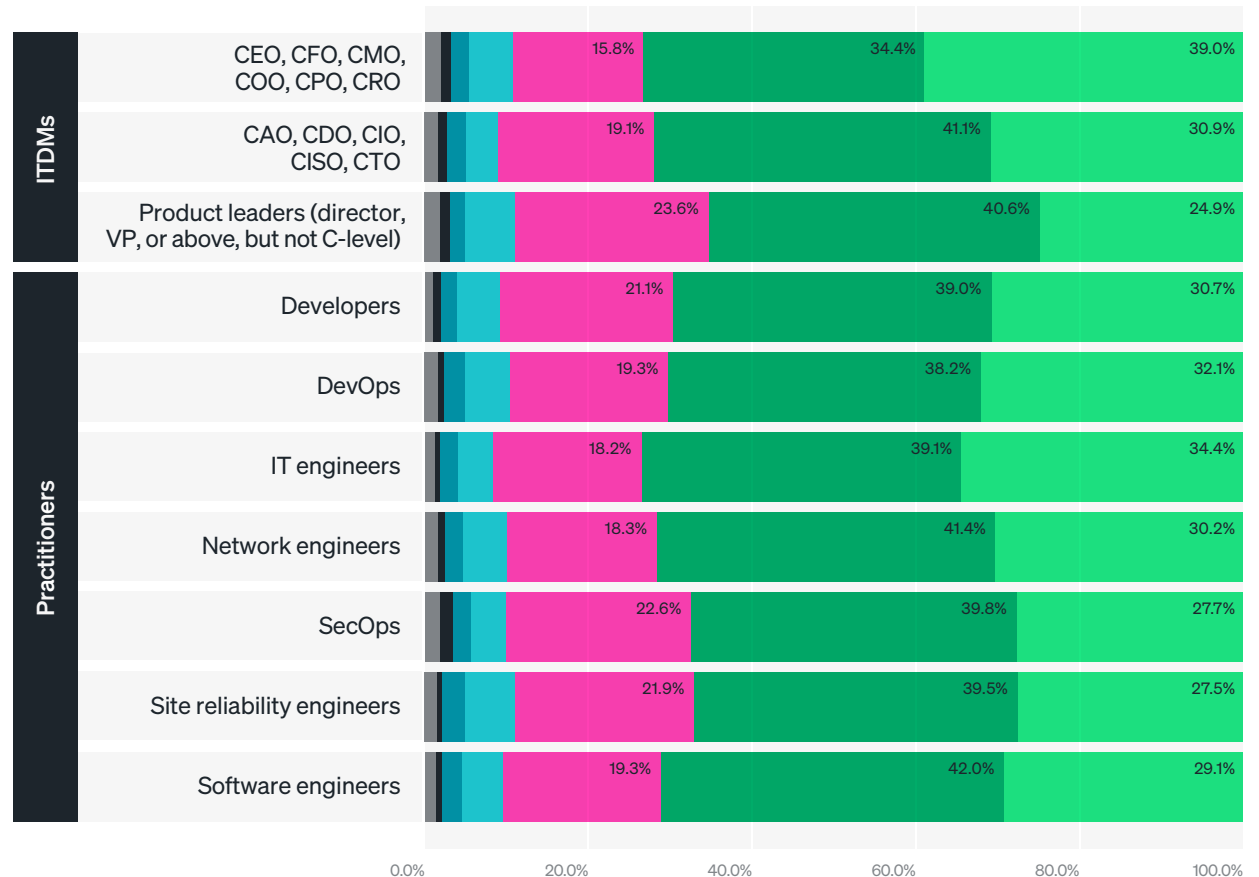
**<10%** resisted observability

Legend:
- ● Strongly advocates
- ● Advocates
- ● Aware
- ● Aware, but neither advocates nor resists
- ● Resists
- ● Unaware
- ● I'm not sure

**Figure 18.** Levels of observability advocacy by role

Chart data:

**ITDMs**
- CEO, CFO, CMO, COO, CPO, CRO: 15.8%, 34.4%, 39.0%
- CAO, CDO, CIO, CISO, CTO: 19.1%, 41.1%, 30.9%
- Product leaders (director, VP, or above, but not C-level): 23.6%, 40.6%, 24.9%

**Practitioners**
- Developers: 21.1%, 39.0%, 30.7%
- DevOps: 19.3%, 38.2%, 32.1%
- IT engineers: 18.2%, 39.1%, 34.4%
- Network engineers: 18.3%, 41.4%, 30.2%
- SecOps: 22.6%, 39.8%, 27.7%
- Site reliability engineers: 21.9%, 39.5%, 27.5%
- Software engineers: 19.3%, 42.0%, 29.1%

# Purpose of observability

We were curious about the perceived purpose of observability—do practitioners and ITDMs see observability as more of a key enabler for achieving core business goals or more for incident response/insurance? We found that:

- Half thought observability is more of a key enabler for achieving core business goals
- More than a quarter (28%) indicated that business goals and incident response equally enable observability in their organizations
- Just over a fifth (21%) said observability is more for incident response/insurance

The fact that more than three-quarters of respondents (78%) saw observability as a key enabler for achieving core business goals implies that observability has become a board-level proofpoint.

# 78%
saw observability as a key enabler for achieving core business goals



**Figure 19.** Observability as a key enabler for achieving core business goals or for incident response/insurance

Legend:
- Completely for core business goals
- Generally for core business goals
- Equally for core business goals and incident response/insurance
- Completely for incident response/insurance
- Generally for incident response/insurance
- I'm not sure (1.0%)

---
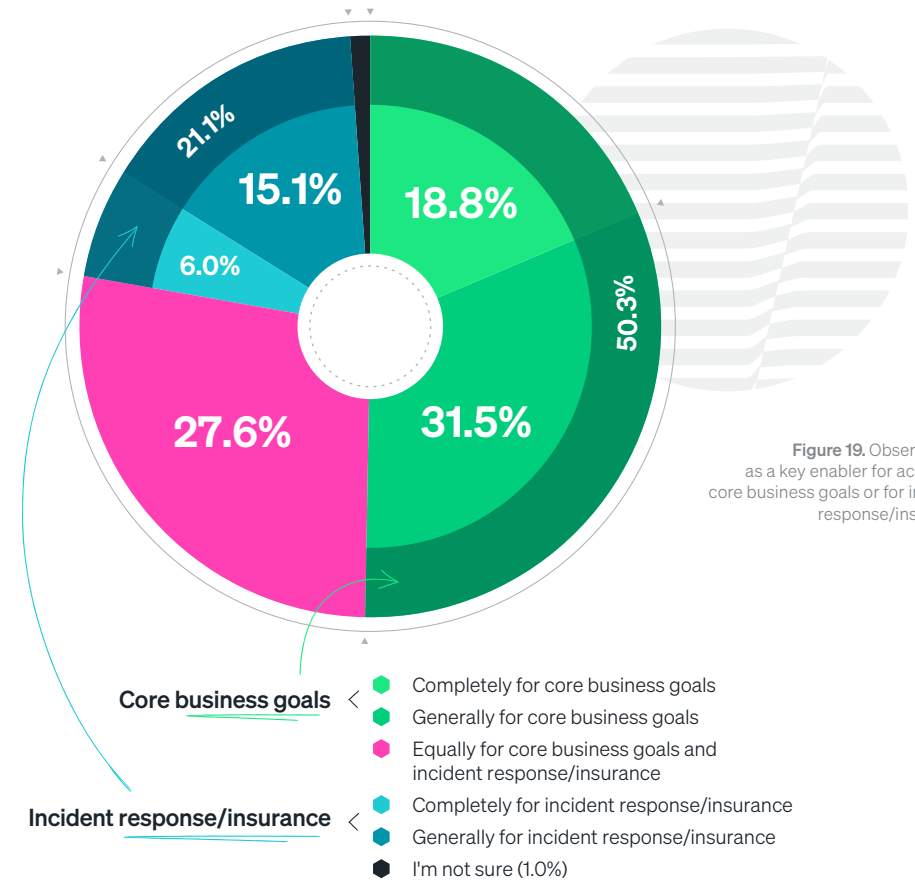
**Regional insight**

Respondents surveyed in the Asia Pacific region were the most likely to view observability as more of a key enabler for achieving core business goals (58%), compared to 48% surveyed in North America and Europe. Conversely, respondents surveyed in Asia Pacific were the least likely to say that observability is more for incident response/insurance (15%), compared to 22% surveyed in North America and 24% surveyed in Europe.

**Role insight**

Unsurprisingly, executives were the most likely to view observability as more of a key enabler for achieving core business goals (56%), compared to 51% for non-executive managers and 48% for practitioners. Conversely, executives were the least likely to say that observability is more for incident response/insurance (16%), compared to 17% for non-executive managers and 24% for practitioners.

**Organization size insight**

Respondents from midsize organizations were the most likely to view observability as more of a key enabler for achieving core business goals (54%), while small organizations were the least likely (42%). And midsize organizations were the least likely to say that observability is more for incident response/insurance (19%), while large organizations were the most likely (25%).

**Industry insight**

The most likely to view observability as more of a key enabler for achieving core business goals were respondents from the retail/consumer (57%), financial/insurance (54%), and IT/telco (52%) industries. Conversely, the most likely to view observability as more for incident response/insurance were those from the energy/utilities (33%), services/consulting (28%), and nonprofit/unspecified (26%) industries.

# SDLC stages using observability

Originally, monitoring was focused on the operate (or run) stage of the software development lifecycle (SDLC). But there is potential for that data to span the entire SDLC, helping teams be more data-driven as they plan, build, deploy, operate, and then iterate. Historically, many engineers who work earlier in the SDLC (plan, build, and deploy stages) were not aware that observability could help them do their jobs better.

Even so, we found that most respondents used some level of data-driven observability insights in all stages of the SDLC. However, only about a third of respondents used full observability in each stage:

- **Plan:** 34% used full observability in the plan stage
- **Build:** 30% used full observability in the build stage
- **Deploy:** 34% used full observability in the deploy stage
- **Operate:** 37% used full observability in the operate stage

Those with a mature observability practice (by our definition) were notably more likely to use full observability in all SDLC stages (53% for plan, 46% for build, 51% for deploy, and 54% for operate) than those without.

Those who had full-stack observability (by our definition) were also more likely to use full observability in all SDLC stages (38% for plan, 36% for build, 42% for deploy, and 46% for operate) than those who didn't have it.

Developers often spend too much time debugging as opposed to shipping new features. It's crucial for them to have an all-in-one observability platform that can streamline the entire SDLC.

⚡ **Regional insight**

Respondents surveyed in Asia Pacific were the most likely to use extensive or full observability in the plan (72%) and build (75%) stages, while those surveyed in North America were the most likely to use it in the deploy (75%) and operate (81%) stages. Those surveyed in Europe were the least likely to use extensive or full observability across the board with 63% for plan, 65% for build, 67% for deploy, and 69% for operate.

📊 **Industry insight**

Overall, respondents in the financial/insurance and retail/consumer industries were the most likely to use extensive or full observability in all stages of the SDLC, including 83% in the operate stage, followed by those from IT/telco. Government respondents were the least likely to use extensive or full observability in all stages of the SDLC, followed by those from education.
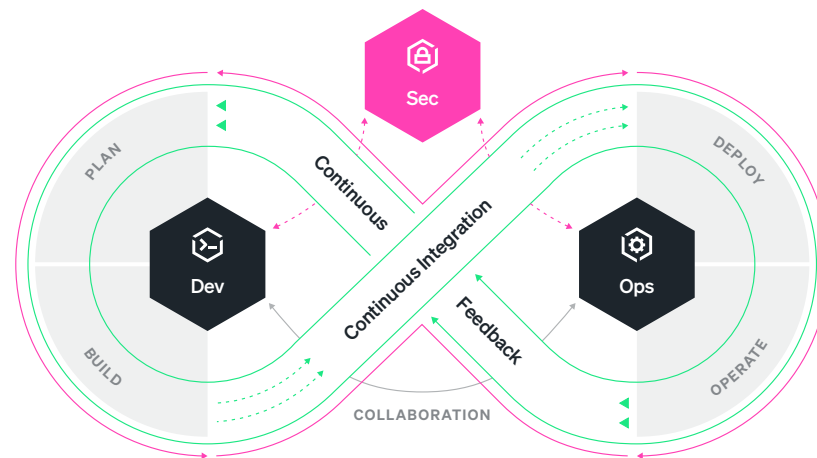


**Figure 20.** Software development lifecycle for DevSecOps
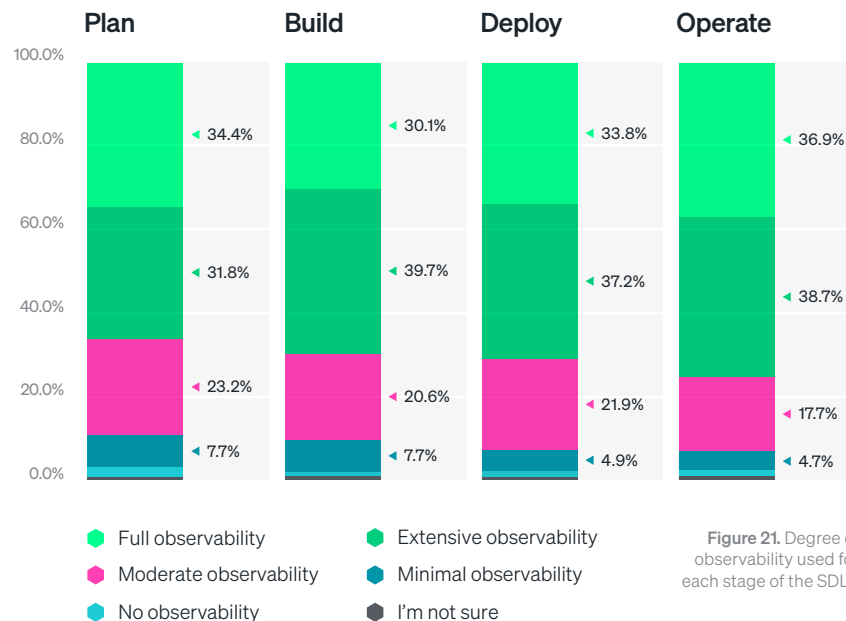


**Figure 21.** Degree of observability used for each stage of the SDLC

# Teams responsible for observability

In asking survey respondents which teams are primarily responsible for the implementation, maintenance, and usage of observability at their organizations, we found that:

- IT operations teams were the most likely to be responsible for observability followed by network operations and DevOps teams
- Application development and SRE teams were more likely to be responsible for the implementation of observability than the maintenance or usage of it
- SecOps and DevSecOps teams were more likely to be responsible for the usage of observability than the implementation or maintenance of it

While most organizations had a dedicated IT operations team, it seems that they were less likely to have dedicated DevSecOps and SecOps teams that are primarily responsible for observability. This could indicate that security teams are possibly using separate security-related observability tools. A comprehensive, all-in-one observability approach supports the cultural shift that brings development, security, and operations teams together more seamlessly (DevSecOps). As organizations prioritize security, it will be interesting to see how this dynamic changes in the next few years.



**Implementation**

- ◄ 18.8%
- ◄ 12.6%
- ◄ 1.7%
- ◄ 37.5%
- ◄ 15.6%
- ◄ 2.7%
- ◄ 10.7%

**Maintenance**

- ◄ 12.3%
- ◄ 16.1%
- ◄ 2.7%
- ◄ 33.1%
- ◄ 20.5%
- ◄ 6.7%
- ◄ 8.2%

**Usage**

- ◄ 11.1%
- ◄ 17.0%
- ◄ 7.3%
- ◄ 25.9%
- ◄ 18.6%
- ◄ 13.5%
- ◄ 4.9%

Legend:
- ● Application development only
- ● DevOps
- ● DevSecOps
- ● IT operations only
- ● Network operations
- ● SecOps
- ● Site reliability engineering only
- ● I'm not sure
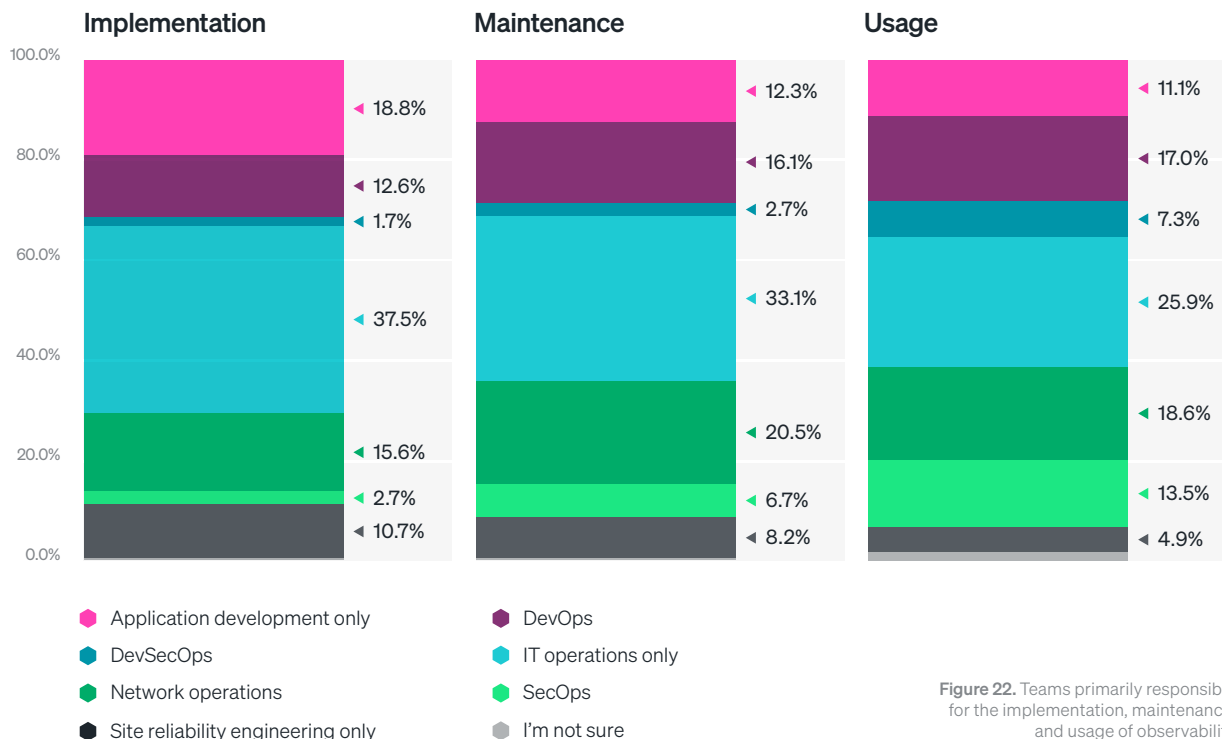
**Figure 22.** Teams primarily responsible for the implementation, maintenance, and usage of observability

**Regional insight**

In North America, the observability involvement of IT operations teams was slightly higher than in other regions. While in Asia Pacific, the observability involvement of DevSecOps teams was slightly higher than in other regions.

# Pricing, billing, and spending

We wanted to know about budget allocation as well as pricing and billing preferences when it comes to observability tools.

## Budget allocation

When we asked survey-takers what percentage of their IT budget they were currently allocating for observability tools, we found that:

- Most (69%) allocate more than 5% but less than 15%, with 14% allocating more than 15%
- Just 3% allocate more than 20%
- Only 16% allocate less than 5%

So, like last year, most organizations allocated less than 20% of IT budgets for observability tools.

Organizations with more mature observability practices (by our definition) tended to spend more on observability: more than a quarter (29%) of those that were mature allocated more than 15%, compared to the 14% that were less mature.

And organizations that had the most capabilities deployed tended to have the biggest observability budgets: almost three-quarters (73%) of those that allocated more than 20%, and more than half (57%) of those that allocated more than 15% had nine or more capabilities deployed.

Learn about their budget plans for next year.



Legend:
- Less than 1%
- More than 1% but less than 5%
- More than 5% but less than 10%
- More than 10% but less than 15%
- More than 15% but less than 20%
- More than 20%
- I'm not sure
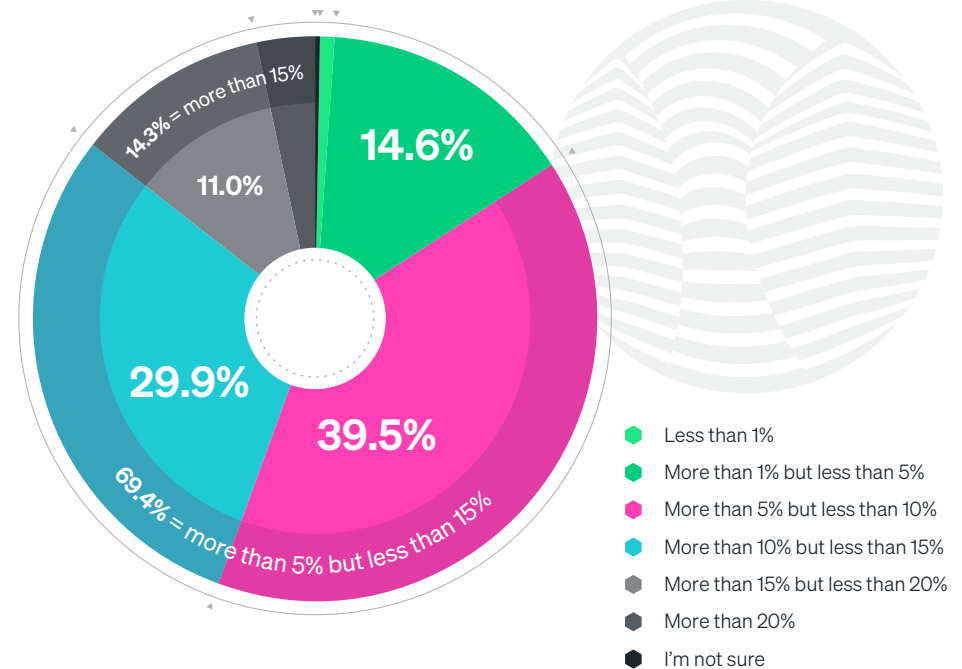
**Figure 23.** Percentage of IT budget allocated for observability tools

⚡ **Regional insight**

Respondents surveyed in Asia Pacific were more likely to say they allocate more than 10% of their IT budgets for observability tools (50%), while those surveyed in Europe and North America were more likely to say they allocate less than 10% (60% and 54% respectively). And 21% of those surveyed in Asia Pacific said they allocate 15% or more, compared to 14% of those surveyed in North America and 11% in Europe.

🏭 **Industry insight**

Respondents from the energy/utilities and industrials/materials/manufacturing industries indicated that they allocate more than 10% but less than 15% of their IT budgets for observability tools as their top choice, while those from all other industries were more likely to select more than 5% but less than 10%. This could be because the energy/utilities and industrial/materials/manufacturing industries tend to be more sensitive to downtime, are more regulated, and may be more likely to use technologies like AI, ML, and IoT.

# Pricing features

In addition to pricing model preferences, we looked at what pricing features were the most important to respondents and their organizations for their observability tools/platform. We found that:

- Budget-friendly pricing ranked the most important overall; transparent pricing, a single license metric across all telemetry, and having a low-cost entry point were also frequently cited
- Hybrid pricing models ranked higher than user-, host-, and agent-based-only pricing models
- The single-SKU and bundle-of-SKUs approaches were neck and neck

The two hybrid pricing models (hybrid user + data-ingestion pricing and hybrid host + data-ingestion pricing) are the dominant pricing models in the market, so it follows that these options ranked highly in the survey. Respondents clearly favored usage-based pricing for data ingest.

| | |
|---|---|
| Budget-friendly pricing | 35.6% |
| Hybrid of user- and data ingestion-based pricing | 33.9% |
| Hybrid of host- and data ingestion-based pricing | 33.6% |
| Ability to select SKUs for individual capabilities (bundle-of-SKUs approach) | 31.5% |
| Transparent pricing | 30.7% |
| Single license metric across all telemetry | 30.4% |
| Single-SKU approach with access to the full observability platform | 29.2% |
| Low-cost entry point | 26.6% |
| User-based pricing only | 26.1% |
| Host-based pricing only | 25.0% |
| Agent-based pricing only | 22.4% |
| I'm not sure | 0.9% |

**Figure 24.** Pricing feature preferences

**Regional insight**

Respondents surveyed in North America were the most likely to select budget-friendly pricing; they also favored a single license metric across all telemetry more than those in other regions did. While those surveyed in Asia Pacific were more likely to favor hybrid pricing models the most.

**Role insight**

Role insight: Interestingly, practitioners were the most likely to select budget-friendly pricing as their top answer. They were also more likely to select a low-cost entry point. Executives, however, pegged budget-friendly pricing as the sixth most important, and they instead favored hybrid pricing models the most. Non-executive managers were the least likely to favor a bundle-of-SKUs approach, a single license metric across all telemetry, and a host- or agent-based-only pricing model.

**Organization size insight**

Small organizations were slightly more likely to favor a single-SKU approach (34%, compared to 29% for midsize and large) and a low-cost entry point (31%, compared to 26% for midsize and large). Large organizations were slightly more likely to value transparent pricing (33%, compared to 31% for small and 29% for midsize).

# Billing features

We also wanted to understand what billing models and features were the most important to survey respondents. We found that:

- The flexibility to scale usage based on consumption with no monthly minimum was the top choice overall
- Usage-based billing models (whether usage is based on monthly provisioned use or active use) were preferred over subscription-based
- The ability to ingest any telemetry data type and autoscale with no penalties as well as predictable spending also ranked high

In supplemental interviews with ITDMs by ETR during the execution of this study, interviewees most commonly desired predictability in pricing and billing. No matter the technical design of a pricing or billing model, ITDMs desired the ability to predict accurately what the bill would be in advance.



| Billing feature | % |
|---|---|
| Flexibility to scale usage based on consumption with no monthly minimum | 37.7% |
| Ability to ingest any telemetry data type with no penalties | 33.1% |
| Usage-based billing model (usage is based on monthly provisioned use) | 33.1% |
| Usage-based billing model (usage is based on monthly active use) | 33.0% |
| Ability to autoscale without penalty | 32.0% |
| Predictable spending | 30.8% |
| Subscription-based billing model | 30.6% |
| Ability to pay as you go | 27.5% |
| Ability to pay with a credit card | 26.7% |
| No premium overage fees | 25.8% |
| No shelfware | 12.1% |
| I'm not sure | 1.0% |

**Figure 25.** Billing feature preferences

---

**Regional insight**

Respondents surveyed in Europe were the least likely to care about the type of billing model and flexibility to scale usage based on consumption with no monthly minimum. Those surveyed in Asia Pacific were the least likely to care about the ability to autoscale without penalty. While those surveyed in North America were more likely to care about the ability to pay with a credit card and no premium overage fees or shelfware.

**Role insight**

Practitioners cared the most about predictable spending. While non-executive managers were the least likely to prefer a subscription-based billing model, the ability to pay as they go, and no shelfware.

**Organization size insight**

Small organizations were more likely to prefer a usage-based billing model where usage is based on monthly provisioned use instead of active provisioned use. Midsize organizations were slightly more likely to care about the ability to ingest any telemetry data type without penalties (34%, compared to 32% for small and 33% for large) and to pay as they go (34%, compared to 32% for small and 29% for large). Large organizations were the most likely to care about the flexibility to scale usage based on consumption with no monthly minimum (42%, compared to 35% for midsize and 33% for small) and predictable spending (36%, compared to 32% for midsize and 29% for small).

"I often need to establish my budget 16–18 months ahead of where I'm actually going to spend it. And to the extent that I can predict accurately, that's obviously the preferred way to go."

SVP AND CTO, LARGE RETAIL ENTERPRISE

# Benefits of observability

Now for the good stuff. We were curious about the overall primary benefits of observability as well as what use cases it's used for, whether it helps improve service-level metrics, and how it most helps improve the lives of software engineers and developers.

We found that respondents saw clear benefits as a result of their current observability deployments. Observability continues to deliver a clear, positive business impact, such as improved:

- Uptime, performance, and reliability
- Operational efficiency
- Customer experience
- Innovation
- Business and/or revenue growth

These results indicate how observability can transform an organization's business, technology, and/or revenue.



| Benefit | % |
|---|---|
| Improved uptime and reliability | 35.6% |
| Increased operational efficiency | 34.6% |
| Proactive detection of issues before they impact customers | 33.3% |
| Improved customer experience | 33.1% |
| Developer confidence that our apps and/or systems are resilient | 31.1% |
| Ability to redirect resources to value-added tasks and/or accelerated innovation | 29.5% |
| Increased velocity of software delivery to market | 29.5% |
| Consolidation of IT tooling | 28.4% |
| Business and/or revenue growth | 25.6% |
| Decreased cloud hosting costs | 25.6% |
| Reduction in employee burnout | 23.9% |
| I'm not sure | 0.6% |

**Figure 26.** Primary benefits enabled by observability deployment

## ⚡ Regional insight

Respondents surveyed in Europe were the least likely to select improved uptime and reliability (32%) and proactive detection of issues before they impact customers (28%) as benefits of observability. While those surveyed in Asia Pacific were the most likely to note that proactive detection of issues before they impact customers (40%) is a benefit of observability, they were least likely to note consolidation of IT tooling (25%) and decreased cloud hosting costs (22%).

## 👤 Role insight

Executives were the least likely to say their organizations increased operational efficiency (31%), while practitioners were the most likely (36%). Non-executive managers were the most likely to say their organizations benefited from proactive detection of issues before they impact customers (40%) and the least likely to cite business/revenue growth (19%).

## ⬈ Organization size insight

Respondents from small organizations were the most likely to note that consolidation of IT tooling (38%) and business/revenue growth (32%) are benefits of observability, and the least likely to note proactive detection of issues before they impact customers (26%). Those from midsize organizations were the least likely to note improved uptime and reliability (33%) and business/revenue growth (23%). While those from large organizations were the most likely to note increased operational efficiency (39%), proactive detection of issues before they impact customers (38%), and improved customer experience (36%).

## 📊 Industry insight

Respondents from the energy/utilities industry were the most likely to note that developers having high confidence in the resilience of their apps/systems (51%) is a benefit of observability. Government respondents were the most likely to note a reduction in employee burnout (55%). Healthcare/pharma respondents were the most likely to note an improved customer experience (43%) and business/revenue growth (39%). IT/telco respondents were the most likely to note the ability to redirect resources to value-added tasks and/or accelerated innovation (35%). Nonprofit/unspecified respondents were most likely to note an increased operational efficiency (52%). And services/consulting respondents were the most likely to note improved uptime and reliability (49%).

# Use cases

We investigated the technical use cases/purposes where observability was most important to respondents. Results showed a wide range of use cases with the most common being to:

1. Optimize cloud resource usage and spend (31%)
2. Support digital transformation efforts to improve and gain a competitive advantage from the digital customer's experience (31%)
3. Manage containerized and serverless environments (29%)
4. Increase speed to market for new products/services (29%)
5. Support an organizational IT move to DevOps (29%)



| | |
|---|---|
| Optimize cloud resource usage and spend | 31.2% |
| Support digital transformation efforts to improve and gain competitive advantage from the digital customer's experience | 30.8% |
| Manage containerized and serverless environments | 29.3% |
| Increase speed to market for new products and/or services | 29.2% |
| Support organizational IT move to DevOps | 29.2% |
| Minimize risk of migrating core legacy applications to the cloud | 28.4% |
| Troubleshoot distributed systems | 28.2% |
| Connect IoT device monitoring into the full observability of estate | 26.9% |
| Support cost-cutting efforts (consolidating tools) | 26.8% |
| Automate software release cycles | 26.2% |
| Expanding observability because of a recent M&A event | 26.1% |
| Visibility to migrate from monolith to microservices | 25.0% |
| Better deliver against SLOs and/or SLAs | 24.5% |
| I'm not sure | 0.5% |
| Other | 0.1% |

**Figure 27.** Observability use cases/purposes

---

### ⚡ Regional insight

The top choice for respondents surveyed in Asia Pacific was to support digital transformation efforts, followed by increase speed to market for new products/services, minimize the risk of migrating core legacy applications to the cloud, and manage containerized and serverless environments. The second choice for those surveyed in North America was to support an organizational IT move to DevOps. European selections aligned closely with average results for all regions.

### ⊙ Role insight

Executives were the most likely to say their organizations use observability to support an organizational IT move to DevOps (34%), connect IoT device monitoring into the full observability of their estate (30%), and support cost-cutting efforts (29%). Non-executive managers were the most likely to say their organizations use it to troubleshoot distributed systems (31%) and better deliver against SLOs/SLAs (27%). Practitioners were the most likely to say that their organizations use it to minimize the risk of migrating core legacy applications to the cloud (30%).

### ⬏ Organization size insight

Respondents from small organizations were the most likely to say they use observability to support cost-cutting efforts (34%), while those from large organizations were the least likely (26%). Respondents from large organizations were the most likely to use it to manage containerized and serverless environments (35%), support an organizational IT move to DevOps (33%), and automate software-release cycles (32%).

### ⊞ Industry insight

Education respondents were the most likely to say they use observability to optimize cloud resource usage and spend (63%) and support digital transformation efforts (47%). Energy/utilities respondents were the most likely to use it to support cost-cutting efforts (40%), increase speed to market for new products/services (40%), minimize the risk of migrating core legacy applications to the cloud (38%), expand observability because of a recent M&A event (36%), and manage containerized and serverless environments (34%; tied with services/consulting). Government respondents were the most likely to use it to troubleshoot distributed systems (50%). Industrial/materials/manufacturing respondents were the most likely to use it to support an organizational IT move to DevOps (35%). Services/consulting respondents were the most likely to use it to automate software release cycles (40%).

# Incident response

Developers and engineers often use observability to solve three key business and technical challenges:

| ↓ **Reducing downtime** |
| ↓ **Reducing latency** |
| ↑ **Improving efficiency** |

Outage frequency, mean time to detection (MTTD), and mean time to resolution (MTTR) are common service-level metrics used in security and IT incident management. The survey results found that observability improves service-level metrics, with those who had full-stack observability and those who had prioritized/achieved observability experiencing fewer outages and faster MTTD and MTTR.

**Prioritizing/achieving full-stack observability** =



fewer outages

faster MTTD

faster MTTR

**Figure 28.** Prioritizing/achieving observability results in fewer outages and faster MTTD and MTTR

## Outage frequency

So, how often are outages occurring that affect customers and end users? Survey results showed that:

- Outages happen fairly frequently (52–72% noted once per week or more)
- Low-business-impact outages happen the most frequently (72% noted once per week or more)
- High-business-impact outages happen the least frequently (two to three times per month or fewer) but more than half (52%) still experience them once per week or more

| | MOST FREQUENT OUTAGES (once per week or more) | LEAST FREQUENT OUTAGES (2–3 times per month or fewer) |
|---|---|---|
| **High business impact** | 51.9% | 45.8% |
| **Medium business impact** | 62.9% | 35.3% |
| **Low business impact** | 71.6% | 26.8% |

**Table 04.** Most frequent compared to least frequent outages by high, medium, and low business impact

Given the relative frequency of outages, the findings of how often manual effort and incident tickets are the sources of knowledge for these outages are noteworthy.



**Figure 29.** Outage frequency by high, medium, and low business impact

**52%** experienced high-business-impact outages once per week or more

---

**Regional insight**

Respondents surveyed in North America were more likely to say that their organizations experience outages less frequently (two to three times per month or fewer), while those surveyed in Europe were more likely to say more frequently (once per week or more).

**Role insight**

Executives were more likely to say that their organizations experience outages less frequently (two to three times per month or fewer), while practitioners were more likely to say more frequently (once per week or more).

**Organization size insight**

Small organizations were more likely to experience low-business-impact outages once per week or more and medium- and high-business-impact outages two to three times per month or fewer. Midsize and large organizations were more likely to experience outages once per week or more.

There's a clear connection between those who have achieved full-stack observability and a lower frequency of outages. Respondents from organizations that have achieved full-stack observability (based on our definition) were also more likely to experience the least frequent outages (two to three times per month or fewer) and less likely to experience the most frequent outages (once per week or more).

| | MOST FREQUENT OUTAGES (once per week or more) | | LEAST FREQUENT OUTAGES (2–3 times per month or fewer) | |
|---|---|---|---|---|
| | WITH full-stack observability | WITHOUT full-stack observability | WITH full-stack observability | WITHOUT full-stack observability |
| High business impact | 41.3% | 55.9% | 56.4% | 41.9% |
| Medium business impact | 51.2% | 67.3% | 46.4% | 31.2% |
| Low business impact | 59.6% | 76.1% | 38.2% | 22.5% |

**Table 05.** Most frequent compared to least frequent outages by high, medium, and low business impact and with or without full-stack observability

And respondents who indicated that they have already prioritized/achieved full-stack observability were also more likely to experience the least frequent outages (two to three times per month or fewer) and less likely to experience the most frequent outages (once per week or more).

The data supports a strong correlation between full-stack observability and less frequent outages.

| | MOST FREQUENT OUTAGES (once per week or more) | | LEAST FREQUENT OUTAGES (2–3 times per month or fewer) | |
|---|---|---|---|---|
| | Have prioritized/achieved full-stack observability | Have NOT prioritized/ achieved full-stack observability | Have prioritized/achieved full-stack observability | Have NOT prioritized/ achieved full-stack observability |
| High business impact | 34.1% | 52.4% | 65.9% | 45.3% |
| Medium business impact | 36.4% | 63.6% | 63.6% | 34.5% |
| Low business impact | 34.1% | 72.7% | 63.6% | 25.7% |

**Table 06.** Most frequent compared to least frequent outages by high, medium, and low business impact and have or have not prioritized/achieved full-stack observability

## MTTD

When we looked at the mean time to detect an outage, a common service-level metric used in security and IT incident management, the survey results showed:

- The majority had an MTTD of more than five but less than 60 minutes
- In general, it took more time to detect high- compared to low-business-impact outages
- More than one in five (22%) took more than an hour to detect high-business-impact outages

| | FASTEST MTTD (less than 30 minutes) | SLOWEST MTTD (more than 30 minutes) |
|---|---|---|
| High-business-impact outages | 44.5% | 53.1% |
| Medium-business-impact-outages | 49.1% | 49.1% |
| Low-business-impact outages | 58.6% | 39.5% |

**Table 07.** Fastest compared to slowest MTTD by high-, medium-, and low-business-impact outages



High-business-impact outages
- 15.9%
- 28.6%
- 30.7%
- 16.6%

Medium-business-impact outages
- 12.8%
- 36.2%
- 35.7%
- 12.0%

Low-business-impact outages
- 17.6%
- 41.0%
- 28.4%
- 8.6%

- Less than 5 minutes
- More than 5 but less than 30 minutes
- More than 30 but less than 60 minutes
- More than 60 but less than 120 minutes
- More than 120 minutes
- I'm not sure

**Figure 30.** MTTD by high-, medium-, and low-business-impact outages

### Regional insight

For high-business-impact outages, respondents surveyed in Europe were the least likely to have an MTTD of more than 60 minutes (19%, compared to 26% for those surveyed in Asia Pacific and 24% for those surveyed in North America). For medium-business-impact outages, Asia Pacific organizations were more likely to have a faster MTTD (55%), while North American organizations were the least likely (53%). For low-business-impact outages, North American organizations were more likely to have a faster MTTD (62%) and European organizations were the least likely (57%).

### Role insight

For low-business-impact outages, executives and practitioners were more optimistic about the MTTD time than non-executive managers. And for high-business-impact outages, ITDMs were more optimistic than practitioners.

### Organization size insight

Small organizations were the most likely to detect high-business-impact outages in 30 minutes or less (48%, compared to 44% for midsize and 45% for large).

## 22%

were taking more than an hour to detect high-business-impact outages

Another interesting finding is that respondents from organizations that have achieved full-stack observability (based on our definition) and those who indicated that they have already prioritized/achieved full-stack observability were also more likely to experience the fastest MTTD (less than five minutes).

| | FASTEST MTTD (less than 5 minutes) | | | |
|---|---|---|---|---|
| | WITH full-stack observability | WITHOUT full-stack observability | Have prioritized/achieved full-stack observability | Have NOT prioritized/ achieved full-stack observability |
| High-business-impact outages | 20.1% | 14.3% | 25.0% | 15.6% |
| Medium-business-impact outages | 16.9% | 11.3% | 31.8% | 12.3% |
| Low-business-impact outages | 24.2% | 15.1% | 34.1% | 17.1% |

Table 08. Fastest MTTD by high-, medium-, and low-business-impact outages and with or without full-stack observability or have and have not prioritized/achieved full-stack observability

Respondents who indicated that they have already prioritized/achieved full-stack observability were more likely to have the fastest MTTD (less than 30 minutes) and less likely to have the slowest MTTD (more than 30 minutes).

The data supports a strong correlation between full-stack observability and a faster MTTD.

| | FASTEST MTTD (less than 30 minutes) | | SLOWEST MTTD (more than 30 minutes) | |
|---|---|---|---|---|
| | Have prioritized/achieved full-stack observability | Have NOT prioritized/ achieved full-stack observability | Have prioritized/achieved full-stack observability | Have NOT prioritized/ achieved full-stack observability |
| High-business-impact outages | 68.2% | 43.8% | 31.8% | 53.7% |
| Medium-business-impact outages | 65.9% | 48.6% | 34.1% | 49.5% |
| Low-business-impact outages | 65.9% | 58.4% | 31.8% | 39.7% |

Table 09. Fastest MTTD compared to slowest MTTD by high-, medium-, and low-business-impact outages and have and have not prioritized/achieved full-stack observability

## MTTR

We see similar patterns with MTTR, another common service-level metric used in security and IT incident management:

- The majority had an MTTR of more than five but less than 60 minutes
- In general, it took more time to resolve high- and medium- compared to low-business-impact outages
- Almost a third (29%) took more than an hour to resolve high-business-impact outages

| | FASTEST MTTR (less than 30 minutes) | SLOWEST MTTR (more than 30 minutes) |
|---|---|---|
| High-business-impact outages | 38.2% | 59.7% |
| Medium-business-impact outages | 43.6% | 54.6% |
| Low-business-impact outages | 54.0% | 44.2% |

**Table 10.** Fastest compared to slowest MTTR by high-, medium-, and low-business-impact outages



High-business-impact outages
- ◄ 10.8%
- ◄ 27.4%
- ◄ 31.1%
- ◄ 19.5%
- ◄ 9.1%

Medium-business-impact outages
- ◄ 10.4%
- ◄ 33.2%
- ◄ 36.5%
- ◄ 14.9%

Low-business-impact outages
- ◄ 15.2%
- ◄ 38.8%
- ◄ 31.2%
- ◄ 9.6%

Legend:
- ● Less than 5 minutes
- ● More than 5 but less than 30 minutes
- ● More than 30 but less than 60 minutes
- ● More than 60 but less than 120 minutes
- ● More than 120 minutes
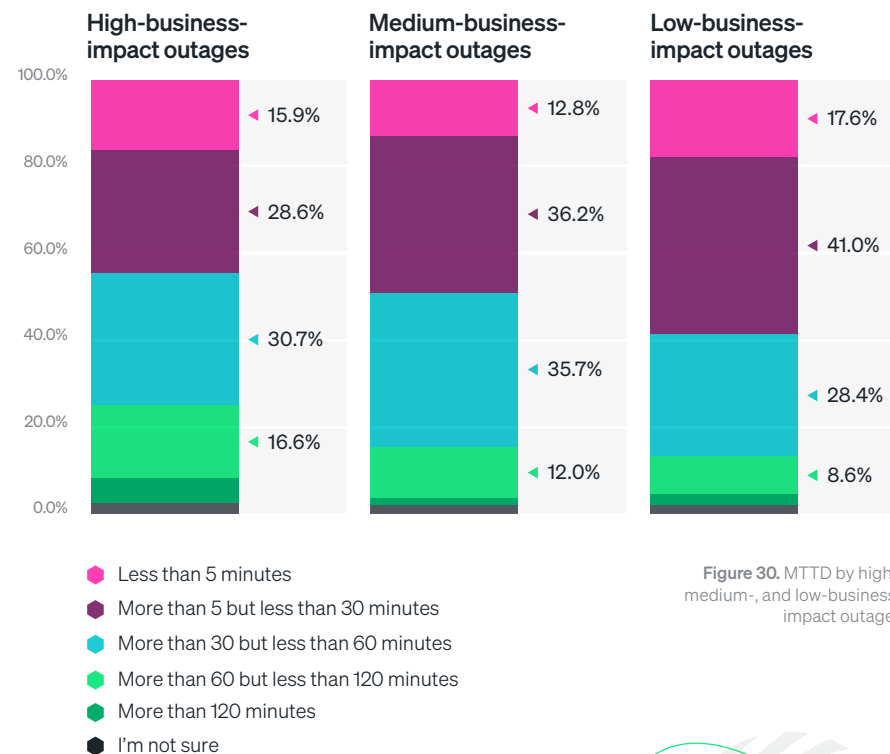- ● I'm not sure

**Figure 31.** MTTR by high-, medium-, and low-business-impact outages

### Regional insight

For high- and medium-business-impact outages, respondents surveyed in Europe were the most likely to have an MTTR of less than five minutes and the least likely to have an MTTR of more than an hour.

### Role insight

For high- and medium-business-impact outages, non-executive managers were more likely to select an MTTR of more than an hour than executives and practitioners. And for low-business-impact outages, executives and practitioners were more optimistic about the MTTR time than non-executive managers.

### Organization size insight

Large organizations were the most likely to take more than an hour to detect high- and medium-business-impact outages.

## 29%
took more than an hour to resolve high-business-impact outages

Respondents from organizations that have achieved full-stack observability (based on our definition) and those who indicated that they have already prioritized/achieved full-stack observability were also more likely to experience the fastest MTTR (less than five minutes).

| | FASTEST MTTR (less than 5 minutes) | | | |
|---|---|---|---|---|
| | WITH full-stack observability | WITHOUT full-stack observability | Have prioritized/achieved full-stack observability | Have NOT prioritized/ achieved full-stack observability |
| High-business-impact outages | 13.0% | 9.9% | 25.0% | 10.4% |
| Medium-business-impact outages | 10.7% | 10.3% | 22.7% | 10.1% |
| Low-business-impact outages | 18.7% | 13.9% | 34.1% | 14.7% |

Table 11. Fastest MTTR by high-, medium-, and low-business-impact outages and with or without full-stack observability or have and have not prioritized/achieved full-stack observability

Respondents who indicated that they have already prioritized/achieved full-stack observability were also more likely to have the fastest MTTR (less than 30 minutes), while those who had not prioritized/achieved full-stack observability had the slowest MTTR (more than 30 minutes).

The data supports a strong correlation between full-stack observability and a faster MTTR. Clearly, there's a link between full-stack observability and the best outage frequency, MTTD, and MTTR performance indicators.

Learn how they plan to reduce MTTR.

| | FASTEST MTTR (less than 30 minutes) | | SLOWEST MTTR (more than 30 minutes) | |
|---|---|---|---|---|
| | Have prioritized/achieved full-stack observability | Have NOT prioritized/ achieved full-stack observability | Have prioritized/achieved full-stack observability | Have NOT prioritized/ achieved full-stack observability |
| High-business-impact outages | 61.4% | 37.5% | 38.6% | 60.3% |
| Medium-business-impact outages | 59.1% | 43.2% | 40.9% | 55.0% |
| Low-business-impact outages | 65.9% | 53.6% | 29.6% | 44.6% |

Table 12. Fastest MTTR compared to slowest MTTR by high-, medium-, and low-business-impact outages and have and have not prioritized/achieved full-stack observability

## Predictors of MTTD/MTTR by capability

In addition, the data predicts a positive association between certain capabilities—including AIOps, distributed tracing, security monitoring, custom dashboards, synthetic monitoring, APM, database monitoring, alerts, and infrastructure monitoring—and a faster MTTD/MTTR (less than 30 minutes). Of those capabilities, **AIOps is statistically significant within 10% significance levels.**
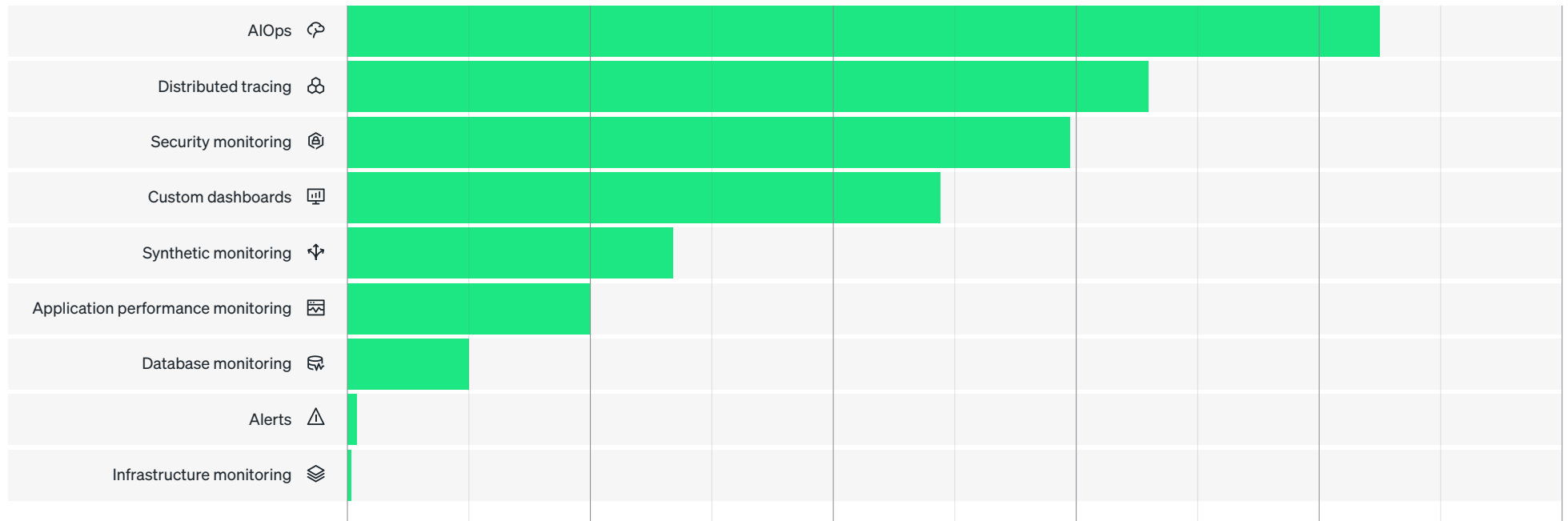


**Figure 32.** Capabilities that predict an MTTD/MTTR of less than 30 minutes

# Day-to-day life for developers and engineers

We asked the practitioners themselves, as well as ITDMs, how observability helps developers and engineers the most. We found:

- At least 30% said it increases productivity and enables cross-team collaboration and less guesswork when managing complicated and distributed tech stacks
- About three out of 10 said it makes developer/engineer lives easier and improves work/life balance and skillset/hireability
- Roughly a quarter felt that it helps confirm/overcome assumptions, overcome opinions, and fill in gaps

These findings suggest that developers and engineers seek solutions that reduce toil, increase cross-team collaboration, and help them use their time proactively. A data-driven approach to engineering and an all-in-one observability platform make developer and engineer lives better and easier through:

- Less guesswork managing complicated and distributed tech stacks involving containers, multi-clouds, and multiple tools
- A better signal-to-noise ratio in the understanding of why incidents took place, not just what happened
- Resolving issues faster and freeing up time to focus on the higher-priority, business-impacting, and creative coding they love

| Category | % |
|---|---|
| Increases productivity (find and resolve issues faster) | 34.4% |
| Enables cross-team collaboration (DevOps, DevSecOps) | 32.5% |
| Enables less guesswork when managing complicated and distributed tech stacks | 30.0% |
| Improves skillset/hireability | 29.4% |
| Makes job easier | 28.9% |
| Improves work/life balance | 28.9% |
| Enables time prioritization | 27.6% |
| Increases innovation | 26.9% |
| Frees up time to work on other projects | 26.8% |
| Helps confirm assumptions | 24.9% |
| Helps overcome assumptions | 23.5% |
| Helps fill in the gaps | 23.3% |
| Helps overcome opinions | 23.1% |
| I'm not sure | 0.3% |
| None of the above, observability does not help | 0.1% |

Figure 33. How observability helps improve the lives of developers/engineers the most

## Regional insight

Respondents surveyed in Asia Pacific were the most likely to select increases productivity (41%, compared to 30% for those surveyed in Europe and 35% for those surveyed in North America). Those surveyed in Europe were the most likely to select making developer/engineer lives easier as their top choice (31%). While those surveyed in North America were the most likely to say it increases innovation (32%, compared to 24% for those surveyed in Asia Pacific and 25% for those surveyed in North America) and frees up time to work on other projects (30%, compared to 27% for those surveyed in Asia Pacific and 24% for those surveyed in Europe).

## Role insight

Executives were more likely to think that observability improves work/life balance for practitioners (32%) than the practitioners themselves (28%). While non-executive managers were the most likely to feel that it frees up time for practitioners to work on other projects (34%) and the least likely to feel that it makes their jobs easier (22%), increases innovation (23%), or enables cross-team collaboration (26%).

## Industry insight

Respondents from the education industry were more likely to think that observability enables less guesswork (43%), makes jobs easier (40%), confirms assumptions (37%), and improves skillset/hireability (37%) than those from most other industries. Those from the energy/utilities industry were also more likely to say it enables less guesswork and improves work/life balance (42% for both). Government respondents also ranked enables less guesswork higher (42%). And services/consulting respondents were more partial to improving skillset/hireability (36%) and enabling time prioritization (38%) and cross-team collaboration (43%) than most others.

# 29%
said observability makes developer/engineer lives easier and improves work/life balance and skillset/hireability

# Challenges preventing full-stack observability

So, if full-stack observability provides so many benefits, what's preventing organizations from prioritizing/achieving it? We found that:

- A lack of understanding of the benefits and feelings that current IT performance is adequate enough were the most frequently cited challenges (28% for both)
- More than a quarter of respondents (27%) noted they do not have the budget
- A quarter said they have too many monitoring tools
- Just under a quarter struggled with a lengthy sales cycle, un-instrumented systems, a lack of strategy, and a disparate tech stack
- Nearly one in five (19%) indicated they do not have the skills

In addition, of those who said that their IT performance is adequate (no need to improve current performance), 51% said that they allocate more than 20% of their budget to observability tools.

Taken together, these results suggest a number of different hurdles and pain points when it comes to pursuing full-stack observability. To achieve full-stack observability, technology professionals should have a clearer rationale for its benefits, and large organizations, in particular, should weave this rationale into a clear business strategy.



| Challenge | % |
|---|---|
| Lack of understanding of benefits (we don't see the value in prioritizing right now) | 28.3% |
| Our IT performance is adequate (no need to improve current performance) | 28.3% |
| Lack of budget | 26.9% |
| Too many monitoring tools | 25.1% |
| Lengthy sales cycle | 24.9% |
| Not enough of our systems are instrumented | 24.8% |
| Lack of strategy | 24.3% |
| Disparate tech stack | 24.2% |
| Too expensive | 22.4% |
| We don't have dedicated personnel | 22.2% |
| Siloed data | 21.7% |
| We don't have the skills | 19.1% |
| None (we have already prioritized and/or achieved observability) | 2.7% |
| I'm not sure | 0.9% |
| Other | 0.1% |

**Figure 34.** Primary challenges preventing the prioritization or achievement of full-stack observability

### Regional insight

In the Asia Pacific region where 55% claimed that they prefer a single, consolidated platform, their top barriers were that not enough of their systems are instrumented and too many monitoring tools (both 28%). While respondents surveyed in Europe were slightly more likely to cite a lack of budget (29%) and less likely to cite a lack of strategy (21%) and that not enough of their systems are instrumented (22%). And those surveyed in North America were more likely to cite a lack of understanding of benefits (32%) and adequate IT performance (31%).

### Role insight

Many practitioners and executives felt that a lack of understanding of benefits was a primary challenge to adopting full-stack observability (29%), but non-executive managers were more likely to feel that their current IT performance is adequate (31%). Practitioners were the least likely to say that their IT performance is adequate (26%) or that they don't have the skills (17%), while more likely to cite a disparate tech stack (26%) and siloed data (23%).

### Organization size insight

Small organizations said the biggest challenge was that it was too expensive (33%), followed by a lack of budget (29%). Midsize organizations struggled the most with a lack of understanding of the benefits (30%). Large organizations were the most likely to say that their IT performance is adequate (32%), while the largest—those with 5,000 or more employees—were the most likely to note a lack of strategy (34%).

# 3%
said they have already prioritized/achieved full-stack observability

# Future of observability

## Organizations see the business value of observability—and expect to invest more in it.
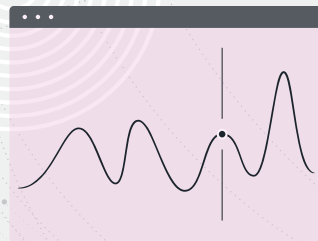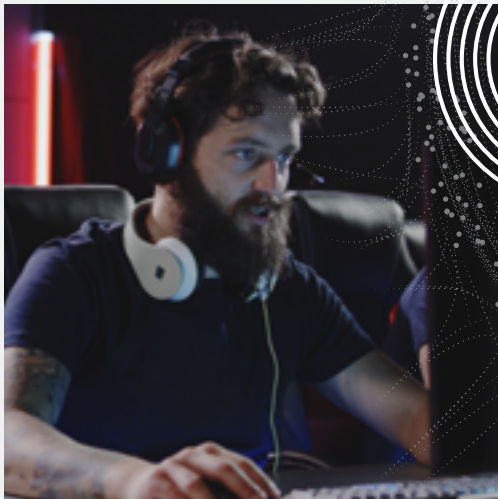
# Reducing MTTR

We asked respondents what would do the most to help reduce MTTR, a critical question considering 44–60% said they take 30 minutes or more to resolve outages. Overall, their top choices were:

1. Better DevOps practices (39%)
2. Automated incident response workflows (38%)
3. Staff training for observability tools (36%)

Those with full-stack observability were notably more likely to say automated incident response workflows to reduce MTTR (42%) than those without full-stack observability (36%).

| | |
|---|---|
| Better DevOps practices such as incident learning and establishing SLOs (best practices) | 38.8% |
| Automated incident response workflows (operational efficiency) | 37.6% |
| Staff training for observability tools (training) | 36.0% |
| Centralized view of available data (wider access) | 34.9% |
| Predictive anomaly detection (insightful metrics) | 32.9% |
| Extended coverage across systems (breadth of coverage) | 32.2% |
| More thorough instrumentation (depth of coverage) | 31.5% |
| More staff (hiring) | 24.8% |
| I'm not sure | 0.7% |

**Figure 35.** Ways to most help reduce MTTR for outages

**Regional insight**

Unlike respondents surveyed in Asia Pacific and Europe, those surveyed in North America were the most likely to select staff training for observability tools as the top way to reduce MTTR (40%), and their fourth choice was better DevOps practices. While those surveyed in Asia Pacific were the most likely to select better DevOps practices (42%).

**Role insight**

Practitioners were the most likely to select staff training for observability tools (37%). Executives were the least likely to select more staff (22%). And non-executive managers were the least likely to select a centralized view of available data (32%) and predictive anomaly detection (30%).

**Organization size insight**

The top choices for respondents from small organizations included staff training for observability tools (40%), more thorough instrumentation (36%), and predictive anomaly detection (35%). While the top choices for midsize and large organizations aligned with the overall results.

**Industry insight**

Government and healthcare/pharma industry respondents were the only ones to select more staff as their top choice. Those from the education, energy/utilities, financial/insurance, and retail/consumer industries all selected automated incident response workflows as their top choice. Nonprofit/unspecified and services/consulting respondents chose staff training for observability tools. While industrials/materials/manufacturing and IT/telco chose better DevOps practices.

# Deployment plans

Forward-looking enterprise leaders are implementing observability as a business imperative. It's interesting to see how aggressively respondents expect to have most capabilities deployed in the next year and the next three years.

## Next year

This will be a big year for deploying additional observability capabilities—by the end of 2023, respondents expected that 72–86% of capabilities will be deployed:

- Almost a third (32%) expected to deploy 1–5 new capabilities
- More than half (56%) expected to deploy 6–10 new capabilities
- Only 5% expected to deploy 11–14 new capabilities
- Just 8% did not expect to deploy new capabilities

Notably, more than 40% expected to deploy ML model performance monitoring and AIOps in the next year.

When we look one year out, capability deployment is in the mid-80% range for capabilities like network monitoring, security monitoring, log management, database monitoring, alerts, and infrastructure monitoring.

Even with some of the capabilities that respondents were less likely to expect to deploy next year (like Kubernetes monitoring, synthetic monitoring, distributed tracing, and the like), we see numbers in the mid-70% range.

## Next three years

Looking out to 2025, we see that nearly all respondents expected to deploy observability capabilities like network monitoring, security monitoring, log management, and more.

The majority of respondents indicated that they would have most capabilities (88–97%) deployed by 2025. Over the next two to three years:

- Most (60%) expected to deploy 1–5 new capabilities
- Just 8% expected to deploy 6 or more new capabilities
- About a third (32%) did not expect to deploy new capabilities (presumably because they will have already been deployed)
- One respondent indicated that they expect to deploy all 17 capabilities

And even among some of the least commonly deployed capabilities, like Kubernetes monitoring, we saw that an overwhelming 88% of respondents said they had deployed it or expected to have it deployed in three years.
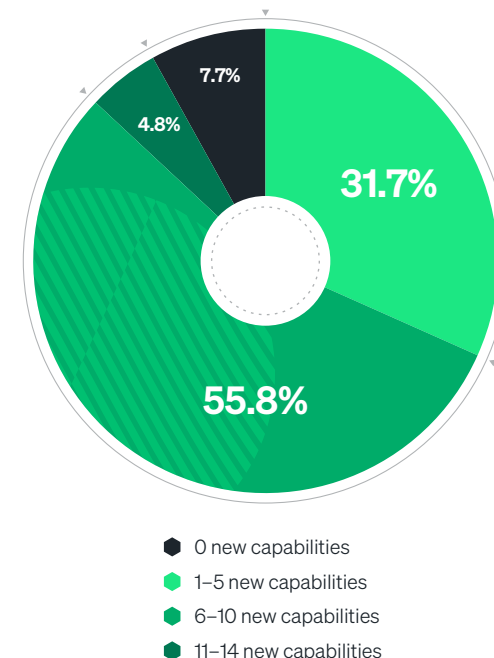


- 0 new capabilities
- 1–5 new capabilities
- 6–10 new capabilities
- 11–14 new capabilities

**Figure 36.** Capabilities deployment expectations for the next year

# 88–97%

of 17 different observability capabilities should be deployed by 2025

# Capability deployment summary

By 2025, 88–97% of 17 different observability capabilities are expected to be deployed. Very few of our survey respondents did not expect to deploy these observability capabilities (2–7%).

- ⬢ % not deployed, no plans to add
- ⬢ % currently deployed
- ⬢ % planned to deploy by 2023
- ⬢ % planned to deploy by 2025

This stated intent to deploy a large number of observability capabilities is one of the most eye-opening results from this study as it suggests that most organizations may have robust observability practices in place by 2025. The finding highlights the current state of observability and growth potential in the near future.

"With remote work, there is the need for more monitoring and automatic alerting. There is a need for tools that fully monitor all the aspects and alert them quickly. I think it's going to move to a much higher percentage. You're probably going to end up easily closing in on 90% of them being monitored."

SENIOR ENGINEER, LARGE FINANCIAL ENTERPRISE

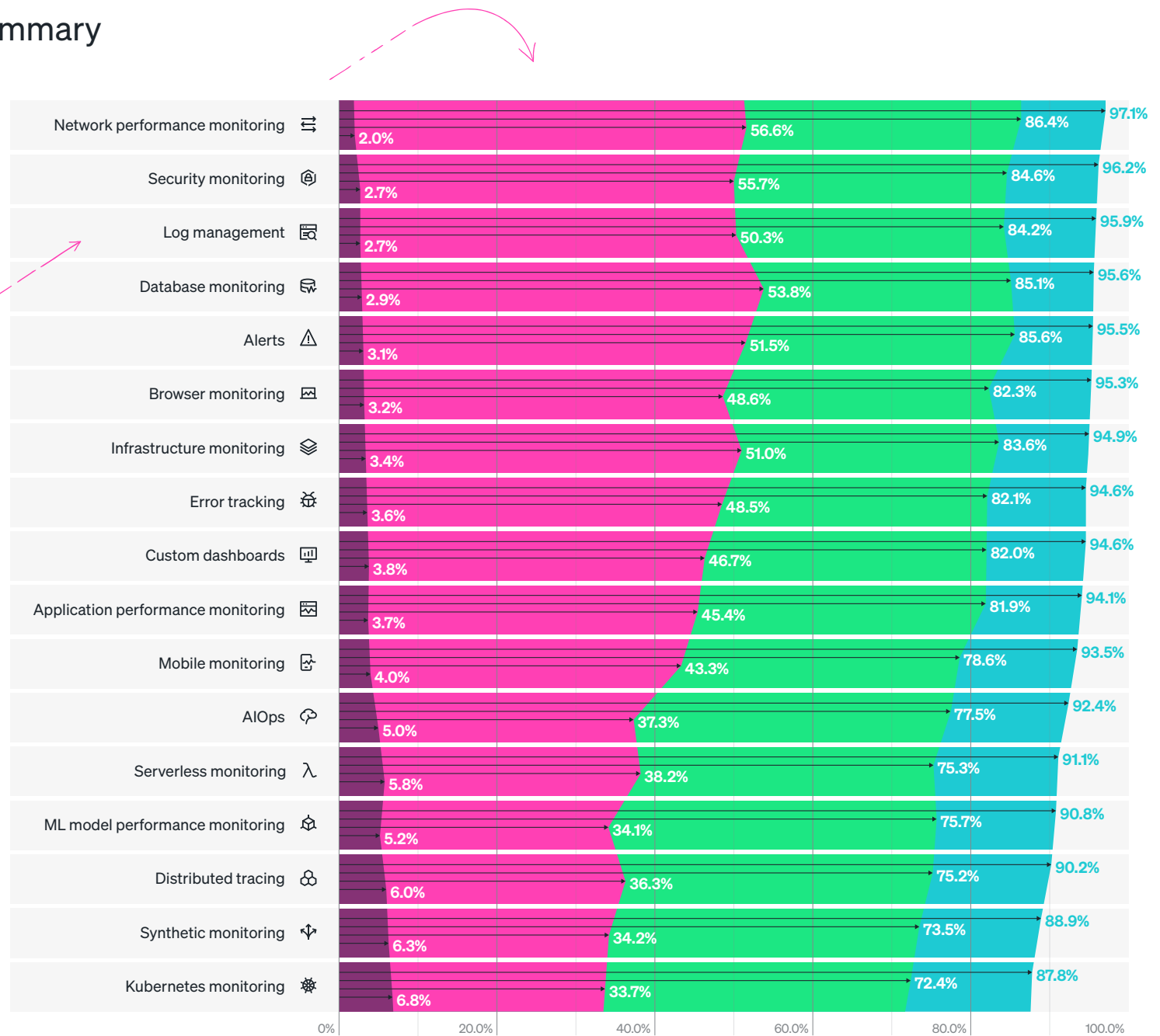| Capability | % not deployed | % currently deployed | % planned by 2023 | % planned by 2025 |
|---|---|---|---|---|
| Network performance monitoring | 2.0% | 56.6% | 86.4% | 97.1% |
| Security monitoring | 2.7% | 55.7% | 84.6% | 96.2% |
| Log management | 2.7% | 50.3% | 84.2% | 95.9% |
| Database monitoring | 2.9% | 53.8% | 85.1% | 95.6% |
| Alerts | 3.1% | 51.5% | 85.6% | 95.5% |
| Browser monitoring | 3.2% | 48.6% | 82.3% | 95.3% |
| Infrastructure monitoring | 3.4% | 51.0% | 83.6% | 94.9% |
| Error tracking | 3.6% | 48.5% | 82.1% | 94.6% |
| Custom dashboards | 3.8% | 46.7% | 82.0% | 94.6% |
| Application performance monitoring | 3.7% | 45.4% | 81.9% | 94.1% |
| Mobile monitoring | 4.0% | 43.3% | 78.6% | 93.5% |
| AIOps | 5.0% | 37.3% | 77.5% | 92.4% |
| Serverless monitoring | 5.8% | 38.2% | 75.3% | 91.1% |
| ML model performance monitoring | 5.2% | 34.1% | 75.7% | 90.8% |
| Distributed tracing | 6.0% | 36.3% | 75.2% | 90.2% |
| Synthetic monitoring | 6.3% | 34.2% | 73.5% | 88.9% |
| Kubernetes monitoring | 6.8% | 33.7% | 72.4% | 87.8% |

**Figure 37.** Capabilities deployment summary for 2022 through 2025

# Budget plans

So, how do respondents' budget plans align with their aforementioned aggressive observability capability deployment plans? We asked respondents about their observability budget plans for the next year and found that:

- More than half (52%) expect observability budgets to increase (38% somewhat and 14% significantly or extensively)
- One out of five respondents expect to maintain their observability budgets (within + or - 5%)
- Only 27% expect to decrease their observability budgets (12% somewhat and 15% significantly or extensively)

Surprisingly, respondents who expected to deploy the least number of capabilities (0–3) in the next year were the most likely to say their observability budgets will increase or stay the same (80% range). While those who expected to deploy the most capabilities (4–14) were, for the most part, more likely to say their observability budgets will decrease. This could indicate that those who make decisions about what to deploy are not aligned with those who make budget decisions—or that decision-makers are using or expect to use an observability vendor that doesn't charge extra for each capability (like New Relic).

Those who had achieved full-stack observability (based on our definition) were more likely to say their observability budgets will increase or stay the same over the next year (79%), compared to those who hadn't achieved full-stack observability (69%).

And those who had a mature observability practice (based on our definition) were also more likely to say their observability budgets will increase or stay the same over the next year (86%), compared to those who didn't have a mature observability practice (71%).

Interestingly, those who saw observability as completely for incident response/ insurance were also the most likely to expect their observability budgets to increase or stay the same over the next year (83%). While those who saw observability as completely for core business goals were less likely to expect to increase their observability budgets or keep them the same (70%).

All-in-all, observability continues to be a budget priority for organizations.
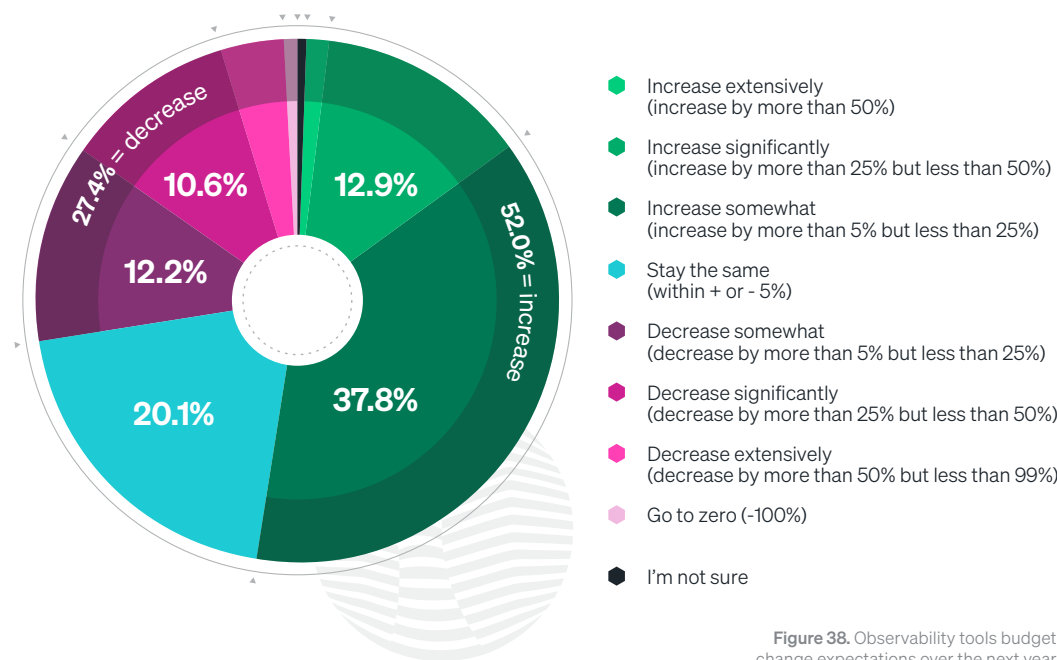


- ● Increase extensively
  (increase by more than 50%)
- ● Increase significantly
  (increase by more than 25% but less than 50%)
- ● Increase somewhat
  (increase by more than 5% but less than 25%)
- ● Stay the same
  (within + or - 5%)
- ● Decrease somewhat
  (decrease by more than 5% but less than 25%)
- ● Decrease significantly
  (decrease by more than 25% but less than 50%)
- ● Decrease extensively
  (decrease by more than 50% but less than 99%)
- ● Go to zero (-100%)
- ● I'm not sure

**Figure 38.** Observability tools budget change expectations over the next year

---

⬚ **Regional insight**

Respondents in North America were more likely to say they expect to increase their budgets in the next year than those from other regions (63%, compared to 51% for those surveyed in Asia Pacific and 45% for those surveyed in Europe).

---

⬚ **Role insight**

Over the next year, 57% of executives expected to increase their budgets for observability tools, including 16% who expected to increase them significantly or extensively.

---

⬚ **Organization size insight**

Respondents from large organizations were more likely to say their observability budgets will increase over the next year (57%), midsize to say they will decrease (30%), and small to say they will stay the same (28%).

---

# 72%

expected to increase or maintain their observability budgets next year

# Market opportunities

We also wanted to know what other types of technology respondents foresee their organizations most needing observability for in the next three years. The survey results show that:

- More established technologies that are likely to be on executive priority roadmaps—including artificial intelligence (AI) and the Internet of Things (IoT)—stood out as the top choice (mid-40% range)
- Second-wave technologies or those on the way out—including business applications, 5G, blockchain, and edge computing—were all in the low- to mid-30% range
- Emerging technologies or those on the way up—including cloud gaming, indiscriminate personalization, super apps, Web3, and the metaverse—were all in the low-20% range or slightly less

As observability can help make newer technologies like AI, 5G, and blockchain more manageable to deploy and leverage as a competitive advantage, their prioritization isn't surprising.
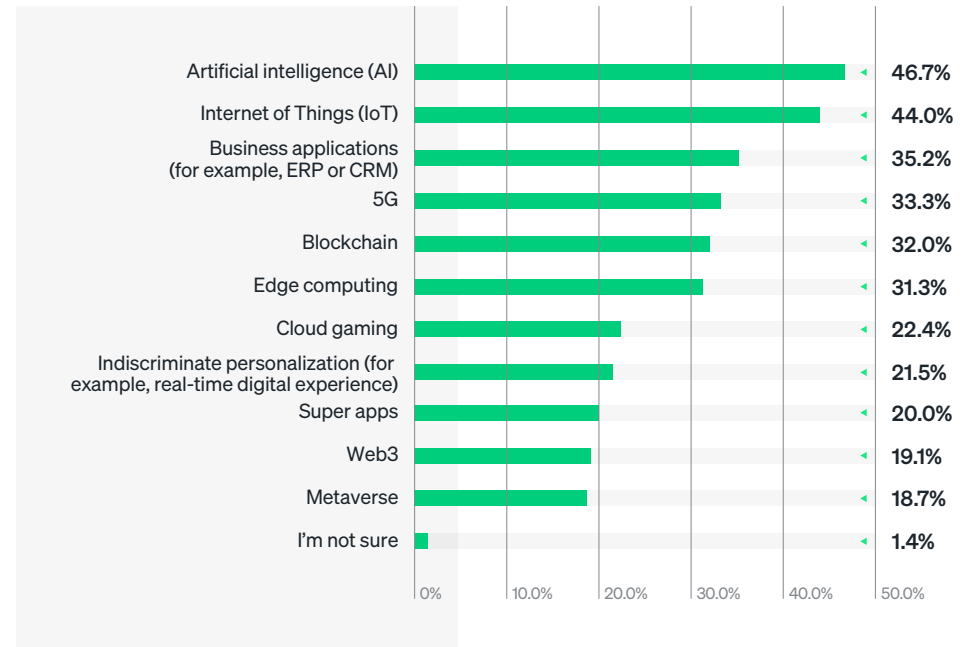
Learn more about each of these 11 technologies.



| Technology | % |
|---|---|
| Artificial intelligence (AI) | 46.7% |
| Internet of Things (IoT) | 44.0% |
| Business applications (for example, ERP or CRM) | 35.2% |
| 5G | 33.3% |
| Blockchain | 32.0% |
| Edge computing | 31.3% |
| Cloud gaming | 22.4% |
| Indiscriminate personalization (for example, real-time digital experience) | 21.5% |
| Super apps | 20.0% |
| Web3 | 19.1% |
| Metaverse | 18.7% |
| I'm not sure | 1.4% |

**Figure 39.** Technologies most needing observability in the next three years

---

**Regional insight**

Respondents surveyed in North America were more likely to foresee needing observability for AI in the next three years (52%, compared to 46% for those surveyed in Asia Pacific and 43% for those surveyed in Europe). Those surveyed in Asia Pacific were slightly more likely to select indiscriminate personalization such as real-time digital experience (26%, compared to 19% for those surveyed in Europe and 22% for those surveyed in North America). While those surveyed in Europe were less likely to select blockchain (29%, compared to 35% for those surveyed in Asia Pacific and 34% for those surveyed in North America).

**Role insight**

In the next three years, executives were more likely to foresee needing observability for AI (51%, compared to 41% for non-executive managers and 46% for practitioners) and edge computing (38%, compared to 31% for non-executive managers and 29% for practitioners).

**Industry insight**

IoT was the top choice for respondents in several industries, including education (51%), energy/utilities (61%), financial/insurance (42%), healthcare/pharma (47%), and industrials/materials/manufacturing (43%). Respondents from the industrials/materials/manufacturing industry were the only ones to select business apps such as enterprise resource planning (ERP) and customer relationship management (CRM) as their top choice (43%, tied with IoT), while it was the second choice for retail/consumer respondents (40%).

Respondents from the energy/utilities and services/consulting industries were more likely to select edge computing than those from other industries (42% and 45% respectively). Those from energy/utilities were also more likely to select metaverse than those from other industries (31%). While 5G was the third choice for IT/telco respondents (36%).

# Summary, conclusion, and key takeaways

## Data, team, and tool fragmentation are challenging but observability benefits are clear.
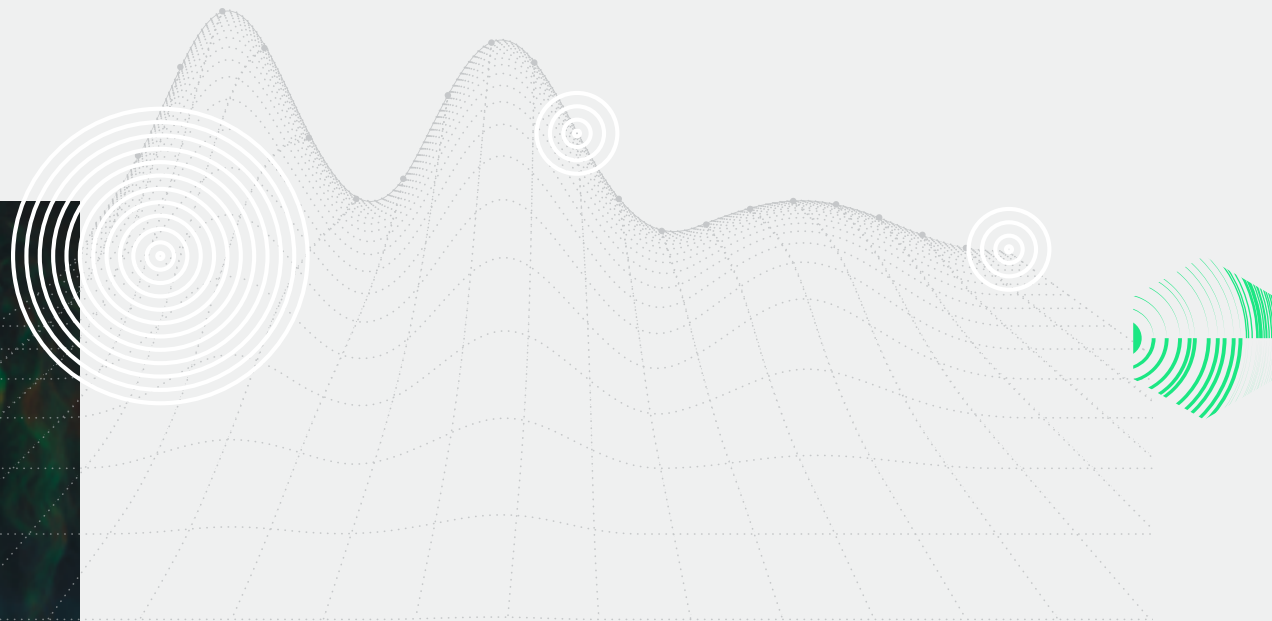
# Data, tools, and teams are fragmented

Technology professionals today deal with a complex patchwork of data and tools to monitor and keep their tech portfolios up, running, and secure. We see that the current state of observability is frequently multi-tool and still involves engineers in significant amounts of manual effort and coordination between several systems and streams of data. For most organizations, the current state of observability:

- Is largely multi-tool
- Is not covering the full tech stack
- Involves significant coordination and complexity between data streams and systems
- Requires manual effort and incident tickets to detect problems
- Has outage frequency, MTTD, and MTTR performance that could be improved

Respondents clearly seem to long for the simplicity of a single tool that does more to free them to pursue higher-value initiatives. Survey results show strong interest in a seamless, integrated future.

Organizations need to tackle fragmentation—of data, tools, and teams—that slows everyone down. Such fragmentation causes a host of downstream challenges, including suboptimal customer experiences, spiraling IT costs, engineer time wasted on toilsome/reactive tasks, inefficient allocation of resources, increasing competitive threats, and security vulnerabilities, among others.

We believe that they can achieve the best digital customer experience by consolidating disparate systems, tools, and information sources into a single observability platform. Maintaining the consistency, availability, and security of digital experiences is the key to success.

# Observability improves service-level metrics

Prioritizing/achieving full-stack observability can help:

↓ Reduce outage frequency
↑ Improve detection time of outages (MTTD)
↑ Improve resolution time of outages (MTTR)

# Organizations are investing in observability

Despite many survey respondents citing a lack of understanding of the benefits of observability as a primary challenge to prioritizing/achieving it, the results taken as a whole indicate that they do see bottom-line benefits. Respondents are investing in their observability practices and want more, better, simpler observability. Organizations have bold expectations to ramp up observability capabilities and budgets sharply in the next three years, indicating a more mature and full-stack state of observability in the near future.

The potential of an all-in-one observability platform for every engineer at every stage of the software lifecycle is becoming increasingly clear. We're right on the cusp of transformation in this area—an inflection point where organizations make the jump into deliberate, unified observability practices with less complexity and more ways to make work easier. In a few years, most organizations may look back and wonder how they managed to make do without full-stack observability.

# Tips to attain the ideal state of observability

Based on the survey results, we believe the ideal state of observability is one where organizations monitor the entire tech stack in all stages of the SDLC, employ mature observability practice characteristics, and have unified telemetry data and a unified dashboard or visualization of that data—ideally in a single, consolidated platform. So, how can organizations get to the ideal state of observability? They can start by addressing the challenges that often prevent it.

| Challenges | Solutions |
|---|---|
| **Poor perception**<br>• Lack of understanding of benefits (don't see the value in prioritizing right now)<br>• Belief that IT performance is adequate (no need to improve current performance) | **Educate users about the benefits and value of observability, including improved IT performance. For example, highlight common use cases:**<br>• Optimize cloud resource usage and spend<br>• Support digital transformation efforts to improve and gain a competitive advantage from the digital customer's experience<br>• Manage containerized and serverless environments<br>• Increase speed to market for new products/services<br>• Support an organizational IT move to DevOps<br>• Minimize the risk of migrating core legacy applications to the cloud<br>• Troubleshoot distributed systems |
| **Tool fragmentation**<br>• Too many monitoring tools<br>• Disparate tech stack | **Move towards an all-in-one observability platform:**<br>• Consolidate monitoring tools to a single platform<br>• Provide a centralized view of available data (wider access)<br>• Unify telemetry data in a single pane for consumption across teams |
| **Data fragmentation**<br>• Not enough systems are instrumented<br>• Siloed data | **Prioritize and achieve full-stack observability:**<br>• Capture telemetry data across the full tech stack<br>• Extend coverage across systems (breadth of coverage)<br>• Instrument more thoroughly (depth of coverage)<br>• Automate instrumentation<br>• Provide users with broad access to telemetry data and visualization |
| **Insufficient organizational support**<br>• Lack of strategy<br>• Lack of budget<br>• Lack of dedicated personnel<br>• Lack of skills | **Plan to support observability goals:**<br>• Create a comprehensive observability strategy<br>• Allocate a sufficient budget according to current and future observability needs<br>• Hire additional staff as needed<br>• Train staff on observability tools |
| **Team fragmentation**<br>• Teams using different tools<br>• Lack of collaboration | **Incorporate observability into all stages of the SDLC (including shift left):**<br>• Establish better DevOps best practices such as incident learning and SLOs<br>• Automate incident response workflows (operational efficiency)<br>• Employ predictive anomaly detection (insightful metrics)<br>• Automate incident response as much as possible<br>• Provision and orchestrate infrastructure using automation tooling<br>• Use CI/CD practices for software deployment<br>• Collaborate with other teams |
| **Purchasing, pricing, and billing concerns**<br>• Too expensive<br>• Lengthy sales cycle<br>• Lack of predictability | **Select the right observability platform and vendor. Top 10 aspects to look for:**<br>• Capabilities covered (now and in the future)<br>• Budget-friendly pricing<br>• Transparent pricing<br>• Single license metric across all telemetry<br>• Flexibility to scale usage based on consumption with no monthly minimum<br>• Ability to ingest any telemetry data type with no penalties<br>• Ability to autoscale without penalty<br>• Predictable spending<br>• Ability to pay as you go<br>• No premium overage fees |

**Table 13.** Challenges and solutions for attaining the ideal state of observability

# Outcomes to expect

Once organizations have attained this ideal state of observability, the data shows that they see many positive outcomes.

### Improved uptime, performance, and reliability

- Mitigates service disruptions and business risk
- Improves service-level metrics
- Improves customer experience

### Business and revenue growth

- Improves revenue retention by deepening understanding of customer behaviors
- Creates new revenue-generating use cases

### Happy developers and engineers

- Shifts developer and engineer time from incident response (reactive) towards higher-value work (proactive)
- Improves skillset/hireability
- Makes job easier
- Improves work/life balance
- Increases innovation

### Operational efficiency

- Includes telemetry data with business context to quantify the business impact of events and incidents
- Enables less guesswork when managing complicated and distributed tech stacks
- Increases productivity (developers and engineers find and resolve issues faster)
- Enables time prioritization
- Helps fill in the gaps, confirm assumptions, and overcome assumptions and opinions

### Cross-team collaboration

- Improves collaboration across teams when making decisions related to the software stack (DevOps, DevSecOps)
- Provides feedback for all SDLC stages

Learn About New Relic Platform

# Appendix

View meaningful trends by observability capability, market opportunity, industry, and region/country.

# Highlights for each capability

We mined a wealth of information about 17 observability capabilities, including what respondents had deployed at the time of the survey and what they expect to deploy over the next year and the next two to three years.

## AIOps

*Uses artificial intelligence to improve processes and gain insights.*

Only 37% of survey respondents had deployed AIOps. However, **40% expected to deploy it in the next year—which would make it the second-most deployed for next year**—and 15% expected to deploy it in two to three years. This means that while AIOps was one of the least deployed capabilities, 78% will deploy it by 2023, and **92% will deploy AIOps by 2025**. Only 5% did not expect to deploy AIOps.

## Alerts

*Provides notifications triggered by an important event, such as an error.*

More than half of survey respondents (52%) had deployed alerts, making it the **fourth-most deployed capability**. Plus 34% expected to deploy it in the next year, and 10% expected to deploy it in two to three years. This means 86% will deploy it by 2023, and **96% will deploy alerts by 2025**. Only 3% did not expect to deploy alerts.

## APM

*Monitors applications for performance and errors.*

Almost half of survey respondents (45%) had deployed APM, 37% expected to deploy it in the next year, and 12% expected to deploy it in two to three years. This means 82% will deploy it by 2023, and **94% will deploy APM by 2025**. Only 4% did not expect to deploy APM.

## Browser monitoring

*Tracks browser and web application activity and performance.*

Just under half of survey respondents (49%) had deployed browser monitoring, 34% expected to deploy it in the next year, and 13% expected to deploy it in two to three years. This means 82% will deploy it by 2023, and **95% will deploy browser monitoring by 2025**. Only 3% did not expect to deploy browser monitoring.

## Custom dashboards

*Provides an overview of important monitoring metrics.*

Nearly half of survey respondents (47%) had deployed custom dashboards, 35% expected to deploy them in the next year, and 13% expected to deploy them in two to three years. This means 82% will deploy them by 2023, and **95% will deploy custom dashboards by 2025**. Only 4% did not expect to deploy custom dashboards.

## Database monitoring

*Gathers essential performance metrics to measure and optimize database performance.*

Over half of survey respondents (54%) had deployed database monitoring, making it the **third-most deployed capability**. Plus 31% expected to deploy it in the next year, and 11% expected to deploy it in two to three years. This means 85% will deploy it by 2023, and **96% will deploy database monitoring by 2025**. Only 3% did not expect to deploy database monitoring.

## Distributed tracing

*Tracks and observes service requests as they flow through distributed systems.*

Only 36% of respondents had deployed distributed tracing, 39% expected to deploy it in the next year, and 15% expected to deploy it in two to three years. This means that while distributed tracing was one of the least deployed capabilities, 75% will deploy it by 2023, and **90% will deploy distributed tracing by 2025**. Only 6% did not expect to deploy distributed tracing.

## Error tracking

*Tracks and traces errors to troubleshoot issues.*

Nearly half of survey respondents (49%) had deployed error tracking, 34% expected to deploy it in the next year, and 13% expected to deploy it in two to three years. This means 82% will deploy it by 2023, and **95% will deploy error tracking by 2025**. Only 4% did not expect to deploy error tracking.

## Infrastructure monitoring

*Monitors network infrastructure like databases and servers.*

More than half of survey respondents (51%) had deployed infrastructure monitoring, making it the **fifth-most deployed capability**. Plus 33% expected to deploy it in the next year, and 11% expected to deploy it in two to three years. This means 84% will deploy it by 2023, and **95% will deploy infrastructure monitoring by 2025**. Only 3% did not expect to deploy database monitoring.

## Kubernetes monitoring

*Monitors Kubernetes deployments by providing visibility into clusters and workloads.*

Just 34% of respondents had deployed Kubernetes monitoring, 39% expected to deploy it in the next year, and 16% expected to deploy it in two to three years. This means that while Kubernetes monitoring was the least deployed capability, 72% will deploy it by 2023, and **88% will deploy Kubernetes monitoring by 2025**. Only 7% did not expect to deploy Kubernetes monitoring. These findings align with the fact that 36% were containerizing applications and workloads.

## Log management

*Stores and searches error and event logs.*

Half of survey respondents (50%) had deployed logs, making it the **sixth-most deployed capability**. Plus 34% expected to deploy it in the next year, and 12% expected to deploy it in two to three years. This means 84% will deploy it by 2023, and **96% will deploy logs by 2025**. Only 3% did not expect to deploy logs.

## ML model performance monitoring

*Monitors machine-learning-model performance.*

Only 34% of survey respondents had deployed ML model performance monitoring (MLOps), **42% expected to deploy it in the next year—more than any other capability**—and 15% expected to deploy it in two to three years. This means that while ML model performance monitoring was one of the least deployed capabilities, 76% will deploy it by 2023, and **91% will deploy ML model performance monitoring by 2025**. Only 5% did not expect to deploy ML model performance monitoring.

## Mobile monitoring

*Monitors mobile application and device performance.*

Less than half of survey respondents (43%) had deployed mobile monitoring, 35% expected to deploy it in the next year, and 15% expected to deploy it in two to three years. This means 79% will deploy it by 2023, and **94% will deploy mobile monitoring by 2025**. Only 4% did not expect to deploy mobile monitoring.

## Network monitoring

*Monitors network traffic and performance metrics.*

More than half of survey respondents (57%) had deployed network monitoring, making it the **most deployed capability**. Plus 30% expected to deploy it in the next year, and 11% expected to deploy it in two to three years. This means 86% will deploy it by 2023, and **97% will deploy network monitoring by 2025**. Only 2% did not expect to deploy network monitoring.

## Security monitoring

*Collects and analyzes vulnerability indicators of potential security threats*

More than half of survey respondents (56%) had deployed security monitoring, making it the **second-most deployed capability**. Plus 29% expected to deploy it in the next year, and 12% expected to deploy it in two to three years. This means 85% will deploy it by 2023, and **96% will deploy security monitoring by 2025**. Only 3% did not expect to deploy security monitoring.

## Serverless monitoring

*Monitors serverless application performance metrics and errors.*

Just 38% of survey respondents had deployed serverless monitoring, 37% expected to deploy it in the next year, and 16% expected to deploy it in two to three years. This means that while serverless monitoring was one of the least deployed capabilities, 75% will deploy it by 2023, and **91% will deploy serverless monitoring by 2025**. Only 6% did not expect to deploy serverless monitoring. These findings align with the fact that 36% of respondents were adopting serverless computing.

## Synthetic monitoring

*Monitors simulated usage to predict performance.*

Only 34% of survey respondents had deployed synthetic monitoring, **39% expected to deploy it in the next year— making it the third-most deployed for next year**—and 15% expected to deploy it in two to three years. This means that while synthetic monitoring was one of the least deployed capabilities, 74% will deploy it by 2023, and **89% will deploy synthetic monitoring by 2025**. Only 6% did not expect to deploy synthetic monitoring.

# Highlights for market opportunities

We also looked closely at 11 technologies that respondents most needed observability for over the next three years.

## ⧉ 5G

*Fifth-generation technology standard for broadband cellular networks*

A third of respondents foresaw their organizations needing observability for 5G the most in the next three years, making it the fourth choice overall. Practitioners were slightly more likely to select 5G (35% and fourth choice, compared to 30% and sixth choice for ITDMs). Those from small and large organizations were also more likely to select 5G (38% and third choice, compared to 30% and sixth choice for midsize organizations). It was the third choice for respondents in the healthcare/pharma (44%), education (40%), and IT/telco (36%) industries. Interestingly, of the 47% who selected AI, more than half (52%) also selected 5G as a top choice.

## ⧉ Artificial intelligence

*Simulation of human-intelligence processes by machines*

Nearly half of survey respondents (47%) indicated that they foresee their organizations needing observability for AI the most in the next three years, making it the number one choice overall. It was more than half for respondents surveyed in North America (52%), executives (51%), and those from several industries, including services/consulting (62%), energy/utilities (60%), government (58%), and IT/telco (51%). Interestingly, of the 47% who selected AI, more than half also selected 5G, blockchain, or IoT as a top choice.

## ⧉ Blockchain

*Technology based on decentralization, often associated with cryptocurrencies*

Almost a third of respondents (32%) foresaw their organizations needing observability for blockchain the most in the next three years, making it the fifth choice overall. Non-executive managers were the least likely to see the need for it (26%, compared to 36% for executives and 32% for practitioners), as were those surveyed in Europe (29%, compared to 35% for those surveyed in Asia Pacific and 34% for those surveyed in North America). Those more likely to foresee the need for it included respondents from the energy/utilities (40%) and IT/telco (35%) industries, where it was the fourth choice. Interestingly, of the 47% who selected AI, more than half (52%) also selected blockchain.

## ⧉ Business applications

*Apps important to running a business such as ERP and CRM*

More than a third of survey respondents (35%) indicated that they foresee needing observability for business apps the most in the next three years, making it the third choice overall. Only those from the industrials/materials/manufacturing industry selected business apps as their top choice (43%, tied with IoT), while it was the second choice for retail/consumer respondents (40%). Interestingly, of the 35% who selected business apps, 42% also selected indiscriminate personalization as a top choice.

## ⧉ Cloud gaming

*Playing video games hosted on remote servers in data centers, aka gaming on demand or gaming-as-a-service*

Less than a quarter of respondents (22%) foresaw their organizations needing observability for cloud gaming, making it the seventh choice overall. Respondents from the IT/telco industry were the most likely to foresee the need for it (27%). While cloud gaming often uses edge computing, we didn't see any strong correlation between the two as far as observability expectations in the next few years.

## ⧉ Edge computing

*Architecture that moves processes from the cloud to local locations like an IoT device*

Edge computing was the respondents' sixth choice (31%). In fact, 41% of those who selected IoT also selected edge computing. Respondents from the energy/utilities and services/consulting industries were more likely to select edge computing than those from other industries (42% and 45% respectively). Executives were also more likely to foresee needing observability for edge computing (38%, compared to 31% for non-executive managers and 29% for practitioners).

## Indiscriminate personalization

*Personalized, real-time digital experience*

About one out of five respondents (22%) foresaw needing observability for indiscriminate personalization the most, making it the eighth choice overall. Those surveyed in Asia Pacific were more likely to foresee the need for it (26%, compared to 19% for those surveyed in Europe and 22% for those surveyed in North America), as were those from the education and retail/consumer industries (34% and 26% respectively). While the least likely were those from small organizations (18%, compared to 21% for midsize and 24% for large) and those from the services/consulting (17%), healthcare/pharma (13%), and nonprofit/unspecified (11%) industries. Interestingly, of the 35% who selected business apps, 42% also selected indiscriminate personalization as a top choice.

## Internet of Things

*System of devices connected over the internet or other networks*

IoT was the respondents' overall second choice for a technology that they foresee their organizations needing observability for the most in the next three years (44%). However, IoT was the top choice for respondents in several industries, including energy/utilities (61%), education (51%), healthcare/pharma (47%), industrials/materials/manufacturing (43%), and financial/insurance (42%). Large organizations were also more likely to select IoT (48%, compared to 39% for small and 43% for midsize organizations). Interestingly, of the 47% who selected AI, more than half (52%) also selected IoT as a top choice.

## Metaverse

*Simulating aspects of life virtually with AI, IoT, edge computing, blockchain, Web3, virtual reality (VR), and/or augmented reality (AR)*

The metaverse was the least popular choice. Only 19% of respondents foresaw needing observability for it in the next three years. It was a slightly more popular choice for those surveyed in Asia Pacific (22%, compared to 18% for those surveyed in Europe and 17% for those surveyed in North America), those from small organizations (22%, compared to 18% for midsize and large organizations), and those from the energy/utilities (31%), healthcare/pharma (23%), and services/consulting (21%) industries. Interestingly, of the 33% who selected 5G, 39% also selected metaverse as a top choice. And of the 32% who selected blockchain, 38% also selected metaverse as a top choice.

## Super apps

*Digital platforms that leverage one or more core business assets across multiple use cases*

Only 20% of respondents foresaw needing observability for super apps in the next three years. Super apps tend to be more applicable for larger organizations with multiple lines of business in predominantly mobile-first countries (Japan and the United States are the only countries that are browser-first). They are especially popular in Asia Pacific, Latin America, Eastern Europe, Africa, and the Middle East. So, fewer organizations use super apps but, for those that do, they are all-encompassing, massive projects for which observability becomes supercritical.

## Web3

*Based on blockchain technology, an approach billed as the third generation of the internet*

About one in five (19%) foresaw needing observability the most for Web3 in the next three years, making it the second least popular choice overall. It came in dead last for those surveyed in Asia Pacific (17%) but was slightly more popular with Europeans (21%). Respondents from the energy/utilities industry were more likely to foresee the need for it (25%), and government and nonprofit/unspecified respondents were the least likely (15% and 14% respectively). While Web3 uses blockchain technology, we don't see any strong correlation between the two as far as observability expectations.

# Industry highlights

We found some interesting differences comparing data from each of the 10 industries represented in the survey.

## ⊕ Education

Respondents from the education industry were the **most likely** to:

- Say they use observability to optimize cloud resource usage and spend (63%) and support digital transformation efforts (47%)
- Care about predictable spending (54%)
- Foresee their organizations most needing observability for IoT in the next three years (51%)
- Say automated incident response workflows would most help to reduce MTTR (49%)
- Indicate that an improved customer experience is a top benefit of observability (47%)
- Prefer a hybrid of user- and data-ingestion-based pricing (40%)
- Use a single tool for observability (9%)

They were **more likely** to:

- Cite lack of budget (51%) and too expensive (31%) as the top barriers to prioritizing/ achieving full-stack observability
- Say that observability helps improve the lives of engineers/developers the most by enabling less guesswork (43%), making jobs easier (40%), confirming assumptions (37%), and improving skill set/hireability (37%)
- Take less than 30 minutes to detect and resolve low- and medium-business-impact outages

They were **less likely** to use extensive or full observability in all stages of the SDLC.

## ⊿ Energy/utilities

Respondents from the energy/utilities industry were the **most likely** to:

- Say that migration to a multi-cloud environment is their top observability driver (60%)
- Foresee their organizations most needing observability for AI in the next three years (60%)
- Note that developer confidence in the resilience of their apps/systems is a primary benefit of observability (51%)
- Care about the ability to autoscale with no penalties (42%)
- Say that not having enough of their systems instrumented is a barrier to prioritizing/ achieving full-stack observability (38%)
- View observability as more for incident response/insurance (33%)
- Claim they have all 17 capabilities deployed (10%)
- Have a mature observability practice based on our definition (10%)

They were **more likely** to:

- Say they have unified telemetry data (54%)
- Say automated incident response workflows and better DevOps practices would most help to reduce MTTR (both 44%)
- Indicate that their organizations allocate more than 10% but less than 15% of their IT budgets for observability tools (43%)
- Say that observability helps improve the lives of engineers/developers by enabling less guesswork and improving work/life balance (42% for both)
- Foresee their organizations most needing observability for edge computing (42%) and metaverse (31%) in the next three years
- Experience outages once per week or more
- Take less than 30 minutes to detect low- and medium-business-impact outages and more than 30 minutes to detect high-business-impact outages

They were the **least likely** to select budget-friendly pricing as the most important pricing feature for their observability tools/platform (27%).

## 💰 Financial/insurance

Respondents from the financial/insurance industry were the **most likely** to:

- Prefer a single, consolidated platform (60%)
- Select a lack of understanding of benefits as the top barrier to prioritizing/achieving full-stack observability (28%)
- Use extensive or full observability in all stages of the SDLC, including 83% in the operate stage

They were **more likely** to:

- View observability as more of a key enabler for achieving core business goals (54%)
- Foresee their organizations most needing observability for IoT in the next three years (42%)
- Prefer usage-based billing and the ability to ingest any telemetry data type with no penalties as the most important pricing features for their observability tools/ platform (both 31%)
- Favor user-based pricing, especially the hybrid version (29%), as the most important pricing feature for their observability tools/platform
- Learn about software and system interruptions with one observability platform (24%)
- Experience outages once per week or more

They were the **least likely** to have achieved full-stack observability based on our definition (17%).

## 🏛 Government

Respondents from the government were the **most likely** to:

- Note a reduction in employee count (55%) and consolidation of IT tooling (40%) as primary benefits of observability
- Use observability to troubleshoot distributed systems (50%)
- Have achieved full-stack observability based on our definition (42%)
- Select more staff as their top choice for how best to reduce MTTR (41%)

They were **more likely** to:

- Say that development of cloud-native application architectures drives the need for observability (58%)
- Care about predictable spending (50%)
- Say observability most helps improve the lives of engineers/developers by enabling less guesswork when managing complicated and distributed tech stacks (42%)
- Deem budget-friendly pricing, transparent pricing, and hybrid pricing models as the most important pricing features for their observability tools/platforms (all 39%)
- Cite too expensive (35%) and lack of budget (31%) as the top barriers to prioritizing/ achieving full-stack observability
- Experience medium- and high-business-impact outages two to three times per month or fewer

They were the **least likely** to:

- Use extensive or full observability in all stages of the SDLC
- Use observability to support an organizational IT move to DevOps, support cost-cutting efforts (consolidating tools), and increase speed to market for new products/ services (all 15%)

## ⊕ Healthcare/pharmaceutical

Respondents from the healthcare/pharma industry were the **most likely** to:

- Cite the adoption of serverless computing as their top observability driver (49%)
- Note an improved customer experience as the top benefit (43%) and business/revenue growth (39%) as one of the top benefits of observability
- Say that the most important characteristic of a mature observability practice is mitigating service disruptions and business risks (33%)

They were **more likely** to:

- Say they have unified telemetry data (54%)
- Note budget-friendly pricing as the most important pricing feature for their observability/tools platform (47%)
- Foresee their organization needing observability for IoT in the next three years (47%)
- Say observability helps improve the lives of developers/engineers the most by enabling cross-team collaboration (42%)
- Indicate that staff training for observability tools is the best way to reduce MTTR (40%)
- Cite lack of budget and not having enough of their systems instrumented as top barriers to prioritizing/achieving full-stack observability (both 31%)
- Have a mature observability practice based on our definition (7%)
- Experience outages once per week or more

## 🚚 Industrials/materials/manufacturing

Respondents from the industrials/materials/manufacturing industry were the **most likely** to:

- Foresee their organizations most needing observability for business apps such as ERP and CRM in the next three years (43%, tied with IoT)
- Use observability to support an organizational IT move to DevOps (35%)
- Say that improved collaboration across teams to make decisions related to the software stack is the most important characteristic of a mature observability practice (34%)
- Cite a lengthy sales cycle as the top barrier to prioritizing/achieving full-stack observability (27%)

They were **more likely** to:

- Prefer a single, consolidated platform (54%)
- Select better DevOps practices as their top choice for how best to reduce MTTR (42%)
- Select transparent pricing as the most important pricing feature for their observability tools/platform (36%)
- Allocate more than 10% but less than 15% of their IT budgets for observability tools (30%)
- Say they have already prioritized/achieved full-stack observability (5%)
- Take less than 30 minutes to detect low-business-impact outages and more than 30 minutes to detect and resolve high-business-impact outages

## 🖥 IT/telecommunications

Respondents from the IT/telco industry were the **most likely** to note the ability to redirect resources to value-added tasks and/or accelerated innovation as a primary benefit of observability (35%).

They were **more likely** to:

- View observability as more of a key enabler for achieving core business goals (52%)
- Say they have unified telemetry data (52%)
- Say their software deployment uses CI/CD practices (52%)
- Select better DevOps practices as their top choice for how best to reduce MTTR (41%)
- Prefer usage-based billing (35%)
- Think that their IT performance is adequate (34%)
- Learn about software and system interruptions with one observability platform (24%)
- Experience outages once per week or more

## 📦 Nonprofit/unspecified

Respondents from the nonprofit/unspecified industry were the **most likely** to:

- Select budget-friendly pricing as the most important pricing feature for their observability tools/platform (54%)
- Note an increased operational efficiency as a primary benefit of observability (52%)
- Say that the ability to query data on the fly is the most important characteristic of a mature observability practice (39%)
- Select the ability to pay as they go as the most important billing feature for their observability tools/platform (39%)
- Say the visualization/dashboarding of their telemetry data is disparate (36%)

They were **more likely** to:

- Say that migration to a multi-cloud environment is their top driver for observability (43%)
- Say observability helps improve the lives of developers/engineers the most by enabling cross-team collaboration (43%)
- Indicate that staff training for observability tools is the best way to reduce MTTR (39%)
- Cite too expensive as the top barrier to prioritizing/achieving full-stack observability (39%)
- Select transparent pricing as one of the most important pricing features for their observability tools/platform (39%)
- Experience outages two to three times per month or fewer
- Take less than 30 minutes to detect low- and high-business-impact outages

## 🛍 Retail/consumer

Respondents from the retail/consumer industry were the **most likely** to:

- Say they have unified telemetry data (60%) and that the visualization/dashboarding of that data is unified (79%)
- View observability as more of a key enabler for achieving core business goals (57%)
- Say that the most important characteristic of a mature observability practice is improved collaboration across teams to make decisions related to the software stack (31%)
- Use extensive or full observability in all stages of the SDLC, including 83% in the operate stage
- Use 10 or more tools for observability (7%)

They were **more likely** to:

- Say automated incident response workflows and better DevOps practices would most help to reduce MTTR (both 42%)
- Expect to most need observability for business apps such as ERP and CRM in the next three years (40%)
- Say that they don't understand the benefits of observability (34%)
- Have a mature observability practice based on our definition (6%)
- Prefer usage-based billing
- Take less than 30 minutes to detect outages

## 👤💬 Services/consulting

Respondents from the services/consulting industry were the **most likely** to:

- Say their software deployment uses CI/CD practices (57%)
- Note improved uptime and reliability as a primary benefit of observability (49%)
- Say their telemetry data is siloed (45%)
- Use observability to automate software release cycles (40%)
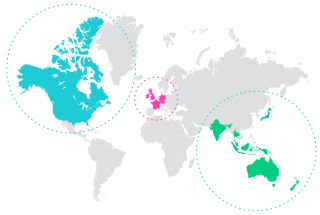- Say they have already prioritized/achieved full-stack observability (6%)

They were **more likely** to:

- Foresee their organizations most needing observability for edge computing (45%) and business apps such as ERP and CRM (40%) in the next three years
- Say staff training for observability tools is the best way to reduce MTTR (43%)
- Select transparent pricing as one of the most important pricing features for their observability tools/platform (43%)
- Say observability helps improve the lives of developers/engineers the most by enabling cross-team collaboration (43%)
- Cite too expensive (34%) and lack of budget (30%) as their top barriers to prioritizing/achieving full-stack observability
- Experience medium- and high-business-impact outages two to three times per month or fewer
- Take more than 30 minutes to resolve outages

They were the **least likely** to use observability to optimize cloud resource usage and spend (17%).

# Regional highlights

Here we take a closer look at the differences in survey responses by region.

| | Asia Pacific | Europe | North America |
|---|---|---|---|
| **Current deployment** | Most capabilities deployed and most likely to have achieved full-stack observability and use extensive or full observability in the plan and build stages of the SDLC | Least capabilities deployed and least likely to have achieved full-stack observability, to have a mature observability practice, and to use extensive or full observability in all stages of the SDLC | Most likely to have a mature observability practice and use extensive or full observability in the deploy and operate stages of the SDLC |
| **Telemetry data** | Most likely to have siloed data (including 15% entirely siloed) and multiple visualization solutions without cross-communication (including 11% entirely disparate) | More likely to have unified telemetry data and telemetry data visualized in a single dashboarding solution | Most likely to have unified telemetry data and telemetry data visualized in a single dashboarding solution |
| **Strategy** | Most likely to view observability as more of a key enabler for achieving core business goals | Most likely to view observability as more for incident response/insurance | More likely to view observability as more of a key enabler for achieving core business goals |
| **Budget allocation** | Most likely to allocate 15% or more of IT budgets for observability tools and more likely to say they expect to increase their budgets in the next year | Most likely to allocate less than 10% of IT budgets for observability tools and least likely to say they expect increase their budgets in the next year | More likely to allocate less than 10% of IT budgets for observability tools and most likely to say they expect to increase their budgets in the next year |
| **Service-level metrics** | Most likely to experience outages multiple times per day and more likely to take more than 60 minutes to detect outages | Most likely to experience outages once per week or more and most likely to resolve outages in less than 30 minutes | Least frequent outages and most likely to detect outages in less than 30 minutes |
| **Top observability benefits** | Proactive detection of issues before they impact customers and increases developer/engineer productivity | Increased operational efficiency and makes developer/engineer jobs easier | Improved uptime and reliability and enables cross-team collaboration (DevOps, DevSecOps) |
| **Top observability use cases** | Support digital transformation efforts | Optimize cloud resource usage and spend | Support an organizational IT move to DevOps and optimize cloud resource usage and spend (tie) |
| **Top challenges for prioritizing/achieving full-stack observability** | Too many monitoring tools and not enough systems are instrumented (tie) | Lack of budget | Lack of understanding of benefits |

**Table 14.** Key differences in survey responses by region

# Asia Pacific

Asia Pacific is home to a diversity of cultures and business practices. However, there are still some interesting comparisons to make between Asia Pacific and other regions. For example, as a whole, the survey found that respondents surveyed in Asia Pacific had the most observability capabilities deployed compared to respondents surveyed in Europe and North America. Asia Pacific organizations were the most likely to have achieved full-stack observability by our definition (33%). Additionally, they were the most likely to view observability as more of a key enabler for achieving core business goals (58%).

**Moving to a consolidated platform**
Compared to other regions, they were the most likely to prefer a single, consolidated platform (55.3%), but their top barriers to prioritizing/achieving full-stack observability were too many monitoring tools and not enough of their systems being instrumented (both 28%). They were also the least likely to experience consolidation of IT tooling (25%) and the most likely to have siloed data (45%, including 15% entirely siloed) and multiple visualization solutions without cross-communication (33%, including 11% entirely disparate). In sum, respondents surveyed in Asia Pacific wanted a single consolidated platform but also lacked system instrumentation to get to full-stack observability.

**Proactive detection and better DevOps practices**
They were the most likely to say they experience proactive detection of issues before they impact customers (40%). However, they were also the most likely to experience outages multiple times per day and more likely to take more than 60 minutes to detect outages. They were the most likely to select better DevOps practices as a way to reduce MTTR (42%).

**Deploying more observability capabilities**
Looking forward, most (91%) expected to deploy additional observability capabilities over the next year, including 62% who expected to deploy five or more additional capabilities. Of these, ML model performance monitoring was the most popular capability for future deployment at 43%, followed by APM at 39%, Kubernetes and synthetic monitoring at 38%, and AIOps and distributed tracing at 37%. Only 10% did not expect to deploy additional capabilities. About half (51%) said that they expect to increase their budgets over the next year to match their future deployment plans.

**Highlights by country**
When we look at the results for each country, the diversity of the Asia Pacific region becomes apparent in the different ways they are leveraging observability adoption:

**Australia** 🇦🇺 and **New Zealand** 🇳🇿 were focused on tool consolidation and cost-cutting

**India** 🇮🇳 and **Indonesia** 🇮🇩 looked to observability to support the IT move to DevOps

**Japan** 🇯🇵 indicated a focus on using observability to support the move to serverless and containerization

**Malaysia** 🇲🇾 technology teams were still grappling with digital transformation and distributed systems

**Singapore** 🇸🇬 organizations were applying observability to automate their software release cycles

**Thailand** 🇹🇭 had a focus on connecting IoT device monitoring into the full observability estate, optimizing cloud-resource usage and spend, and supporting digital transformation efforts

n=400
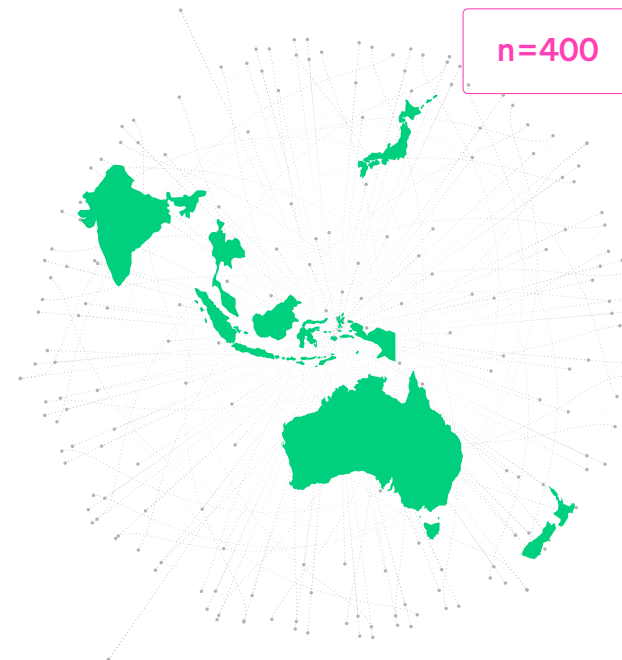
# Asia Pacific

## Association of Southeast Asian Nations

Across the Association of Southeast Asian Nations (ASEAN), which includes Indonesia, Malaysia, Singapore, and Thailand, survey respondents used observability predominately as an integral tool to support digital transformation initiatives, improve the digital customer experience, and support future plans to roll out AI and IoT.

**Indonesia** 🇮🇩 : DevOps, IoT, and risk mitigation were high priorities

**Malaysia** 🇲🇾 : Security, risk, and compliance were key factors in driving observability strategies

**Singapore** 🇸🇬 : Applying observability to automate software release cycles was key

**Thailand** 🇹🇭 : AI, IoT, and the development of cloud-native application architectures were high priorities

### Digital transformation and customer experience

Respondents surveyed across ASEAN have used observability primarily to support digital transformation initiatives and improve the digital customer experience. Across ASEAN, 43% of respondents said they apply observability to support digital transformation efforts to improve and gain a competitive advantage from the digital customer experience.

More than a third (34%) said that they apply observability to automate software release cycles, increase speed to market for new products/services, and optimize cloud resource usage and spend.

### Education and AI opportunities

The data shows an opportunity to educate technology teams about the potential power of observability and the importance of a clear observability strategy. Almost a third (32%) of respondents surveyed across ASEAN cited a lack of strategy as the primary challenge to prioritizing/achieving full-stack observability.

Only 26% said that they apply observability to deliver against SLOs and SLAs.

In the next three years, they expect to make AI a primary focus, with more than half (51%) foreseeing the need for observability for AI.

### Tool fragmentation

Tool sprawl creates a patchwork problem for technology teams.

Half of respondents surveyed across ASEAN said they learn about software and system interruptions through multiple monitoring tools, while 39% said they still learn primarily through manual checks/tests, incident tickets, and complaints.

Only 11% said they primarily learn about interruptions through one observability platform.

### Future observability plans

Respondents surveyed across ASEAN were the most likely to say they expect to deploy synthetic monitoring and ML model performance monitoring over the next year (41%), followed by APM (37%), Kubernetes monitoring (36%), AIOps (33%), and serverless monitoring (32%).

The majority predicted they'll have most observability capabilities (90–99%) deployed by 2025. However, only 39% said they'll increase their budgets over the next year to match their deployment plans—the lowest across the Asia Pacific region—while 27% said they would keep them the same, and 34% said they would decrease them.

## 26%
applied observability to deliver against SLOs and SLAs

# Asia Pacific

## Australia and New Zealand

Across Australia and New Zealand (ANZ), the key driving factors cited for using observability were cost-cutting and tool consolidation. Almost a third (28%) of ANZ respondents cited a lack of budget as a primary challenge to achieving full-stack observability. The results also show respondents surveyed in New Zealand used observability to support an organizational move to DevOps, while respondents surveyed in Australia expected to use observability for AI within the next three years.

### Tool consolidation

A third of respondents surveyed in Australia and more than a quarter (28%) of respondents surveyed in New Zealand said they use observability to support cost-cutting efforts (consolidating tools).

More than half (57%) of respondents surveyed in Australia used six or seven tools for observability. Notably, none used just one tool.

More than half (52%) of respondents surveyed in Australia indicated they primarily learn about software and system interruptions through multiple monitoring tools, compared to only 21% through one observability platform. And 27% indicated they still primarily learn through manual checks/ tests or through incident tickets and complaints.

Almost a quarter of respondents surveyed in ANZ indicated that too many monitoring tools (24%) and siloed data (23%) are primary challenges preventing them from prioritizing/achieving full-stack observability.

### DevOps, AI, and C-suite advocacy

New Zealand is trying to get to a state of DevOps but in Australia, this isn't really the case. Close to half (44%) of respondents surveyed in New Zealand indicated they apply observability to support an organizational IT move to DevOps, compared to only 22% of respondents surveyed in Australia.

Almost half (49%) of respondents surveyed in Australia foresaw their organizations needing observability for AI in the next three years, compared to 35% of respondents surveyed in New Zealand.

C-suite advocacy for observability was high. Most respondents surveyed in ANZ indicated that C-suite executives advocate for observability, including 83% for less technical-focused and 75% for more technical-focused C-suite executives.

### Lack of budget and dedicated personnel

The biggest challenges to prioritizing/achieving full-stack observability centered around low performance levels and a lack of budget or personnel.

Only 30% of respondents surveyed in Australia said their IT performance is adequate (no need to improve current performance).

More than a third (35%) of respondents surveyed in New Zealand cited a lack of budget as a primary challenge to prioritizing/achieving full-stack observability.

Almost a third (29%) of respondents surveyed in ANZ cited a lack of dedicated personnel as a primary challenge to prioritizing/achieving full-stack observability.

### Future observability plans

Respondents surveyed in ANZ were the most likely to say that they expect to deploy APM and ML model performance monitoring over the next year (45%), followed by synthetic monitoring (39%), serverless monitoring and custom dashboards (both 37%), and distributed tracing (36%).

The majority of respondents surveyed in ANZ predicted they will have almost all observability capabilities (86– 99%) deployed by 2025. Accordingly, nearly half (47%) said they expect to increase their budgets over the next year to match their future deployment plans, while 21% said they expect to keep them the same, and 31% said they expect to decrease them.

# 29%

lacked the dedicated personnel to prioritize/ achieve full-stack observability
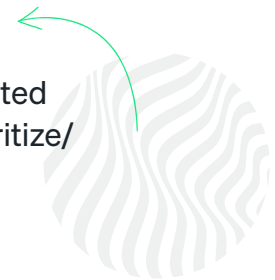
# Asia Pacific

## India

Despite having a strong emphasis on the customer experience, respondents surveyed in India considered IT performance a challenge with only 35% who said their IT performance is adequate. In addition, almost half (48%) said they primarily learn about outages through multiple monitoring tools, and almost a third (31%) said they primarily learn about software and system interruptions through manual checks/tests or incident tickets and complaints.

### Subpar IT performance
IT performance has room for improvement.

Only 35% of respondents surveyed in India said their IT performance is adequate (no need to improve current performance).

Almost half (48%) said they primarily learn about software and system interruptions through multiple monitoring tools, while 31% said they still learn primarily through manual checks/tests or through incident tickets and complaints. Only 21% said they primarily learn about these interruptions through one observability platform.

### Developer confidence
Developer confidence and risk mitigation drove the need for observability.

More than half (56%) of respondents surveyed in India said an increased focus on security, governance, risk, and compliance represents a key strategy driving the need for observability.

And more than half (51%) said developer confidence in the resiliency of their apps/system is the primary benefit of their observability deployment, followed by proactive detection of issues before they impact customers (44%).

### DevOps and AI
DevOps and AI are on the radar.

Close to half (44%) of respondents surveyed in India indicated that they apply observability to support an organizational IT move to DevOps.

And 54% foresaw their organizations needing observability for AI in the next three years. While 53% predicted their organizations will need observability for IoT in the next three years.

### Future observability plans
Respondents surveyed in India were the most likely to say they expect to deploy Kubernetes monitoring and ML model performance monitoring over the next year (44% each), followed by distributed tracing (42%), AIOps (40%), synthetic monitoring (38%), and mobile monitoring (35%).

The majority predicted they will have most observability capabilities (83–97%) deployed by 2025. They also budgeted notably more than any other country across the Asia Pacific region, with 70% who said they expect to increase their observability budgets over the next year, 13% who said they expect to keep them the same, and 17% who said they expect to decrease them.

# 31%
still learned about interruptions primarily through manual checks/tests or incident tickets and complaints
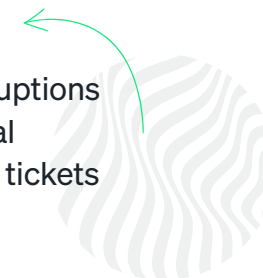
# Asia Pacific

## Japan

More than any other country in the Asia Pacific region, respondents surveyed in Japan experienced significant tool sprawl. Three-quarters routinely used between five and eight tools as part of their observability strategy, despite more than half (52%) who said they prefer to use a single, consolidated platform. But at the same time, they had the fewest capabilities deployed in the Asia Pacific region. Almost a third (30%) said they use observability to manage containerization and serverless environments, making them the only ones in Asia Pacific to list it as the most common use case for observability.

**Containerization and serverless**
Containerization and serverless were key priorities for respondents surveyed in Japan.

Almost a third (30%) indicated the most common use case for applying observability is to manage containerization and serverless environments.

The second most common use case was to minimize the risk of migrating core legacy applications to the cloud (27%).

The primary benefits enabled by observability deployments were the increased velocity of software delivery to market (36%), closely followed by improved customer experience (34%) and proactive detection of issues before they impact customers (32%).

**Low observability benefit awareness**
There's an opportunity to educate Japanese organizations about the power of observability.

Almost a quarter (24%) of respondents surveyed in Japan listed a lack of understanding of benefits with the belief that their IT performance is adequate as the primary challenges preventing their organizations from prioritizing/achieving full-stack observability.

This finding suggests an opportunity to educate the Japanese market on the value and power of full-stack observability.

**Tool fragmentation**
Tool sprawl was significant despite the preference for a single, consolidated platform.

Three-quarters of respondents surveyed in Japan said they use between five and eight tools as part of their observability strategy, even though 52% said they prefer to use a single, consolidated platform.

**Future observability plans**
Respondents surveyed in Japan were the most likely to say that they expect to deploy APM over the next year (50%), followed by ML model performance monitoring and network monitoring (42% each), and log management and custom dashboards (41% each).

The majority predicted they'll have most observability capabilities (89–95%) deployed by 2025. When it comes to budgets, 47% said they expect to increase their observability budgets over the next year, 16% said they expect to keep them the same, and 38% said they expect to decrease them.

# 75%

used 5–8 monitoring tools as a part of their observability strategy
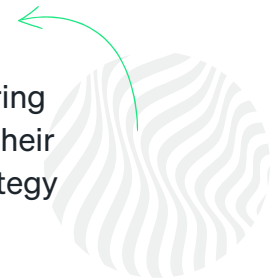
# Europe

New data and software regulations are being introduced in Europe, such as the General Data Protection Regulation (GDPR) and the Payment Services Directive (PSD2). So, it's no surprise that respondents from all four of the European countries represented in the survey—France, Germany, Ireland, and the United Kingdom—indicated that security, governance, risk, and compliance are top drivers for observability. While respondents surveyed in Europe reported less mature observability practices compared to other regions, they expected to increase their observability budgets over the next year and deploy more capabilities over the next three years.

**Moving toward full-stack observability—slowly**
Compared to other regions surveyed, they had the least capabilities deployed and were least likely to have achieved full-stack observability by our definition (21%), have a mature observability practice by our definition (4%), and use extensive or full observability in all stages of the SDLC. They were also slightly less likely to say they had already prioritized/achieved observability (2%). They were more likely to have unified telemetry data (51%) and telemetry data visualized in a single dashboarding solution (67%), and slightly less likely to say that not enough of their systems are instrumented (22%).

**Focused on incident response**
While they were the most likely to experience outages once per week or more, they detected and resolved them fairly quickly. In fact, they were the most likely to resolve outages in less than 30 minutes. They were also

the least likely to say they experience improved uptime and reliability (32%) and proactive detection of issues before they impact customers (28%) as a result of their observability deployments. However, they were the most likely to view observability as more for incident response/insurance (52%).

**Ambitious deployment plans, but will the budgets match?**
They allocated a smaller percentage of their IT budgets for observability tools than those in other regions (most likely to allocate less than 10%) and were the least likely to say they expect to increase their budgets in the next year (45%), despite ambitious deployment expectations. They were slightly more likely to cite a lack of budget (29%) as a challenge to prioritizing/achieving full-stack observability.

**Highlights by country**
Here's a snapshot of the key observability takeaways from each European country represented in the survey:

**France** 🇫🇷 focused on ramping up observability based on security, open-source, multi-cloud, and IoT needs

**Germany** 🇩🇪 applied observability to optimize cloud resource usage and spend as well as to support digital transformation efforts

**Ireland** 🇮🇪 and the **United Kingdom** 🇬🇧 had a high number of observability capabilities deployed, but struggled with high costs and lack of budget

**n=706**
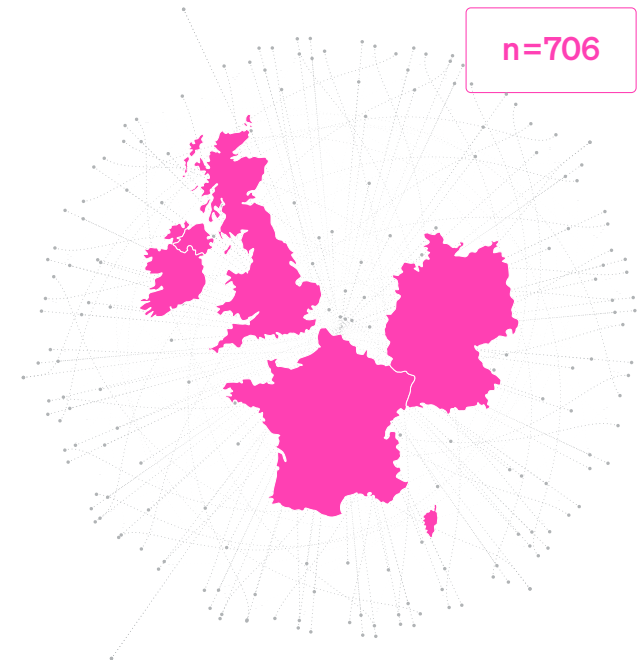
# Europe

🇫🇷  France

Overall results show respondents surveyed in France experienced many observability benefits, including improved uptime and reliability (37%) and customer experience (35%), developer confidence that apps/systems are resilient (32%), and increased operational efficiency (31%). More than 30% noted observability helps improve the lives of developers and engineers by overcoming opinions, enabling cross-team collaboration, and improving work/life balance. About three-quarters (74%) thought observability is a key enabler to achieving core business goals. There was low resistance to observability (15% or less), with the less technical-focused C-suite executives cited as the most likely to strongly advocate for observability (34%).

**Frequent outages and slow MTTD and MTTR**
Respondents surveyed in France reported frequent outages—up to 78% once per week or more and up to 29% once per day or more. When it came to detecting and resolving those outages, up to 62% had an MTTD of more than 30 minutes, while up to 66% had an MTTR of more than 30 minutes. Despite these findings, 31% thought their IT performance is adequate.

However, those with full-stack observability (by our definition) and those who said their organizations had already prioritized/achieved observability had notably fewer outages and a faster MTTD and MTTR. In fact, 52% indicated observability is for incident response/insurance. And 31% said observability mitigates service disruptions and business risk (top choice for the most important characteristic of a mature observability practice).

**Tool fragmentation**
Most (95%) respondents surveyed in France said they use multiple tools for their observability needs (79% used four to eight tools). Just 2% said they use only one tool, despite 43% who said they prefer to use a single, consolidated observability platform.

In addition, 48% said their IT teams primarily learn about interruptions through multiple monitoring tools. More than a quarter thought the consolidation of IT tooling is a primary benefit of observability (29%) and too many monitoring tools prevent them from prioritizing/achieving full-stack observability (26%).

This tool fragmentation may have contributed to the frequent outages they reported and the time it took to detect and resolve those outages.

**Full tech stack not being monitored/observed**
Almost two-thirds (64%) of respondents surveyed in France had four to eight capabilities deployed. Compared to those from most other countries included in the survey, they were less likely to say they had deployed alerts, database monitoring, infrastructure monitoring, log management, security monitoring, and synthetic monitoring.

Only 2% said they had already prioritized/achieved full-stack observability, and 18% had achieved full-stack observability based on our definition. Just 3% had a mature observability practice based on our definition.

**Future observability plans and trends**
To help support future deployment plans, 69% expected to increase or maintain their observability budgets next year.

The top priority driving the need for observability was an increased focus on security, governance, risk, and compliance (44%), followed closely by the adoption of open-source technologies and migration to a multi-cloud environment (both 43%). Compared to other countries in Europe, only respondents surveyed in France selected open-source technologies as one of the top three priorities driving the need for observability.

They were also one of the only respondents to select connecting IoT device monitoring into the full observability of estate (33%) as the top use case for observability. In addition, 43% foresaw their organizations needing observability the most for IoT in the next three years.

# 43%

foresaw their organizations most needing observability for IoT in the next three years
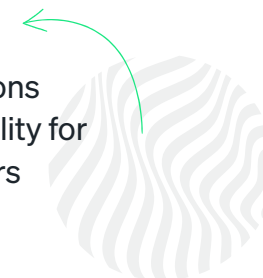
# Europe

### 🇩🇪 Germany

Respondents surveyed in Germany experienced frequent outages, slow MTTD and MTTR, and data and tool fragmentation, but they also clearly experienced the business benefits of observability and had a high level of advocacy for it, especially among the less technical-focused C-suite executives. While only 20% had achieved full-stack observability by our definition and just 3% said they had prioritized/achieved full-stack observability, they expected to deploy most capabilities by 2025.

**Frequent outages and slow MTTD and MTTR**
Respondents surveyed in Germany experienced more frequent outages than those from any other European country surveyed—up to 82% once per week or more and up to 33% once per day or more.

When it came to detecting and resolving those outages, up to 50% had an MTTD of more than 30 minutes, while up to 51% had an MTTR of more than 30 minutes.

Despite these findings, 23% thought their IT performance is adequate.

However, those with full-stack observability (by our definition) and those who said their organizations had already prioritized/achieved observability had fewer outages and a faster MTTD and MTTR.

In fact, 51% indicated observability is for incident response/insurance, and 31% said observability mitigates service disruptions and business risks.

**Data and tool fragmentation**
More than a quarter of respondents surveyed in Germany said their organizations' telemetry data is more siloed and that a disparate tech stack and siloed data prevent prioritizing/achieving full-stack observability.

Tool sprawl was also common. Three-quarters said they use five or more tools for their observability needs. Only 2% said they use one observability tool, despite 42% who said they prefer to use a single, consolidated platform and 29% who said consolidation of IT tooling is a primary benefit of observability.

Two in five said their IT teams primarily learn about software and system interruptions with multiple monitoring tools. Only 21% said they primarily learn about interruptions with one observability platform. And more than a quarter thought the consolidation of IT tooling is a primary benefit of observability (29%) and too many monitoring tools prevent them from prioritizing/achieving full-stack observability (27%).

**Business benefits**
More than 30% of respondents surveyed in Germany said they apply observability to optimize cloud resource usage and spend as well as to support digital transformation efforts.

And more than 30% reported increased operational efficiency and improved uptime and reliability. In fact, 79% said that observability is a key enabler to achieve core business goals. Almost a third (31%) said observability helps make developer/engineer jobs easier.

Advocacy for observability was high for all groups. Notably, 45% said the less technical-focused C-suite executives strongly advocate for observability—more than any other group.

**Future observability plans**
More than 40% of respondents surveyed in Germany said the strategies and trends driving the need for observability included an increased focus on security, governance, risk, and compliance as well as customer experience management, migration to a multi-cloud environment, development of cloud-native application architectures, and the prioritization of faster software release cycles.

Most (85%) expected to deploy five or more additional capabilities in the next year, and 42% expected to increase their observability budgets next year to support their observability plans.

Over the next three years, they foresaw needing observability the most for emerging technologies like IoT (41%), AI (40%), 5G (32%), and blockchain (27%).

# 31%
said observability helps make developer/engineer jobs easier

# Europe

### Ireland and the United Kingdom

Most respondents surveyed in Ireland and the United Kingdom (84%) had five or more observability capabilities deployed. Half said observability led to improved collaboration across teams to make decisions related to the software stack, 42% said it increases productivity for developers and engineers, and 35% said it increased operational efficiency.

Despite these compelling benefits, only 27% had achieved full-stack observability by our definition, and just 2% said they had already prioritized/achieved full-stack observability. However, they predicted that they will have most of the 17 capabilities deployed by 2025.

**Tool and data fragmentation**
Just 2% of respondents surveyed in Ireland and the United Kingdom said they use one tool for their observability needs, despite 49% who said they prefer a single, consolidated platform. While two-thirds said they use five or more tools. In addition, 38% said their organizations' telemetry data is siloed, including 12% who said it was entirely siloed, and another 17% said it is roughly equally siloed and unified. And 29% said the visualization/dashboarding of that telemetry data is disparate.

Almost a third (30%) cited the consolidation of IT tooling as a primary benefit of observability, while 22% cited a disparate tech stack, and 20% cited too many monitoring tools and siloed data as primary challenges to prioritizing/achieving full-stack observability.

**Room to improve service-level metrics**
Based on the large number of tools used, it's no surprise that 60% of respondents surveyed in Ireland and the United Kingdom said they primarily learn about software and system interruptions with multiple tools, compared to only 15% who said they primarily learn about interruptions with one observability platform. The remaining 25% said they primarily learn about interruptions with manual checks/tests and complaints or incident tickets.

Outages happened fairly frequently, with up to 69% who said they experience outages once per week or more. While they detected those outages fairly quickly (up to 61% said they take less than 30 minutes to detect outages), they took longer to resolve them (up to 62% said they take more than 30 minutes to resolve outages). Despite these findings, 29% thought their IT performance is adequate.

**Strong advocacy, but expensive costs and lack of budget**
Respondents surveyed in Ireland and the United Kingdom said transparent pricing (42%) and budget-friendly pricing (37%) are the most important pricing features for observability tools. And 39% said that predictable spending is the most important billing feature. A third cited a lack of budget as the biggest obstacle to achieving full-stack observability, and 25% said it was too expensive. In fact, 63% said they allocate less than 10% of their IT budgets for observability tools. However, 44% said they expect to increase their budgets next year.

These budget plans likely were influenced by the strong advocacy for observability across all groups in Ireland and the United Kingdom—including 77% of more technical-focused and 70% of less technical-focused C-suite executives—and the fact that 71% saw observability as a key enabler to achieve core business goals.

**Future observability plans**
Like the rest of Europe and other regions, the biggest driver for observability in Ireland and the United Kingdom was an increased focus on security, governance, risk, and compliance. In fact, 60% of respondents surveyed in Ireland and the United Kingdom said they deploy security monitoring already, and most (96%) said they expect to deploy it by 2025.

Next year, 62% said they expect to deploy five or more additional observability capabilities, including distributed tracing (42%), AIOps (40%), and ML model performance monitoring (37%).

Over the next three years, they foresaw needing observability the most for emerging technologies like AI (45%), IoT (44%), and 5G (30%).

## 50% said observability led to improved collaboration across teams to make decisions related to the software stack

# North America

Growth and stability are top of mind for many business leaders. In the North American countries of Canada and the United States, 76% saw observability as a key enabler for achieving core business goals and therefore a catalyst to achieving these outcomes, with improved uptime and reliability among the top benefits of observability deployments. This is also likely a reason for high levels of advocacy among all groups and why respondents surveyed in North America expected their observability budgets to increase over the next year.

## Deployment and budget plans
About three-quarters (76%) said they deploy one to ten observability capabilities. In the next year, 70% expected to deploy five or more additional capabilities. Compared to those in other regions, they were the most likely to say they expect to increase their budgets in the next year (63%, including 18% who expected an increase of more than 25%).

## Achieving full-stack observability
Respondents surveyed in North America were the most likely to use extensive or full observability in the deploy (74%) and operate (81%) stages of the SDLC. However, only 31% had achieved full-stack observability by our definition, and just 3% said they had already prioritized/achieved full-stack observability. Almost a quarter (24%) said too many monitoring tools is a primary challenge for prioritizing/achieving full-stack observability. In fact, most said they use multiple tools, including 73% who said they use five or more tools. Even though 43% said they prefer a single, consolidated platform, only 3% said they are using one tool

for observability. They were the most likely to have unified telemetry data (56%) and telemetry data visualized in a single dashboarding solution (74%).

## Improving service-level metrics
A quarter said their IT teams primarily learn about software and service interruptions with one observability platform—more than those from any other region. This may have contributed to the fact that they reported the least frequent outages and were the most likely to detect outages in less than 30 minutes. Although 40% said outages with high business impact occur once per week or more and nearly 30% of those outages take more than 60 minutes to resolve. Despite this, 31% said their IT performance is adequate. Two out of five said that staff training for observability tools would most help reduce their organizations' MTTR, more than any other region.

## Highlights by country
Here's a snapshot of the key observability takeaways from each North American country represented in the survey:

**Canada** 🇨🇦 saw observability as a key enabler of developer/engineer productivity and collaboration, and most expected to deploy up to 12 additional capabilities over the next year

The **United States** 🇺🇸 saw clear business operation benefits and expected to increase observability budgets next year

n=508
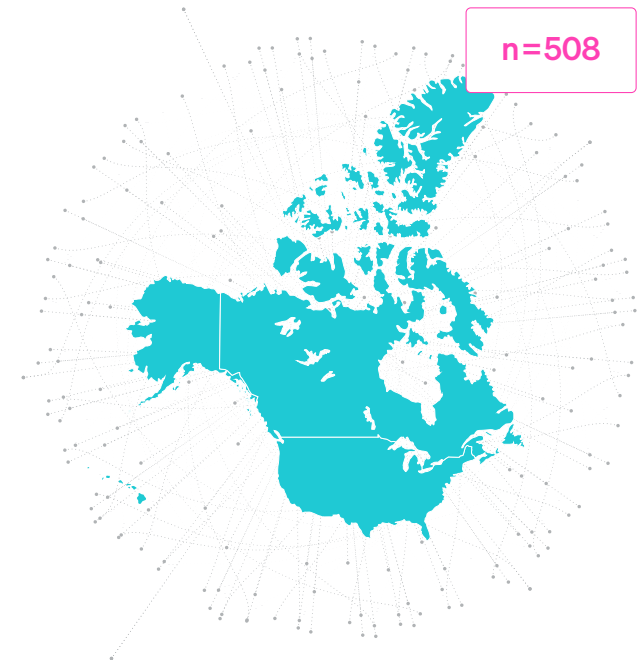
# North America

### Canada

In Canada, observability had a clear impact on developer/ engineer productivity and innovation as well as advocates across all roles. However, organizational challenges, tool fragmentation, and a lack of budget prevented them from prioritizing/achieving full-stack observability—in fact, only 7% said they had prioritized/achieved full-stack observability, and 29% had full-stack observability according to our definition.

Respondents surveyed in Canada viewed observability as a key enabler of future technologies, and they expected to deploy most capabilities over the next three years. To support these expectations, 76% expected their observability budgets to increase or stay the same over the next year.

**Strong advocacy and budget increase goals**
Most (85%) of the respondents surveyed in Canada stated that their organizations' more technical-focused C-suite executives advocate for observability. Additionally, 76% considered their developers to be advocates.

These high levels of advocacy likely contributed to the 54% who said they expect their observability budgets to increase somewhat or significantly over the next year.

**Organizational and tool fragmentation challenges**
Despite the many benefits of full-stack observability, respondents surveyed in Canada cited challenges to prioritizing/achieving it, including a lack of strategy (31%), dedicated personnel (27%), and skills (20%).

And a quarter cited too many tools as a challenge. Nearly three-quarters (74%) stated their organizations use five or more tools, and 46% use seven or more tools. Notably, no respondents indicated they use only one tool, despite 41% who said they prefer a single, consolidated platform.

**Developer/engineer productivity, collaboration, and innovation**
More than half (51%) of respondents surveyed in Canada said observability helps shift developer time from reactive to proactive work, while 46% said it improves collaboration across teams to make decisions related to the software stack.

Nearly half (46%) said observability improves uptime and reliability, and 40% said it increases operational efficiency and improves customer experience.

They also noted that observability helps improve the lives of developers and engineers by enabling cross-team collaboration (40%) and increasing innovation (36%).

**Future observability plans**
More than half (56%) of respondents surveyed in Canada said an increased focus on security, governance, risk, and compliance is driving the need for observability in their organization. They also cited the development of cloud-native application architectures (48%) and migration to a multi-cloud environment (46%).

Looking ahead, most expected to deploy one to 12 additional capabilities over the next year—only 9% did not expect to deploy additional capabilities next year. Over the next three years, they foresaw needing observability the most for emerging technologies like IoT (48%), AI (47%), blockchain (36%), and 5G (28%).

# 76%

expected their observability budgets to increase or stay the same over the next year

# North America

### 🇺🇸 The United States

In the United States, much like the rest of the world, observability tools and practices were fragmented with nearly three-quarters using five or more tools for observability. This fragmentation likely had a detrimental impact on their service-level metrics.

Despite strong advocacy for observability, only 4% of respondents surveyed in the United States said they had already prioritized/achieved full-stack observability, while 31% had full-stack observability according to our definition. However, in the next three years, respondents surveyed in the United States indicated they are eyeing observability to support emerging technologies like AI, IoT, and 5G.

**Data and tool fragmentation**
Almost three-quarters (73%) of respondents surveyed in the United States said they use five or more tools for observability. Just 3% said they use only one tool, despite the fact that 43% said they prefer a single, consolidated platform. Unsurprisingly then, 24% stated too many monitoring tools prevent their organizations from prioritizing/achieving full-stack observability.

Just 8% said their organizations' telemetry data is entirely unified, while only 14% said that all telemetry data can be visualized in a single dashboarding solution.

**Frequent outages and slow MTTD/MTTR**
Nearly half (48%) of respondents surveyed in the United States experienced high-business-impact outages that affect customers and end users once per week or more. What's more, 55% said it takes more than 30 minutes to detect those outages, and 63% said it takes more than 30 minutes to resolve them. Despite these findings, 31% thought their IT performance is adequate.

And 43% said IT teams primarily use multiple monitoring tools to learn about software and system interruptions. Worse, 32% said IT teams primarily rely on manual checks/tests or complaints/incident tickets.

**Clear business operation benefits and advocacy**
More than three-quarters of respondents surveyed in the United States said C-suite executives advocate for observability (79% for the more technical focused and 77% for the less technical focused).

When asked how observability most improves the lives of developers/engineers, 35% said it increases productivity and enables cross-team collaboration, 30% said it increases innovation, and 26% said it makes developer/engineer jobs easier.

About half (49%) viewed observability as a key enabler to achieve core business goals. So, it's not surprising that 65% expected their budgets for observability tools to increase over the next year.

**Future observability plans**
When we asked what strategies and trends are driving the need for observability at their organizations, more than half of respondents surveyed in the United States said an increased focus on security, governance, risk, and compliance, an increased focus on customer experience management, and development of cloud-native application architectures.

Most expected to deploy one to 14 additional capabilities over the next year—only 8% did not expect to deploy additional capabilities next year.

For emerging technologies, more than half (53%) said they'll need observability the most for AI in the next three years, followed by IoT (44%), 5G (35%), blockchain (34%), and Web3 (18%).

## 35%
said observability increases productivity and enables cross-team collaboration

# About us

**new relic.**

As a leader in observability, New Relic empowers engineers with a data-driven approach to planning, building, deploying, and running great software. New Relic delivers the only unified data platform with all telemetry—metrics, events, logs, and traces—paired with powerful full-stack analysis tools to help engineers do their best work with data, not opinion.

Delivered through the industry's first usage-based pricing that's intuitive and predictable, New Relic gives engineers more value for their money by helping improve planning cycle times, change failure rates, release frequency, and MTTR. This helps the world's leading brands and hyper-growth startups to improve uptime, reliability, and operational efficiency and deliver exceptional customer experiences that fuel innovation and growth.

**ETR**

ETR is a technology market research firm that leverages proprietary data from its targeted ITDM community to deliver actionable insights about spending intentions and industry trends. Since 2010, ETR has worked diligently at achieving one goal: eliminating the need for opinions in enterprise research, which are typically formed from incomplete, biased, and statistically insignificant data.

The ETR community of ITDMs represents $1+ trillion in annual IT spend and is uniquely positioned to provide best-in-class customer/evaluator perspectives. Its comprehensive proprietary data and insights from this community empower institutional investors, technology companies, and ITDMs to navigate the complex enterprise technology landscape amid an expanding marketplace.

Learn About New Relic Platform