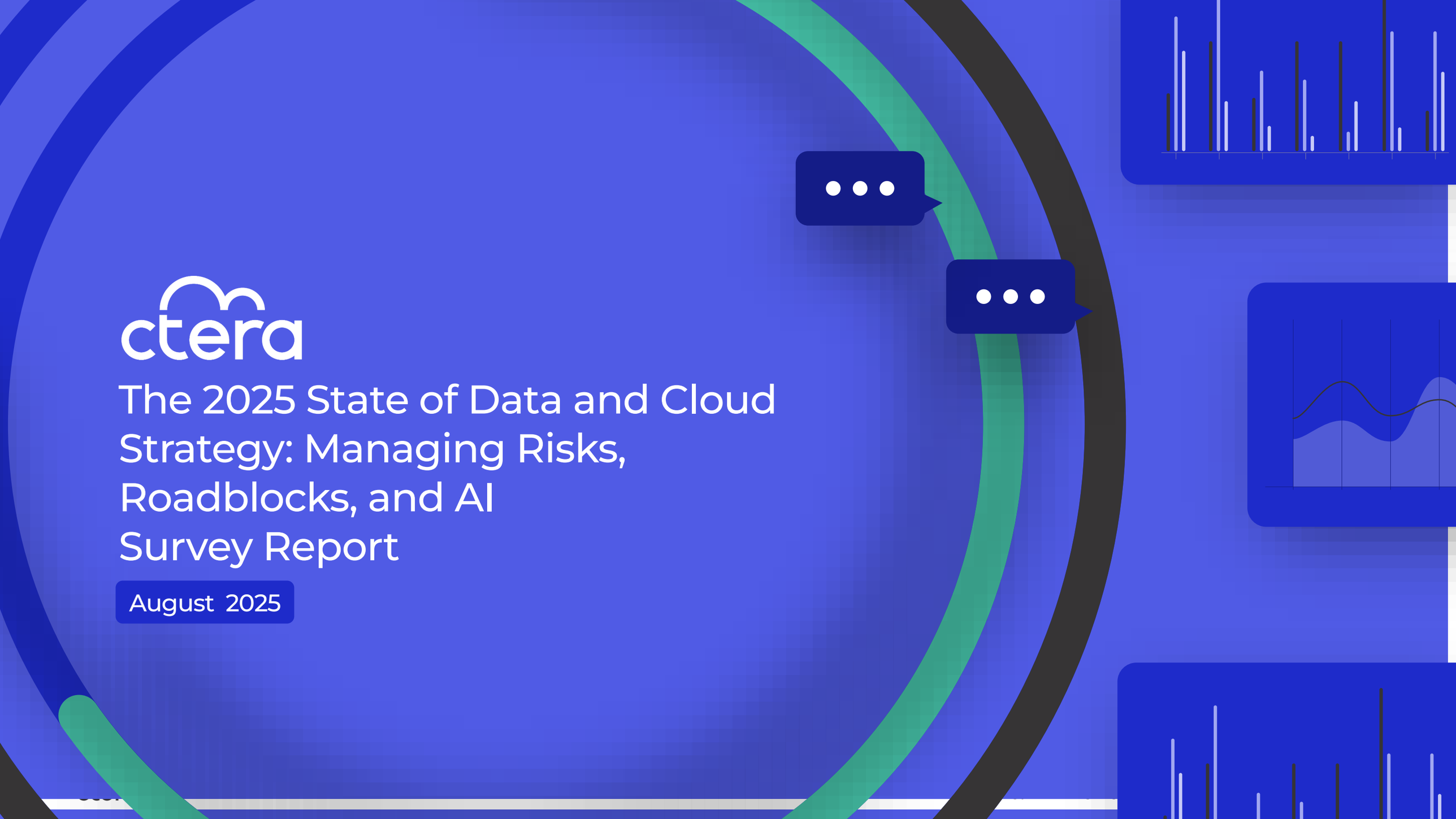

The 2025 State of Data and Cloud Strategy: Managing Risks, Roadblocks, and AI Survey Report

August 2025

Table of Contents

Introduction

Introduction & Methodology

IT and Security leaders are navigating a complex, high-pressure environment shaped by growing infrastructure and data demands, increasing security threats, and rapid AI advancements. These challenges *can* be addressed by modernizing technology and internal processes. However, not all organizations are adapting quickly enough to keep pace with change.

This report explores the roadblocks faced by IT and security teams today, and we deep dive into topics such as data challenges, budgeting concerns, workforce limitations, and the gap between perception versus reality, especially around AI and other emerging technologies.

You'll learn how your organization's priorities, investments, and challenges compare to others like you. For example, are your peers fully deploying AI tools, or just testing the waters? Is ransomware still a rare crisis, or has it become an everyday risk? What's holding organizations back from full cloud adoption, and where do data security, compliance, and cost rank in enterprise decision-making?

Whether you're aligning with the C-suite on strategic priorities or working through practical data challenges, this report provides a valuable benchmark.

Methodology

To understand the true state of data and cloud security today, we commissioned a survey of 300 senior IT and Security leaders from the US, EMEA and APAC. All work in companies with more than 2,500 employees, across Construction, Defense, Financial Services, Government, Healthcare, Manufacturing, and Media industries. We also screened for those that have 100TB+ of file storage, a minimum of 5 sites/locations, and those that are willing to use an EFSS like OneDrive and Dropbox.

This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel, and invited via email to complete the survey, with all responses collected in early 2025. The average amount of time spent on the survey was 7 minutes and 8 seconds. The order of the answers in the majority of the non-numerical questions was randomized, to prevent order bias.

Executive Overview

Key Findings

01 | Despite the Hype, AI Isn't the Highest Priority for Organizations

While adoption of strategic AI continues to dominate headlines, only 57% of IT and Security leaders consider it high priority for 2025, behind cybersecurity (80%) and cost optimization (61%). Surprisingly, data growth management ranks even lower as a priority, with only 54% of leaders citing it as a primary focus, despite being critical to enabling effective AI. Without clean, well-managed data, organizations may struggle to realize the full potential of the same AI strategies they're aiming to adopt.

02 | Ransomware Hits Everyone — But Not Everyone Is Prepared

Every organization surveyed has experienced a ransomware attack in the past, with 65% reporting an incident in the past two years. While most were able to recover from data backups, 10% paid the ransom, 17% lost data, and 14% don't even know how the attack was resolved. The data reveals not just the scale of the threat, but critical gaps in response, visibility, and resilience, which are only set to grow in the era of AI.

03 | Those Who Lead the Cloud Charge May Be Carrying the Greatest Burden

C-level executives are driving the push toward cloud technologies, with 26% strongly prioritizing cloud adoption, which is more than double the average across all roles (12%). Yet this same group is also most likely to see cloud and hybrid migration as a major challenge, with 26% citing it as a significant hurdle, compared to just 15% overall. The data suggests that while the executive tier is championing cloud transformation, it's also where the pressure and the complexity of execution is most deeply felt.

04 | AI Ambitions Are High, But Skills Gaps May Hold Teams Back

Many organizations are being pushed by investors to implement AI for operational efficiencies, and as a result are primarily turning to AI to improve customer experience (64%), enhance predictive intelligence (64%), and boost query accuracy (53%). Yet only 10% cite closing skills gaps as a goal, which reveals a potential disconnect between ambitious outcomes and the readiness to achieve them. Without skilled teams and strong data foundations, even the most promising AI initiatives risk falling short.

05 | Compliance and Security Concerns Dominate AI Deployment Challenges

As 98% of organizations roll out LLM and AI-based tools, compliance (67%) and security risks (57%) are the most widely cited challenges. Data accessibility issues (45%) and implementation costs (44%) also stand out, signalling that AI success isn't just about technology, it's about governance, infrastructure, and long-term sustainability. Organizations must tackle these foundational barriers before they can unlock AI's full potential.

State of Data & Cloud Strategy

2025 Priorities for IT and Security Leaders

As organizations shaped their 2025 roadmaps, we asked IT and Security leaders to indicate the importance of four key business goals. Cybersecurity led the way, with 80% citing it as a high priority, followed by cost optimization at 61%. Strategic AI, despite the surrounding buzz around Artificial Intelligence, was prioritized by just 57%, trailing behind more established concerns of security and cost control.

Managing data growth trailed slightly behind AI strategy, a high priority for 54% of respondents, even though effective data management underpins AI readiness. Without clean and accessible data, organizations may struggle to support the very AI strategies they consider essential.

When diving into the data to look at how strategic AI was placed as a priority by industry, Manufacturing stands out, with 89% of respondents calling it a high priority. This is unsurprising given clear use cases like predictive maintenance, automation, and quality control.

On the other end of the spectrum, only 51% of Media companies ranked strategic AI as a high priority this year. This is notable considering media's deep ties to content creation and marketing, which are two areas often seen as prime targets for AI-driven productivity gains. The hesitation may stem from concerns around brand consistency, tone, and messaging, areas where generative AI still presents challenges.

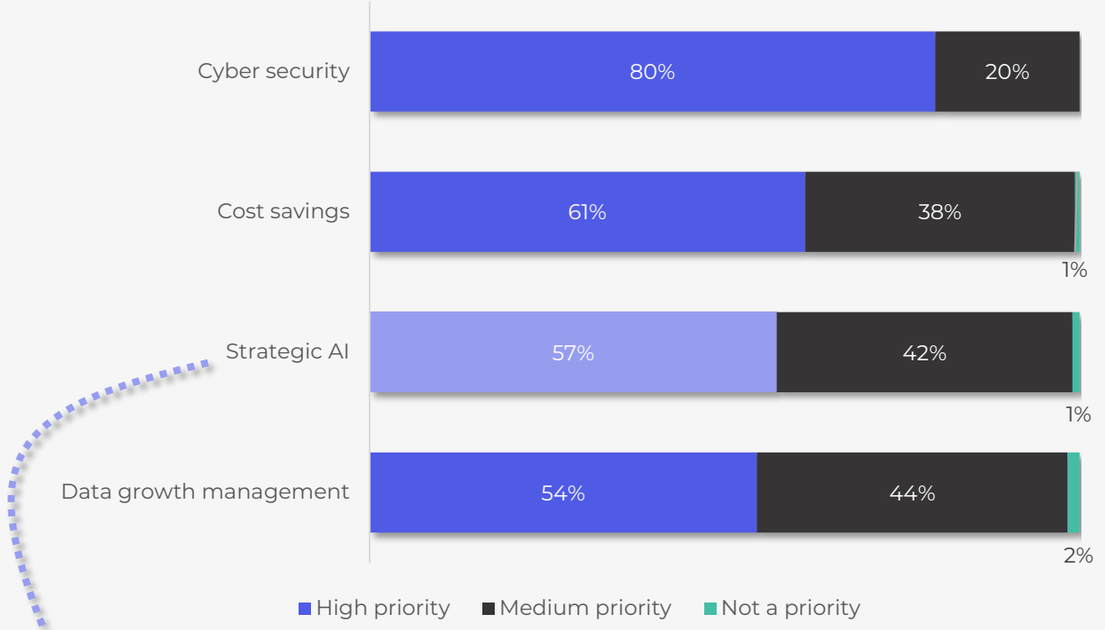

Figure 1: 2025 Priorities for Your Organization

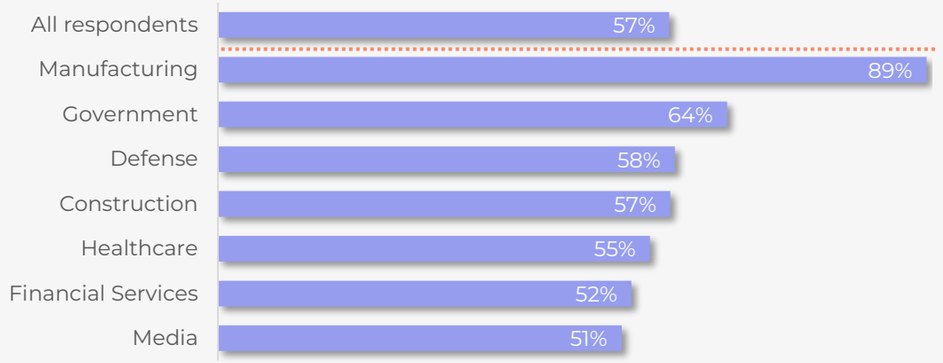

Figure 2: "High Priority" for Strategic AI by Industry

Top Organizational Challenges Around Data

When asked about top data-related challenges, IT and Security leaders pointed to security and compliance burdens (51%) and cost pressures (50%), two areas that continue to dominate strategic conversations. These concerns reflect the ongoing complexity of protecting data in a distributed environment while managing tighter IT budgets.

Cloud migration challenges, ransomware resurgence and legacy storage limitations also rank highly, cited by 31% of respondents as top data challenges, underscoring the growing pressure to modernize data infrastructure while staying resilient against increasingly sophisticated threats.

Interestingly, hybrid work complexity was cited by only 25% of respondents as a top data challenge, a noticeable shift from industry trends circa COVID-19, when remote and hybrid models were a more urgent concern. As an increasing number of organizations return to office or settle into stable hybrid setups, the perceived challenge seems to have shifted to protecting that distributed environment and adhering to compliance requirements.

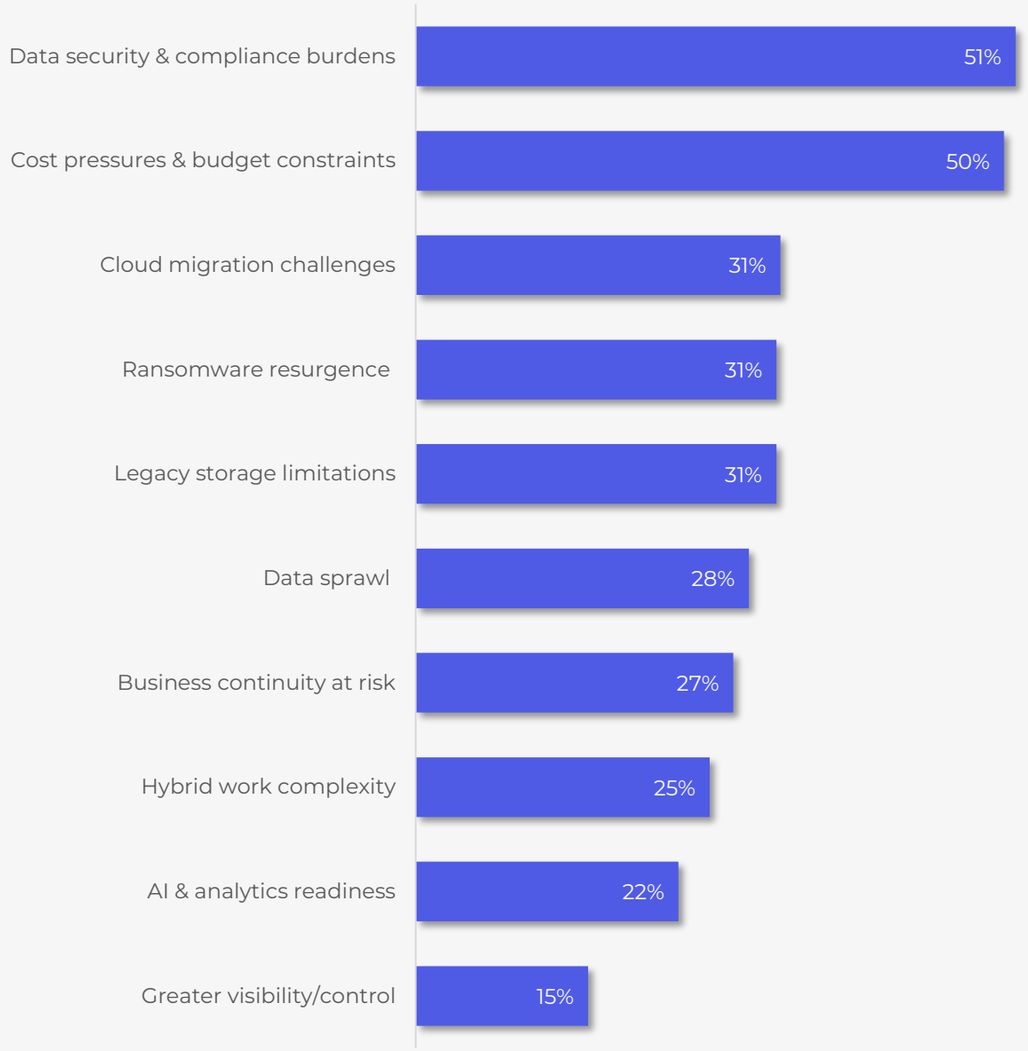

Figure 3: Top Challenges Around Data in Your Organization

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

How Common are Ransomware Attacks in Today's Organizations?

Every IT and Security leader surveyed has experienced a ransomware attack on their organization in the past, highlighting how ubiquitous ransomware has become. The majority (50%) of organizations faced a ransomware attack during the previous 13 to 24 months, with 15% facing an attack in just the past 12 months.

To understand which organizations are most vulnerable to this kind of threat, we broke down the data for those who have experienced a ransomware attack between 7-12 months ago, which amounts to 12% of respondents. Among the group, 45% are from the Healthcare industry. Healthcare is known to be a prime target for ransomware, with high value data as the prize for a successful attack, and legacy infrastructure which often makes it easier for attackers to gain entry.

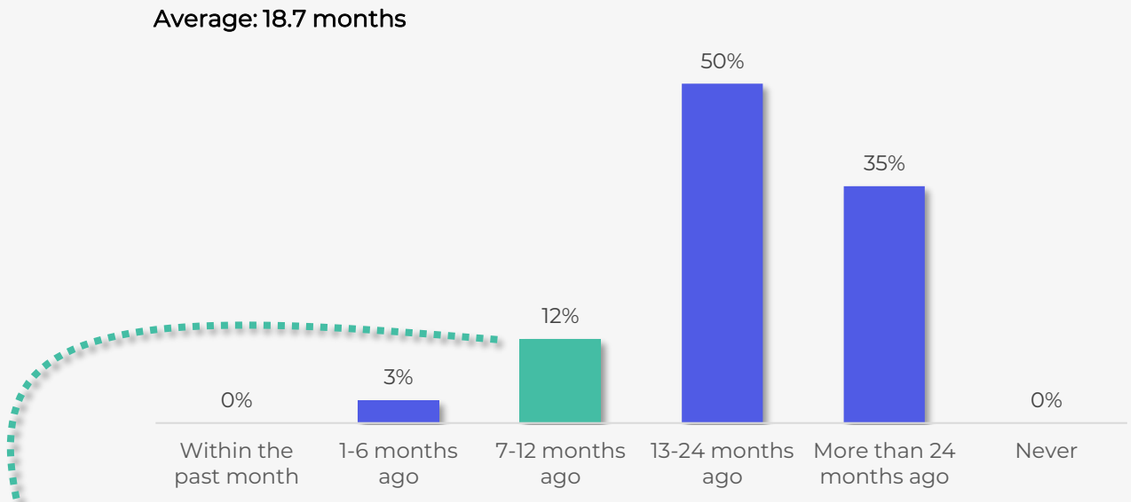

Figure 4: Last Ransomware Attack Experienced by Your Organization

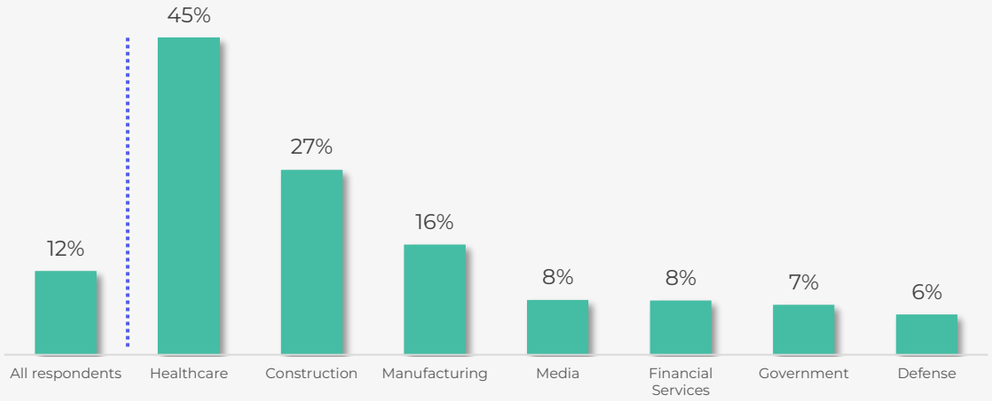

Figure 5: "7-12 months ago" by Industry

Ransomware Attack Resolution: Who Can Restore, and Who Pays the Ransom?

When it comes to resolution, the majority of organizations (59%) cited that they were able to restore their data from backups. However, a concerning number of respondents indicated less favorable outcomes. 17% reported permanent data loss, 10% felt they had no choice but to pay the ransom, and 14% can't say how the situation was resolved, potentially pointing to a lack of visibility or control, or both.

Interestingly, when we looked at the data broken down by seniority and role, we found that senior leaders appear more confident in data restoration as an outcome, and that no-one in the C-suite reported paying a ransom.

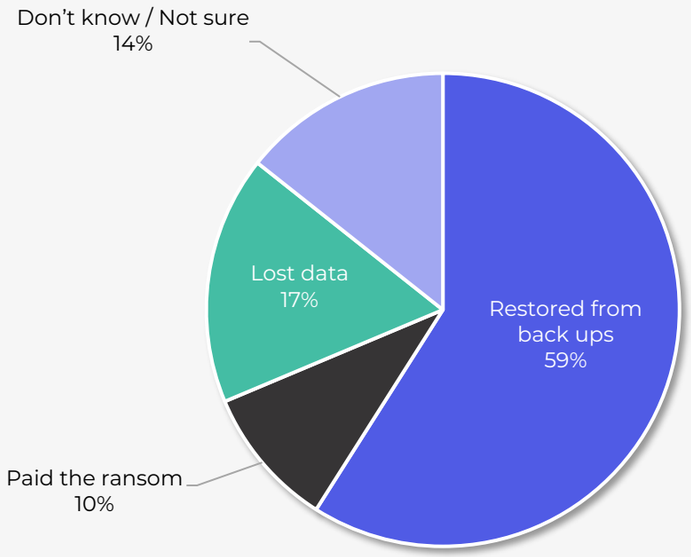

Figure 6: Resolution of Ransomware Attack

Cloud Technology Adoption vs. Return to Private Data Centers

A key strategic decision for today's organizations is whether to prioritize cloud adoption or reinvest in private data centers.

While 37% of those surveyed reported taking a balanced approach, there is a noticeable lean toward cloud-first strategies. 61% of leaders either somewhat or strongly prioritize cloud technologies over private data centers.

A closer look reveals that this push is largely being driven from the top, with 26% of C-level executives strongly prioritizing cloud, compared to just 11% of VPs and 9% of Directors.

This disparity suggests that while the cloud remains a strategic priority at the leadership level, buy-in across the broader organization may be more measured.

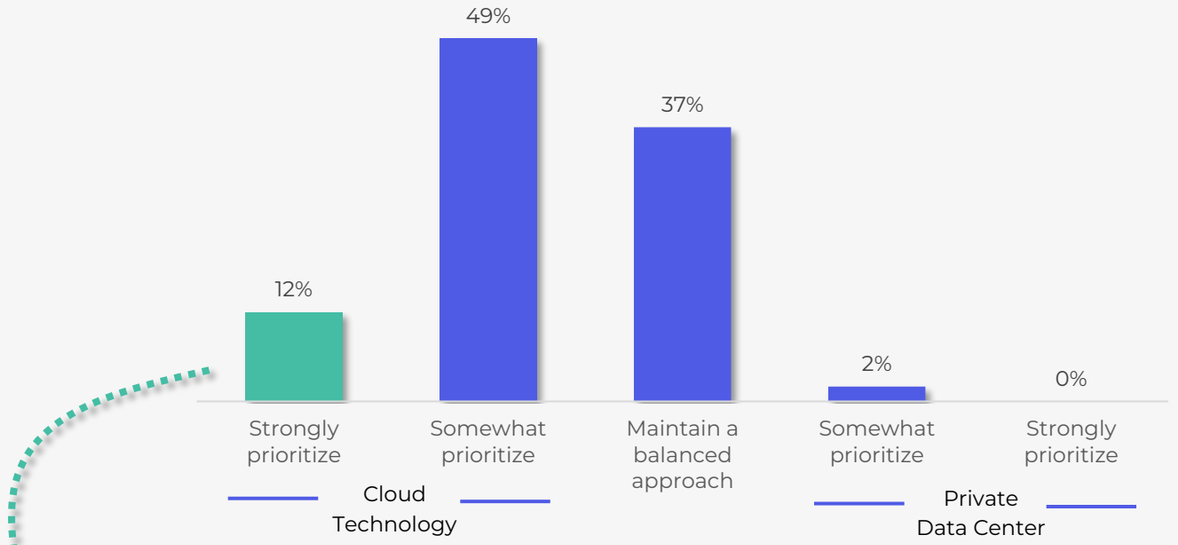

Figure 7: Prioritization of Cloud Technology Adoption vs. Return to Private Data Centers

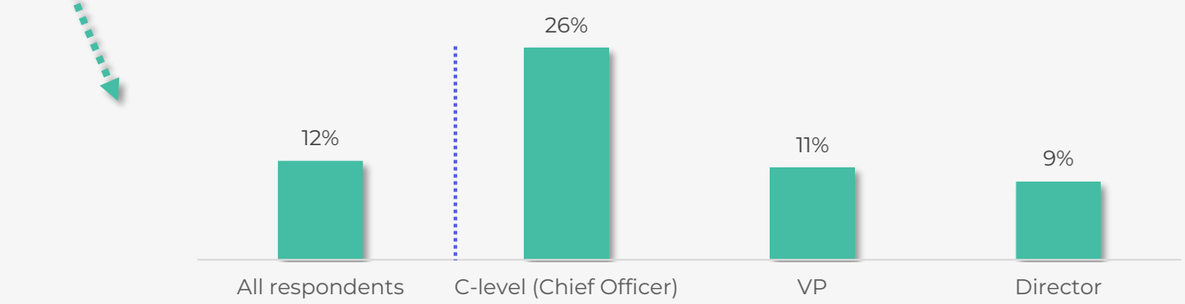

Figure 8: "Strongly prioritize" by Job seniority

Benefits Experienced with Cloud File Storage

Organizations are seeing clear value from their shift to cloud file storage. Every respondent reported at least one benefit, with no-one indicating otherwise.

The most commonly cited advantages include improved collaboration (57%), increased availability and uptime (48%), and broader integration with other platforms (37%). However, fewer organizations reported gains in areas which are cited earlier in the data challenges organizations are facing, such as compliance and governance (18%), risk reduction (18%), or cost savings (32%).

These results suggest that while cloud storage is delivering on performance and productivity, its impact on cost efficiency and regulatory assurance remains less measurable.

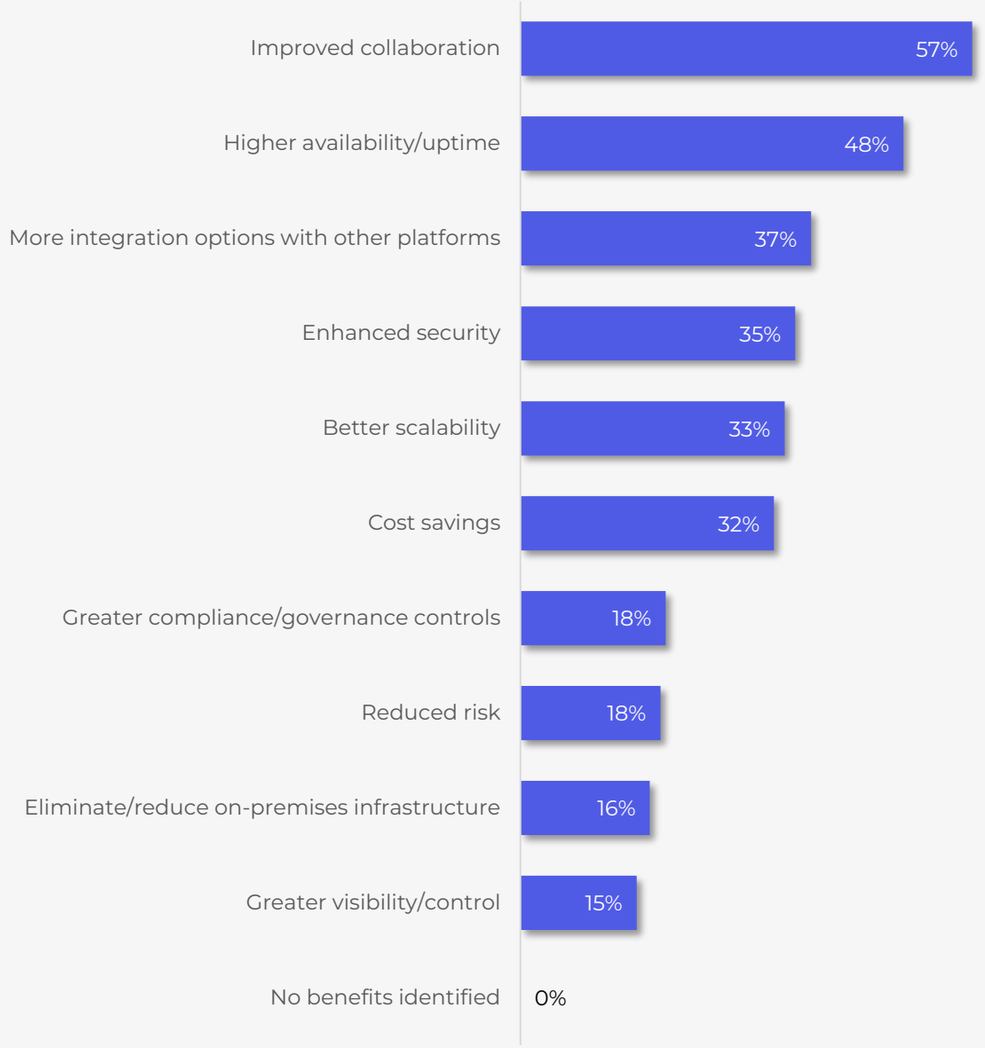

Figure 9: Benefits Experienced with Cloud File Storage

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Annual Investment in Cloud File Storage

Organizations are making substantial investments in cloud file storage, with the average annual spend reported at $167,467. Only 8% of IT and Security leaders are spending less than $100,000 per year, highlighting the scale of commitment across the market.

This data offers a useful benchmark. If your organization is investing below the average, it may be an opportunity to engage leadership on aligning budget with expected outcomes and performance.

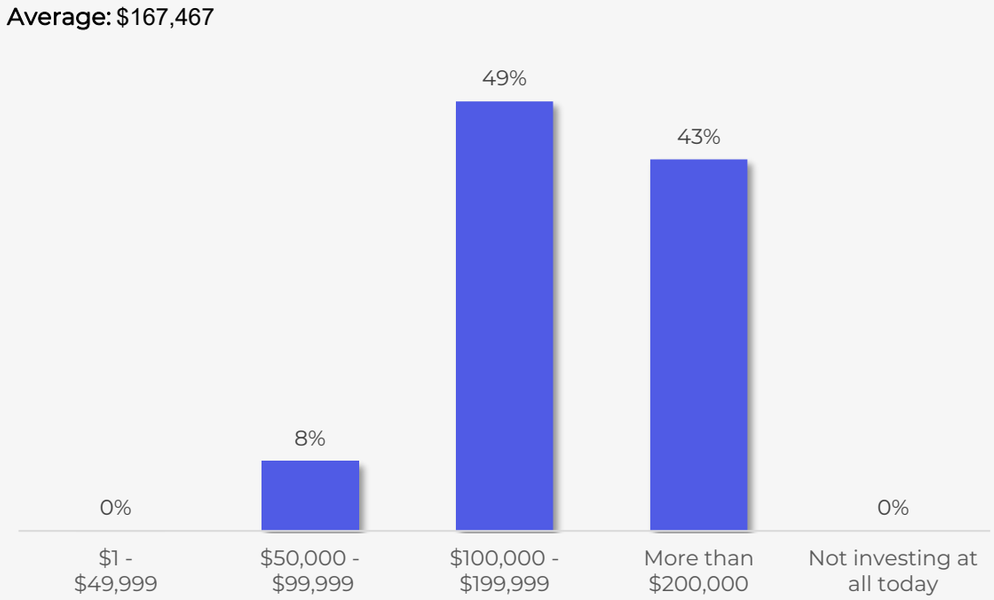

Figure 10: Annual Investment in Cloud File Storage

Current State of Cloud File Storage

Despite growing investments, widespread adoption of cloud file storage remains a challenge. A majority of IT and Security leaders (62%) say their deployment is limited to specific teams or departments, which is a pattern consistent across organizations of all sizes.

Only 9% report full, organization-wide deployment, underscoring the operational and cultural hurdles that can slow a broader rollout. Whether due to legacy systems, change management challenges, or varying team needs, achieving consistent adoption remains a key barrier to unlocking the full value of cloud file storage.

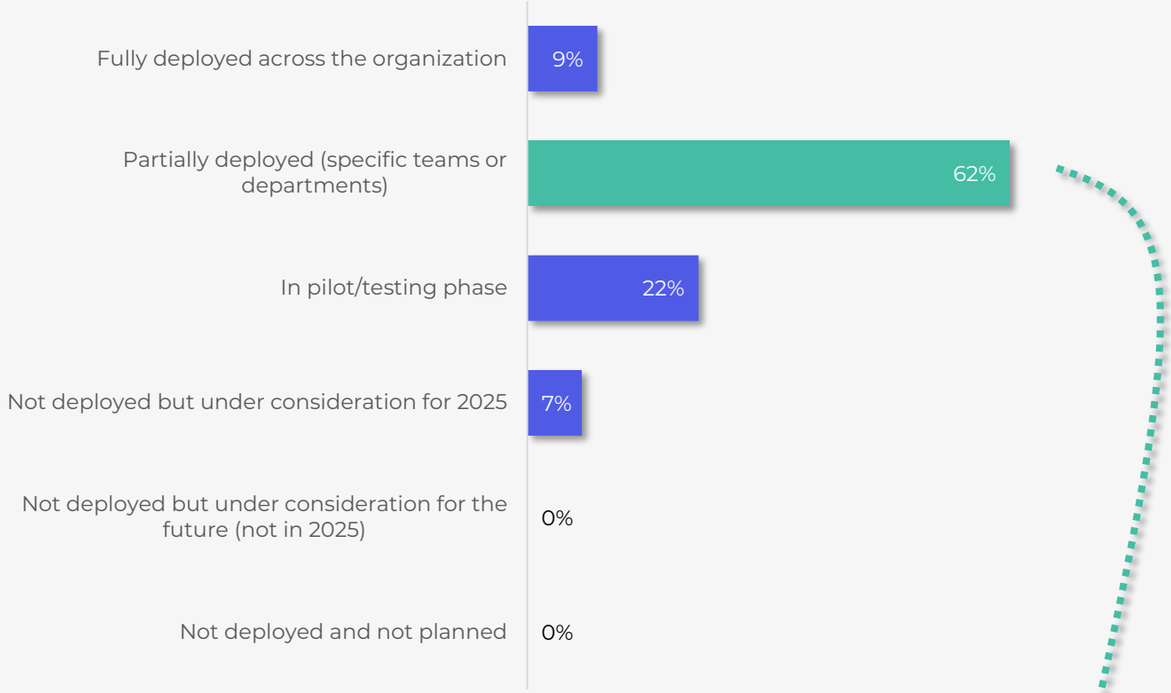

Figure 11: Current State of Cloud File Storage in Your Organization

Figure 12: "Partially deployed" by Company Size

Cloud or Hybrid Migration Anxiety Rises with Seniority

Data migration is broadly seen as a difficult undertaking, because it can greatly disrupt the business, and just 3% of IT and Security leaders believe differently.

The remaining 97% view it as at least somewhat challenging, with 15% identifying it as a significant challenge. However, when we broke down the data by seniority, we uncovered that this concern is most pronounced at the executive level: 26% of C-level leaders see migration as a major hurdle, compared to just 19% of VPs and 9% of Directors. This suggests that senior leaders, responsible for long-term strategy and risk, may feel the pressure of migration more acutely than those focused on execution.

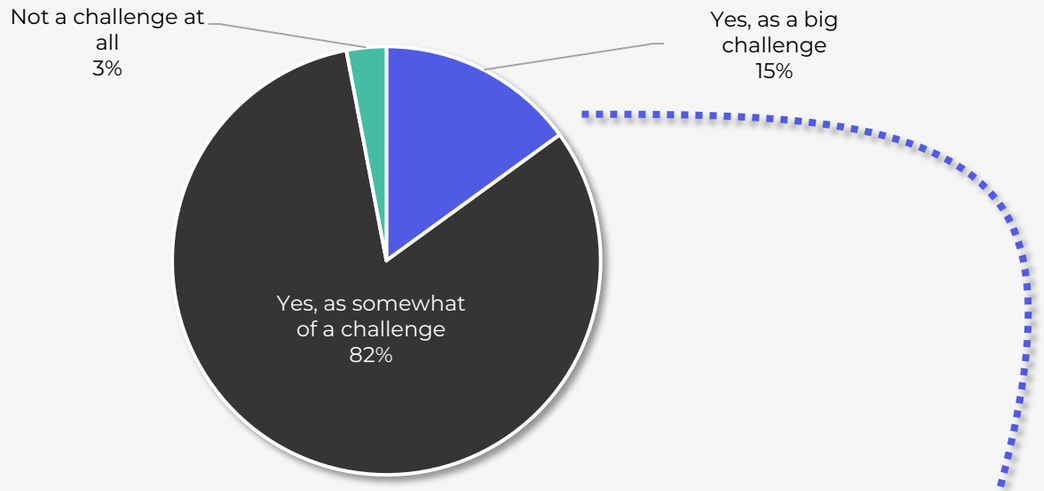

Figure 13: Perception of Cloud or Hybrid Migration as a Challenge

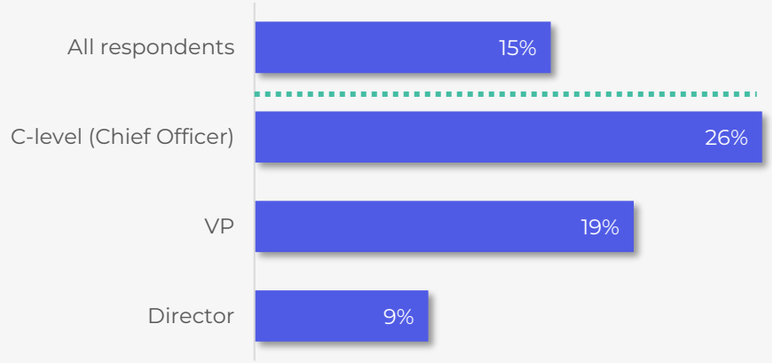

Figure 14: "Yes, as a big challenge" Responses by Job Seniority

What's Holding Back Cloud Migration? It Depends Who You Ask.

What makes moving to the cloud such a challenge for today's IT and Security leaders? We asked respondents to think about the migration impediments they are dealing with and found a broad consensus across the top three issues – security and compliance concerns, cost, and end user disruption.

However, when we look beyond the top three, priorities shift, depending on seniority within the organization.

C-level executives are notably more concerned about vendor lock-in, citing it at nearly twice the rate of other respondents, which may be a reflection of their focus on long-term strategic flexibility. In contrast, VP-level leaders are more focused on operational risks, such as aging infrastructure (39%) and the potential for data loss or corruption (29%). Directors are more likely to worry about data sovereignty (28%), a concern cited by only 17% of the C-suite. Additionally, while 23% of VPs and Directors report lacking the right partner expertise, just 6% of C-level leaders share that concern.

The takeaway? Cloud migration pain points vary significantly by role, shaped by the unique pressures and priorities of each leadership tier.

	All	Job seniority		
	respondents	Director	VP	C-level
Security/Compliance concerns	58%	57%	58%	66%
Cost	54%	55%	54%	51%
End user disruption	45%	45%	43%	57%
Aging pre-existing infrastructure	33%	26%	39%	37%
Data loss/corruption	27%	26%	29%	20%
Data sovereignty	22%	28%	17%	17%
Partner expertise	21%	23%	23%	6%
Organizational buy-in	15%	17%	15%	6%
Vendor lock-in	12%	10%	11%	23%
Staffing	11%	10%	10%	14%

Figure 15: Impediments to Migrating to the Cloud or Hybrid Environment

State of Strategic AI

Current State of LLM/AI-Based Assistance Tools

While strategic AI fell third in the list of priorities for 2025, that doesn't mean organizations aren't starting to experiment and test with these tools. 70% of IT and Security leaders say AI-based assistants are partially deployed in their organization, and an additional 27% are in pilot phases. Even if AI isn't the top focus today, most organizations are actively laying the groundwork for broader integration.

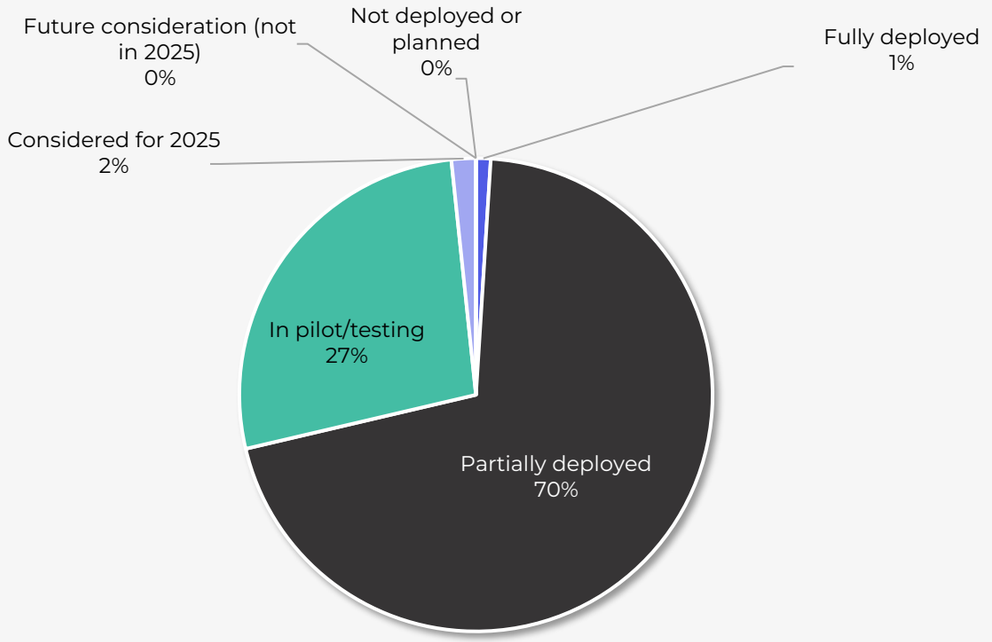

Figure 16: Current State of LLM/AI-Based Assistance Tools in Your Organization

What's Driving Organizations to Implement LLM/AI-Based Assistance Tools?

We asked respondents to consider their goals for implementing LLM or AI-based assistance tools within their products and services, and found three main drivers: improving customer experience (64%), achieving better predictive intelligence over outcomes (64%), and boosting the accuracy of database queries (53%).

In contrast, closing skills gaps is at the bottom of the list, with just 10% of IT and Security leaders calling this out as a driver. Organizations should think hard about their priorities, as before you can take advantage of and implement revenue-driving activities like the top three, and more importantly, you need good data in place, and you need employees who know how to leverage the tools.

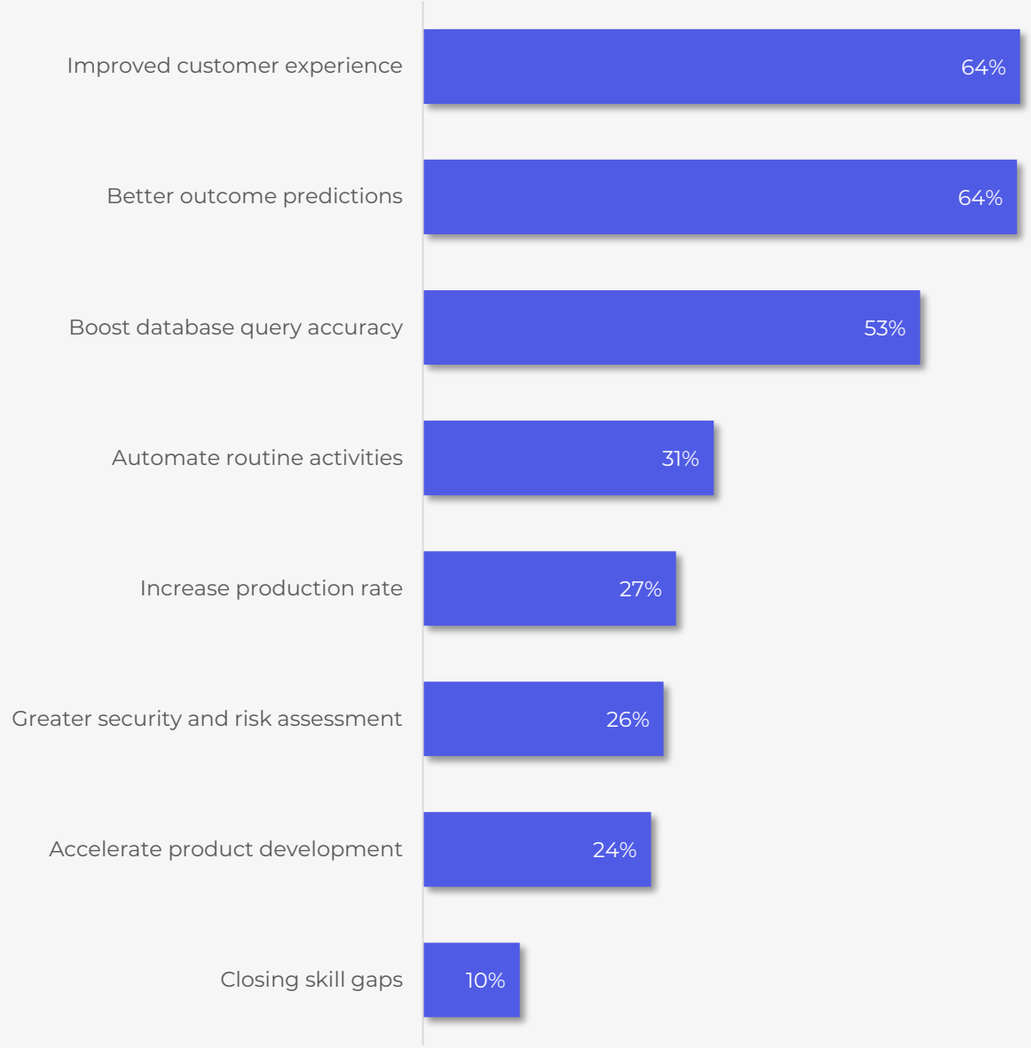

Figure 17: Goals of Implementing LLM/AI-Based Assistance Tools in Your Organization

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Challenges in Deploying LLM/AI-Based Tools

IT and Security leaders were encouraged to consider the challenges that they have already encountered or that they anticipate facing as they deploy LLM/AI-based tools. Respondents could choose as many as apply.

The most significant challenge is compliance and regulatory concerns (67%), followed by security risks such as data exposure or misuse (57%). Additionally, data stored in silos that is not accessible to AI tools is a concern for 45% of respondents, and cost of implementation and maintenance is a challenge for 44%.

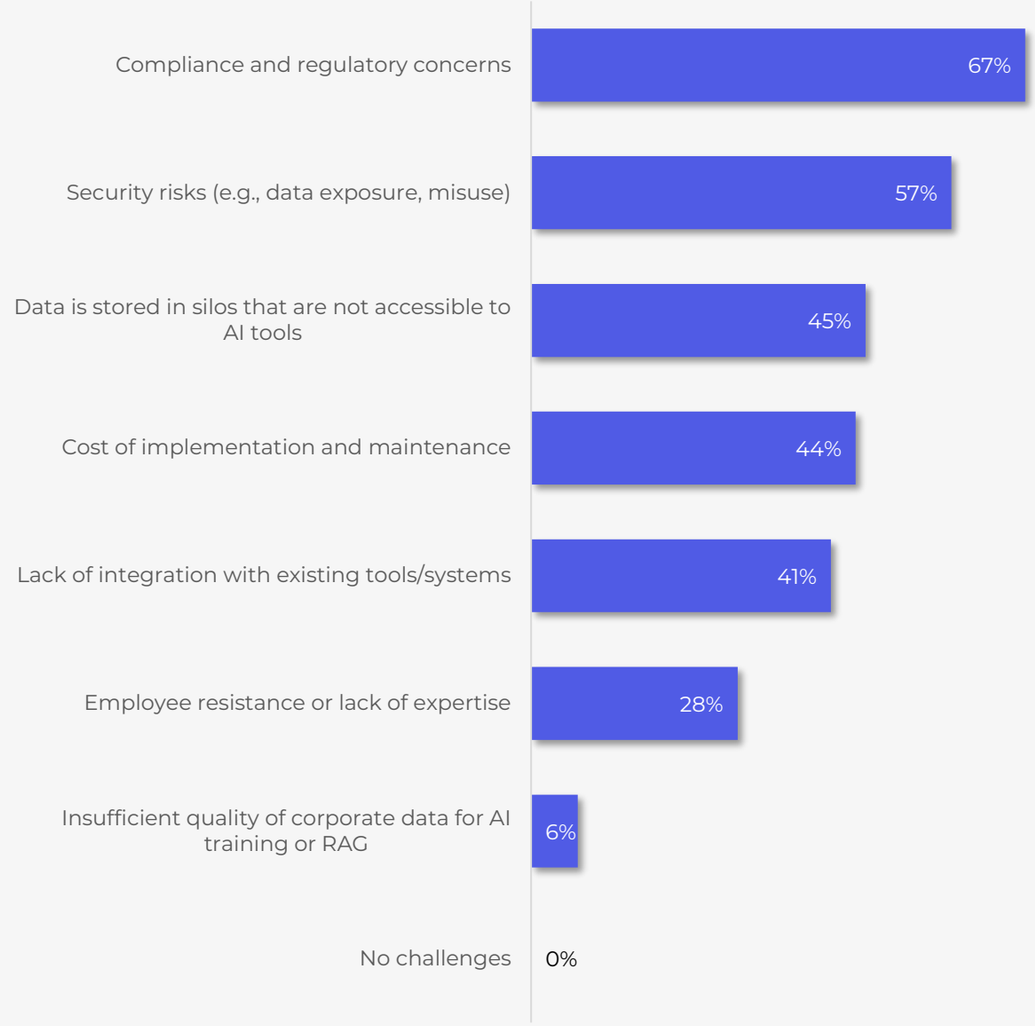

Figure 18: Encountered/Anticipated Challenges in Deploying LLM/AI-Based Tools

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Diving into the Detail: The #1 Greatest Challenge in Deploying AI-Based Tools

We then asked respondents to narrow down their answer and highlight the greatest challenge that they face or anticipate. We found that respondents consistently pointed to compliance and regulatory issues, followed closely by security risks.

This may be related to the maturity of the AI industry overall, which is still in its infancy. Compliance and security are often implementation hurdles, while as organizations move further along their AI journey, and adoption deepens, other obstacles may emerge, such as employee lack of expertise and data silos or data quality, currently low on the list of concerns.

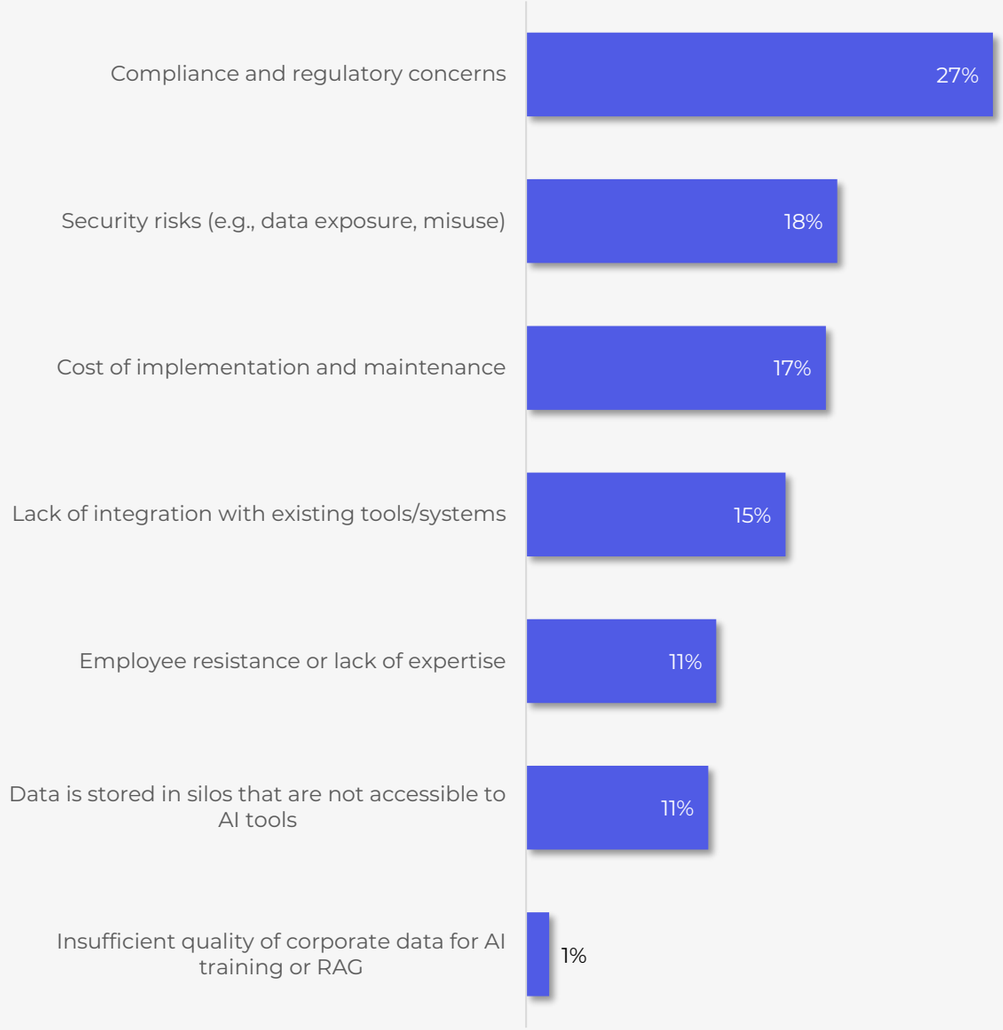

Figure 19: Greatest Challenge in Deploying AI-Based Tools

What Matters Most When Choosing AI Tools to Enhance Data Value?

When selecting AI tools to unlock more value from their data, IT and Security leaders overwhelmingly prioritize security (85%) and compliance (66%), which are two concerns that continue to dominate both adoption and deployment discussions. In fact, these two criteria are becoming increasingly intertwined, as organizations seek tools that not only perform securely but also meet evolving regulatory demands.

Cost (63%) comes next in the list of priorities, although 4% say it's not important, suggesting that while cost matters, some are willing to spend more for the right solution.

Interestingly, performance ranks fourth at 51%, indicating that almost half of organizations prioritize trust, governance, or cost before evaluating whether a tool can actually deliver business results.

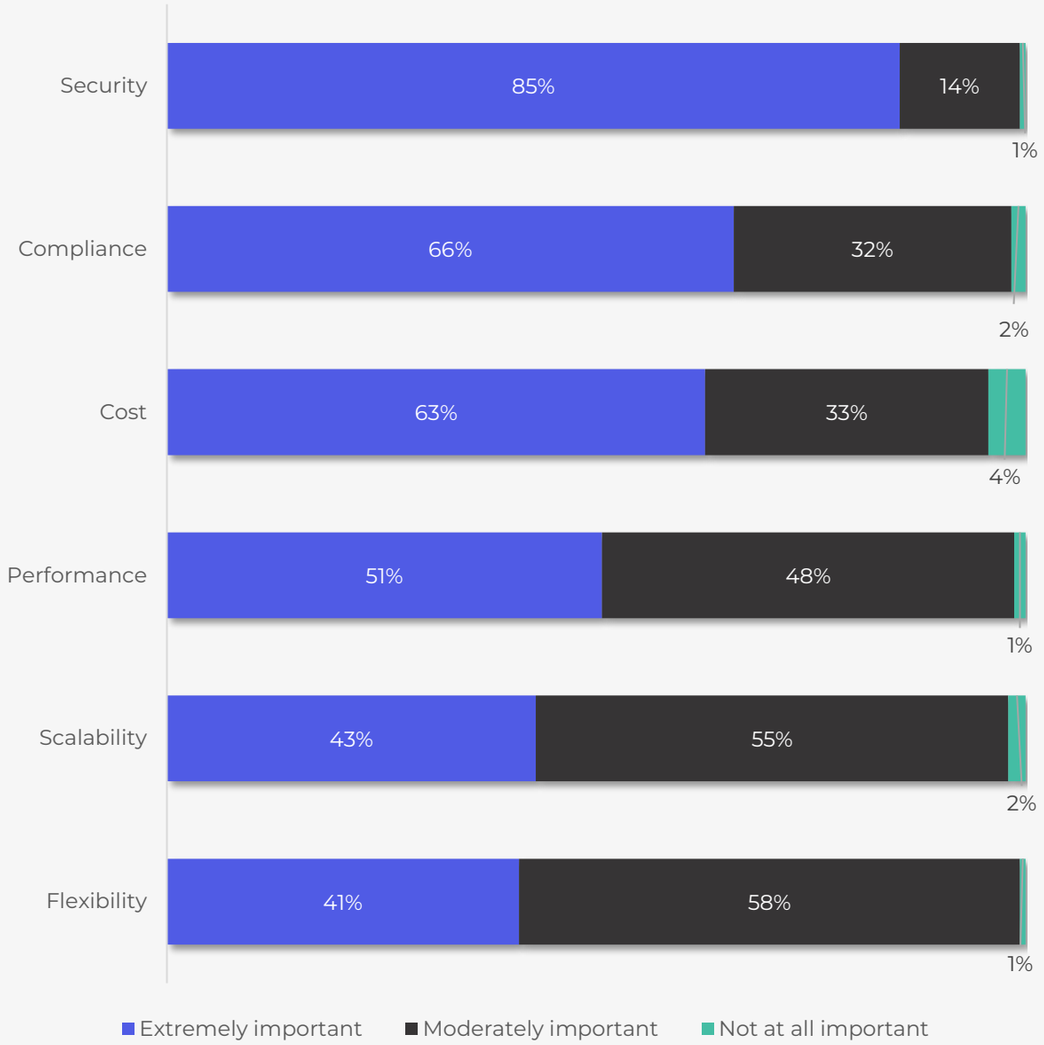

Figure 20: Importance by Criteria to Introduce AI Tools for Enhancing Data Value

Demographics

Country, Industry, Job seniority, Role

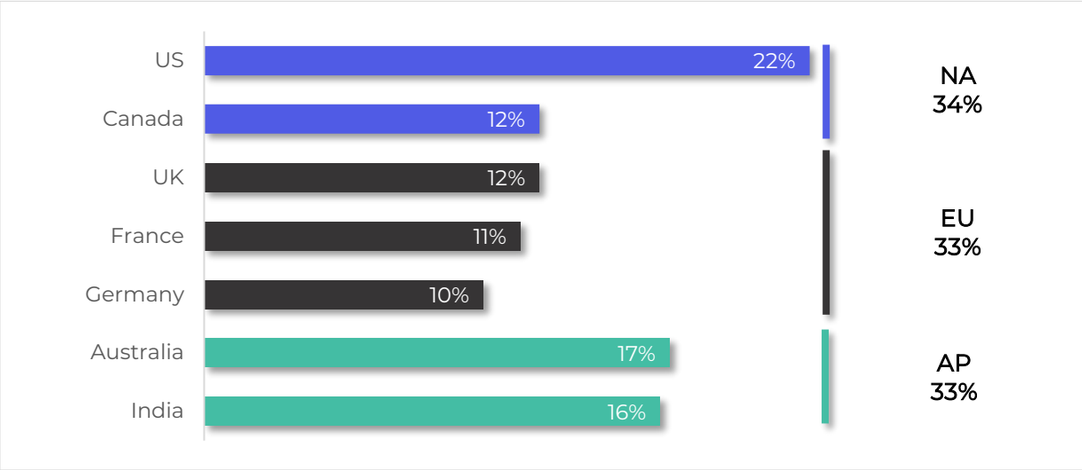

Figure 21: Country

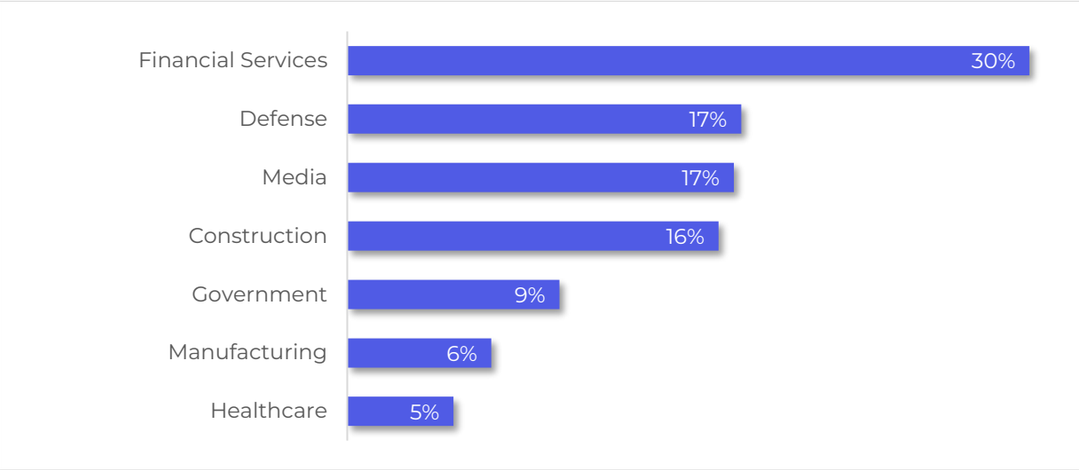

Figure 22: Industry

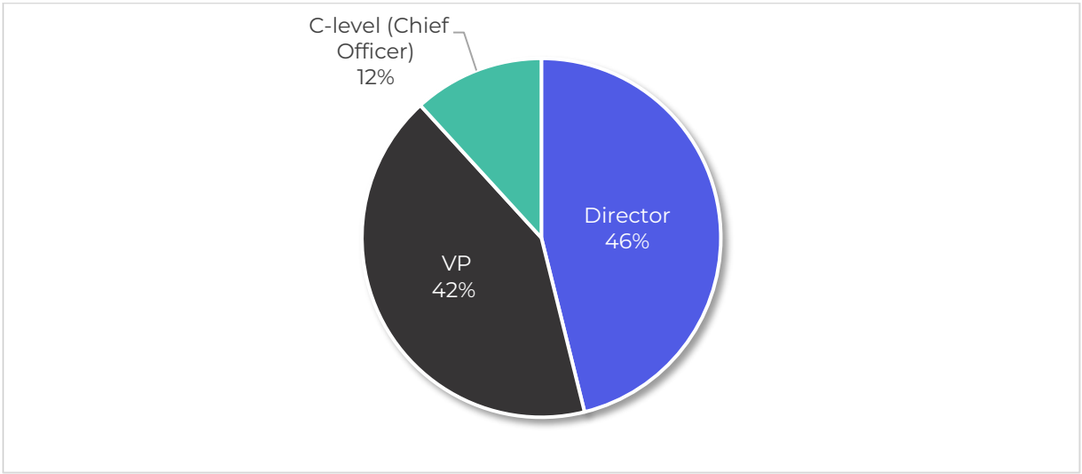

Figure 23: Job seniority

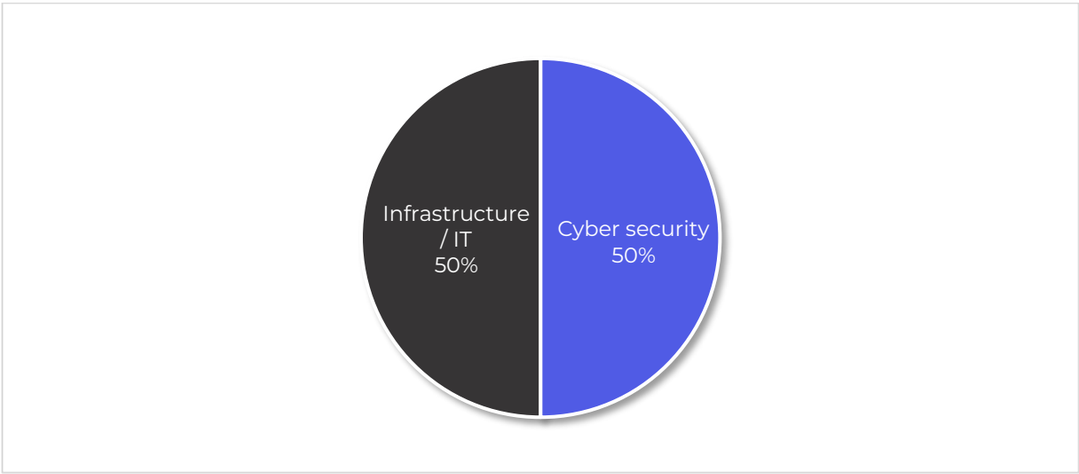

Figure 24: Role

Company Size, Cloud File Storage, Company Sites

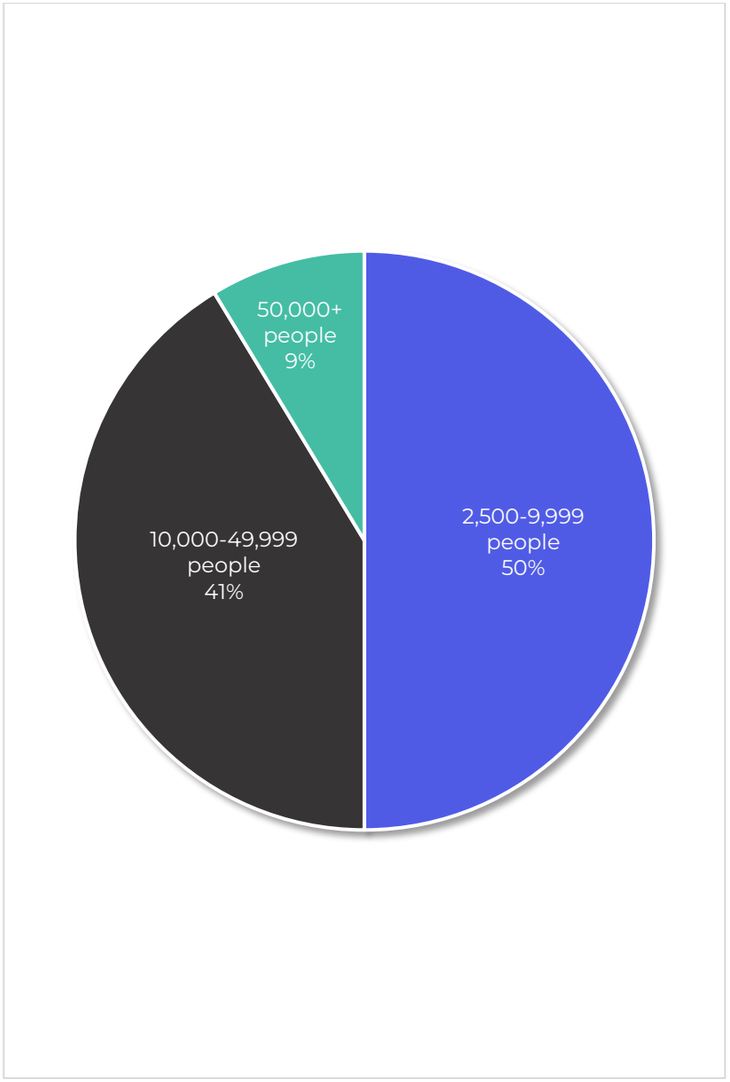

Figure 25: Company Size

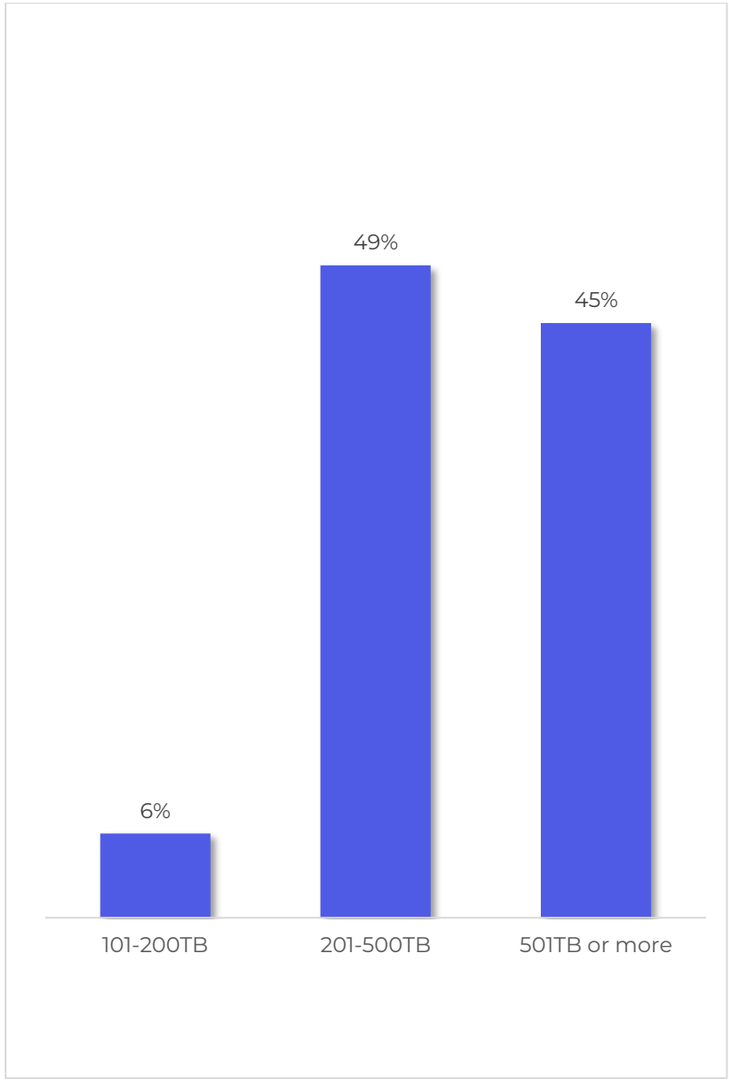

Figure 26: Cloud File Storage

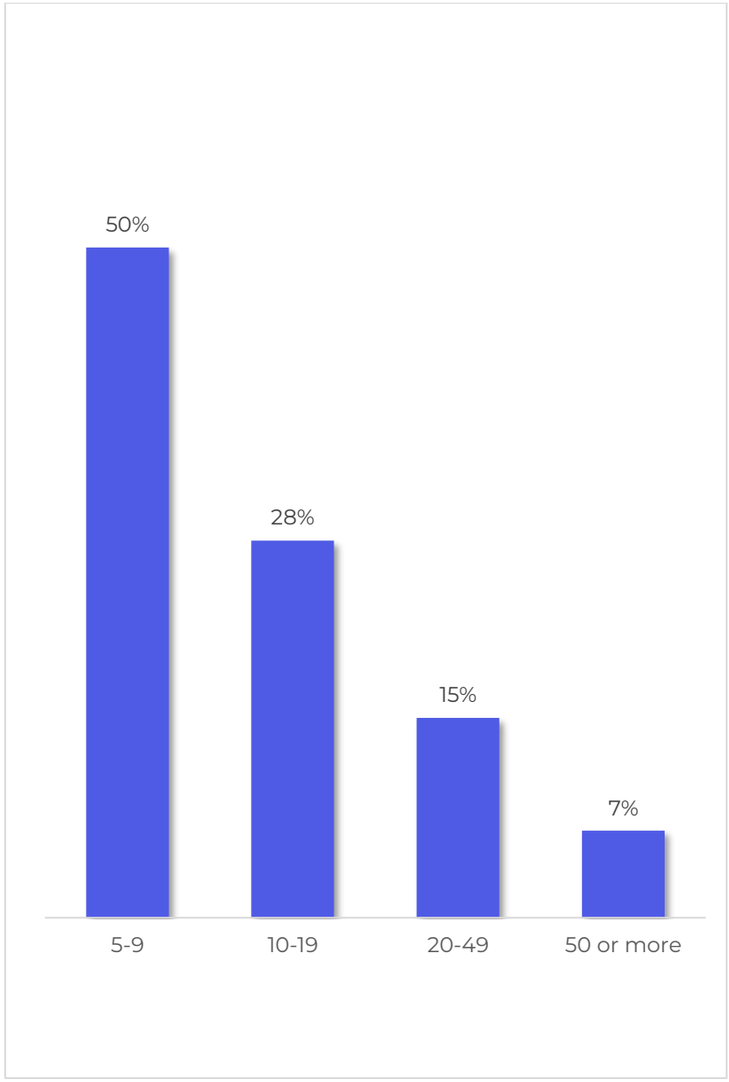

Figure 27: Company Sites

About CTERA

CTERA is the global leader in the integrated data intelligence market enabling organizations of all sizes to efficiently and effectively manage, protect, and leverage their data across highly distributed environments. With a foundation built on security, scale, and seamless integration, the CTERA Intelligent Data Platform empowers organizations to align their data management strategies to continuously deliver against today's business needs and tomorrow's vision.

Request a Demo

Visit us at:

www.ctera.com

Phone: +1 (917) 768-7193 | Email: info@ctera.com