HyperFRAME RESEARCH

HyperFRAME ResearchLens

State of the Enterprise Infrastructure & Operations

1H 2026

June 2026

www.hyperframeresearch.com

Introduction

Enterprise infrastructure is undergoing a period of profound disruption as organizations confront the combined pressures of cloud adoption, escalating cybersecurity threats, rising operational complexity, global data governance requirements, and the resource-intensive demands of enterprise AI. These forces are reshaping how Infrastructure & Operations (I&O) teams plan, deploy, secure, and scale the systems that underpin modern business—at a time when execution speed and architectural integrity are becoming competitive differentiators. The result is an environment where I&O decisions increasingly determine the success, resilience, and velocity of both technology initiatives and the enterprise itself.

The **HyperFRAME Research Lens: State of Enterprise Infrastructure & Operations, 1H 2026** presents the results of a global study designed to illuminate how enterprises are planning, adapting, and executing to meet these challenges—both today and in the months and years ahead. Published as open research and updated every six months, the Lens establishes a foundational baseline for tracking how enterprise priorities, risks, and execution realities evolve over time. It also serves as a companion to the **HyperFRAME Research Lens: State of the Enterprise AI Stack, 1H 2026**, reflecting the growing interdependence between infrastructure strategy and AI readiness.

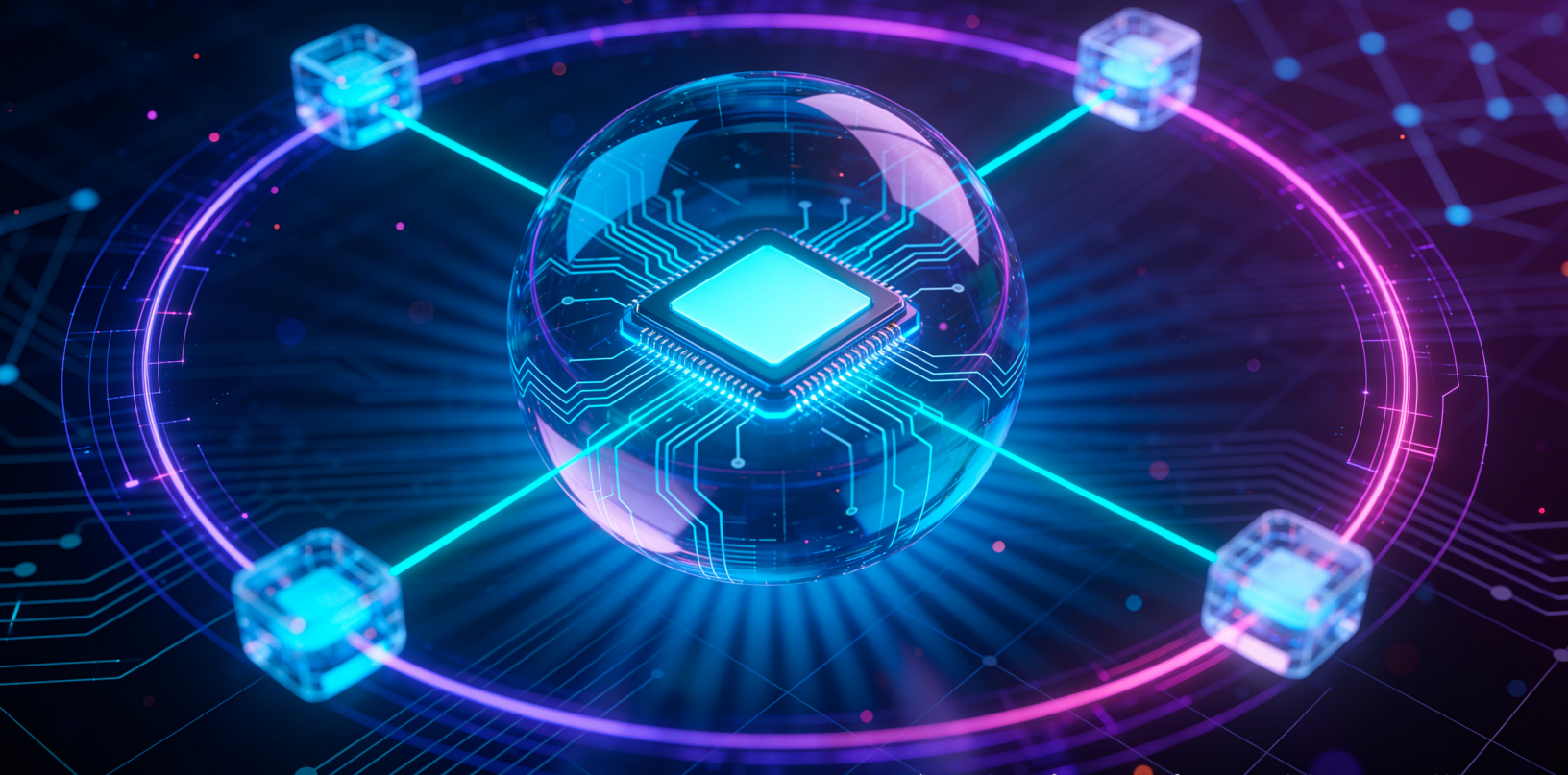
This edition draws on responses from 520 participants across North America, EMEA, APAC, and South/Central America, representing local, regional, and multinational organizations ranging from under 1,000 to more than 50,000 employees. All respondents hold meaningful influence or responsibility within I&O planning, implementation, management, or operations, including Strategic Owners, Decision Leads, Technical Sponsors, and Implementors.

Respondents oversee key areas across the infrastructure ecosystem, including **Architecture & Strategy; Platform, Automation & Reliability; Operations & Service Delivery; Security, Integrity & Protection; and Data, Edge & Specialized Infrastructure**. The study's scope reflects the breadth of today's I&O landscape, examining infrastructure and cloud strategies, budget trends, compute modernization, cyber-resilience, data protection, observability, talent gaps, vendor strategy, and the readiness and risks shaping enterprise AI adoption. Together, these perspectives provide a comprehensive view of the infrastructure ecosystem and the operational realities shaping enterprise modernization.

Together, these results provide a clear, data-driven view of how organizations are prioritizing investments, confronting operational challenges, and adapting their strategies amid rapid technological and regulatory change.

Index

Table of Contents



Section 1

Executive Summary

Enterprise infrastructure priorities continue to shift as organizations balance cloud adoption, security requirements, operational complexity, AI initiatives, and talent constraints. The findings in this study show that while modernization intent remains high, progress is often slowed by fragmentation, security concerns, and widening skills gaps. These pressures are shaping how I&O leaders plan, invest, and execute as they prepare for the next phase of enterprise transformation.

Operational Reality: Four Data-driven Insights

Heading into 2027, I&O leaders are prioritizing infrastructure readiness and operational resilience. This includes accelerating the adoption of unified control planes to simplify distributed environments, strengthening cyber-recovery frameworks, and aligning infrastructure strategy with emerging global regulatory requirements. The data in this study highlights the operational realities shaping these decisions and the constraints that continue to slow progress.

1. **Execution maturity is highlighted by risk avoidance and ROI-led growth.**

- The need for innovation is tempered by discipline: 40% of organizations are Mass Adopters who require validated business cases before investing.
- Success is now defined by operational utility and proven value rather than experimental narratives.

2. **Enterprises are embracing hybrid and multi-cloud but complexity and fragmentation risks remain.**

- While 55% rely on hybrid cloud models only 23% of compute workloads are processed in hybrid environments.
- Architectural complexity is high with 79% of public/hybrid enterprises using multiple cloud providers including 27% using 4 or more different providers.

3. Security risks are the top barrier to achieving infrastructure scale.

- Security is the #1 barrier to scaling for 72% of respondents, with only 30% of leaders feeling very confident in recovery speed after a cyber attack or loss of cloud-based data.
- Organizations currently prioritize high-speed performance in vendor selection while delaying the formal governance needed to manage external hack threats.

4. Progress is constrained by a shortage of specialized technical talent.

- Progress is stopped by a talent wall: 37% of firms face a significant skills gap in Kubernetes, and 49% struggle to find staff with both technical and legal AI expertise.
- Talent gaps are as disruptive as technical barriers, making talent acquisition and upskilling foundational enablers of adoption success.

I&O Strategic Priority & Preparedness

The study's strategic priority framework highlights where organizations assign importance, where they feel prepared, and where gaps remain across execution maturity, architectural integrity, operational resilience, and specialized talent. The data reveals a consistent pattern: organizations understand what must be done, but readiness levels lag behind strategic intent—particularly in unified management, cyber-resilience, and AI governance.

Strategic Focus	Operational Pillar	Importance	Readiness	Insights & Supporting Data
Execution Maturity and Fiscal Discipline Improving delivery consistency while tightly managing financial resources	AI Financial Management	★★★★☆		**Budgetary Overrun:** 84% report that AI deployment has consumed more budget and resources than planned.
	Software Strategy Pivot	★★★★☆		**Rapid COTS Adoption:** 49% project that Commercial off-the-Shelf software will replace custom builds within 24 months.

Strategic Focus	Operational Pillar	Importance	Readiness	Insights & Supporting Data
Architectural Integrity & Hybridity Keeping systems well-designed across mixed, interconnected environments	Unified Operational Management	★★★★☆	◔	**The Platform Gap:** 90% assign value to unified management platforms, but only 15% have achieved a single observability view today.
	Hybrid Cloud Utility	★★★★☆	◔	**Workload Disconnect:** 55% have adopted a hybrid cloud strategy but only 23% of data compute workloads are processed in hybrid clouds.
Operational Risk & Continuity Ensuring services withstand disruptions and remain consistently available	Data Security & Governance	★★★★★	◑	**Action vs. Intent:** 72% see this as a top challenge; only 33% are fully prepared for primary EU AI Act standards.
	Cyber-Resilience & Recovery	★★★★★	◔	**Confidence Gap:** 91% prioritize resilience, yet only 30% are "very confident" in their recovery speed.
	Global AI Regulation	★★★☆☆	◑	**Compliance Lag:** 30% cite the EU AI Act as their primary driver, but only 27% are ready for U.S. Federal Policies.
Specialized Talent & Skills Securing and developing advanced, hard-to-find technical skills	Talent & Skills Alignment	★★★★☆	◔	**The Modern Skill Gap:** 46% rate skill gaps as significant; Kubernetes remains the most acute talent shortage.
	Mainframe-AI Modernization	★★★☆☆	◑	**Legacy Stability:** ~51% are modernizing mainframes; this sector shows high readiness with 42% reporting "No Skills Gap".

Section 2

Infrastructure, Cloud & Networking

Security is rated as the most significant challenge to deploying and scaling IT infrastructure, followed by cost management/ optimization and managing operational complexity.

Highlights

40% identified as Mass Adopters, avoiding experimentation in favor of an evidence-based approach to new technology. These organizations demand proven ROI and validated business cases before committing to new infrastructure.

79% with public or hybrid cloud models use two or more cloud providers including 27% using four or more providers, a potential sign of architectural sprawl and operational complexity.

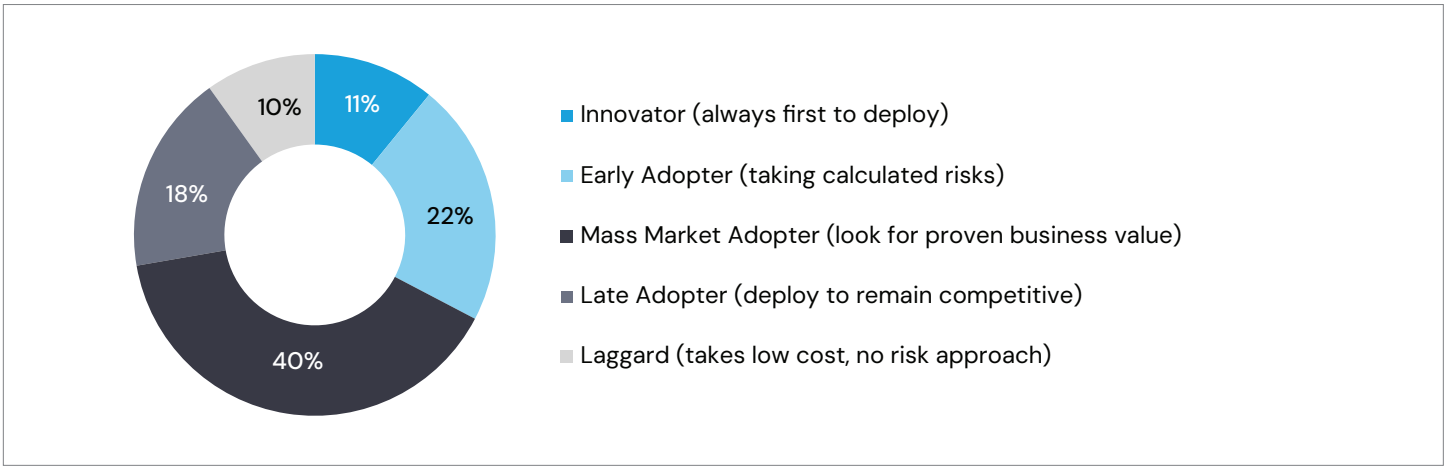
88% of enterprises utilizing public or hybrid cloud models rely on two or more cloud providers to meet their operational needs. This includes 27% who rely on four or more providers with increased risk of architectural sprawl and operational complexity.

55% have adopted hybrid cloud architectures but hybrid clouds only support 23% of overall compute workloads.

27% use 4+ cloud providers, a potential sign of highly distributed requirements and/or architectural sprawl.

Question: Which of the following best describes your organization's overall approach to adopting new technologies?

Figure 1: Organizational Approach to New Technology Adoption



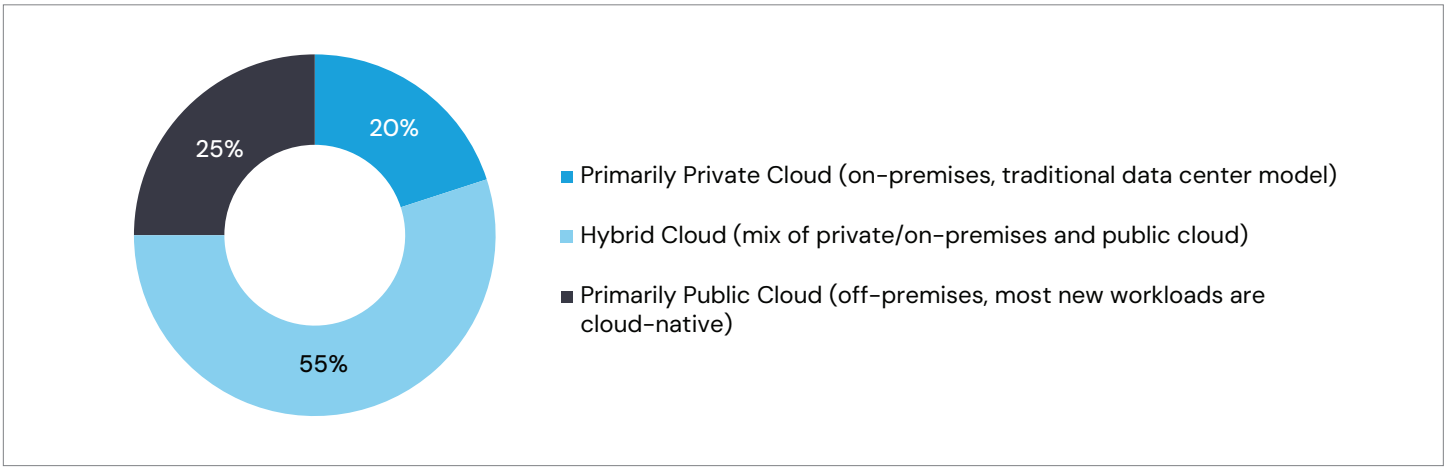
Key Insights

The Preference for "Evidence-Based" Adoption

- The Mass Market Adopter segment represents 40% of the market, marking a clear preference for pragmatic investments. These organizations are avoiding first-in experimental cycles, requiring validated business cases and proven ROI before expanding the Infrastructure & Operations (I&O) stack.
- Nearly a third of organizations are classified as Late Adopters (18%) and Laggards (10%), maintaining a low-risk approach to I&O modernization.

Question: How would you describe your current IT infrastructure model?

Figure 2a: Cloud deployments within IT infrastructure



Key Insights

Prevailing Hybrid Adoption

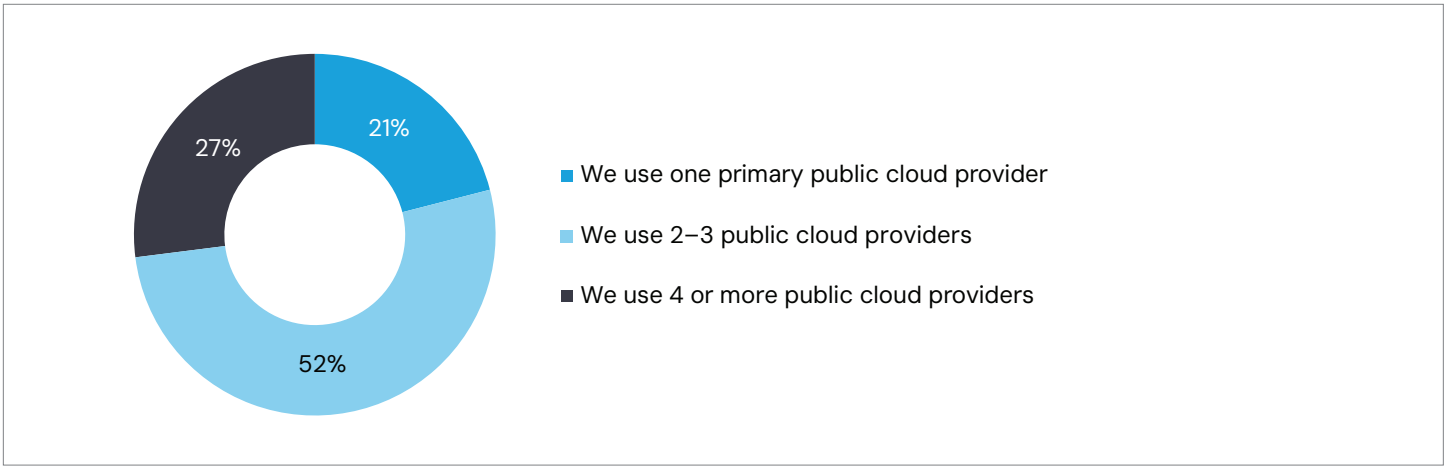
- The hybrid cloud model is the prevailing infrastructure strategy-adopted by 55% respondents, providing both private control security and public cloud flexibility.

Non-Hybrid Organizations Split Across Public and Private Cloud

- Organizations not utilizing Hybrid Clouds (45%) are split roughly equally with 25% favoring Public Cloud and 20% favoring Private Cloud.

Question: (If using Public/Hybrid Cloud) How would you describe your current use of multiple cloud providers?

Figure 2b: Current Utilization of Multiple Public Cloud Providers (for Public/Hybrid Cloud users)



Key Insights

Standardization of Multi-Cloud

- With 79% of organizations (with public or hybrid cloud models) using two or more providers, multi-cloud is somewhat of an operational standard with the vast majority of enterprises opting to not rely on a single vendor to support their infrastructure requirements.

Multi-Cloud Sweet Spot

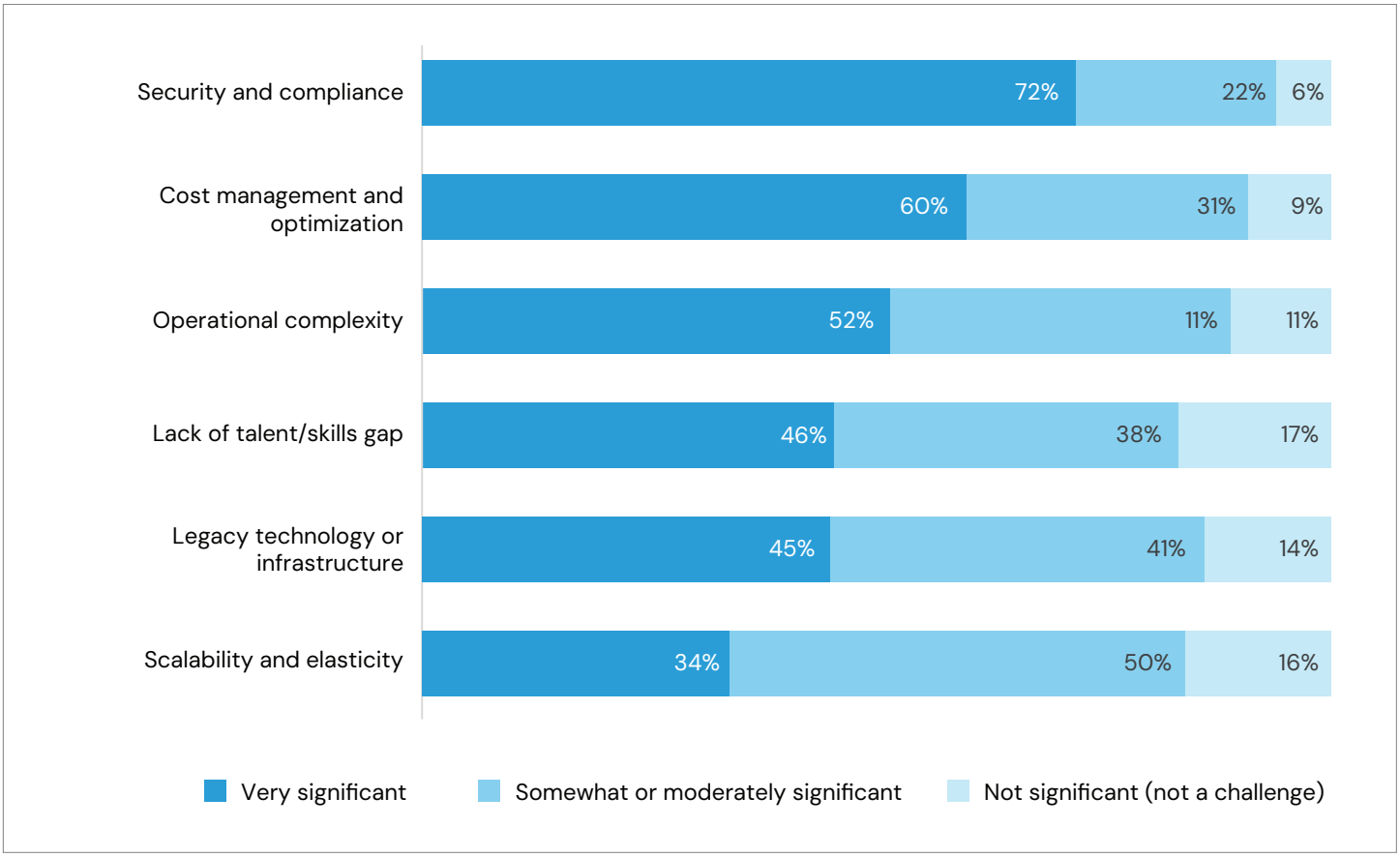
- 52% of these respondents utilize a select 2–3 providers to meet their needs.

Distributed Multi-Cloud Complexity

- With 27% of theses organizations utilizing 4 or more providers, a significant market segment operates across highly distributed environments indicating a requirement for an expansive multi-cloud footprint to address specific architectural, data sovereignty, or workload-optimized requirements and/or the potential for significant architectural sprawl and management overhead.

Question: How significant a challenge to deploying and scaling your IT infrastructure are each of the following?

Figure 3a: Most Significant Challenges to Deploying and Scaling IT Infrastructure



Key Insights

Security is the Leading Overall Concern

- 72% of respondents identify "Security and compliance" as a very significant challenge, and with it a significant source of operational risk.

Cost Management is a Major Barrier

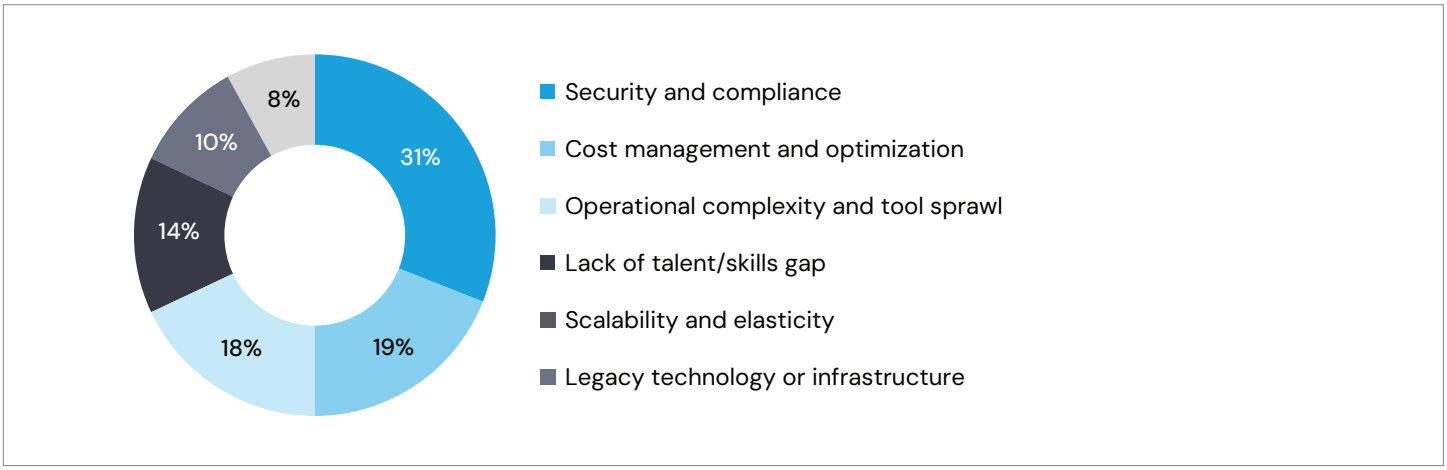
- 91% view cost management and optimization as a moderate (60%) or very significant (31%) challenge, second only to maintaining a strong security posture.

Scalability Itself Is Only a Moderate Struggle

- While "Scalability and elasticity" is viewed as a challenge by 84% of respondents, it is the least likely to be rated "very significant" (34%), suggesting it is often a manageable, moderate hurdle compared to others.

Question: Which challenge to deploying and scaling your IT infrastructure would you consider the most significant and/or difficult to overcome?

Figure 3b: Ranked challenges to deploying and scaling IT infrastructure



Key Insights

Security is the Dominant Barrier

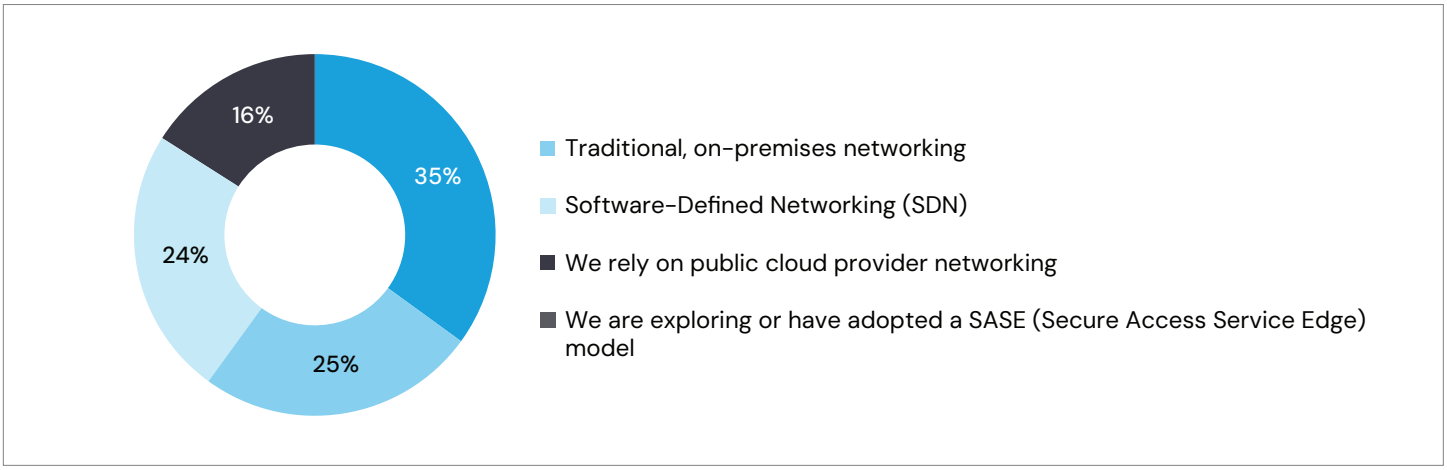
- At 31%, Security and compliance is ranked as the single most difficult hurdle to overcome.

Management vs. Assets

- Respondents find operational issues (Cost Management at 19% and Operational Complexity at 18%) more difficult to solve than the actual physical or digital assets, such as Legacy technology, which only 8% ranked as their most significant challenge.

Question: Which of the following best describes your organization's approach to networking?

Figure 4: Current Organizational Approach to Networking



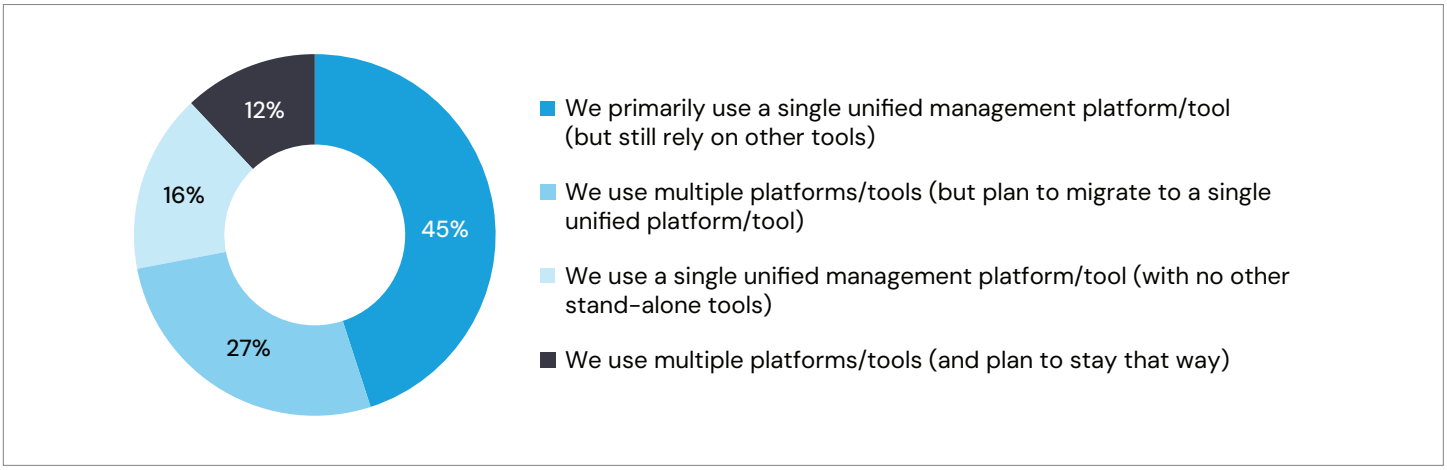
Key Insights

SDN and Cloud Dominance

- ~60% of organizations have transitioned to modern networking architectures, with Software-Defined Networking (35%) and Public Cloud (25%) leading the shift away from legacy on-premises systems.

Question: Which of the following best describes how your organization currently manages your compute, storage, and network resources?

Figure 5: Management Platform Preferences to Managing Compute, Storage, and Network Resources



Key Insights

The "Hybrid" Reality

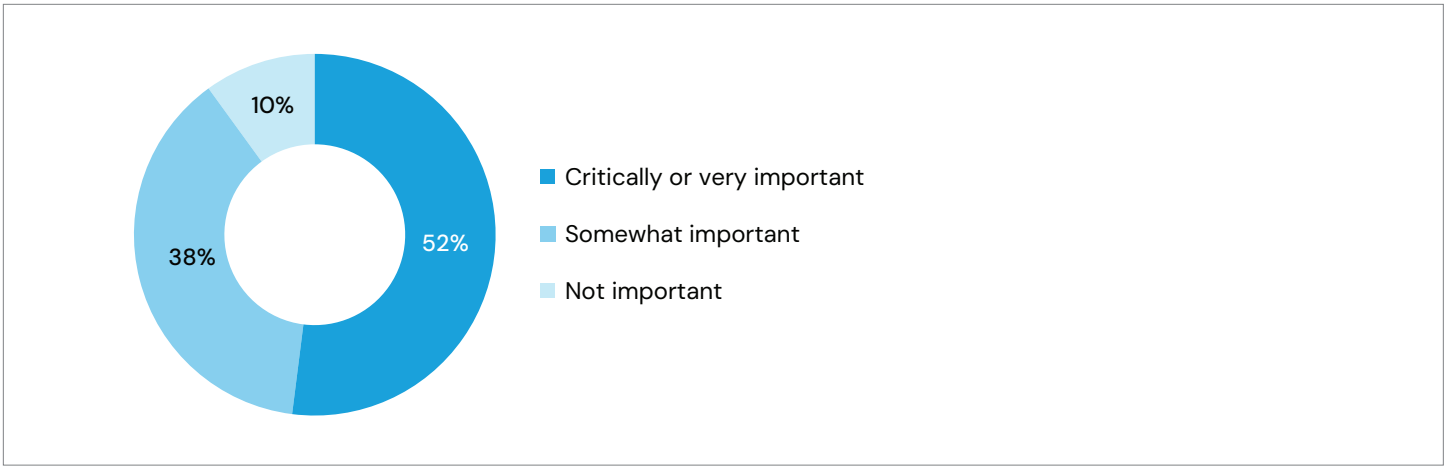
- While 61% of organizations have identified and adopted a primary management platform, 45% still rely on supplemental stand-alone tools alongside their primary platform.

Limited Long-Term Multi-Platform Use

- 12% of organizations intend to continue using multiple platforms indefinitely.

Question: How important is a unified, streamlined management platform for your compute, storage, and network resources?

Figure 6: Importance of a Unified Management Platform for Compute, Storage, and Network Resources



Key Insights

Management Platform as Critical Priority

- Over half of organizations (52%) view a unified management platform as a critically or very important requirement for their compute, storage, and network resources.

Platform Unification Is a Clear Priority

- A total of 90% of respondents assign value to platform unification, leaving only a small 10% minority that considers it "not important."

Section 3

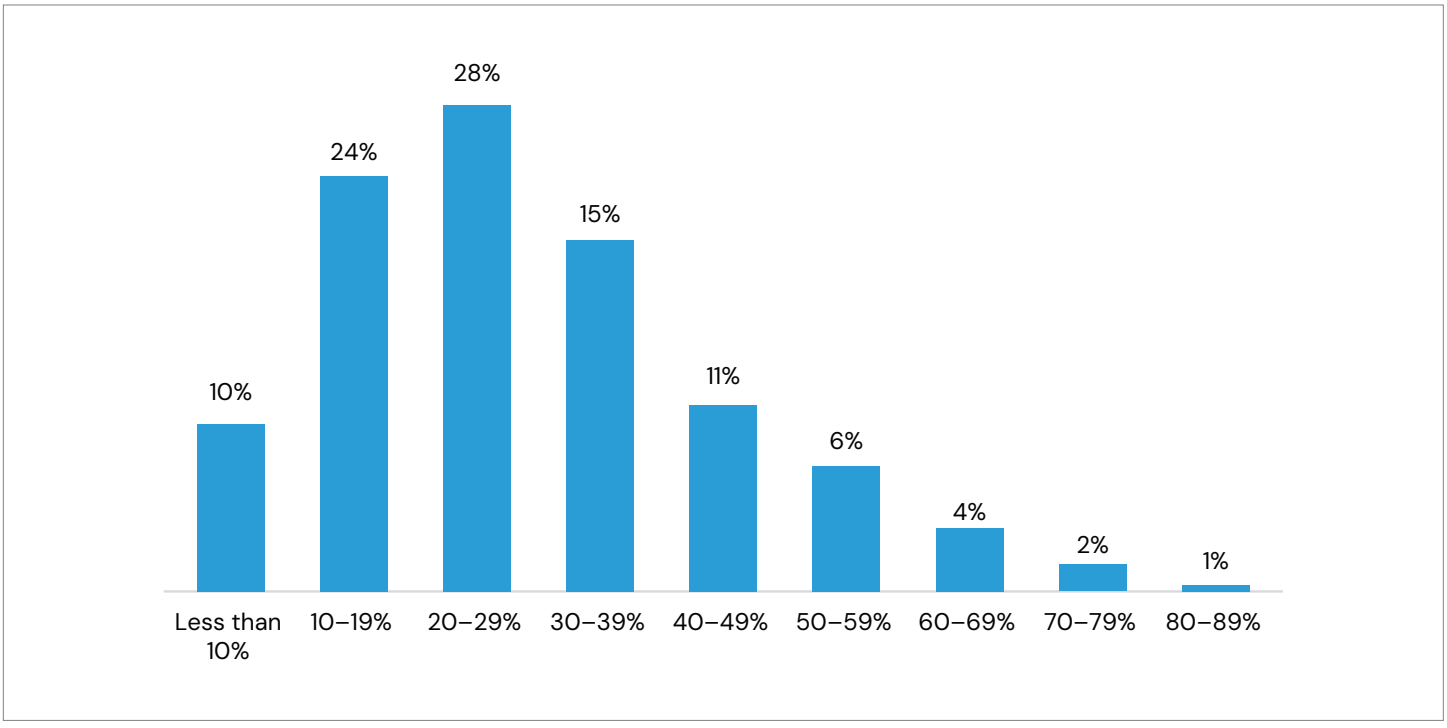
Budget Allocation

Highlights

Budget shift into the 30-39% range as firms "invest up" to protect increasingly complex digital footprints.

Question: Please estimate what percentage of your overall IT budget is currently allocated to infrastructure and operations software?

Figure 7: Current IT Budget Allocation for Infrastructure and Operations Software



Key Insights

Lower Budget Range Dominance

- The majority of organizations (52%) allocate between 10% and 29% of their total IT budget to I&O software, with the 20–29% bracket being the single most common response (28%).

The "Sweet Spot"

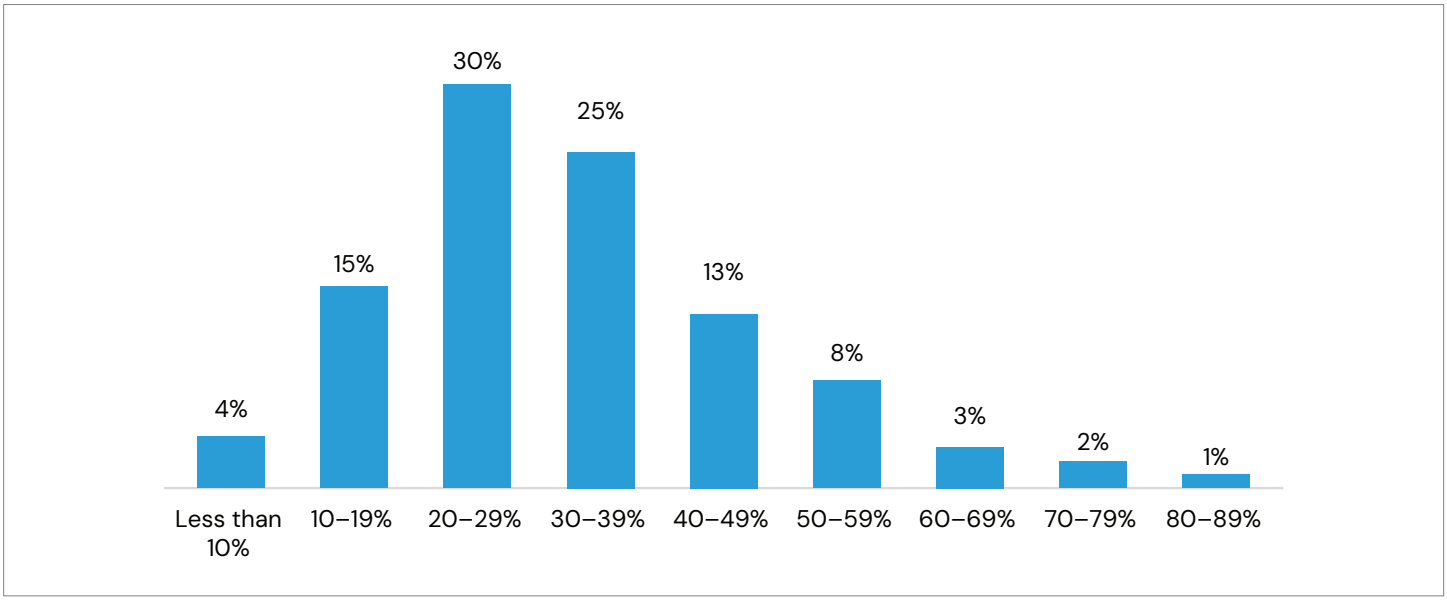
- Roughly 3 out of 4 organizations (77%) keep their I&O software spending below 40% of their overall IT budget, suggesting a standard threshold for infrastructure maintenance versus other IT initiatives.

Limited High-End Allocation

- Spending levels drop sharply at the higher end, with only 13% of organizations allocating 50% or more of their budget to these specific costs.

Question: Thinking ahead, please estimate what percentage of your overall IT budget will be allocated to infrastructure and operations software over the coming 12-24 months?

Figure 8: IT Budget Allocation for Infrastructure and Operations Software (Next 12–24 Months)



Key Insights

Budgets are "Moving to the Middle"

- Companies are shifting away from low spending (10-19%) and moving into the 30-39% range, which is expected to increase from 15% to 25% indicating sustained increases in investments and spend for IT infrastructure over the coming 24 months.

A Consistent Spending Ceiling

- Despite the increase in lower budgets, the percentage of "heavy spenders" (those spending over 50%) stays nearly flat at around 14% indicating a cap on IT spend and potential market growth.

Section 4

Modern Compute Architecture

Highlights

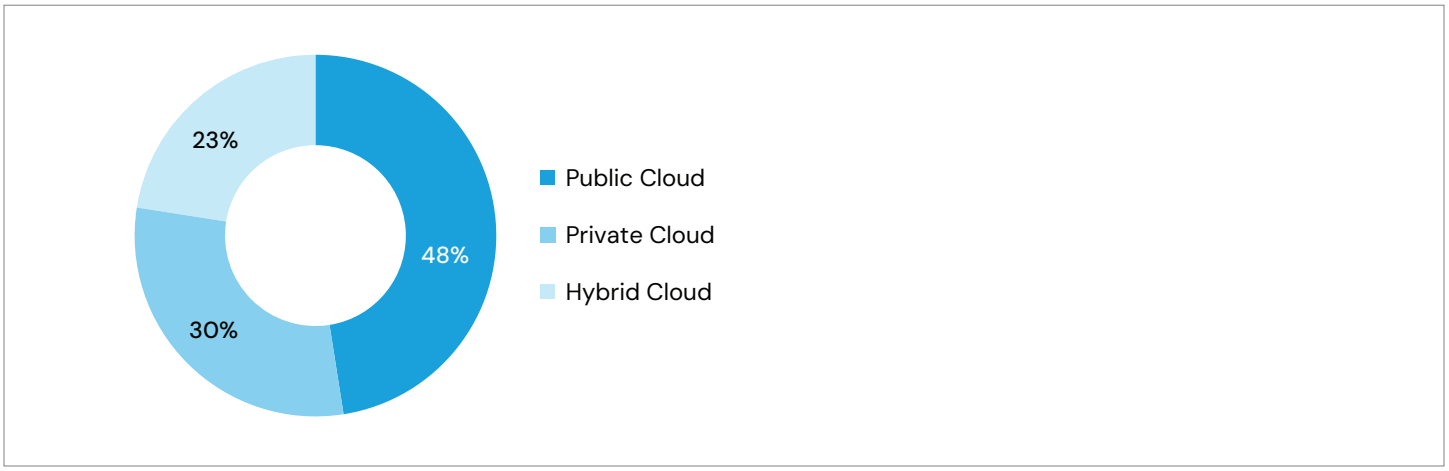
48% of workloads are now hosted in the public cloud, establishing it as the single largest environment for modern computing while still leaving over half of all operations in private or hybrid spaces.

57% of organizations are increasing their virtualization budgets, showing that most firms are choosing to strengthen their existing virtual foundations.

40% of the compute landscape has shifted toward containers and serverless functions, marking a steady move away from managing full servers in favor of more efficient, automated code—a clear shift towards modernization.

Question: What percentage of your data compute workload is currently processed in each of the following cloud environments?

Figure 9: Current Distribution of Data Compute Workloads Across Cloud Environment



Key Insights

Public Cloud Preference

- The Public Cloud processes the largest individual share of data compute workloads at 48%.

Hybrid as the Smallest Segment

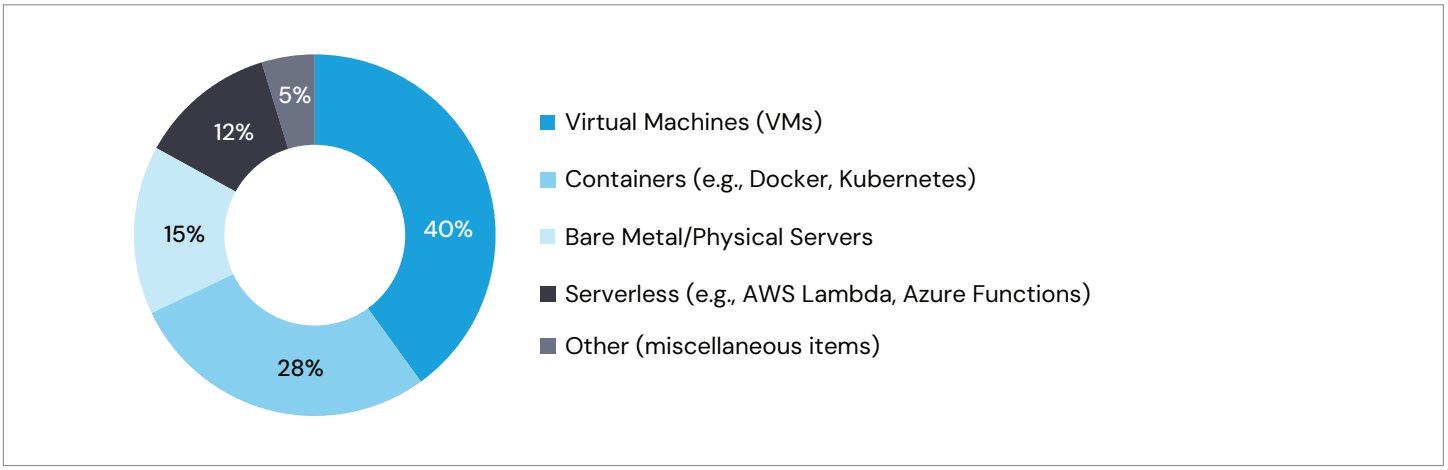
- Despite its popularity in strategy, Hybrid Cloud handles the lowest percentage of actual workloads at 23%.

Preference for private Environments

- Close to a third (30%) of all data compute workloads reside exclusively within private clouds, where issues of sovereignty, security, and regulatory governance are best addressed.

Question: What is the approximate percentage breakdown of your current compute workloads?

Figure 10: Workload Distribution Across Compute Model



Key Insights

Virtual Machines Lead Adoption

- VMs remain the primary compute model, accounting for 40% of all workloads as a foundational element withinin IT infrastructures.

High Penetration of Modern Architectures

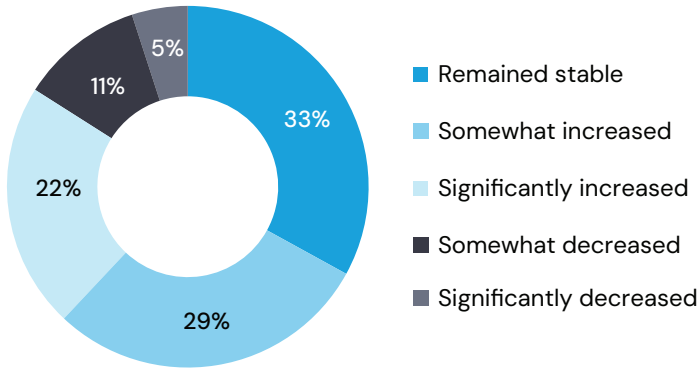
- Containers (28%) and Serverless (12%) together handle over 40% of workloads, showing a significant reliance on cloud-native and automated computing methods.

Persistence of Physical Infrastructure

- Bare Metal/Physical Servers still handle 15% of workloads, suggesting that a portion of the market still requires raw hardware performance or legacy support that virtualization cannot replace.

Question: How has your investment in virtualization technology changed over the past 12 months?

Figure 11: Changes in Virtualization Technology Investment Over the Past 12 Months



Key Insights

Growth in Virtualization Spending

- A majority of organizations (51%) reported an increase in their virtualization investment, even though only 40% of workloads are currently supported by VMs, confirming that this technology remains a key enabler driver for infrastructure expansion.

Maintenance of Existing Footprint

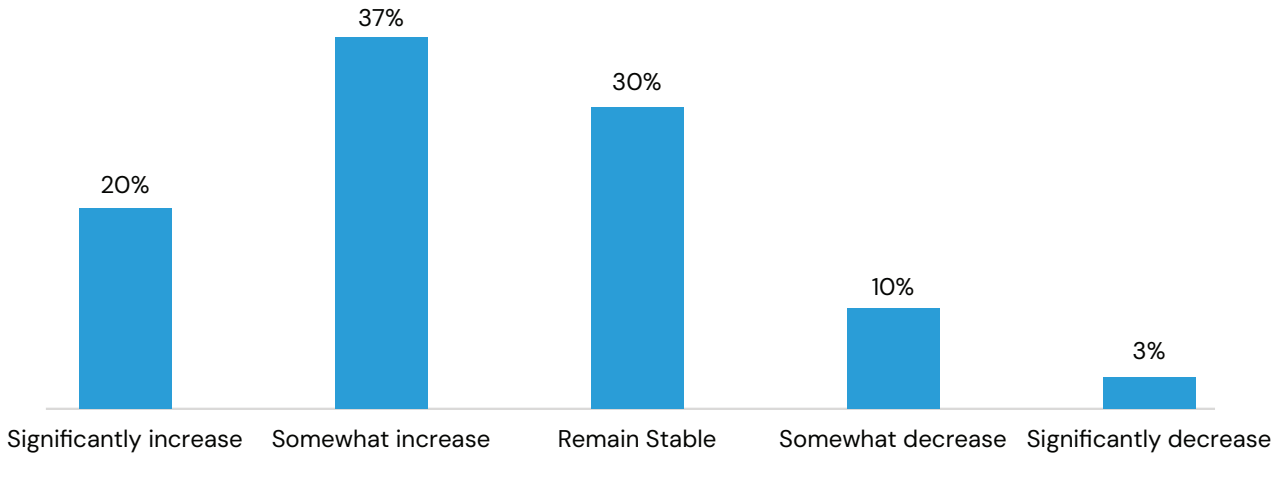
- 33% of respondents kept their investment levels unchanged, showing that virtualization has reached a mature "steady-state" for a third of the market.

Low Rate of Disinvestment

- Only 16% of organizations reduced their spending, indicating that very few companies are actively moving away from virtualization.

Question: How do you anticipate your investment in virtualization technology will change over the coming 12-24 months?

Figure 12. Anticipated Changes in Virtualization Investment (Next 12-24 Months)



Key Insights

Projected Increase in Spending

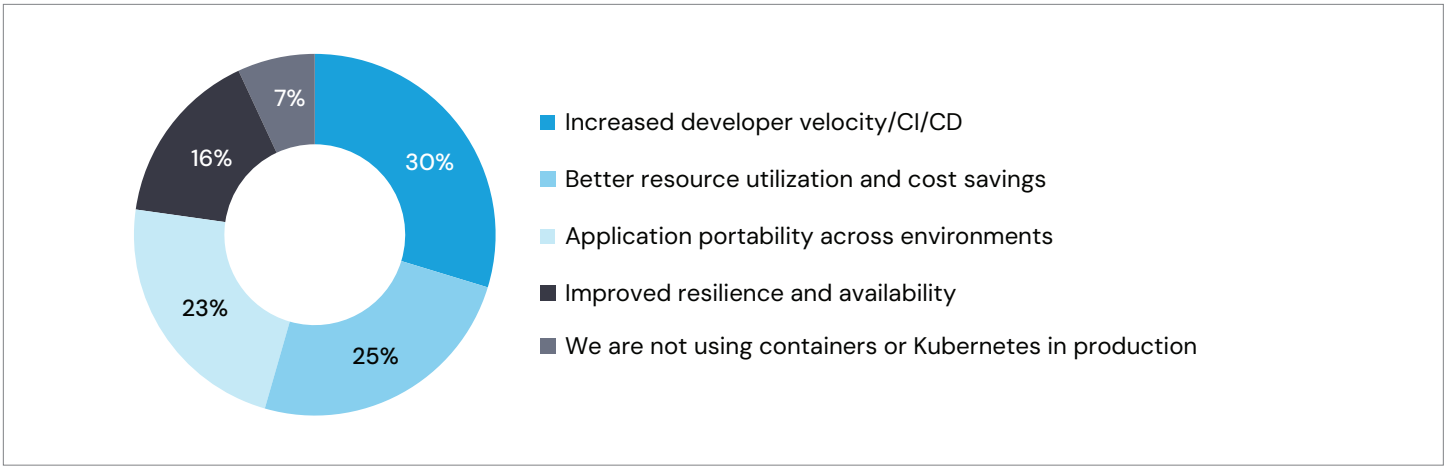
- A clear majority of 57% of organizations plan to grow their virtualization investment, signaling that most firms still view this technology as a key tool for future expansion.

Commitment to Existing Infrastructure

- 30% of respondents intend to keep their spending levels the same, proving that virtualization remains a vital, long-term foundation.

Question: What is the approximate percentage breakdown of your current compute workloads?

Figure 13: Primary reason or driver for organization's adoption of containers and Kubernetes



Key Insights

Developer Productivity as the Top Driver

- The primary motivator for adoption is increased developer velocity and CI/CD, cited by nearly 30% of organizations as their leading reason.

High Production Maturity

- Only a small minority (7%) of organizations are not yet using containers or Kubernetes in production, indicating that these technologies have reached mainstream/mature status across the industry.

Section 5

Mainframe Strategy & AI Readiness

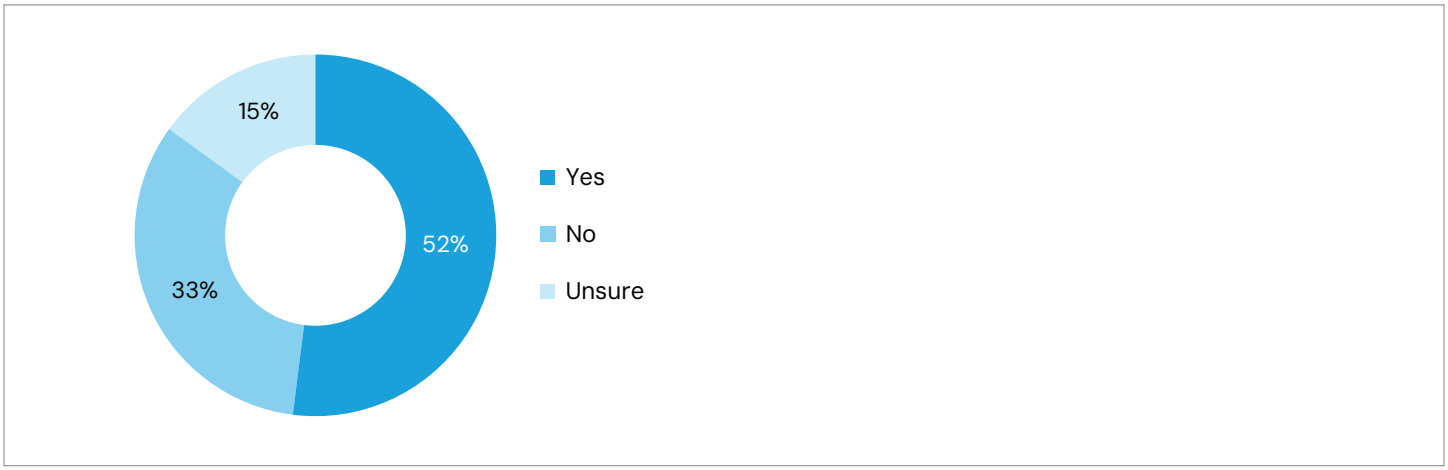
Highlights

52% of companies rely on mainframes to meet their ongoing compute requirement.

63.4% of organizations believe their current mainframe environment is equipped for AI.

Question: Does your organization currently utilize mainframe systems as part of your overall compute strategy?

Figure 14a: Current Utilization of Mainframe Systems in Compute Strategy



Key Insights

Majority Utilization of Mainframes

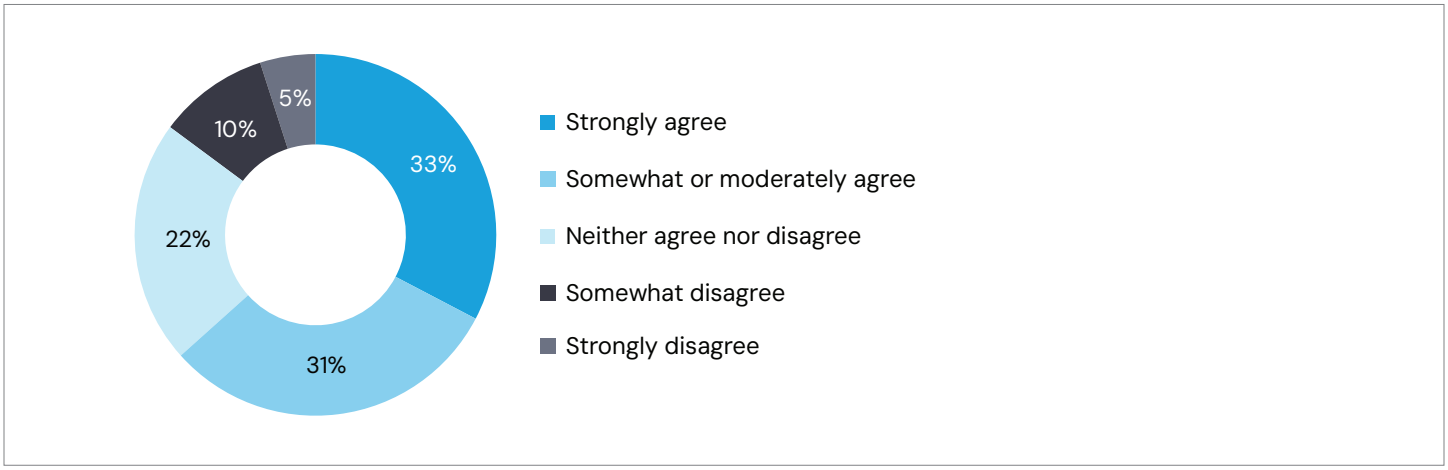
- More than half of all organizations (52%) continue to utilize mainframe systems, demonstrating that these high-capacity servers remain a cornerstone of modern compute strategies.

Non-Mainframe Minority

- 33% of organizations have transitioned to or natively adopted alternative distributed or cloud-only architectures.

Question: If utilizing mainframes as part of an overall compute strategy, how much do you agree or disagree with the statement "Our existing mainframe environment provides all the necessary infrastructure and tooling to support our organization's AI strategy"?

Figure 14b: Perceptions of Mainframe Infrastructure Readiness for AI Strategy



Key Insights

Mainframe As An AI Foundation

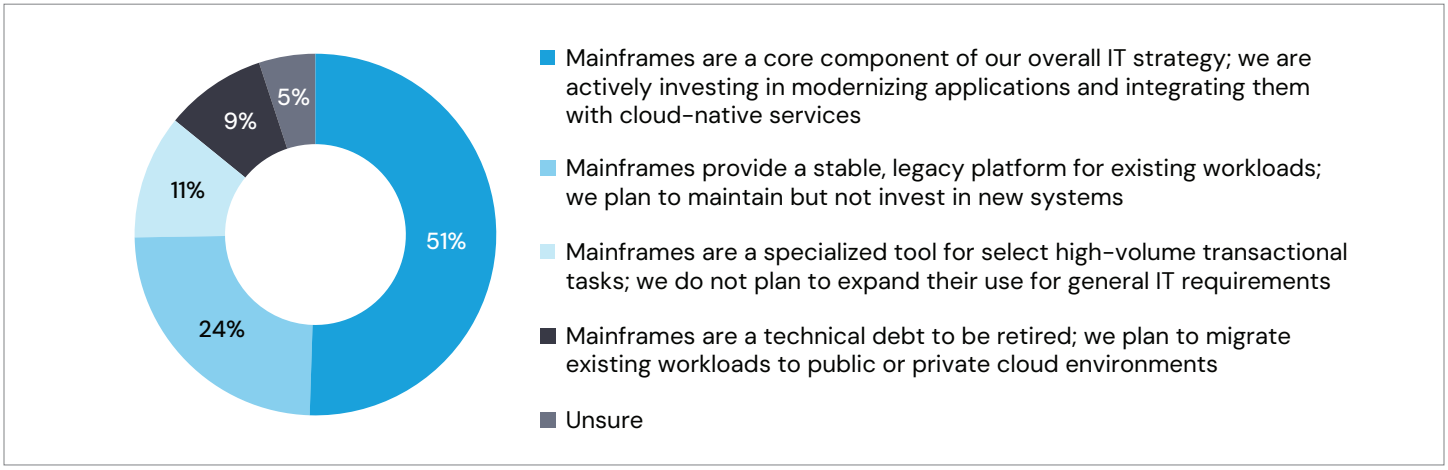
- A substantial majority (63%) of organizations believe their current mainframe environment is equipped for AI, with roughly one-third (33%) strongly agreeing that it provides all necessary infrastructure and tooling.

Mainframe Readiness For AI

- Total disagreement is low; only about 15% of organizations feel their mainframes are inadequate for AI.

Question: If utilizing mainframes as part of an overall compute strategy, which of the following best describes your organization's long-term strategic vision for mainframe use over the coming 3-5 years?

Figure 14c: Long-Term Strategic Vision for Mainframe Utilization (3-5 Year Outlook)



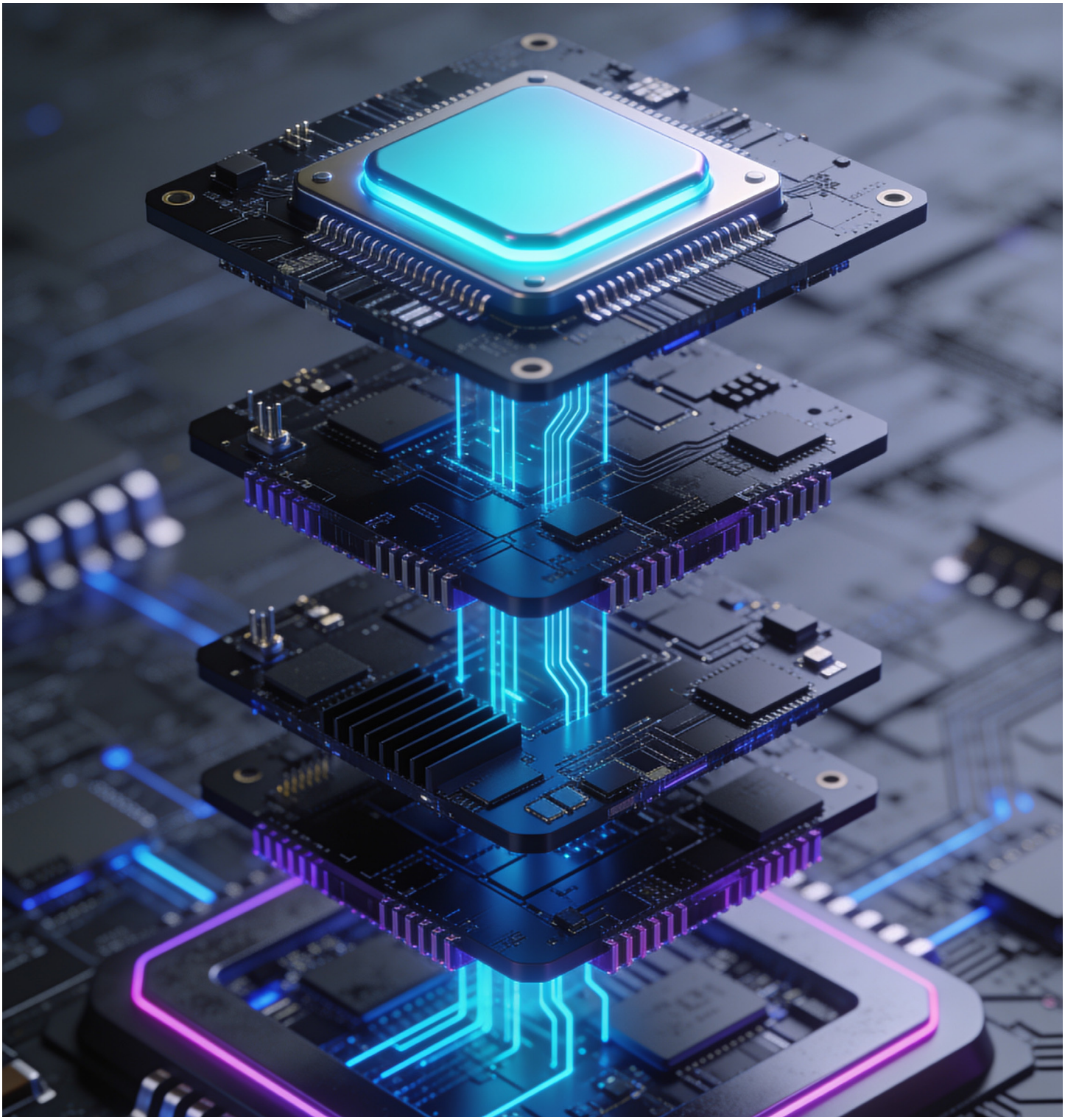
Key Insights

Mainframe Integration and Modernization

- Over half (51%) of mainframe-enabled organizations are actively modernizing mainframe apps to integrate with cloud-native services.

Mainframe Resilience

- Just 9% of organizations leveraging mainframe compute resources today plan to retire mainframes and migrate those workloads to the cloud.



Section 6

Storage Strategy, Cyber-resilience & Security

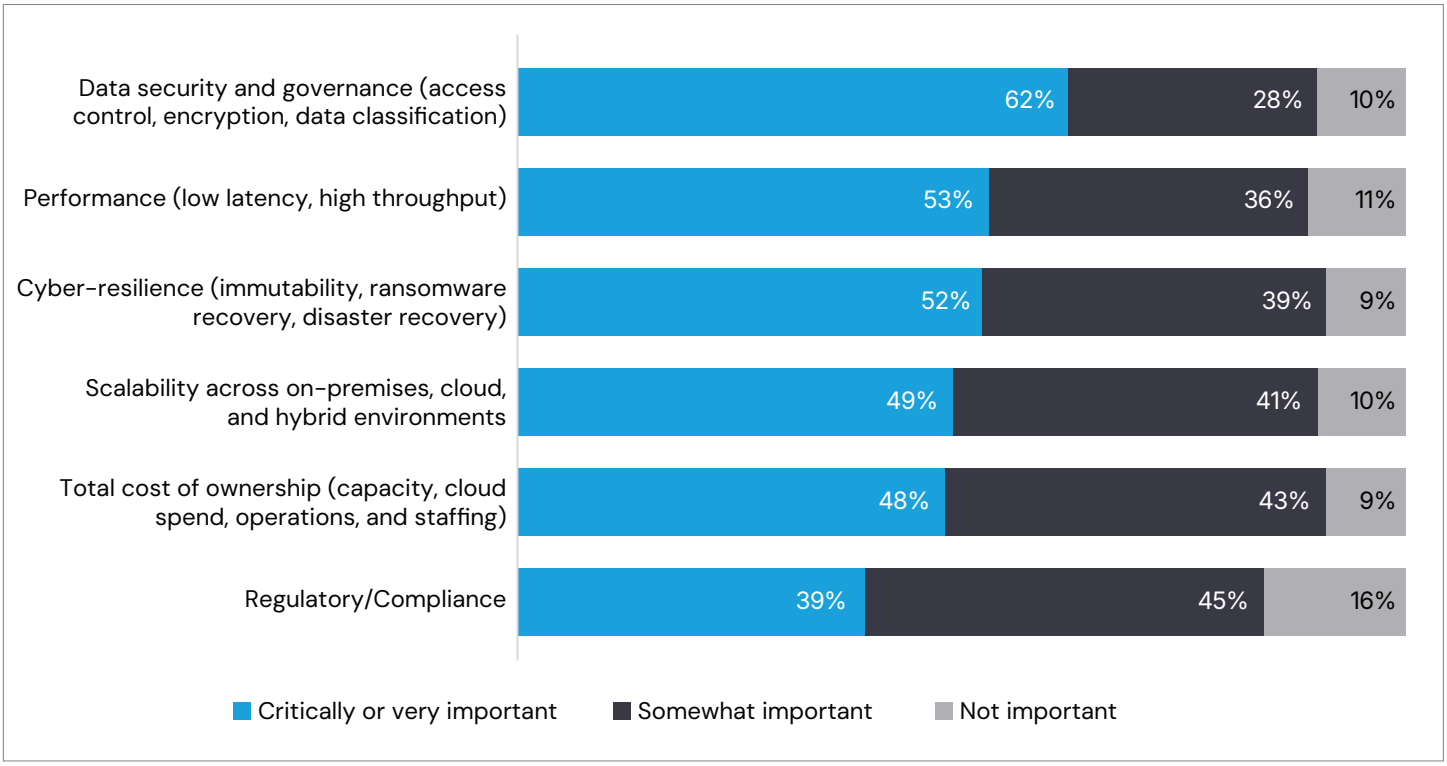
Highlights

62% of organizations identify data security and governance as their top strategic priority, establishing a clear foundation for all storage and recovery investments.

56% of organizations surveyed are "Very concerned" about external hacks, making it the top security threat.

Question: How important are the following in determining your organization's storage strategy over the next 24 months?

Figure 15a: Importance of Key Factors in Determining Storage Strategy (Next 24 Months)



Key Insights

Security and Performance are Non-Negotiable Foundations

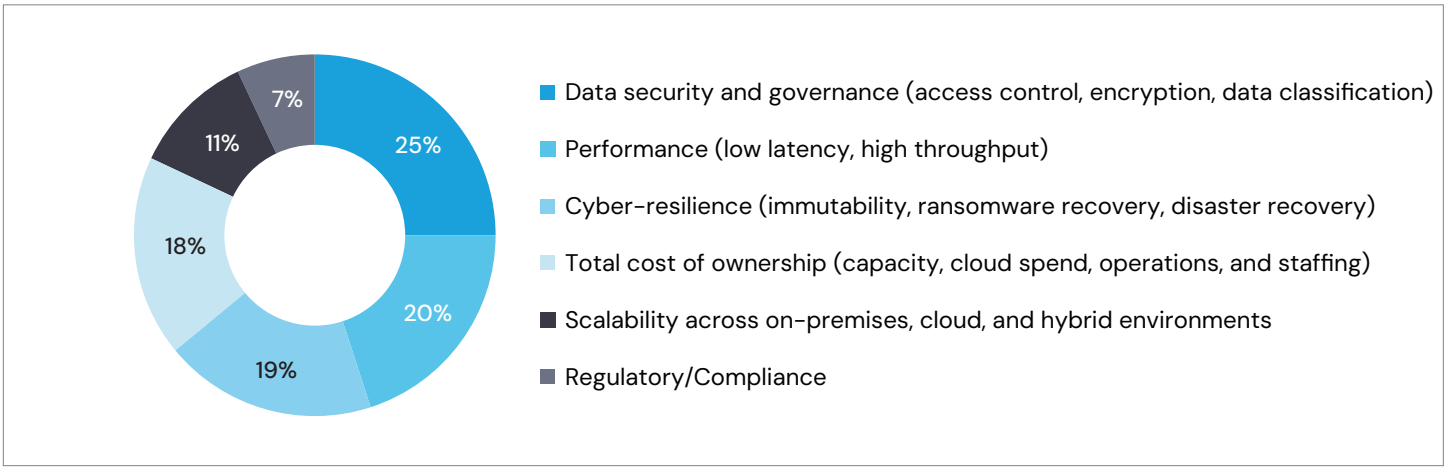
- Data security and governance remains the top priority, with 62% of organizations identifying it as a critical strategic pillar, followed closely by performance at 53%.

Cyber-Resilience is a Top-Tier Strategic Pillar

- Over half of the respondents (52%) classify cyber-resilience—specifically immutability and ransomware recovery—as critically important. When combined with those who deem it "somewhat important," a staggering 91% of organizations are prioritizing these capabilities.

Question: Which would you consider the most important or primary driver for your organization's storage strategy over the next 24 months?

Figure 15b: The Single Most Important Primary Driver of Storage Strategy



Key Insights

Security Leads as the Top Priority

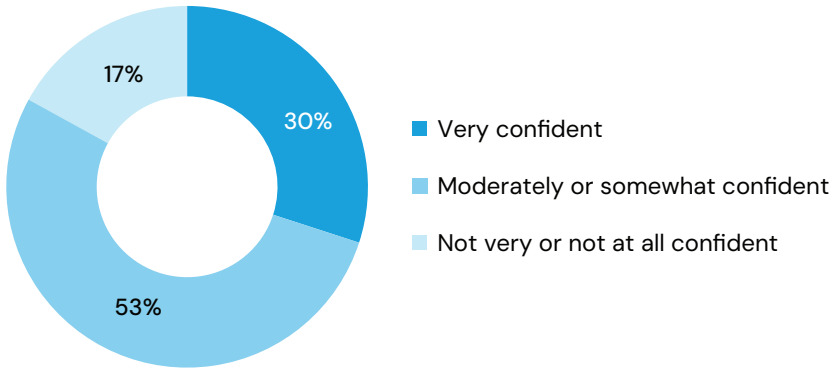
- Data security and governance is the most frequently cited primary driver, accounting for 25% of organizational focus.

Performance and Resilience Are Secondary Priorities With Similar Weight

- Performance (20%) and Cyber-resilience (19%) are the next most significant drivers.

Question: How confident are you in your organization's ability to recover from a major cyber-attack (e.g., ransomware) or loss of cloud-based data (e.g., cloud provider outage) with minimal downtime?

Figure 16: Confidence in Organizational Cyber Recovery Capabilities



Key Insights

Minority Achieving High Resiliency Confidence

- Only 30% of respondents feel very confident in their organization's recovery capabilities, suggesting that high-level operational maturity in cyber resiliency remains a challenge for the majority of the market.

Majority Cautious on Recovery Readiness

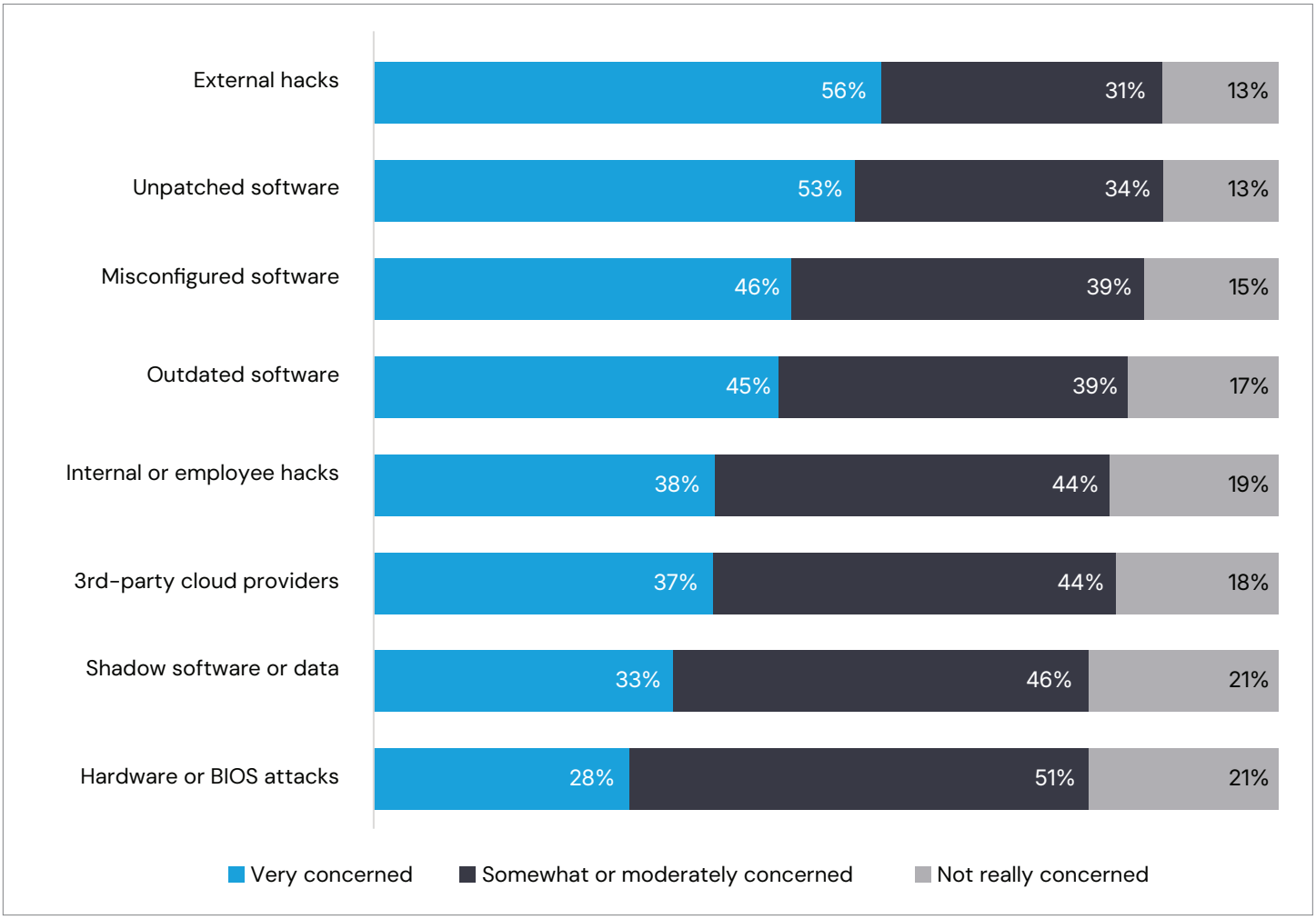
- Over half of the organizations (53%) report being only moderately or somewhat confident in their ability to recover from a major cyber-attack or cloud outage with minimal downtime, indicating a lack of total assurance in current disaster recovery protocols.

Significant Vulnerability Gap

- A notable 17% of organizations admit to being not very or not at all confident in their recovery speed, representing a segment of the market that views itself as highly vulnerable to significant downtime following a security breach or data loss event.

Question: Please rate your organization's level of concern regarding the following types of security threats:

Figure 17: Organizational Concern Levels for Types of Security Threats



Key Insights

Primary Concern for External Vectors

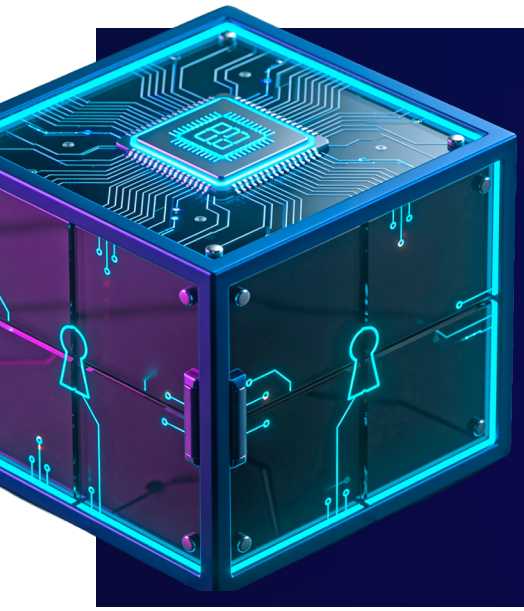
- External hacks represent the most acute security fear, with 56% of organizations reporting they are "Very concerned"—the highest individual concern rating in the dataset.

Risk Sensitivity to Software Hygiene

- Vulnerabilities arising from maintenance gaps are a major priority; both Unpatched software (53%) and Misconfigured software (46%) rank higher in high-level concern than internal employee hacks (38%) or 3rd-party cloud providers (37%).

Section 7

Backup, Recovery & SaaS Data Protection



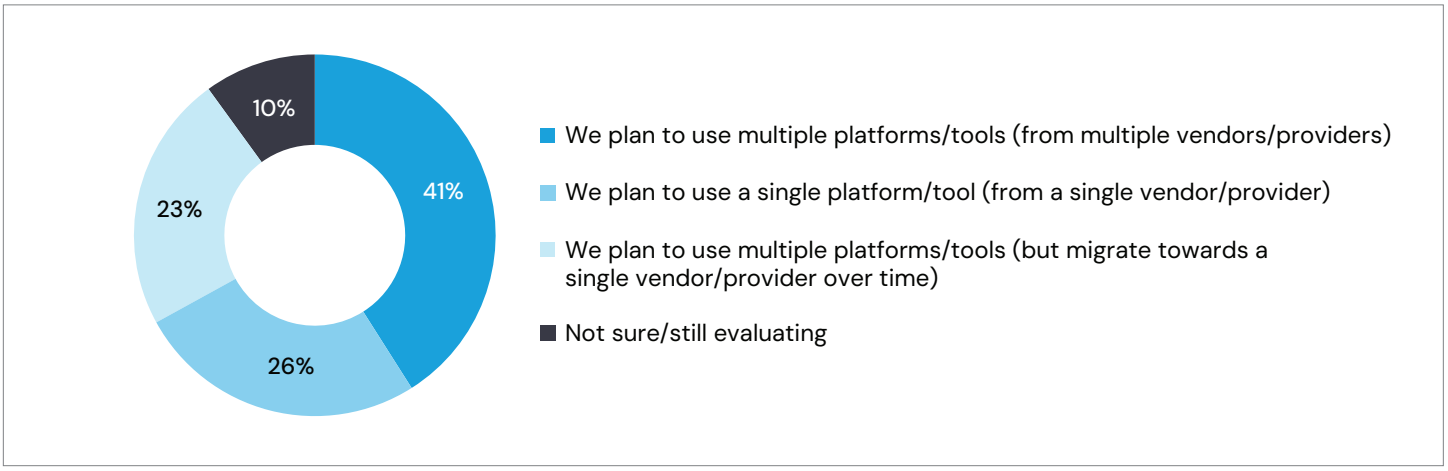
Highlights

41% of Microsoft 365 users plan to adopt a dual-protection strategy (native and immutable) within 24 months, marking the decline of native-only backup.

14% of organizations remain unsure of their specific SaaS backup methods, highlighting a persistent visibility gap despite the increased focus on resilience.

Question: Which of the following best describes your approach to managing storage, backup and recovery?

Figure 18a: Platform Preferences for Storage, Backup, and Recovery



Key Insights

Multi-vendor Dominance:

- A majority of enterprises (64%) rely on multiple vendors for the platforms and tools required to meet their storage, backup, and recovery needs (including a subset of 23% that eventually plan to migrate to a single vendor/platform).

Consolidation Trend

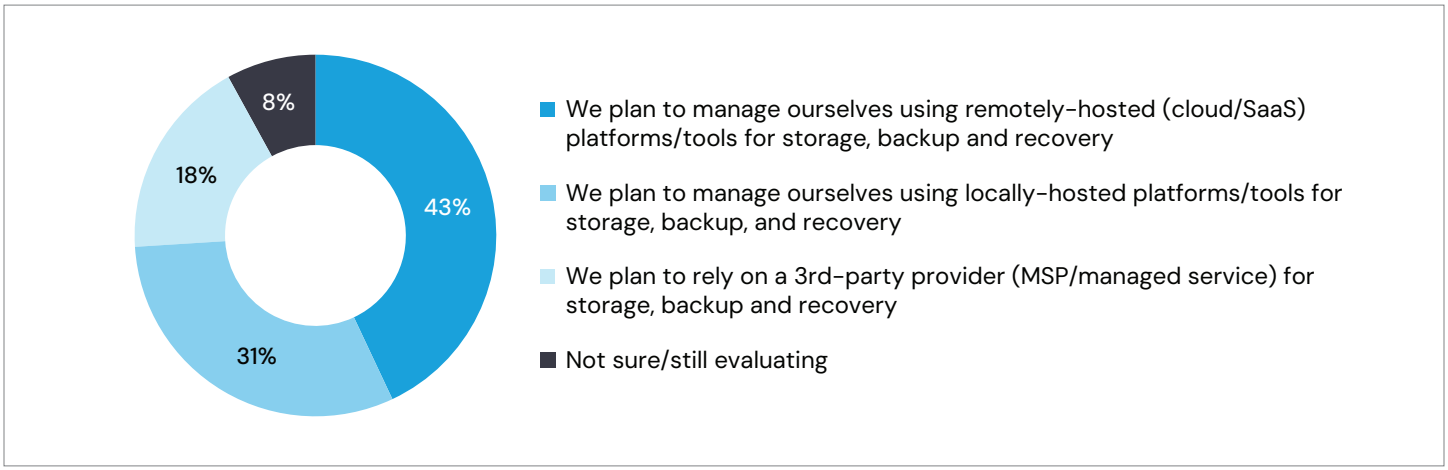
- Nearly half of all respondents (49%) either use a single vendor/ platform now or plan to migrate toward one in the future.

Strategic Uncertainty

- A small segment (10%) remains undecided and unsure how best to manage data storage, backup and recovery.

Question: Thinking about the next 24 months, what is your organization's primary approach to using or managing storage, backup and cyber recovery?

Figure 18b: Ownership of Storage, Backup, and Cyber Recovery Management (Next 24 Months)



Key Insights

The DIY Approach

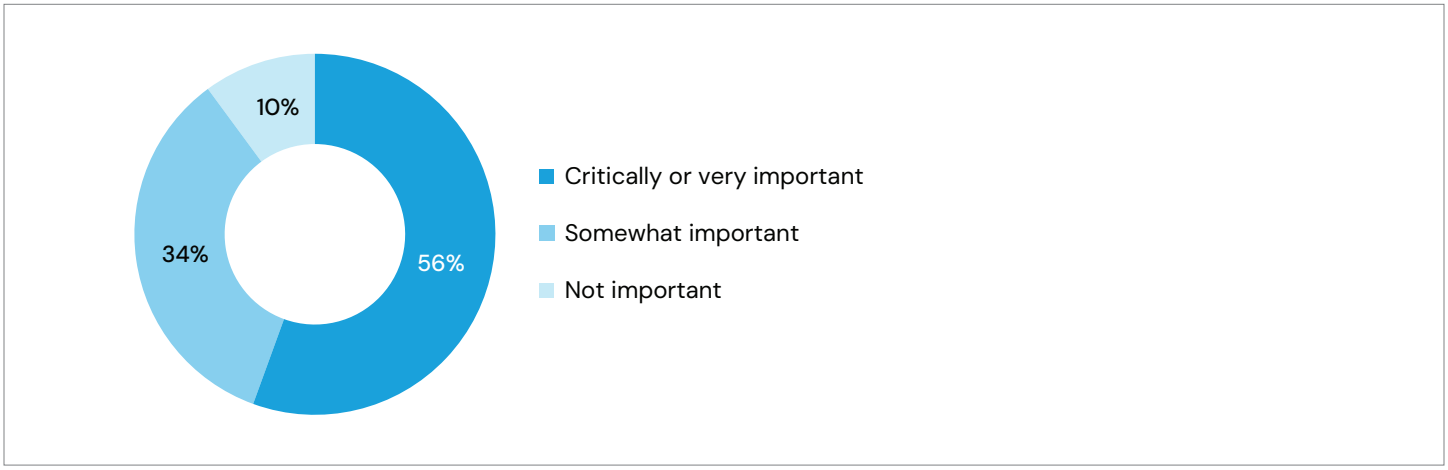
- 74% of organizations plan to manage storage, backup and recovery themselves, with a subset of 43% expecting to use cloud/SaaS offerings rather than locally-hosted platforms/ tools.

The Limited Role of MSPs

- Just 18% of organizations have opted to rely on 3rd-party MSPs (managed service providers) to oversee backup & recovery operations.

Question: How important is the use of immutable backups for SaaS applications to your organization's data resilience strategy?

Figure 19: Importance of Immutable Backups for SaaS Applications in Data Resilience Strategy



Key Insights

Critical Strategic Adoption

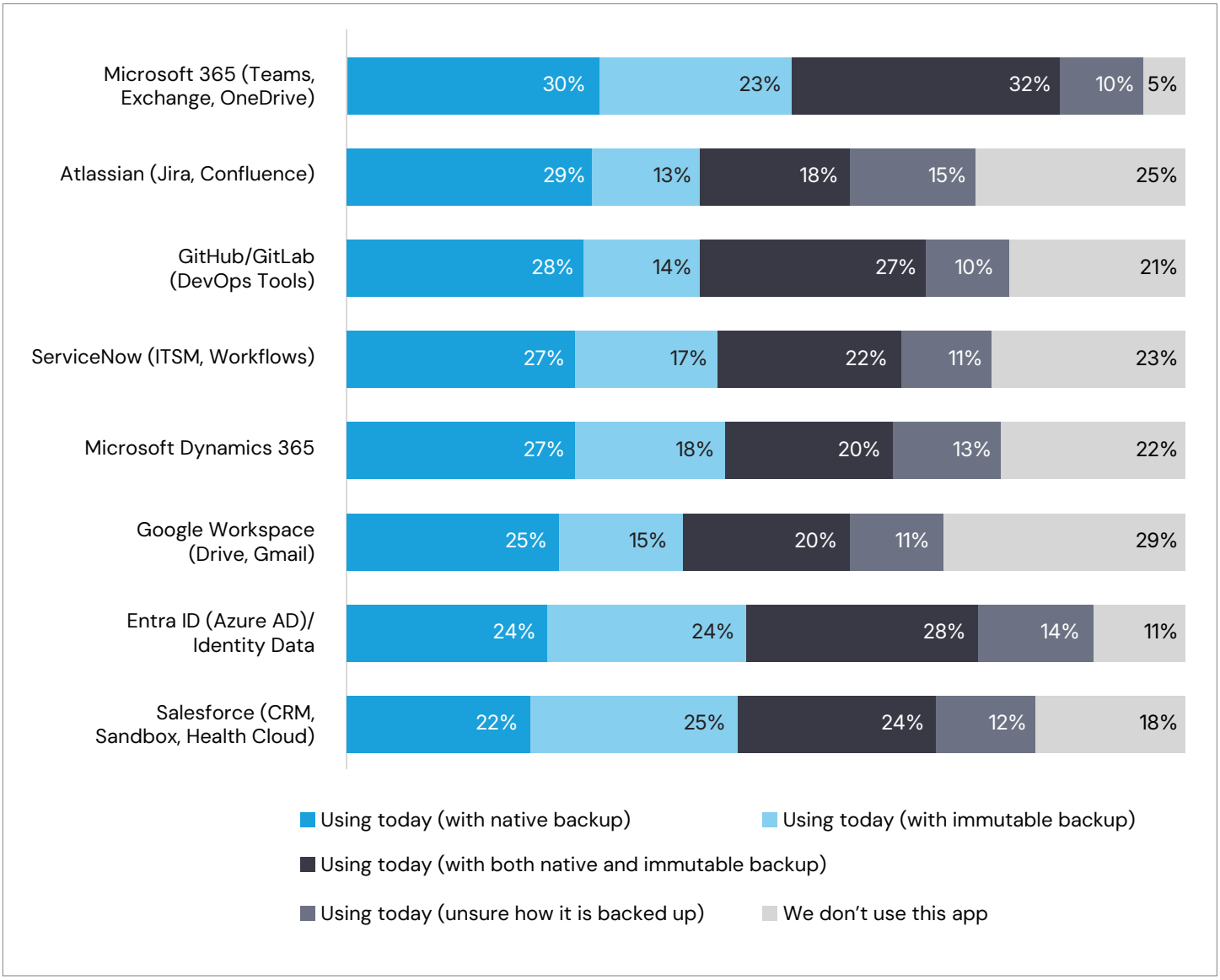
- A clear majority of organizations (56%) consider immutable backups for SaaS applications to be critically or very important to their data resilience strategy.

Broad Industry Consensus

- When including those who view it as "somewhat important," nearly 90% of respondents acknowledge the necessity of immutability in protecting SaaS-based data.

Question: Please indicate if your organization currently uses any of the following SaaS applications and whether you use native (in-app) or immutable (off-site) backups?

Figure 20: Native vs. Immutable Backups for SaaS Applications in Use Today



Key Insights

Most Frequently Deployed Applications

- Microsoft 365 (95%), Entra ID (89%) and Salesforce (82%) are the most frequently deployed applications (note: this is frequency and not breadth of deployment).

Significant Protection Gap

- Across all applications, a notable segment of users (ranging from 10% to 15%) are currently "unsure" how their data is being backed up, representing a potential risk in organizational data governance.

The Hybrid Approach

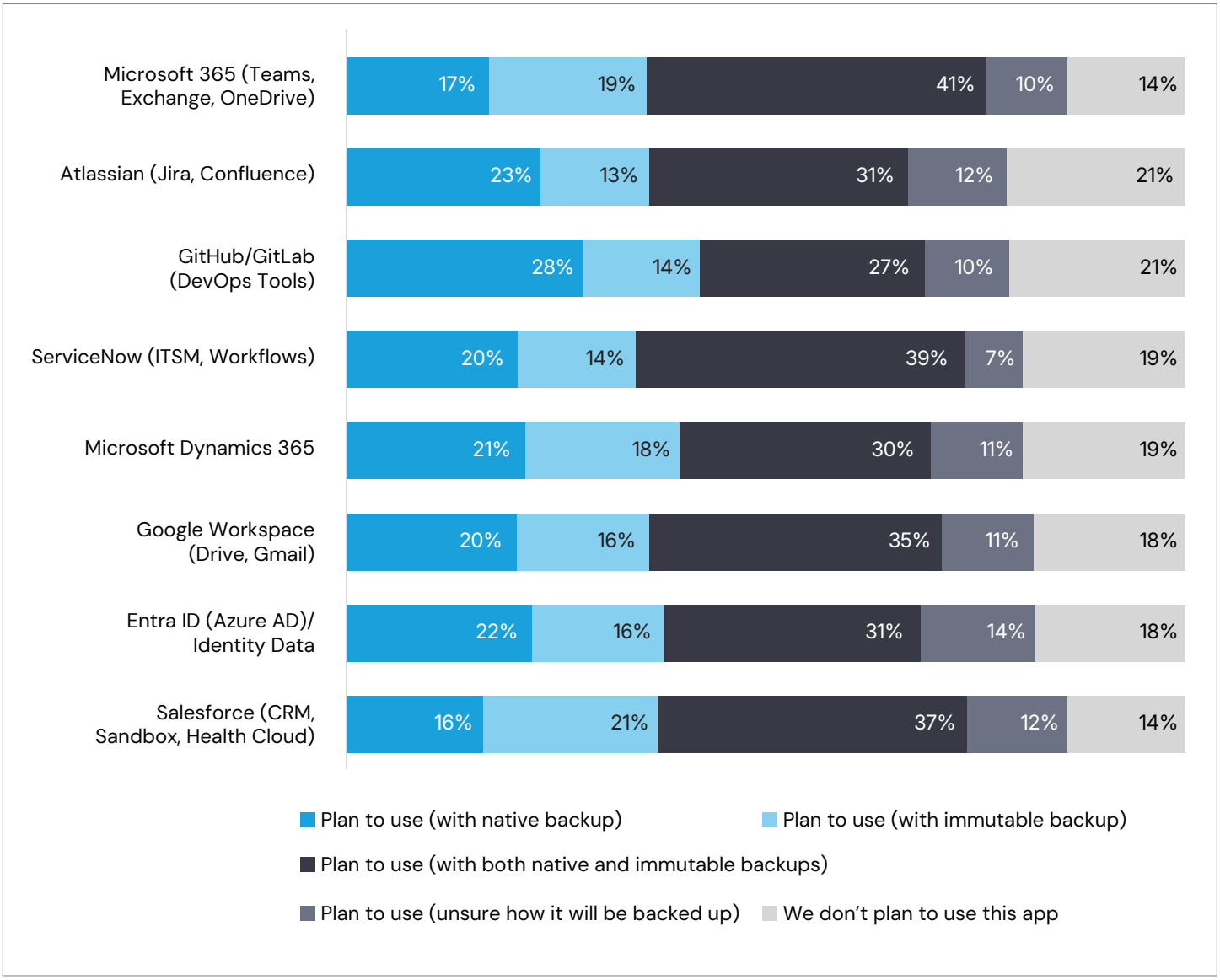
- The percent of applications backed up both natively and immutably ranges from a low of 18% (Atlassian) to a high of 32% (Microsoft 365).

Native vs Immutable

- Salesforce (25% vs 22%) and Entra ID (24% vs 24%) are the only two applications where pure immutable backups equal or surpass pure native backup.

Question: Thinking ahead 12-24 months, which of the following SaaS applications do you plan to use and how will they be backed up?

Figure 21: Planned SaaS Application Adoption and Projected Backup Strategies (12-24 Months)



Key Insights

Shift Toward Hybrid Protection:

- Over the next 12-24 months, the "both native and immutable" model becomes the dominant strategy, led by Microsoft 365 at 41% and ServiceNow at 39%.

Decreasing Native-Only Reliance

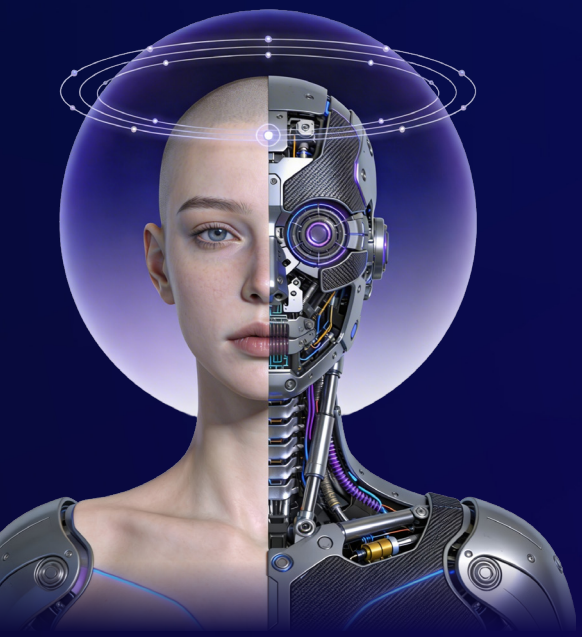
- Compared to current data, fewer organizations plan to rely solely on native backups, with Microsoft 365 seeing a drop to 17% and Salesforce falling to 16%.

Persistent Knowledge Gap

- Despite the strategic shift, roughly 7% to 14% of organizations across all SaaS applications are still "unsure" of their backup method in the coming two years.

Section 8

Observability & Operational Maturity



Highlights

46% of organizations utilize 2–3 different stand-alone monitoring tools. This represents the most common operational state, where teams remain reliant on multiple platforms rather than a unified solution.

26% of organizations cite alert fatigue as their top operational pain point for outage and performance issues.

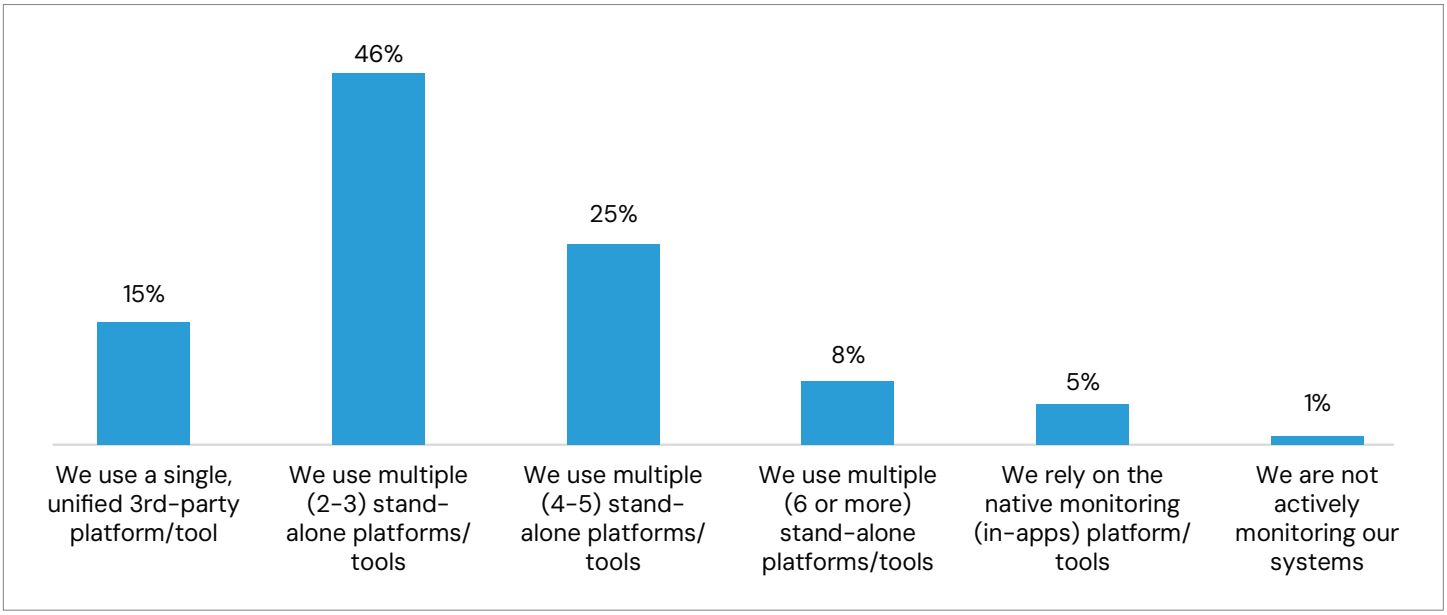
71% of organizations lack deep integration between observability and CI/CD. The vast majority of teams are operating without a seamless connection between observability tools with CI/CD and deployment workflows.

15% of organizations have achieved a single, unified observability view. Despite the move toward more complex workloads, a very small fraction of the market has successfully centralized their monitoring.

21% of organizations have fully implemented AIOps for key functions. While strategic interest is high, only one-fifth of the market has reached a level of high maturity by deeply embedding AI into operations.

Question: How would you describe your organization's primary approach to monitoring and observability today?

Figure 22: Platform/Tool Preferences for Monitoring and Observability



Key Insights

Pervasive Tool Fragmentation

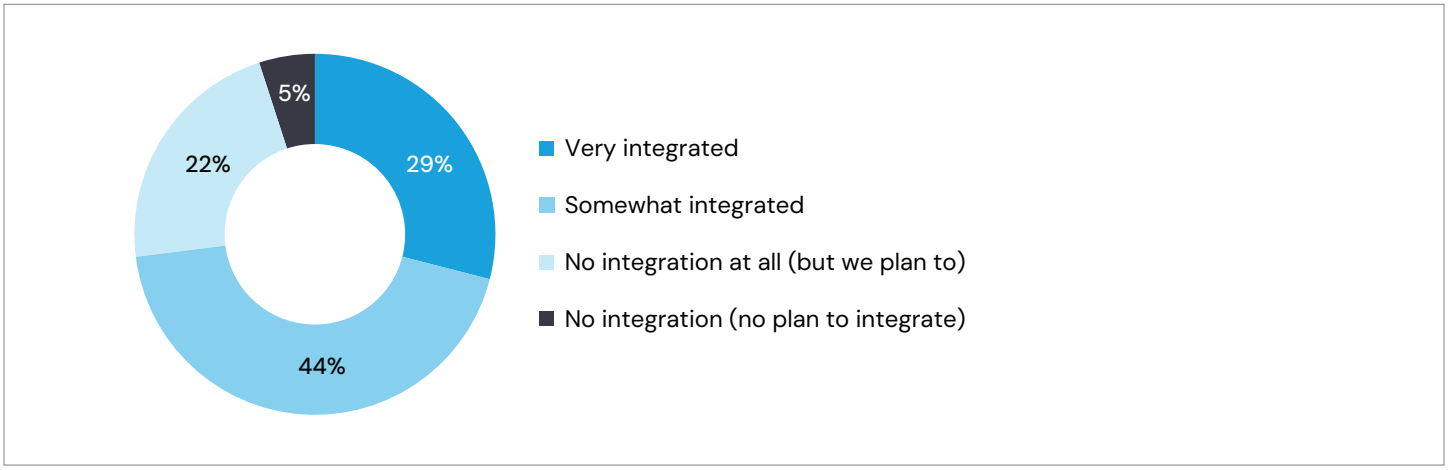
- 79% of organizations operate with multiple monitoring platforms. The vast majority of environments are managed through 2 or more stand-alone tools rather than a consolidated system.

Limited Unified Maturity

- Only 15% have achieved a single, unified observability view. Despite the complexity of enterprise workloads, only a small fraction of organizations has successfully centralized their monitoring into one primary platform.

Question: How well-integrated are your observability tools with your CI/CD and deployment workflows?

Figure 23: Current Level of Integration Between Observability Tools and CI/CD Workflows



Key Insights

Widespread Integration Gaps

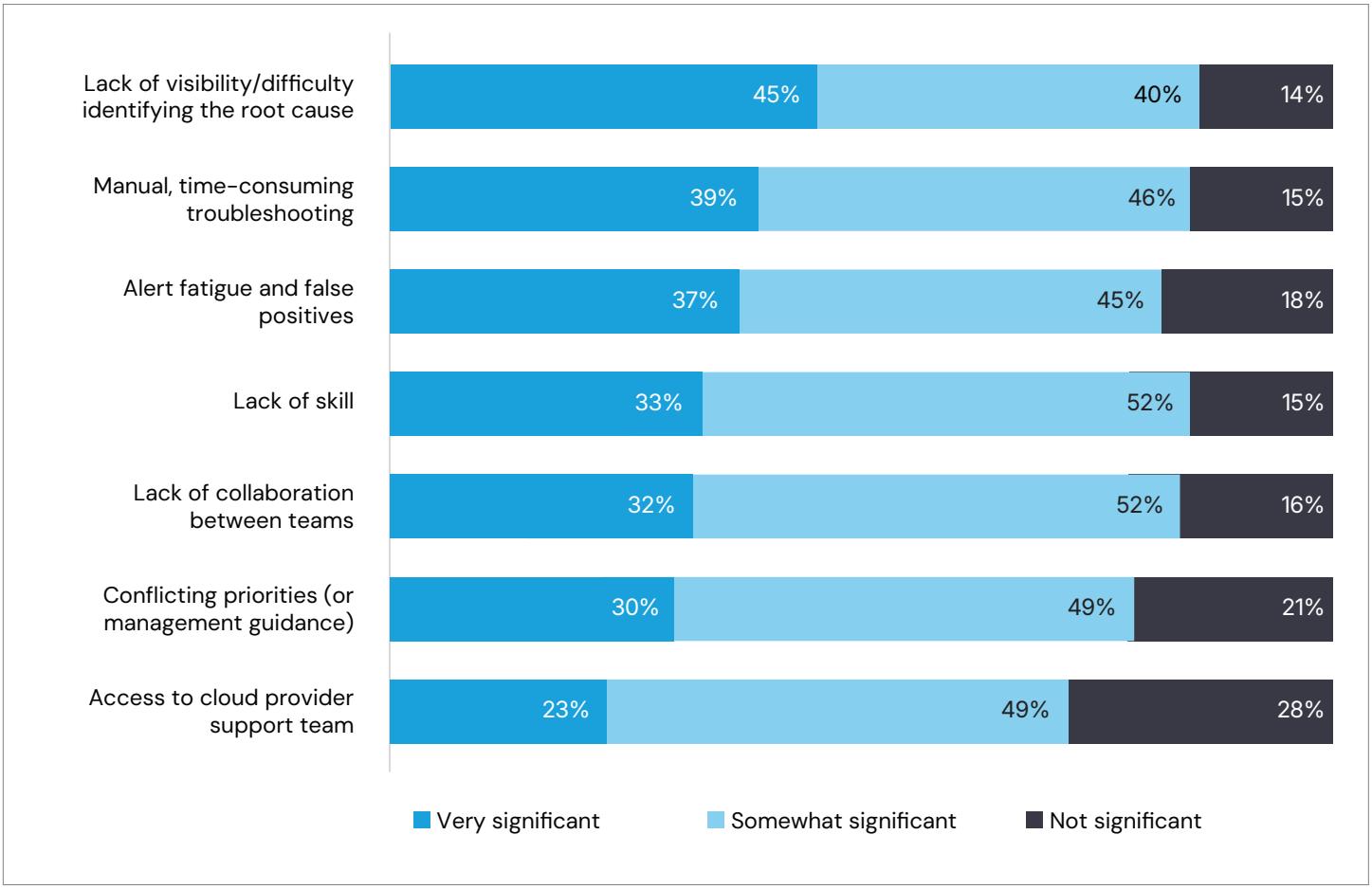
- 71% of organizations lack deep integration between observability and CI/CD. While most have some connection, less than a third of companies have achieved a "very integrated" state for their deployment workflows.

Intentional Future Migration

- 22% of organizations currently have no integration but plan to implement it.

Question: How significant a pain point are the following for your IT teams when responding to an outage or performance issue?

Figure 24a: Significance of Challenges Faced by IT Teams During Outages and Performance Issues



Key Insights

Primary Visibility Barriers

- 85% of organizations struggle with identifying the source of outages. Lack of root cause visibility is the most acute pain point, with 45% of respondents classifying it as a "very significant" hurdle to effective response.

Manual Effort Constraints

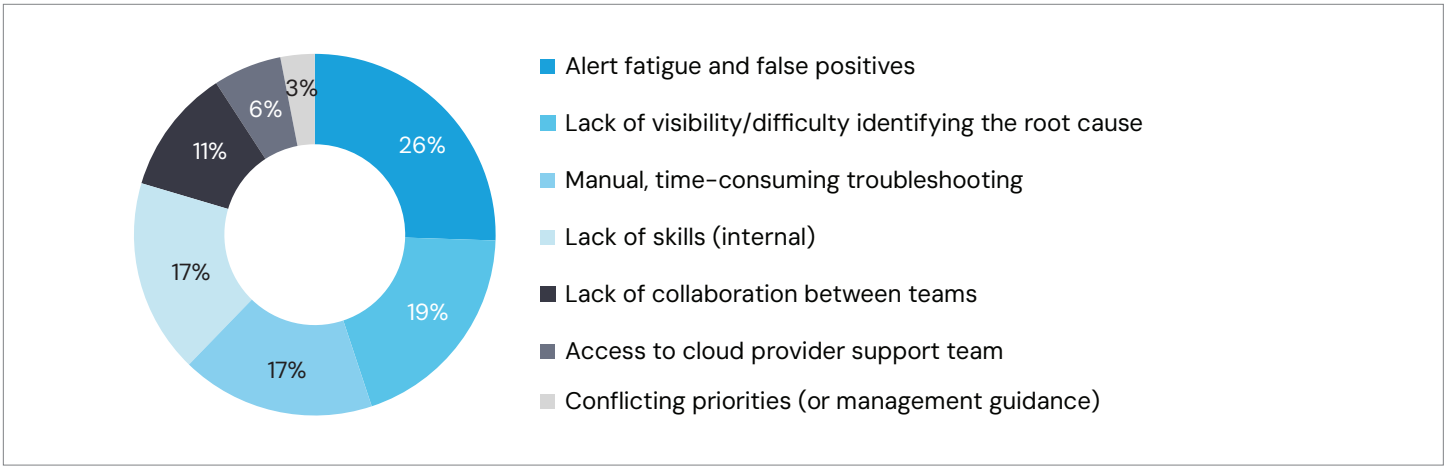
- 85% of teams are hindered by non-automated recovery processes. Manual, time-consuming troubleshooting remains a near-universal bottleneck.

People and Process Friction

- Over 80% of respondents cite skill gaps and poor collaboration as major stressors. These human-centric factors are nearly as disruptive as technical ones, suggesting that tool adoption alone cannot resolve maturity gaps without addressing talent and team silos.

Question: Which of the following pain points is the most significant (when responding to an outage or performance issue)?

Figure 24b: Most Significant Pain Point Impacting IT Response to Outages and Performance Issues



Key Insights

Dominant Alert Fatigue

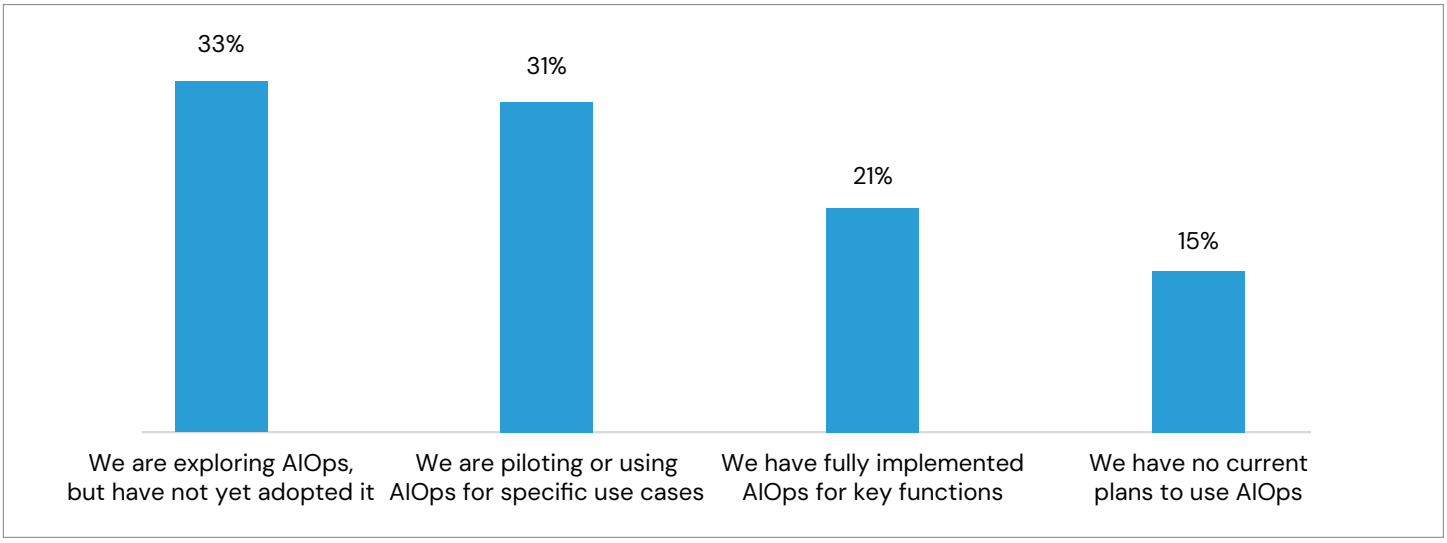
- 26% of organizations identify alert fatigue and false positives as their primary challenge. This is the leading operational burden, outranking visibility gaps and manual labor.

Visibility and Manual Troubleshooting Parity

- 19% and 17% of respondents prioritize root cause visibility and manual troubleshooting respectively. These two technical hurdles combined represent over a third of the market's primary pain points.

Question: To what extent does your organization use AI for IT Operations (AIOps)?

Figure 25: Extent of AIOps Adoption within Organizations at present



Key Insights

Pre-Adoption Exploration Phase

- 33% of organizations are researching AIOps without active deployment, indicating a high level of interest that has not yet translated into technical implementation.

Limited Use Case Focus

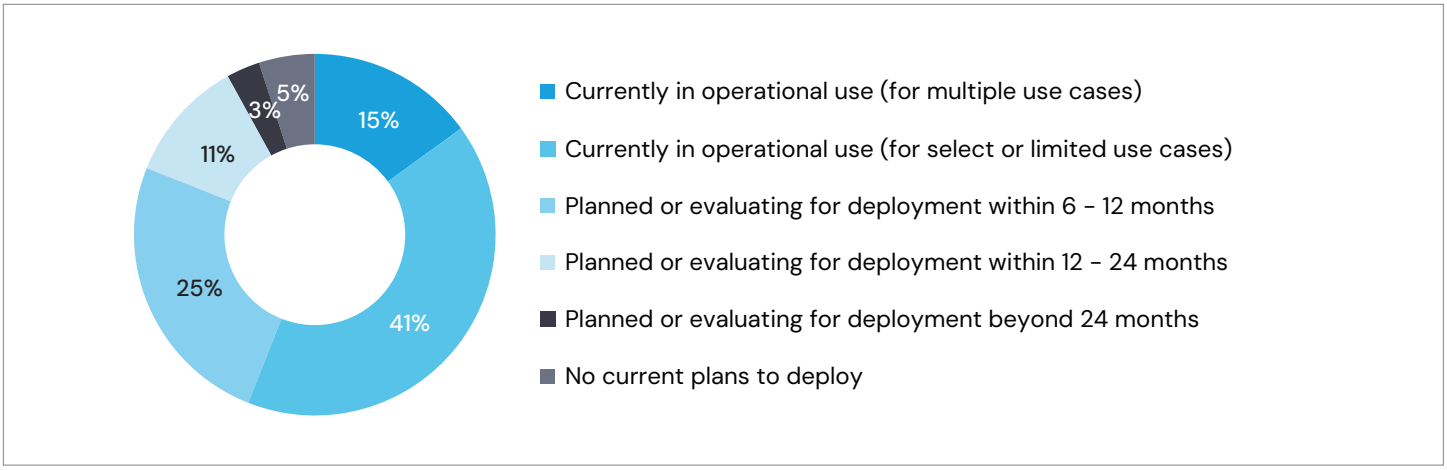
- 31% of respondents are currently piloting or using AIOps for specific tasks.

Minority Full Implementation

- Only 21% of organizations have fully implemented AIOps for key functions. While interest is widespread, only about one-fifth of respondents have reached high operational maturity.

Question: Which of the following best describes your organization's use of AI technologies (AIOps) for suggesting and automating next best actions in operational settings?

Figure 26: Current and Planned Adoption of AIOps for Operational settings



Key Insights

Widespread Adoption of AIOps

- Over half of organizations (56%) currently use AIOps to help manage operational decisions, a subset (of 41%) still limit the use of AIOps to select use cases rather than full-scale deployment.

Imminent Implementation Surge

- 25% of organizations are anticipating deployments and/or evaluations of AIOps within the coming 12 months as the AIOps market nears market saturation (projecting 81% of all organizations will be using, deploying or evaluating AIOps within 12 months).

Near-Universal Interest

- 95% of organizations have AIOps in their current or future plans. While 14% don't anticipate completing evaluations and deployments for at least one or more years, only 5% of organizations have made the decision that AIOps will not be part of their future operations.

Section 9

Talent & Skills Gaps

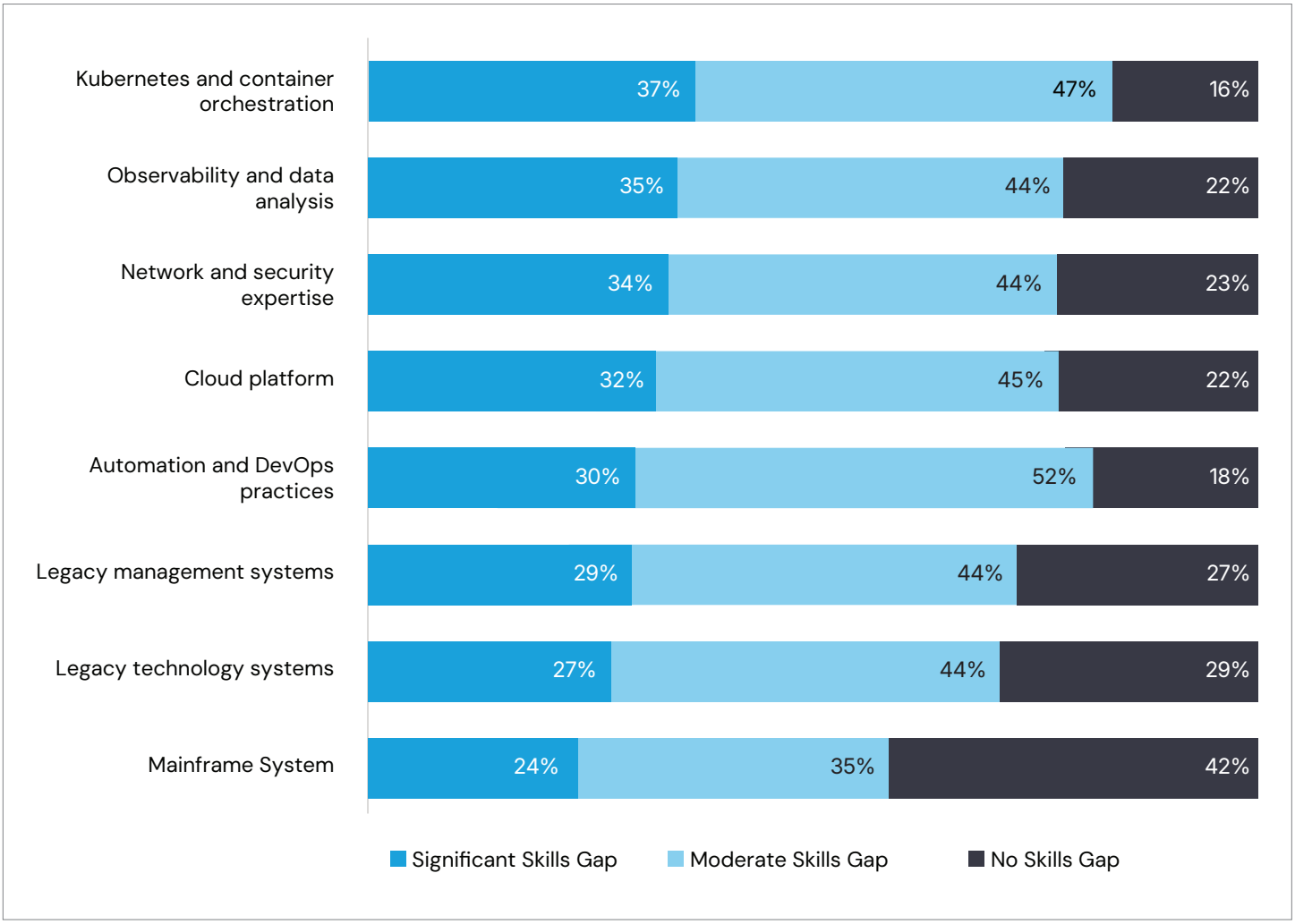
Highlights

37% of organizations face a significant skills gap in Kubernetes, representing the most acute talent shortage in modern infrastructure, whereas legacy Mainframe systems show the highest readiness with a 42% “No Skills Gap” rating.

33% of organizations identify network and security expertise as the single most challenging hurdle to overcome, surpassing the difficulty of managing legacy systems, which are viewed as a top challenge by only 4% of respondents.

Question: How significant a skills gap does your organization face in each of the following?

Figure 27a: Significance of skills gaps across key areas



Key Insights

Primary Skills Gap in Modern Infrastructure

- Kubernetes and container orchestration represents the most acute talent shortage, with 37% of organizations reporting a "Significant Skills Gap"—the highest across all surveyed categories.

Widespread Proficiency Deficit in Automation

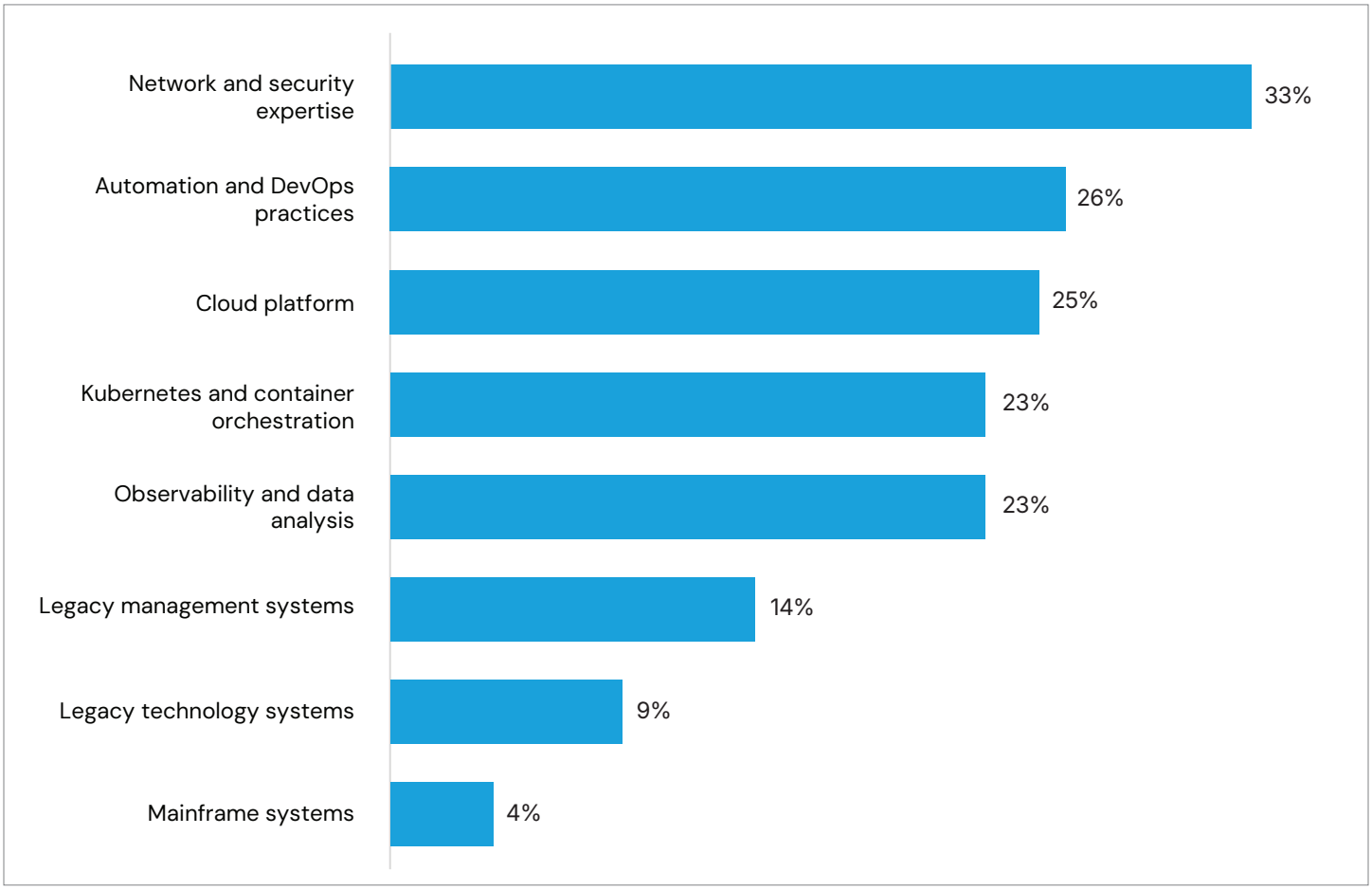
- Automation and DevOps practices face the most common hurdle, with over half of respondents (52%) reporting a "Moderate Skills Gap," indicating that while most teams have some capability, they lack full proficiency.

Legacy vs. Modern Skills Disparity

- Organizations report much higher readiness for older technologies compared to new ones; Mainframe Systems have the highest "No Skills Gap" rating at 42%, nearly triple the gap-free rate for Kubernetes (16%).

Question: Which of the following skills gaps would you consider to be the most significant or challenging to overcome?

Figure 27b: Most Significant Challenges to Overcome



Key Insights

Security and Networking as the Primary Obstacle

- Network and security expertise is identified as the single most challenging hurdle to overcome, cited by 33% of organizations.

Persistent Friction in Automation Adoption

- Despite being a core pillar of modern I&O, Automation and DevOps practices are ranked as the second most significant challenge (26%).

Lower Resistance from Legacy Environments

- Organizations find legacy systems significantly easier to manage or transition from compared to modern stacks; Mainframe systems are considered a top challenge by only 4% of respondents, the lowest in the dataset.

Section 10

Vendor Strategy & Software Deployment

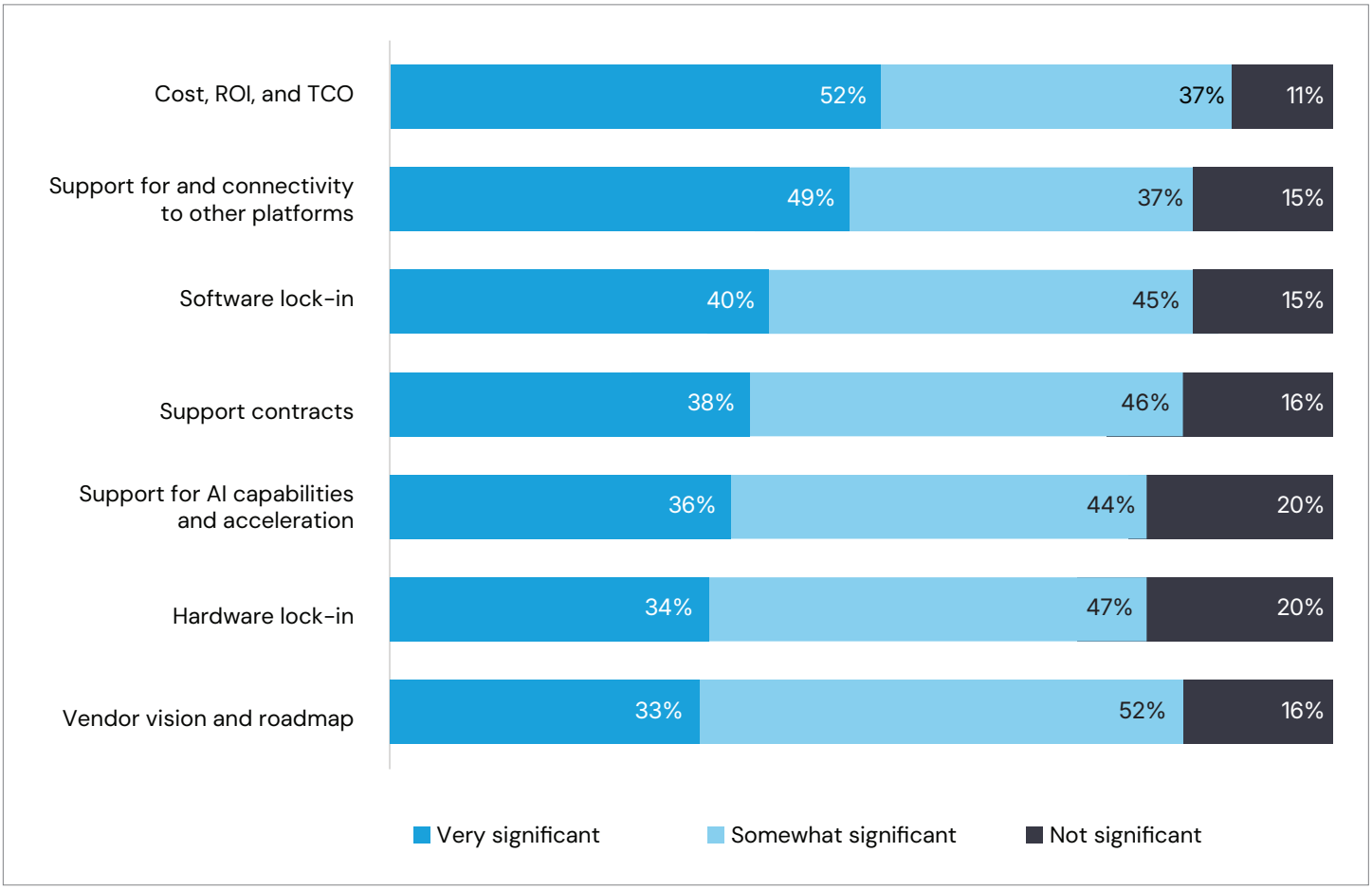
Highlights

52% of decision-makers prioritize Cost, ROI, and TCO as the most significant factor in vendor selection, yet 85% of organizations also consider the vendor's vision and roadmap a key influential driver.

49% of organizations currently rely on proprietary custom software as their primary deployment type, but a major shift is expected within 24 months, as 49% of firms project that Commercial off-the-Shelf (COTS) solutions will become their most widely deployed software.

Question: How significant are the following in influencing decisions on infrastructure procurement and/or vendor selection?

Figure 28: Significance of factors Influencing Infrastructure Procurement and Vendor Selection



Key Insights

Financial Performance as the Primary Driver

- Cost, ROI, and TCO (Total Cost of Ownership) is the most critical factor for decision-makers, with 52% of organizations labeling it as "Very significant"—the highest percentage in that category across all surveyed factors.

Prioritization of Interoperability

- Support for and connectivity to other platforms is the second most influential factor, with nearly half (49%) of respondents considering it very significant.

Widespread Consideration of Vendor Strategy

- While "Vendor vision and roadmap" has the lowest "Very significant" rating (33%), it carries the highest aggregate influence when including "Somewhat significant" responses (85% total), indicating that long-term vendor strategy is a factor in the vast majority of procurement cycles.

Question: Which of the following best describes your organization's approach to managing your IT infrastructure?

Figure 29: Ownership of IT Infrastructure Management

Key Insights

Prevalence of Hybrid Management Models

- The most common approach to IT infrastructure is a balanced partnership, with 29% of organizations utilizing an even mix of 3rd-party managed service providers and internal teams.

Significant External Provider Dependency

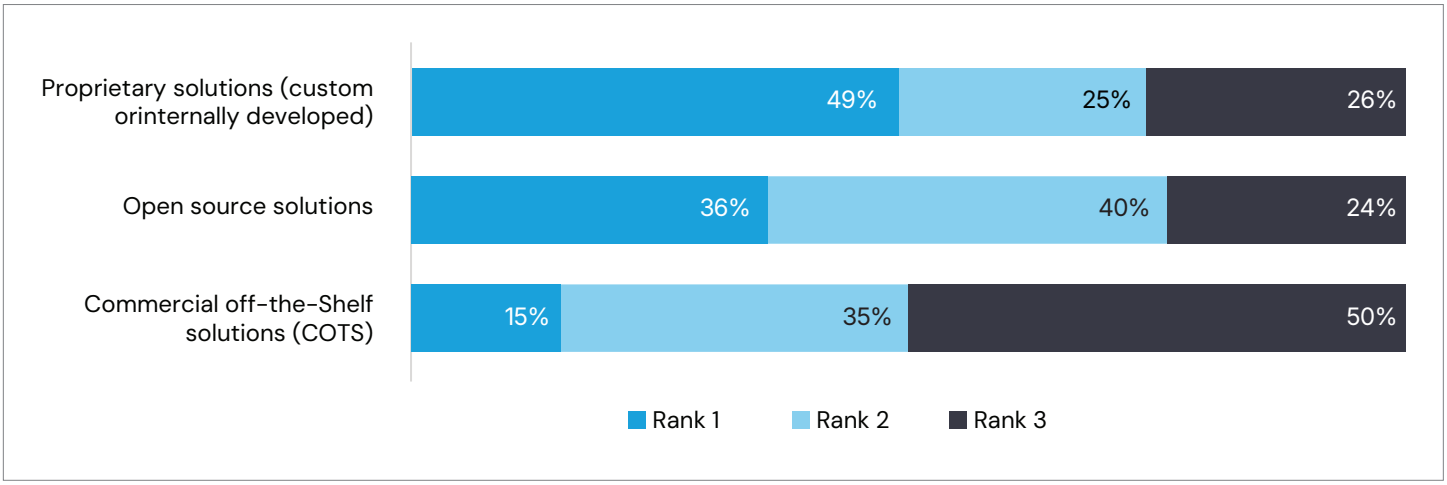
- 24% of organizations primarily use 3rd-party managed service providers with only some internal support, with an additional 13% using only 3rd-party providers.

Internal-First Resource Gap

- While 21% of organizations primarily use internal teams with some 3rd-party support, only a small minority of 12% operate using internal teams exclusively without any external service provider assistance.

Question: Please rank the most to least common type of software currently deployed within your organization's IT infrastructure:

Figure 30: Ranking of Software Types Currently Deployed in IT Infrastructure



Key Insights

Custom Software Leads the Way

- Proprietary solutions (custom or internally developed) are ranked as the top most common type of software deployed, with nearly half (49%) of organizations citing it as the most commonly deployed type of software within IT infrastructure.

Open Source as a Strong Secondary Approach

- Open source solutions maintain a significant presence in the ecosystem, ranked as the top choice for 36% of organizations and the most frequent "Rank 2" selection at 40%.

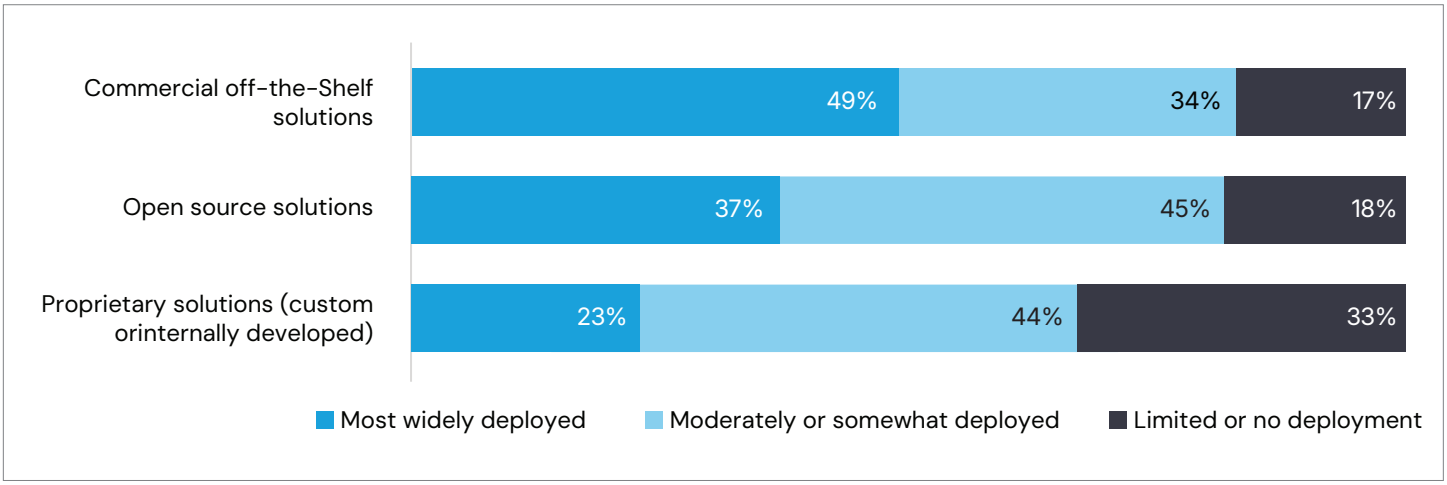
COTS as a Supplementary Layer

- Commercial off-the-shelf solutions (COTS) are the least likely software category to be the ranked as the most commonly deployed (cited by only 15% of organizations today).

.

Question: How widely deployed do you expect COTS, Open Source, or Proprietary software to be within 12-24 months from now?

Figure 31: Expected Deployment Levels of Software Types Over the Next 12–24 Months



Key Insights

Aggressive Growth for Commercial Solutions

- Commercial off-the-Shelf solutions are projected to be the most commonly deployed software category over the next two years, with nearly half (49%) of organizations expecting them to be "Most widely deployed."

Open Source as a Core Secondary Standard

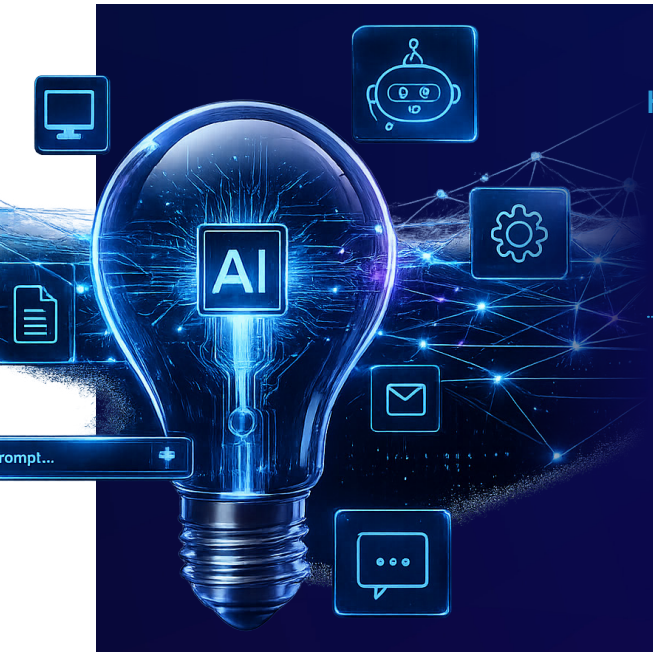
- Open source solutions maintain strong momentum, with 82% of organizations expecting at least moderate to wide deployment.

Shift Away from Custom Development

- Proprietary solutions (custom or internally developed) show the weakest outlook; they are the least likely to be "Most widely deployed" (23%) and the most likely to see "Limited or no deployment" (33%) compared to other solutions categories.

Section 11

AI Adoption & Governance Readiness



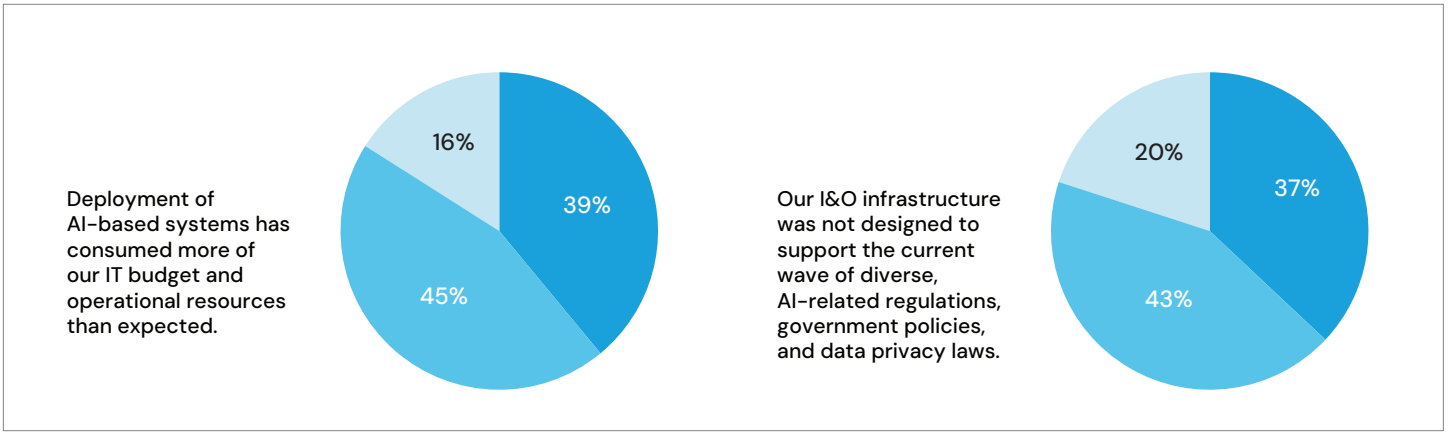
Highlights

84% of organizations report that AI deployment has consumed more budget and operational resources than originally planned.

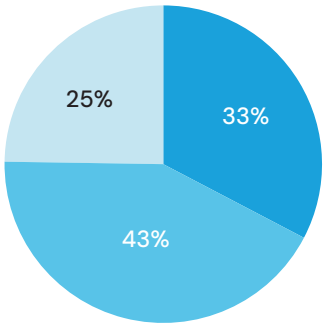
30% of organizations identify the EU AI Act as their primary governance driver, making it the most influential regulatory framework globally, ahead of U.S. Federal Policy (25%) and Sector-Specific rules (21%).

Question: Please state if you agree or disagree with the following on the impact of AI on IT budgets, implementations and/or innovation:

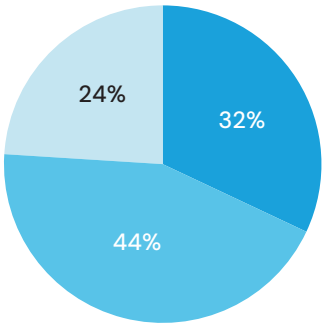
Figure 32: Impact of AI on IT Budgets and Innovation



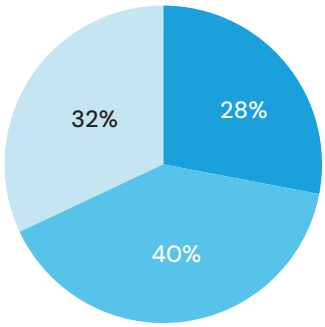
We are increasing on-premises or localized data processing to comply with privacy/ sovereignty mandates.



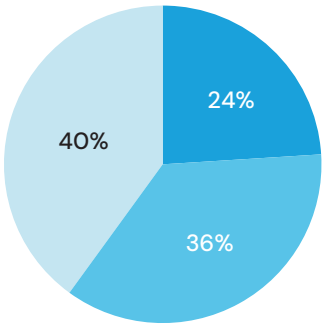
We have moved away from 'black-box' models toward vendors offering greater explainability and technical documentation.



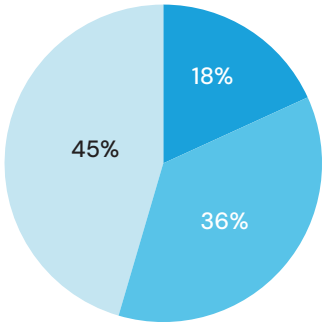
We have paused or delayed AI features to conduct mandatory 'High-Risk' assessments or bias audits.



We have established an internal AI Ethics Committee or 'Human-in-the-loop' protocols specifically to meet legal requirements.



Our pace of IT implementation and/or innovation has remained unchanged.



- Strongly agree
- Somewhat or moderately agree
- Don't really agree

Key Insights

Unforeseen Budgetary and Resource Strain

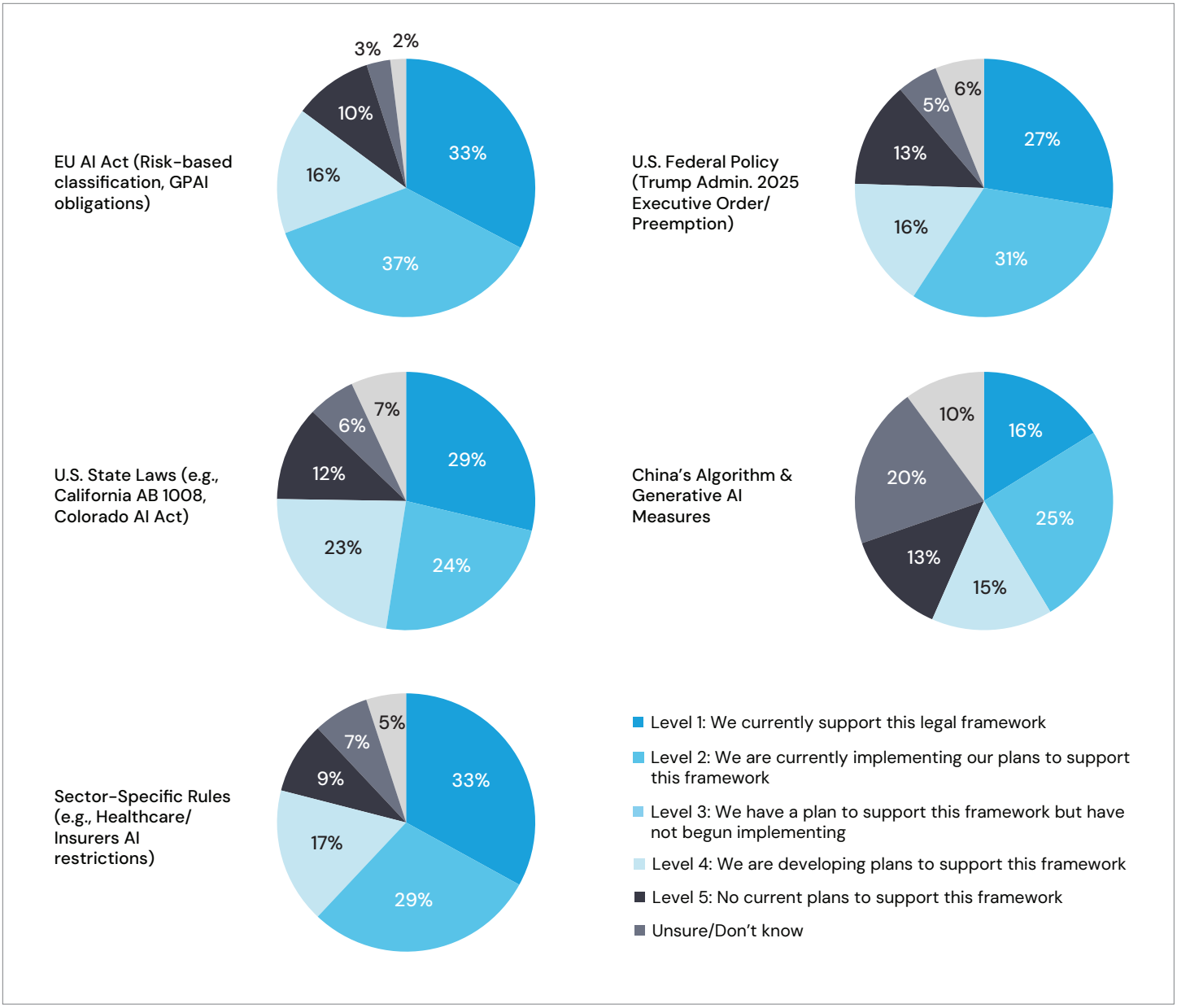
- AI deployment costs can be unpredictable as 84% confirm that the costs of deploying AI have been higher than expected.

Infrastructure Readiness Gap

- Current I&O infrastructure is struggling to keep pace with the regulatory landscape; 37% of respondents strongly agree that their systems were not designed to support the current wave of diverse AI-related regulations and data privacy laws.

Question: Which of the following best describes your organization's readiness to support the following AI regulatory frameworks?

Figure 33a: Organizational Readiness to support various AI Regulatory Frameworks



Key Insights

Leading Readiness for EU Standards

- Organizations demonstrate the highest level of preparation for the EU AI Act, with 33% reporting they are fully prepared and an additional 37% currently implementing necessary framework.

Lagging Compliance for Chinese Standards

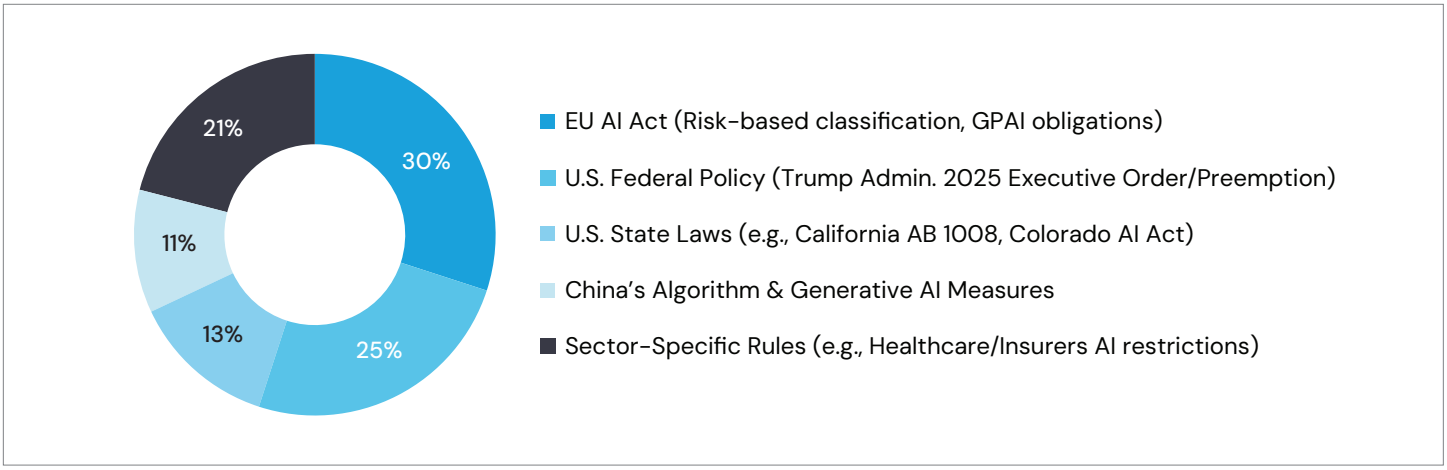
- Readiness for China's Algorithm & Generative AI Measures is the lowest among all surveyed frameworks, with 20% of organizations stating they are not prepared at all and 10% respondents unsure/don't know.

Sector-Specific Readiness Leads Federal Policy Preparedness

- While 33% of organizations feel fully prepared for sector-specific rules (e.g., healthcare/insurance), preparation for U.S. federal policy trails slightly behind, with only 27% having reached full readiness status.

Question: Which one framework best aligns with or would be considered the most important (primary) driver of your organization's AI governance strategy?

Figure 33b: Primary Regulatory Framework Guiding AI Governance Strategy



Key Insights

EU AI Act as the Primary Global Drive

- The EU AI Act is identified as the most significant influence on AI governance, with 30% of organizations citing it as the primary driver of their strategy—the highest among all listed frameworks.

Significant Impact of U.S. Federal Policy

- U.S. Federal Policy (Trump Admin. 2025 Executive Order) serves as a critical secondary driver, acting as the lead guiding framework for 25% of surveyed organizations.

Prioritization of Industry-Specific Regulation

- Sector-Specific Rules (e.g., Healthcare and Insurance restrictions) are considered more influential than regional mandates like U.S. State Laws (13%) or China's measures (11%), with 21% of organizations prioritizing them for their governance strategy.

Section 12

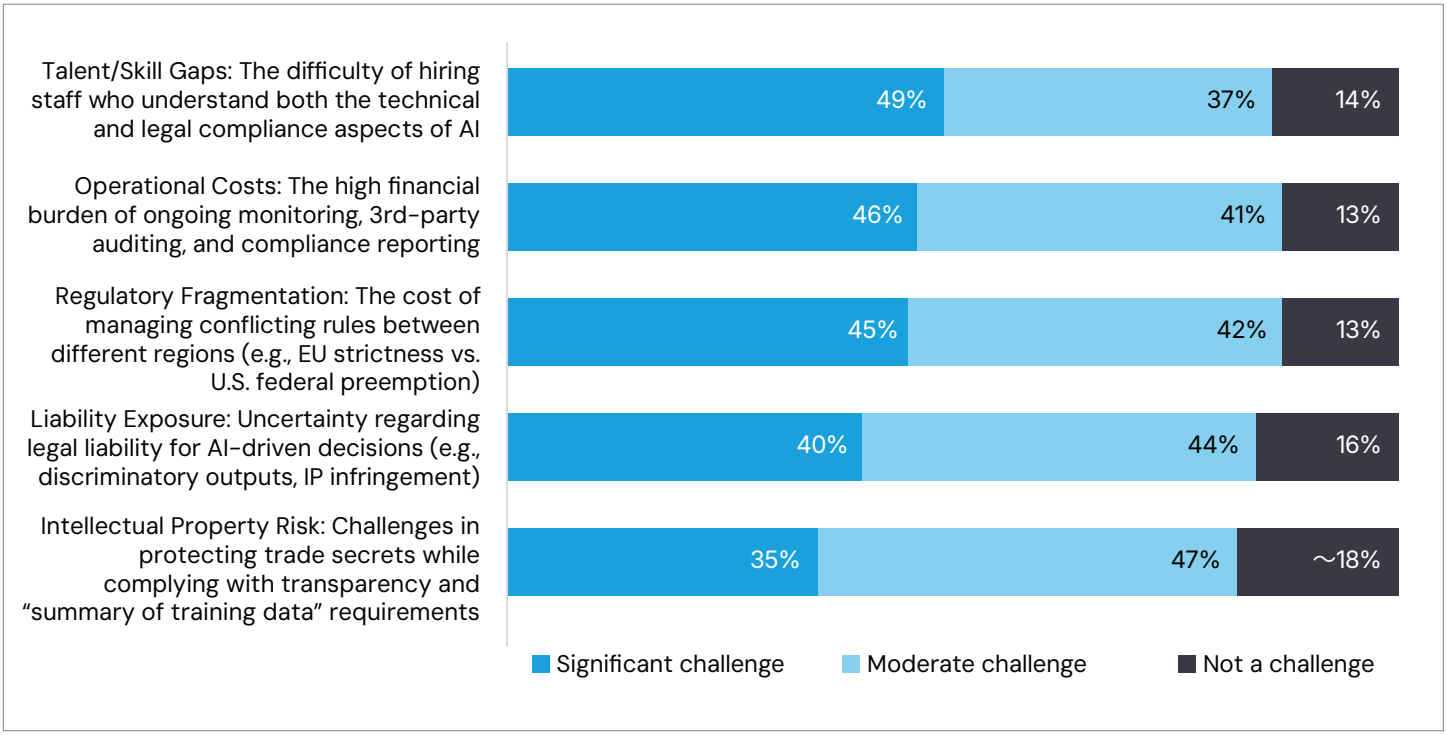
AI Risk Barriers & Competitive Constraints

Highlights

49% of organizations face a significant talent barrier in hiring staff who possess dual expertise in both technical AI development and legal compliance, which is cited as the single most challenging hurdle to overcoming regulatory-driven risks.

Question: How significant a challenge or barrier are the following regulatory-driven risks to your organization's ability to develop and maintain a competitive AI advantage?

Figure 34a: Significance of Regulatory-Driven Risks to AI Competitive Advantage



Key Insights

Critical Shortage of Dual-Expertise

- Talent/Skill Gaps represent the most severe barrier to AI competitiveness, with 49% of organizations identifying the difficulty of hiring staff who understand both technical and legal compliance as a "Significant challenge."

High Operational and Compliance Burden

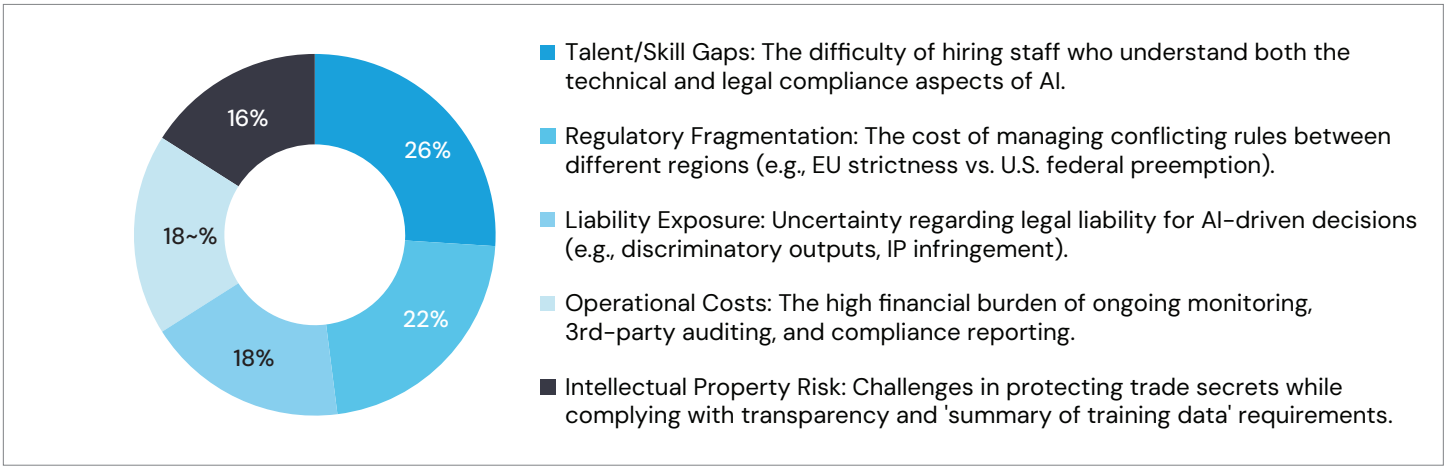
- Financial and structural hurdles are widespread, as 46% of respondents cite Operational Costs (monitoring and auditing) and 45% cite Regulatory Fragmentation (regional rule conflicts) as significant challenges to maintaining an AI advantage.

Widespread Intellectual Property Concerns

- While Intellectual Property Risk has the lowest "Significant challenge" rating (35%), it commands the highest aggregate concern, with 82% of organizations viewing the challenge of protecting trade secrets while meeting transparency requirements as a significant or moderate barrier.

Question: Which of the barriers or risks you identified above is the most significant or challenging to overcome (to maintain a competitive AI advantage)?

Figure 34b: Most Challenging Regulatory Barriers or Risks Impacting AI Competitive Advantage



Key Insights

Talent Shortage as the Top Impediment

- Talent/Skill Gaps are identified as the single most challenging barrier to overcome, with 26% of organizations struggling to find staff who possess the necessary blend of technical AI knowledge and legal compliance expertise.

High Friction from Policy Inconsistency

- Regulatory Fragmentation is the second most significant hurdle, cited by 22% of respondents as the most challenging risk to manage due to the costs associated with navigating conflicting regional rules.

Parity in Liability and Operational Burdens

- Organizations view Liability Exposure and Operational Costs as equally difficult obstacles, with 18% of respondents for each category ranking them as their primary concern, overshadowing the risk to Intellectual Property (16%).

Section 13

Methodology & Demographics

Highlights

25% of participants serve as Strategic Owners and another 25% as Decision Leads, while 23% act as Technical Sponsors, ensuring a high level of decision-making authority across the sample.

The survey captures a truly global perspective from 520 respondents, with an almost even split across **EMEA (26%)**, **North America (25%)** and **APAC (25%).**

While leadership is distributed across titles, the highest concentration of functional roles is found in **Information Technology (30%)**, **Operations (28%)**, and **Information Security (20%)**, highlighting a strong focus on technical infrastructure and delivery.

Figure 35: Stakeholder involvement and responsibilities in organization's overall I&O ecosystem

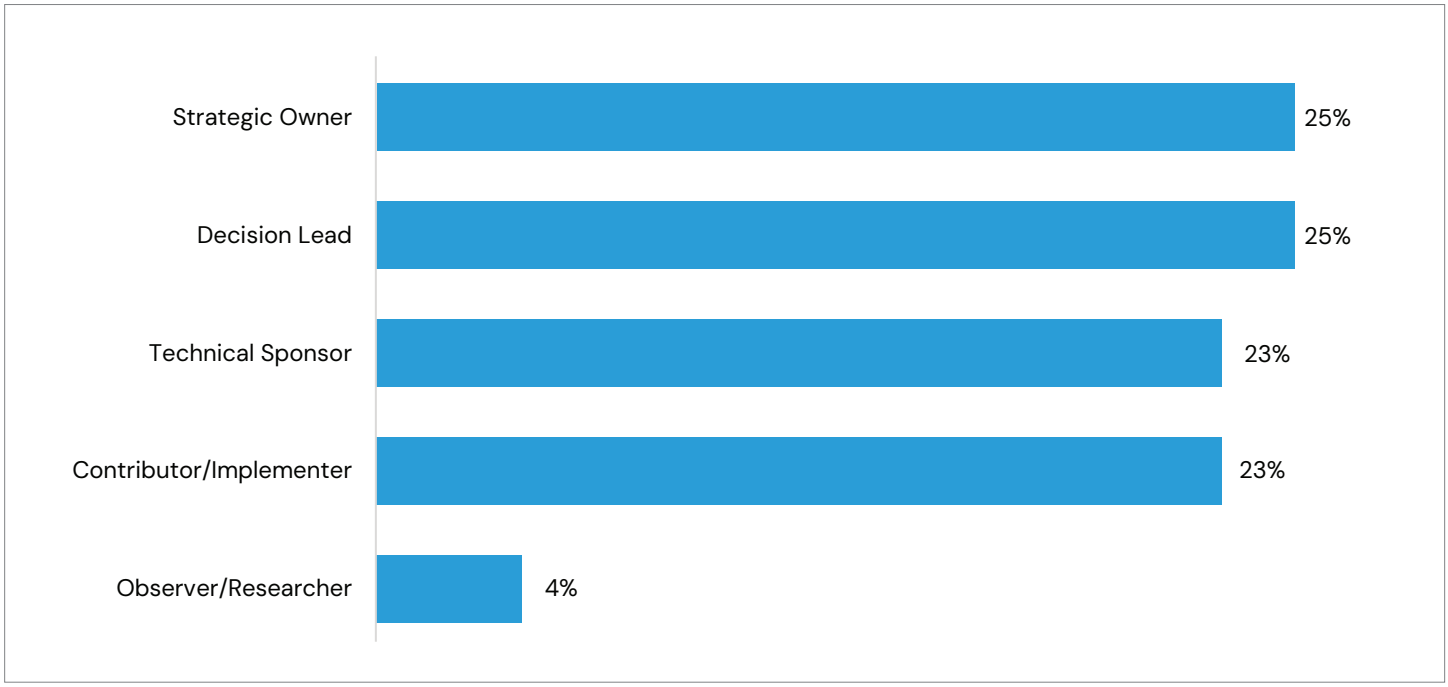


Figure 36: Breakdown of respondents by leadership title

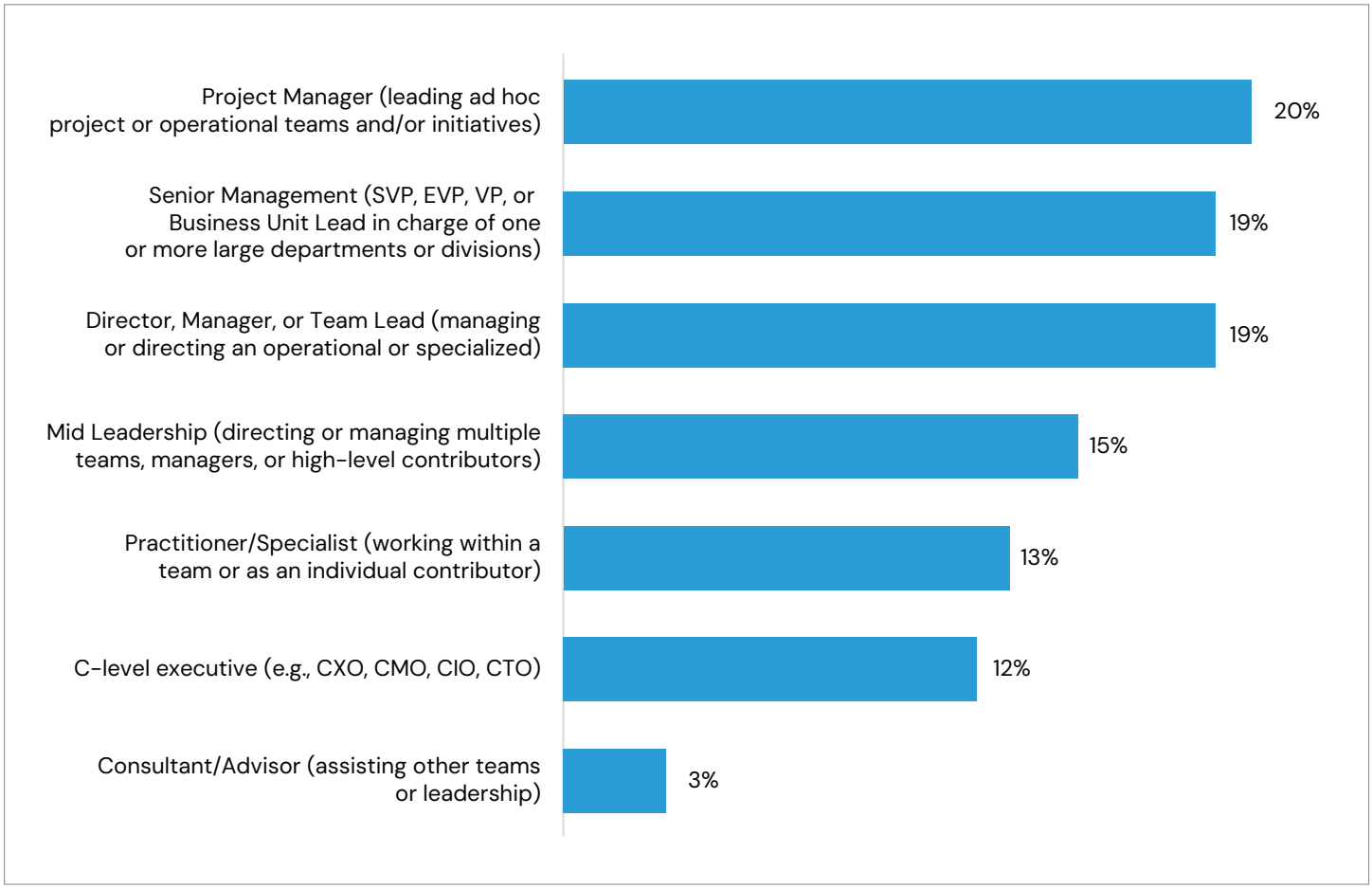


Figure 37: Department/functional role of respondent

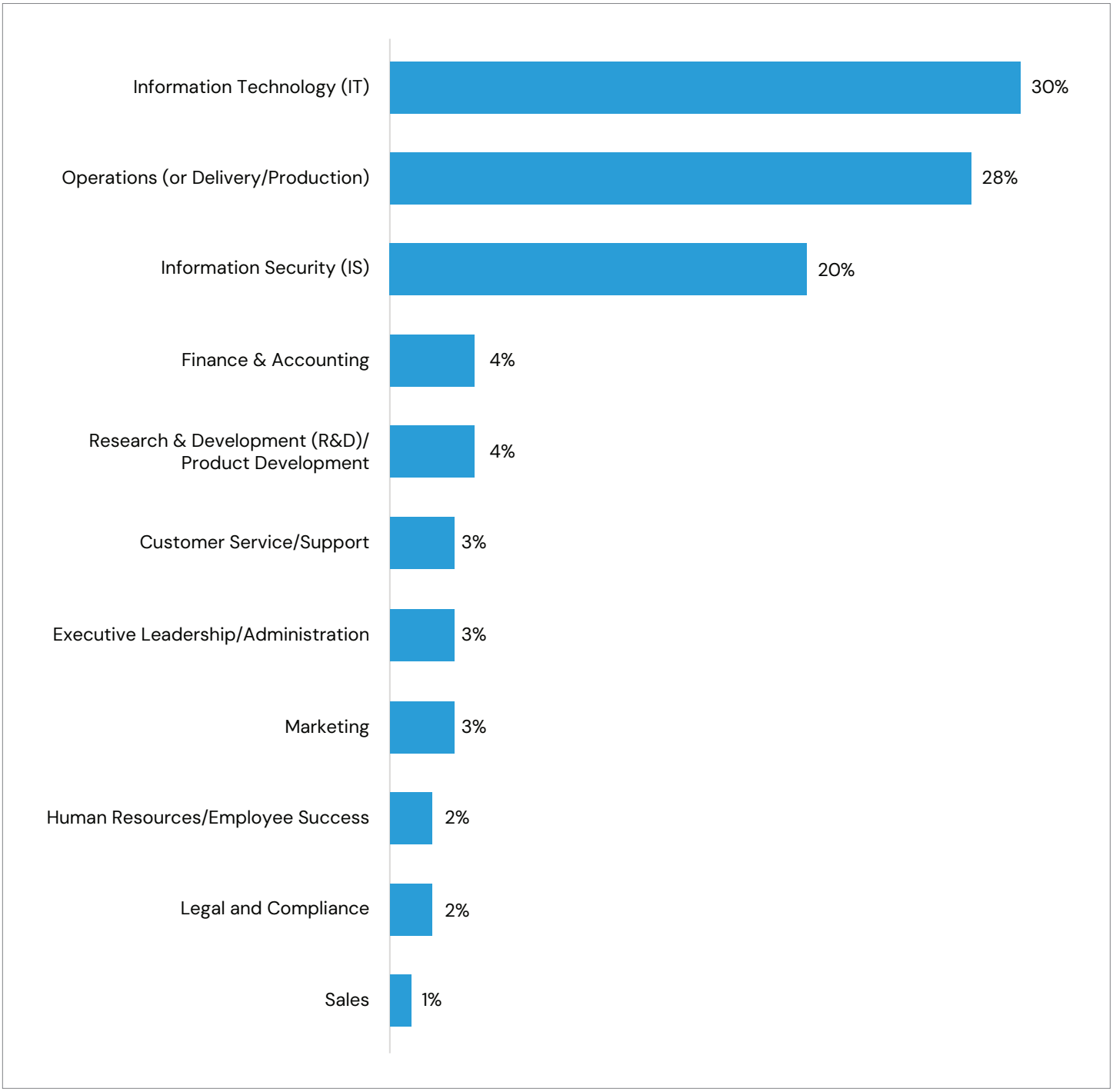
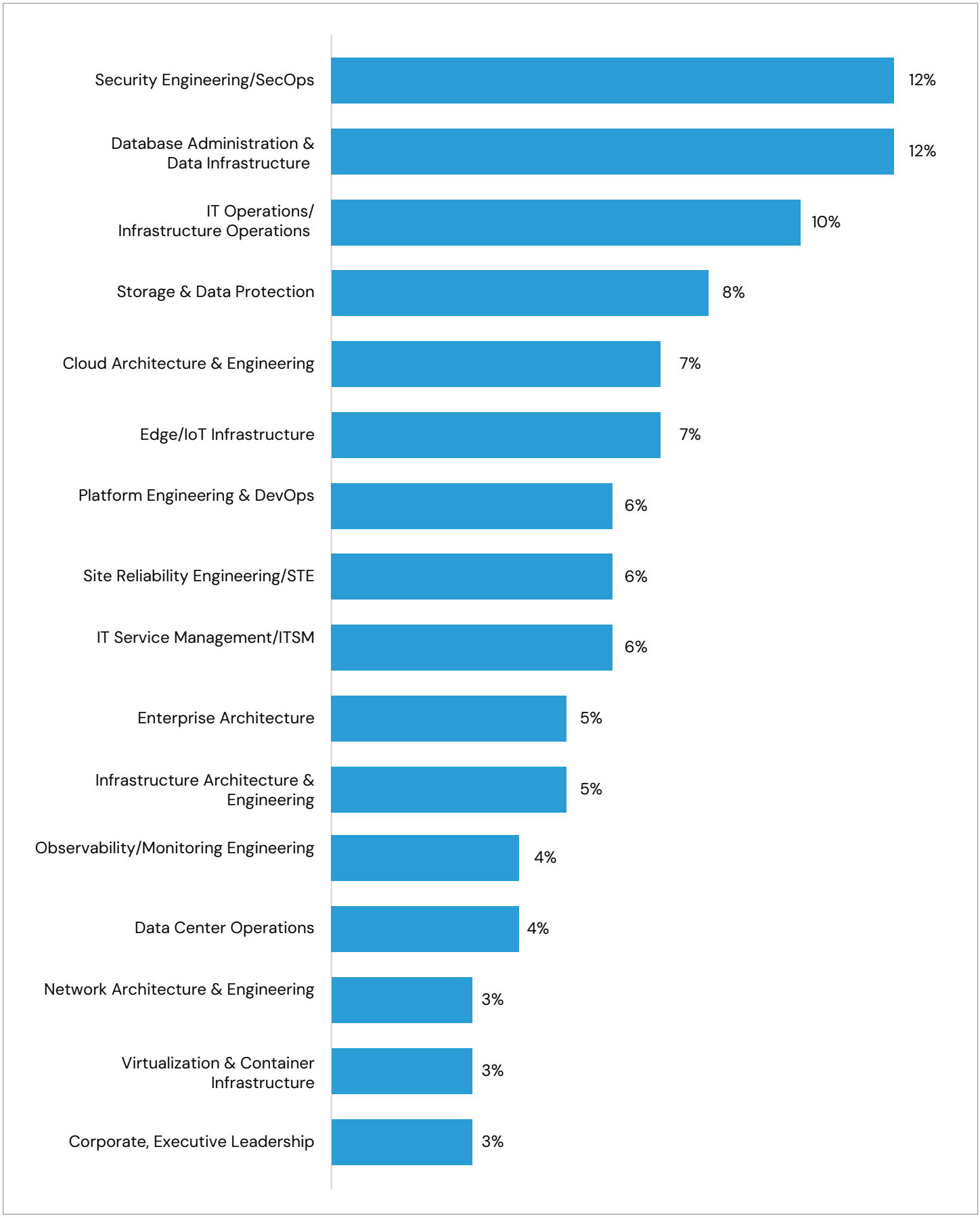


Figure 38: Respondents' primary "technical" role or area of responsibility within organization's IT infrastructure and operations environment



- **Oversight of AI-enabling IT:** Oversight of the technologies and IT teams enabling AI deployment and adoption.
- **Data engineer:** Building and maintaining the data pipelines and infrastructure that feed and support ML models.
- **Data scientist:** Designing models, algorithms, and experiments that drive the AI solution.
- **Oversight of AI-enabling infrastructure:** Oversight of the critical infrastructure within IT (compute, networking, data storage, etc.) that underpins the entire AI Stack.
- **Director of Cloud/Hybrid Cloud:** Making key decisions about the cloud infrastructure, the primary environment for most modern AI stacks.
- **Machine learning (ML) engineer:** Building, deploying, and maintaining ML models at the core of the AI stack.
- **Enterprise architect:** Defining the overall structure and standards for IT systems, ensuring the AI stack aligns with the broader enterprise technology landscape.
- **Senior Systems/Platform Engineer:** Managing or operating platforms and systems that host and run AI applications and models.
- **Data architect:** Designing enterprise data frameworks, including data ingestion, storage, and processing, which are foundational to any AI stack.
- **Security/SecOps engineer:** Securing the sensitive data, models, and deployment pipelines within the AI stack.
- **Site Reliability Engineer (SRE):** Ensuring the reliability, performance, and scaling of AI models in production.

Figure 39: Respondents' Involvement/decision authority in planning, selection, and deployment of I&O elements

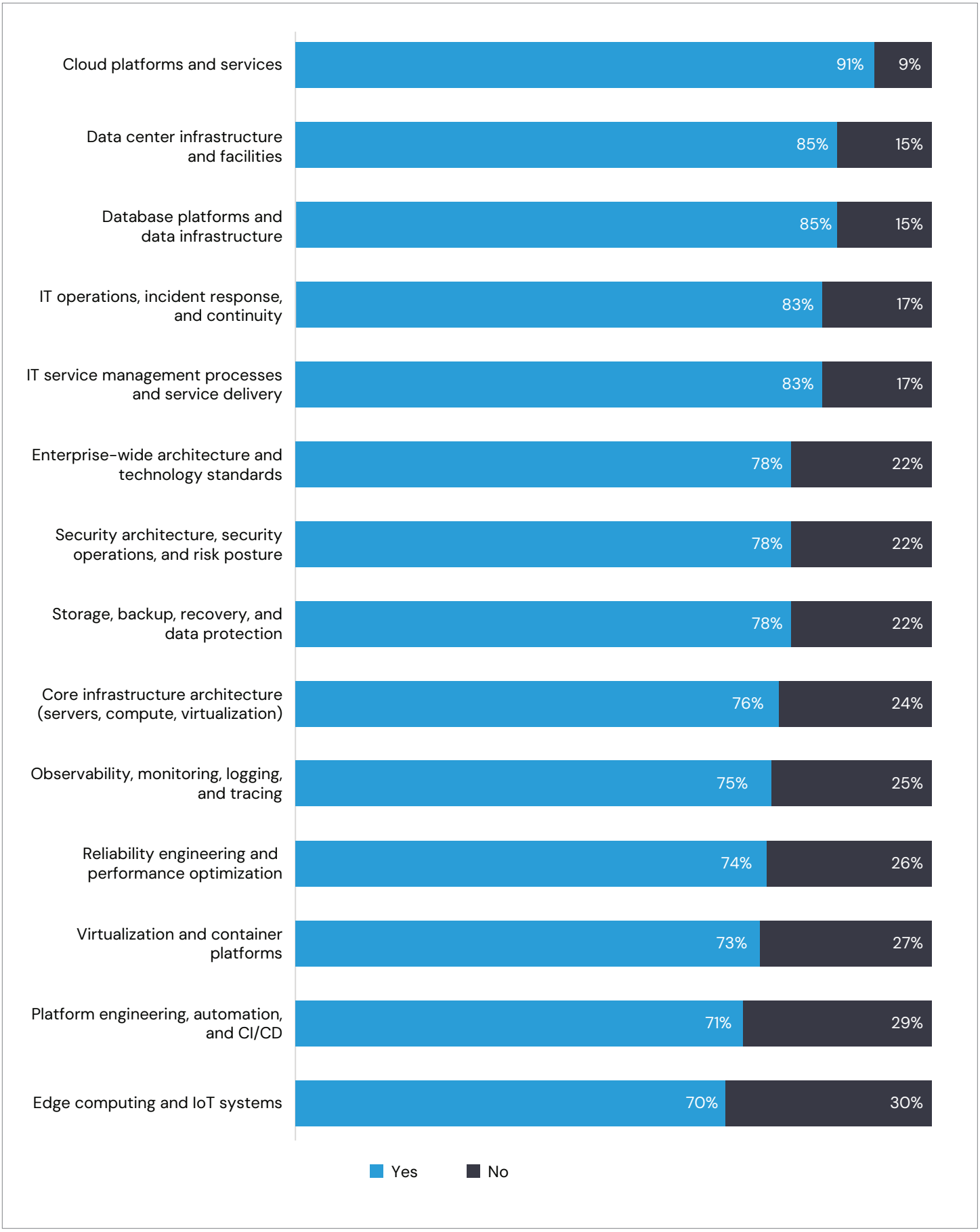


Figure 40: Industry Sector Distribution of Participating Organizations

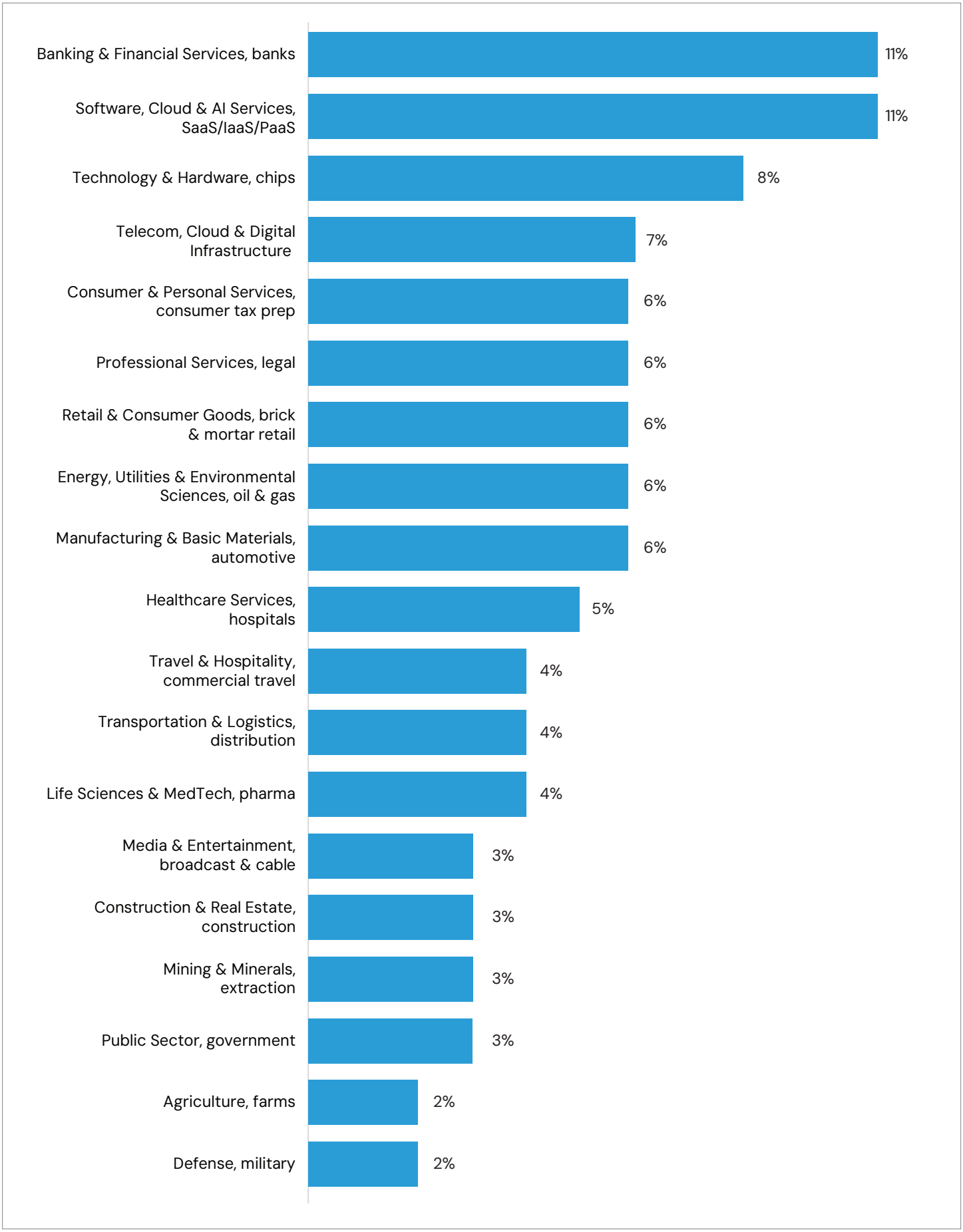


Figure 41: Respondent Representation by Country

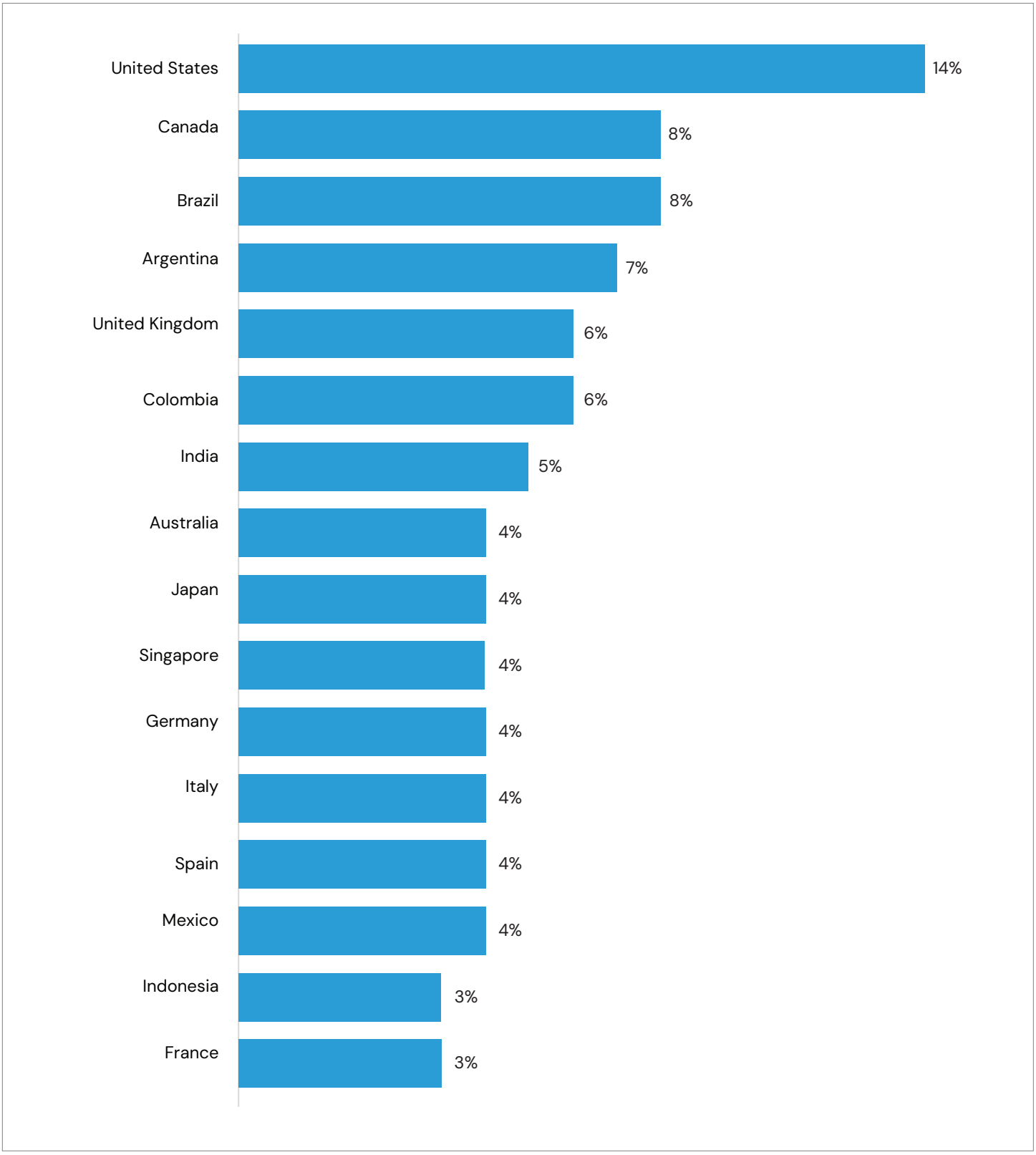
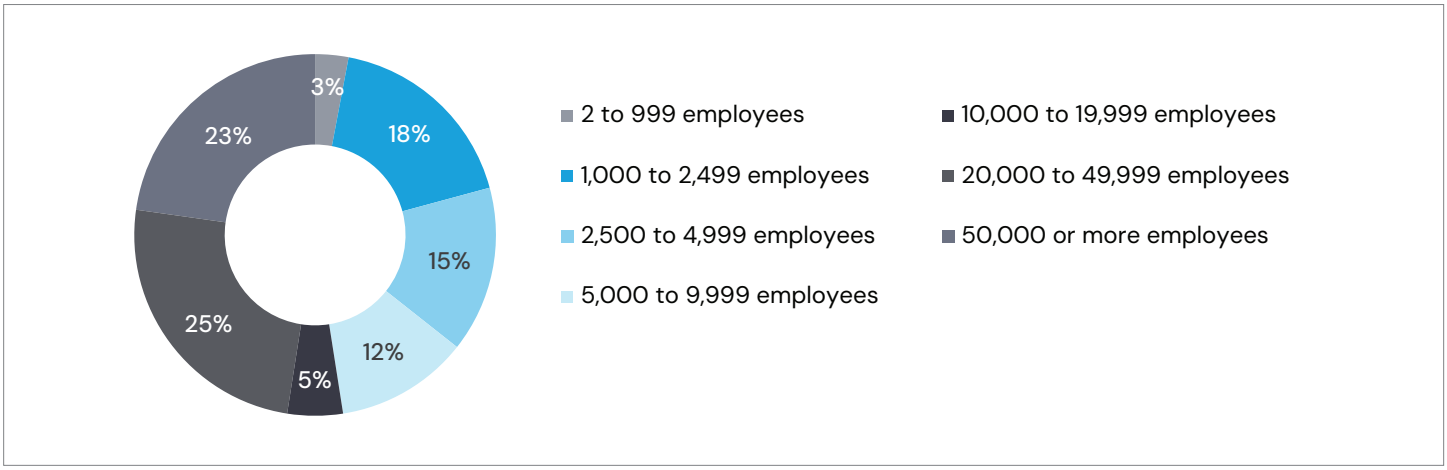


Figure 42: Distribution of participant organizations by country



HyperFRAME RESEARCH

About US

HyperFRAME Research delivers in depth research and insights across the global technology landscape, spanning everything from hyperscale public cloud to the mainframe and everything in between. We offer strategic advisory services, custom research reports, tailored consulting engagements, digital events, go to market planning, message testing, and lead generation programs.

Our industry analysts specialize in rigorous qualitative and quantitative assessments of technology solutions, business challenges, market forces, and end-user demands across industry sectors. HyperFRAME Research collaborates closely with your Analyst Relations, Product, and Marketing teams to build and amplify your thought leadership, positioning your expertise to enhance brand and product recognition. Through content that engages readers, viewers, and listeners alike, we ensure your voice resonates across channels.

Contact HyperFRAME Research:

Email Address: steven.dickens@hyperframeresearch.com
Telephone Number: +1 845 505 1678