The Era of Hybrid Cloud Storage

Research into the impact of digital transformation, AI, and security on storage strategies
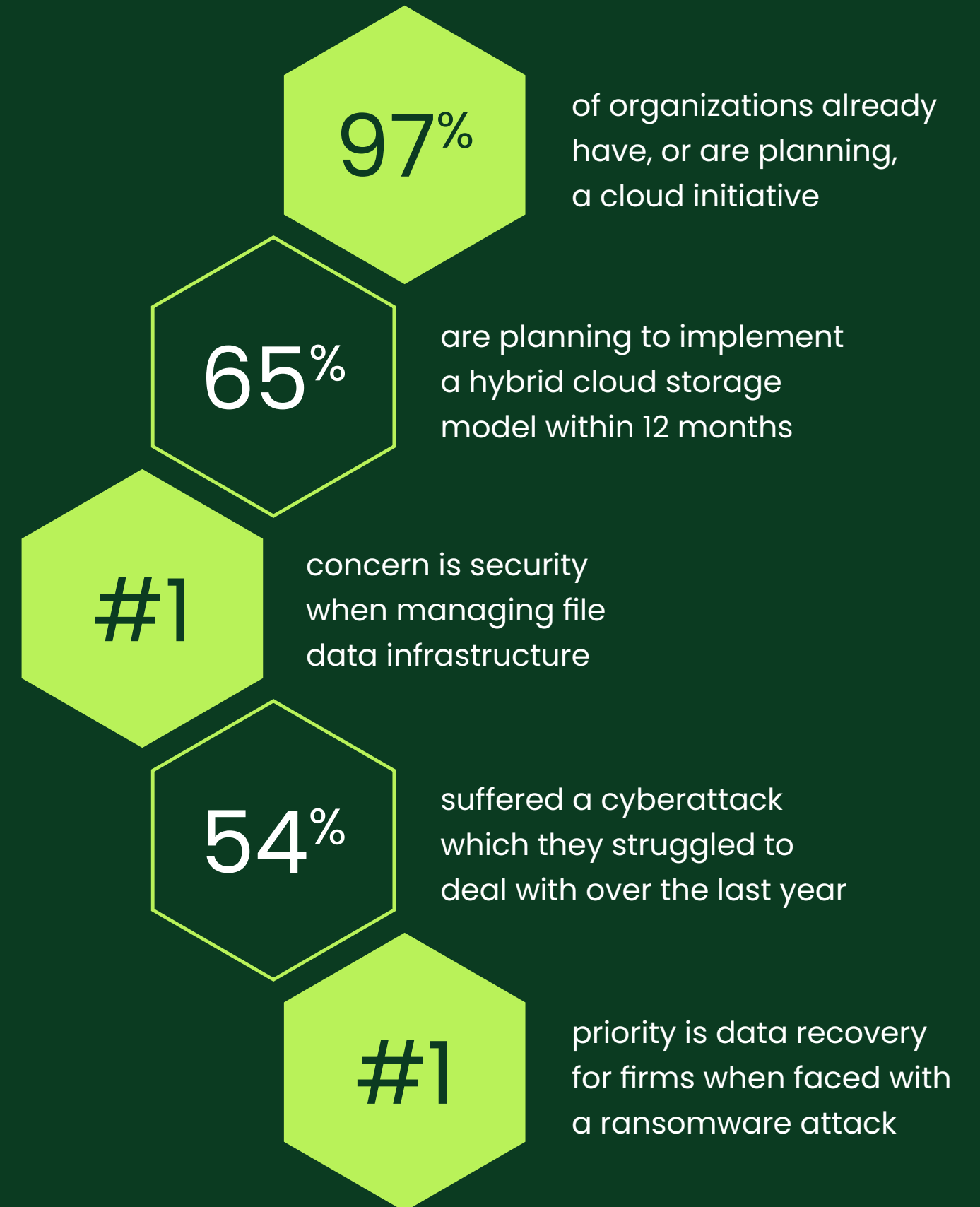
2024

ΞNASUNI

Contents

Introduction

Businesses are increasingly adopting a hybrid cloud model. The hybrid cloud market was worth $85 billion in 2021 and is projected to have more than tripled by 2027[1]. Around 60% of enterprise data will be hybrid by 2027, compared to 20% today[2].

It's clear to see what's driving this trend. Companies that develop a successful data strategy that works across data centers, edge locations, and public cloud infrastructure can find it easier to streamline operations, strengthen security, and scale up.

But one consideration that's often neglected in the shift to hybrid cloud is fit-for-purpose file storage. While time and resources are dedicated to managing workflows and services across different systems, less emphasis is put on successfully securing, accessing, and analyzing data which often sits across disparate file servers and backups.

1   https://www.statista.com/statistics/1232355/hybrid-cloud-market-size/
2   Gartner Research - Modernize Your File Storage and Data Services for the Hybrid Cloud Future, Julia Palmer, Feb 2023, ID# G00775770

97% of organizations already have, or are planning, a cloud initiative

65% are planning to implement a hybrid cloud storage model within 12 months

#1 concern is security when managing file data infrastructure

54% suffered a cyberattack which they struggled to deal with over the last year

#1 priority is data recovery for firms when faced with a ransomware attack

We surveyed more than a thousand purchasing decision makers in the US, UK, and DACH regions to understand how topics such as digital transformation, security, and AI are impacting data storage strategies in the hybrid era.

The survey uncovers some surprising findings...

- Despite the impact of high inflation, slow growth, and energy prices on budgets, **data-related decisions are more likely to be influenced by security considerations than by cost-cutting.**

- There's a feeling of confidence when it comes to organizations' ability to tackle cyberattacks, which doesn't stack up against the reality. **Three-quarters of organizations believe they're well-defended despite more than half of them suffering cyberattacks** resulting in anything from difficulty recovering data to ransom payments.

- The pace of change is striking: while less than one-fifth of firms currently have a hybrid cloud storage solution, **nearly two-thirds are planning to implement one within the year.**

- **When it comes to AI, better management and visibility of data are seen as more valuable outcomes** than lowering costs, automating workflows, or improving customer experience.

- **Almost half of firms will prioritize AI investments over the next eighteen months,** but in order to capitalize on this spend, firms are recognizing the need to become more data-centric.

- Our hope is that the findings in this report will help you benchmark your own organization's progress on your hybrid cloud journey. Additionally, by uncovering prevailing attitudes and changing strategies, **you'll be better equipped to capitalize on one of your most valuable assets—data**—while defending against potential pitfalls along the way.

Methodology
This survey was conducted among 1,150 purchasing decision makers, across the US, UK, and DACH region (Germany, Austria, Switzerland), in organizations with 500+ employees. The interviews were conducted online by Sapio Research in March and April 2024 using an email invitation and an online survey.

What do we mean by hybrid cloud storage?

Hybrid cloud storage blends the scalability advantages of cloud-based object storage with local performance delivered via intelligent file caching at the edge and integrated data security, all in a single, unified platform.

This combination provides unlimited scale to support business growth, while providing a file data platform that can assist with solutions such as support for AI services.

Section 1:
The cloud context

The pace of cloud adoption and what's triggering organizations to invest.

The majority have cloud baked into operational strategy

The benefits of the cloud, for everything from supporting business growth to reducing overhead, are generally acknowledged in today's organizations. An overwhelming **97% of organizations either already have a cloud initiative or are in the planning stage.**

Firms operating in the tech sector are far more likely to already have a cloud initiative in place (94%) than those working in the field of marketing and sales (67%).

"

The software and IT services segments will both see double-digit growth in 2024, largely driven by cloud spending. Global spending on public cloud services is forecast to increase 20.4% in 2024.[3]

Gartner press release, October 2023

3   https://www.gartner.com/en/newsroom/press-releases/2023-10-18-gartner-forecasts-worldwide-it-spending-to-grow-8-percent-in-2024

84%	13%	3%
Yes	**No, but we plan to**	**No, and we do not plan to**

1,150 respondents were asked if they currently have a cloud initiative within their company.
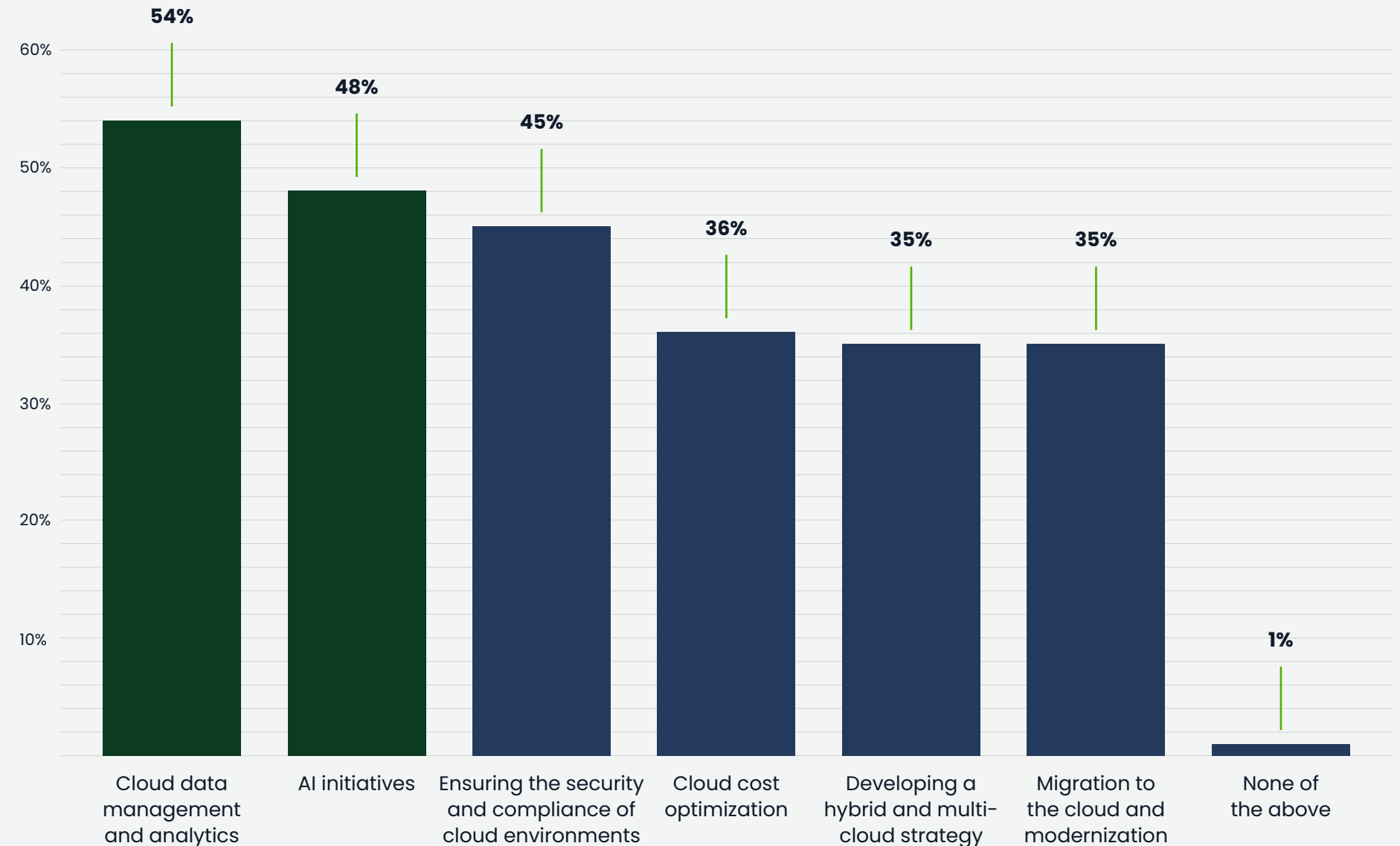
Around half of organizations are investing in analytics and AI

Faced with what Gartner describes as the 'explosive growth of enterprise data'[4] it makes sense that **the top cloud investment area over the next 18 months is data management and analytics (54%).** Once processed and analyzed, companies' data can be used to fuel AI initiatives—the second-most popular investment area (48%), according to our survey respondents.

Organizations are also investing in the security of their cloud environments (45%)—prioritizing this above cost optimization (36%).

When it comes to investing in hybrid and multi-cloud strategies, we see a gulf between industry sectors. Only 18% of government organizations are prioritizing this area, compared to 39% of energy and utilities companies, and 47% of architecture, engineering, and construction (AEC) firms.

---

4 Gartner®, Top Trends in Enterprise Data Storage 2023, Analysts Chandra Mukhyala, Julia Palmer, Jeff Vogel, 29 June 2023

Bar chart:
- Cloud data management and analytics: 54%
- AI initiatives: 48%
- Ensuring the security and compliance of cloud environments: 45%
- Cloud cost optimization: 36%
- Developing a hybrid and multi-cloud strategy: 35%
- Migration to the cloud and modernization: 35%
- None of the above: 1%

1,112* respondents were asked which of the options were key investment areas over the next 18 months.

Cloud delivers on efficiency and security goals

59% of organizations are seeing their cloud initiatives delivering better data security and disaster recovery times.
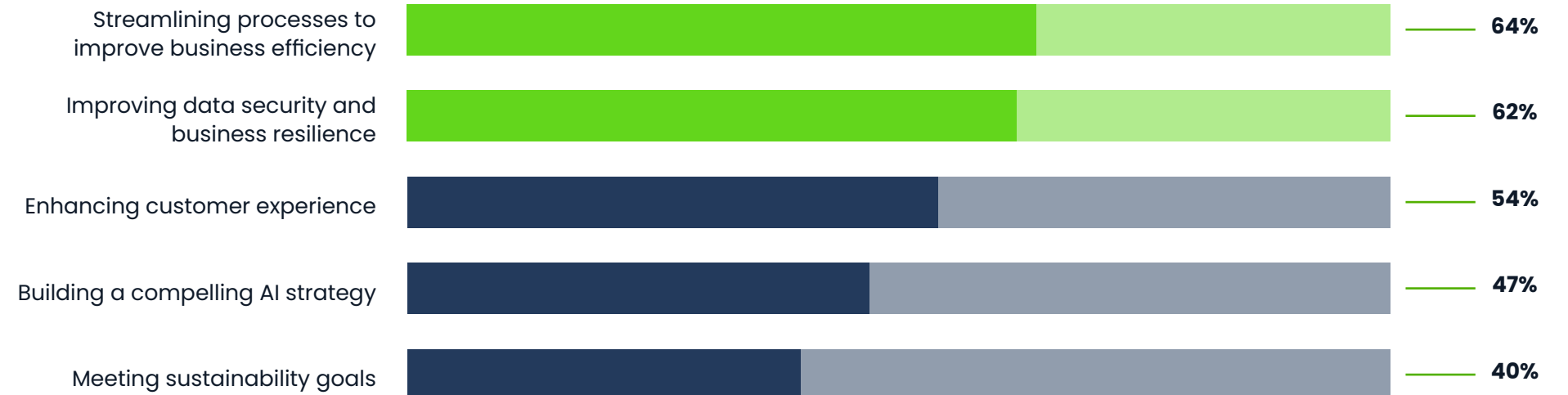
Over half have also experienced improved application performance and feel more equipped to scale their operations.

These benefits are seen as even more important than the cost savings, which can be achieved through cloud initiatives.

Nearly two-thirds of organizations report that their cloud infrastructure strategy is helping to make their business more efficient. **62% say the cloud supports their goal of improving data security and business resilience.**

Benefit	Percentage
Improving data security and disaster recovery times (RPO/RTO)	59%
Improving application performance	56%
Scalability and flexibility	55%
Cost savings	51%
Eliminating disparate data silos	33%
Addressing ESG initiatives	26%

1,112* respondents were asked what they perceive to be the top operational benefits of their cloud initiative.

Goal	Percentage
Streamlining processes to improve business efficiency	64%
Improving data security and business resilience	62%
Enhancing customer experience	54%
Building a compelling AI strategy	47%
Meeting sustainability goals	40%

1,112* respondents were asked to select the business goals that their cloud infrastructure strategy supports or will support.
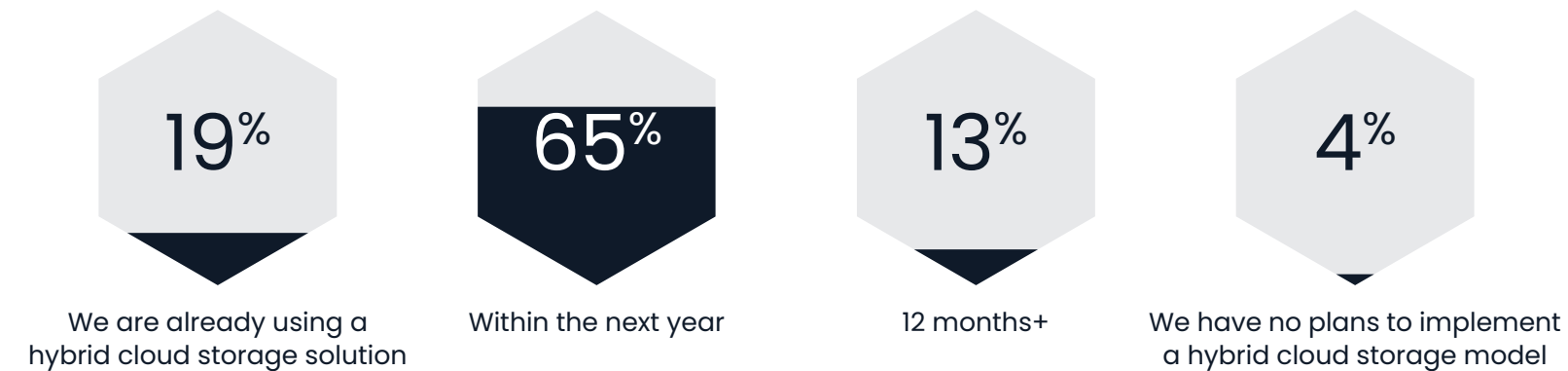
Section 2:
Trends in data storage

The strategies organizations are adopting to deal with increasing volumes of data and data silos.

Organizations rush to adopt hybrid cloud storage within the year

While less than one-fifth of companies currently have a hybrid cloud storage model, **a staggering 65% are planning to implement one within the next year.**

19%	65%	13%	4%
We are already using a hybrid cloud storage solution	Within the next year	12 months+	We have no plans to implement a hybrid cloud storage model

1,112* respondents were asked when, if at all they plan to implement a hybrid cloud storage model.

Of those currently using a hybrid cloud storage solution, 70% are planning to upgrade within the next 18 months.

70%	9%	5%	16%
Yes, in the next 18 months	Yes, in the next 24 months	Yes, in more than 24 months	No, we do not plan to upgrade our hybrid cloud storage solution

Those 208 who are already using one were asked if they have plans to upgrade.

[The] challenges arise from managing the explosive growth of enterprise data, the business need for an on-premises cloud-like consumption model to mitigate cyberattack risks, or leveraging latest storage technologies like QLC or NVMe over fabric for better cost and/or performance.

Modern storage offerings provide solutions to these challenges while continuing to deliver on increasing performance and lower total cost of ownership (TCO).[5]

Gartner®, Top Trends in Enterprise Data Storage 2023

---

5   Gartner®, Top Trends in Enterprise Data Storage 2023, Analysts Chandra Mukhyala, Julia Palmer, Jeff Vogel, 29 June 2023

Reliance on private cloud among 50% of companies

Despite its restrictions – in terms of cost, ongoing maintenance, and limits on scale – **50% of organizations are using private cloud to build their hybrid cloud storage solution.**

This, in comparison to 41% taking a public cloud approach and 9% using both.

50%
Private cloud

41%
Public cloud

9%
Both
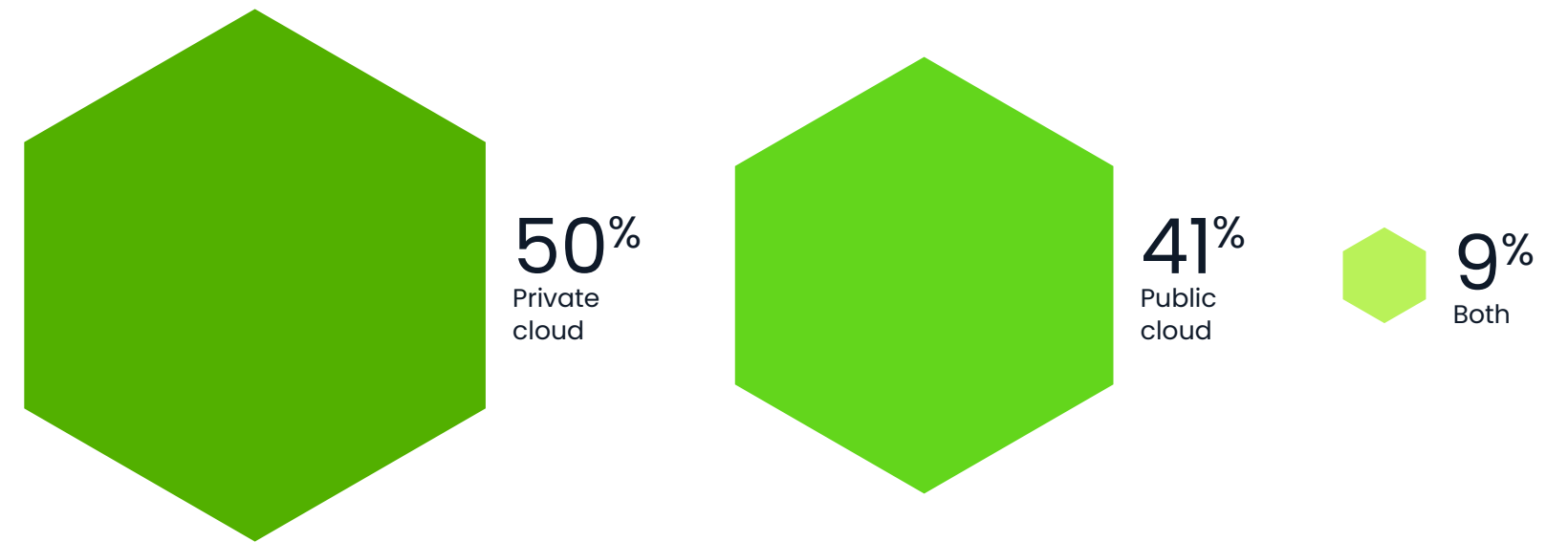
1,071* respondents were asked which of the options they are using to build their hybrid cloud storage solution.

Security tops list of file data challenges and concerns

Security concerns are the top reason firms haven't moved file data into the cloud – and also the top challenge when managing file data.

45% of respondents say concerns around security keep them from moving file data to the cloud – significantly more are prevented by worries about costs, training, or complexity.

For infrastructure teams trying to manage files, perhaps across a patchwork of different offices and systems, securing data and recovering it after an attack can be a headache. **Our respondents ranked security concerns higher than anything else when managing file data infrastructure,** including meeting compliance requirements and supporting inter-departmental collaboration.
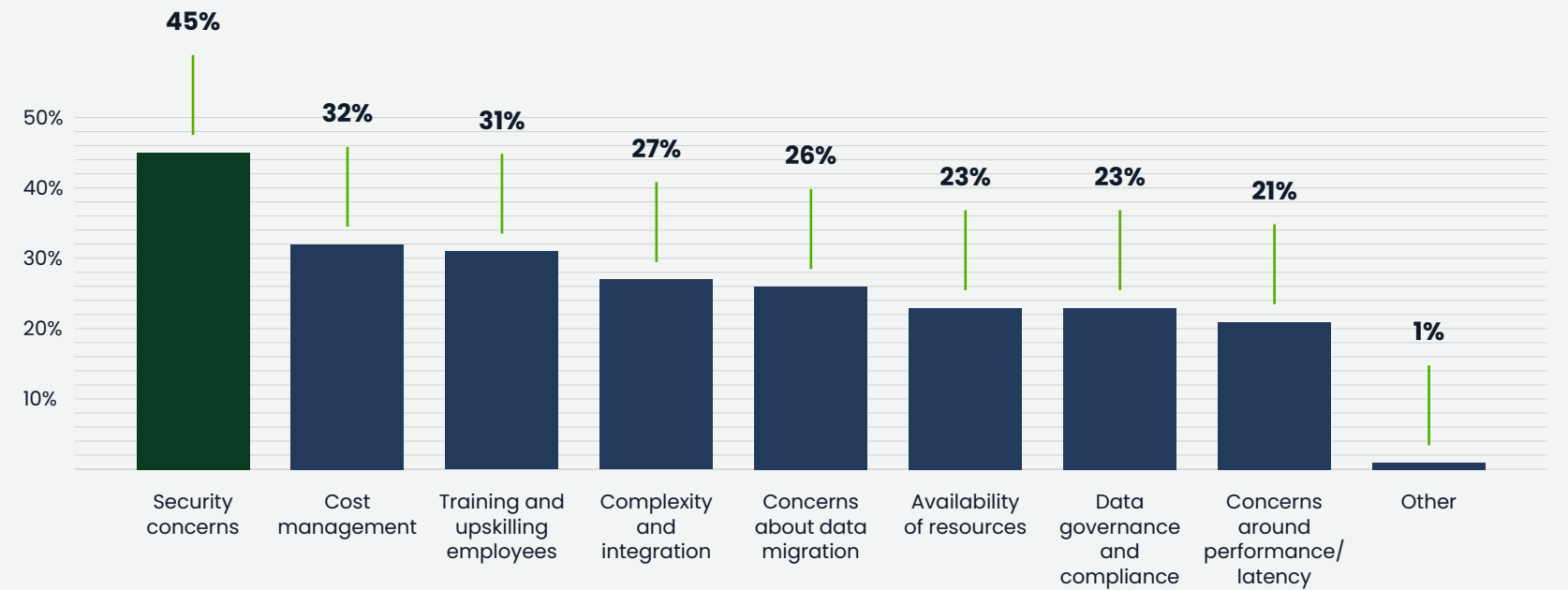
183* respondents were asked what has kept them from moving their file data to the cloud.
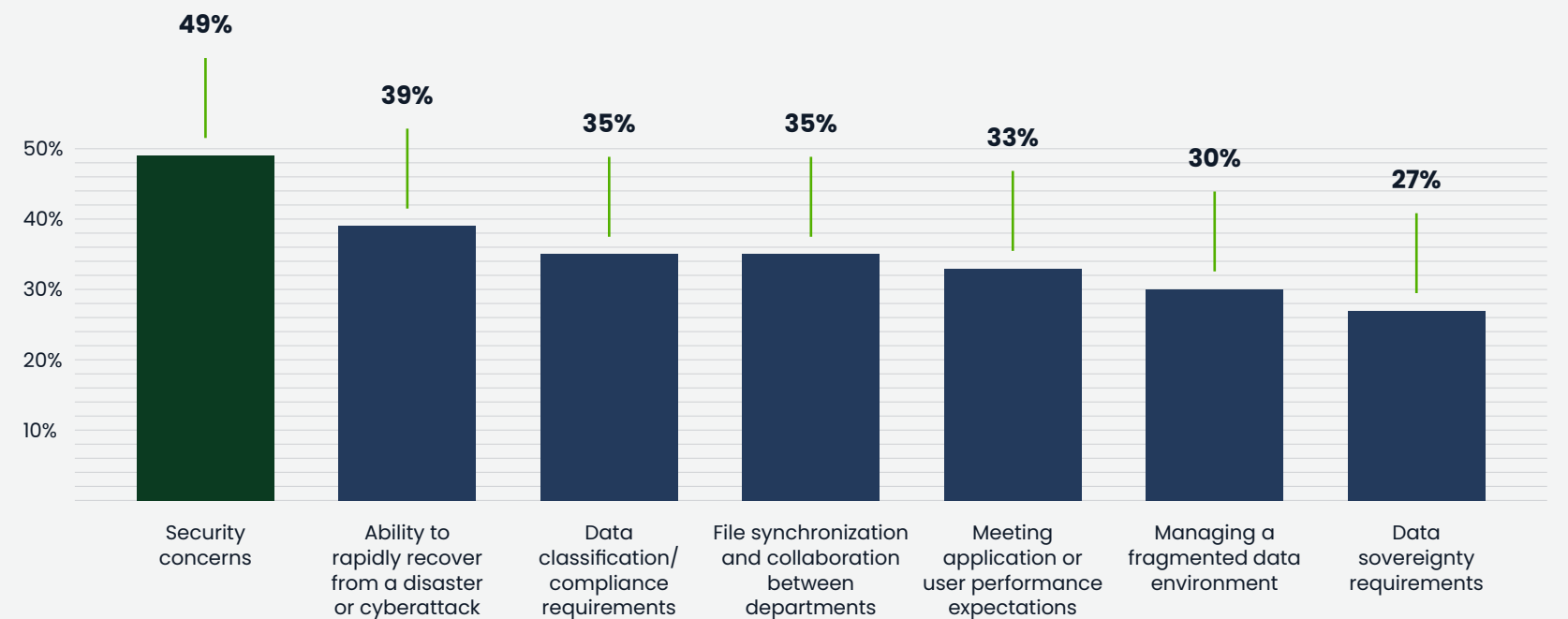
1,150 respondents were asked what their biggest challenges are when managing file data infrastructure today.

Section 3:
The impact of AI

Opportunities and roadblocks encountered
on the AI implementation journey.

The IT department takes the lead on AI initiatives

Despite the explosion of interest in AI across the enterprise, **primary decision-making authority is still most likely (44%) to sit within the IT department.** Around one-third (32%) of respondents reported that their C-suite leads on AI decisions.

44%
IT department

32%
C-suite executives

15%
Cross-functional team involving multiple departments

7%
Data science or analytics department

1,150 respondents were asked who holds the primary decision-making authority regarding AI-related initiatives within their organization.

"

Cloud makes it possible to quickly deploy new technologies at scale while simultaneously reducing risk," said Dave McCarthy, research vice president, Cloud and Edge Infrastructure Services at IDC.

As AI captures the imagination of technology and business leaders, the agility provided by cloud enables organizations to deliver continuous value for both internal and external stakeholders.[6]

IDC FutureScape: Worldwide Cloud 2024 Predictions

Organizations target advanced data management through AI

Advanced data management techniques, such as data mining for improved analysis and forecasting, can provide firms with a competitive edge. **Well over half (60%) of respondents are hoping AI will help them deploy advanced data management and achieve greater visibility.** This goal is marginally more important than even cost savings (58%).

58%
Cost reduction/ savings

57%
Automation of certain workflows

60%
Advanced data management and visibility

52%
Enhanced customer experiences

1%
Other

1,125* respondents were asked what outcomes or return on investment (ROI) they aim to achieve by adopting AI solutions.

Security concerns and skills shortages hamper AI rollout

The biggest roadblocks preventing organizations from either developing or implementing AI solutions are data privacy and security, and skills shortages. As we've seen elsewhere in this report, considerations around security are driving more decisions than cost issues, which in this instance sit at the bottom of the list of impediments.

42%
Data privacy and security concerns

35%
Lack of expertise or skilled personnel in AI technology

30%
Dependence on third-party vendors or AI service providers

27%
Difficulty in identifying suitable AI use cases for the business

22%
Data silos leading to lack of data visibility and control

22%
Insufficient budget or resources

1%
Other
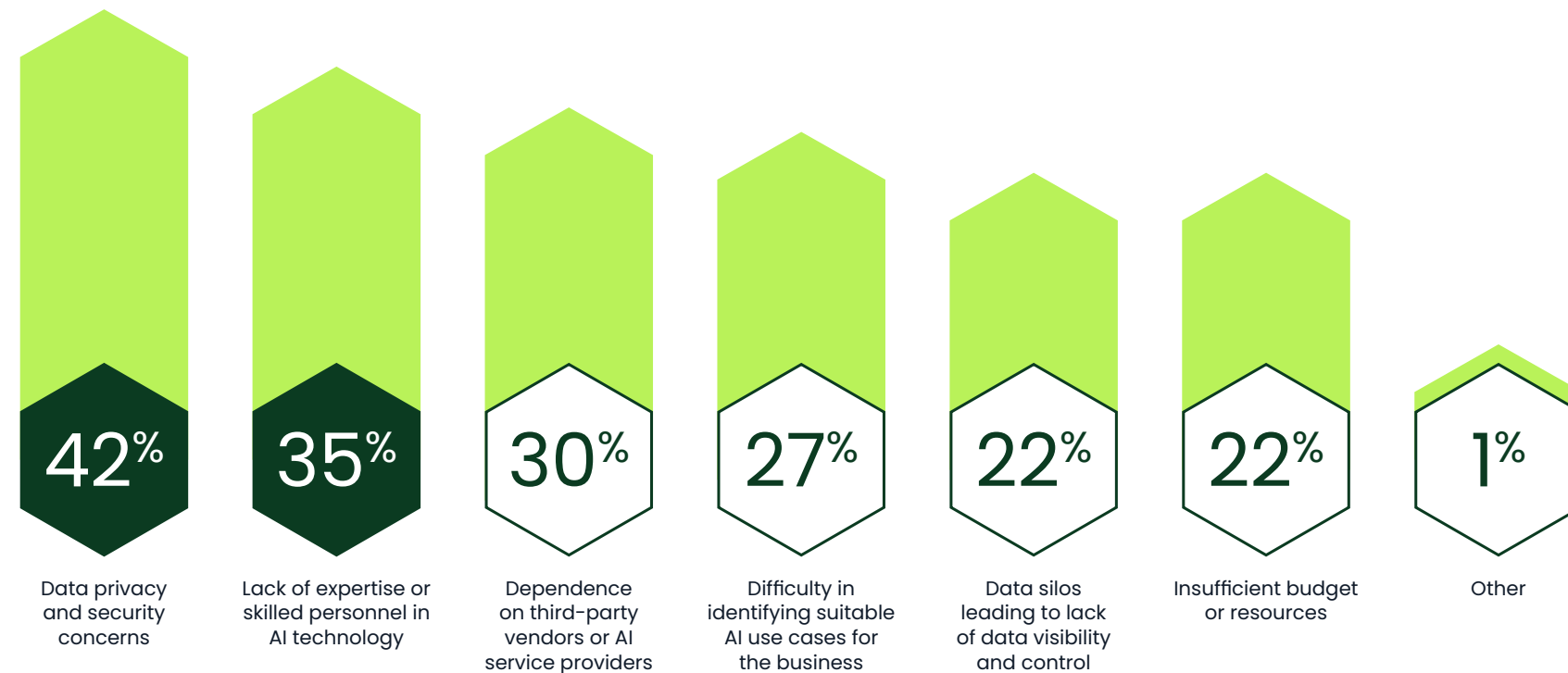
1,125* respondents were asked what their biggest roadblocks are when it comes to developing or implementing AI solutions for the business.

Section 4:
Storage and security

Top concerns in the battle to protect companies' valuable assets from cybercriminals.

Disconnect between firms' cybersecurity confidence and preparedness

Businesses worldwide paid out over $1bn in ransomware payments last year, and 2024 is forecasted to be even worse[7].

In the face of statistics like these, it's no surprise that we've seen security concerns preoccupy our respondents throughout this survey. But there's a chasm between how prepared organizations feel in the face of cyberattacks, and the reality of their ability to protect against them.

Three quarters of respondents feel confident their organization can recover critical unstructured data and cope with a destructive cyberattack. And yet, over the past year, **54% suffered an attack which resulted in either a ransom payment, costly downtime, data loss, reputational damage, or issues recovering the data.**

There is a risk that firms, mistakenly believing themselves to be well-prepared, neglect to make themselves so in reality.

---

7 https://www.fisherphillips.com/en/news-insights/ransomware-costs-businesses-record-high-1-billion-in-2023.html

Three quarters of respondents feel confident

40%
Very confident

We have a multi-layered approach, good security hygiene, and a team regularly trained to cope with any attacks

34%
Confident

We have many tools and a multi-layered approach to cope with attacks

23%
Somewhat confident

We have some tools in place that should help cope with an attack

1%
Not confident

Our organization is not ready to cope with an attack

2%
N/A

I don't have insight into our security strategy

1,150 respondents were asked how confident they are in their organization's ability to recover critical unstructured data and cope with a destructive cyberattack.

- **27%** — We have not experienced any attacks in the last year
- **20%** — We easily detected, mitigated, and recovered from the attack
- **20%** — We were able to recover after costly downtime, data loss, and reputational damage
- **17%** — We were able to detect and mitigate the attack, but struggled to recover data
- **9%** — We were forced to pay the ransom
- **8%** — We were forced to pay the ransom and were attacked again

1,150 respondents were asked what the main outcome was of any cyberattacks experienced in the last year.

Gaps in cybersecurity strategies

While almost half of organizations (49%) have taken steps to make sure their data is backed-up, immutable, and easily recoverable, **60% don't have a well-rehearsed plan in place for if an attack occurs.**

Less than half (47%) have tools capable of detecting attacks in real time, and more than half (53%) lack a dedicated security team overseeing their infrastructure.

49%
We ensure that our data is backed-up, immutable, and easily recoverable

47%
We have a dedicated security team with insight and responsibility for our infrastructure cyber resilience

33%
We have invested in AI and ML to help defend against attacks

30%
We follow a specific framework, such as NIST or Zero-Trust

47%
We have detection tools in place that are able to identify attacks in real time
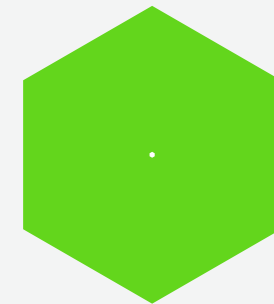
40%
We have a plan in place if an attack occurs, and regularly practice it

32%
We utilize a cyber insurance company to mitigate any damage from cyberattacks

2%
None of the above

1,150 respondents were asked measures their organization has taken to make their data more cyber resilient.

Healthcare organizations are far more likely to say their data is backed up and recoverable (60%) than firms operating in engineering (38%). In the United States alone, healthcare security breaches have almost doubled in the past five years[8].

---

8 https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf

Responsibility for security spans departments

Just over one-third (31%) of companies say their infrastructure and operations (I&O) and security operations (SecOps) teams jointly own hybrid cloud storage security in the business; collaborating on decision making in this area. The figure rises to 41% in the manufacturing sector.

31% I&O and SecOps share responsibility and collaborate on security decisions

23% I&O team has security responsibility and budget, but requires sign off from SecOps

14% SecOps team owns all decisions, budget, and responsibility for security

13% I&O team has security responsibility and budget, with no interaction from SecOps

10% We outsource our cybersecurity decisions and responsibilities

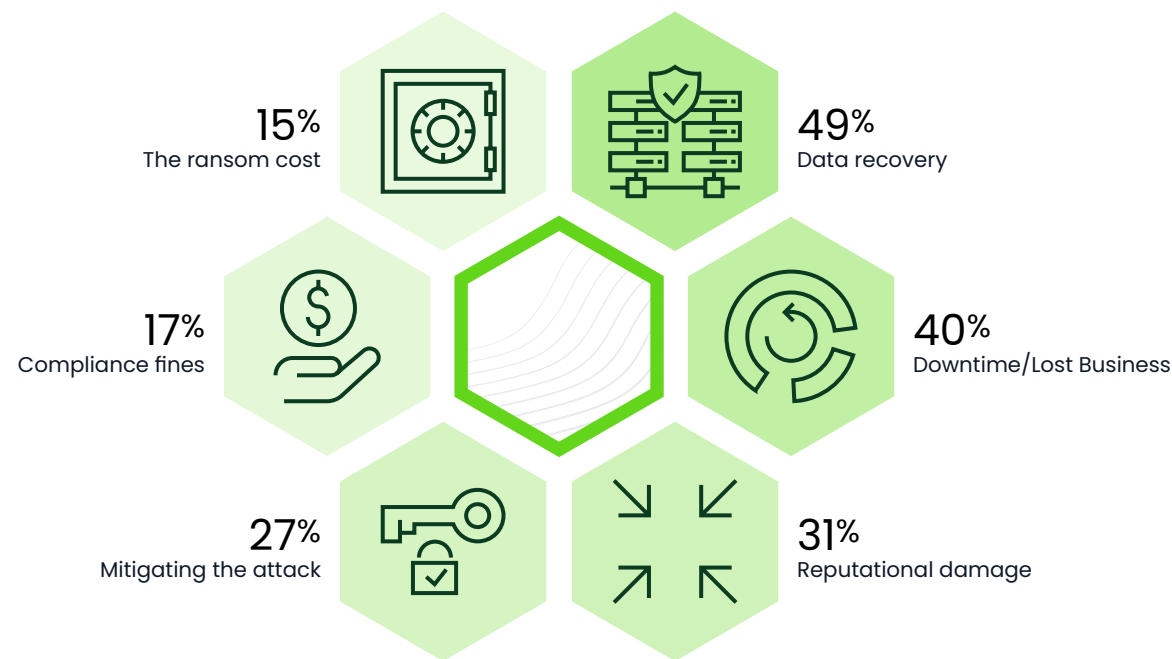**8%** We rely on our cloud vendor's security capabilities

1% Other

1,150 respondents were asked who in their organization has ownership when it comes to hybrid cloud storage security.

Ransomware fears spark data recovery concerns

It takes an average of 277 days for security teams to identify and contain a data breach, according to a 2023 report.[9] That's over nine months of potential operational downtime and resources tied up in recovering or securing data.

When contemplating the prospect of a ransomware attack, organizations' top concern is around data recovery, with 49% of respondents citing this issue.

15%
The ransom cost

49%
Data recovery

17%
Compliance fines

40%
Downtime/Lost Business

27%
Mitigating the attack

31%
Reputational damage

1,150 respondents were asked what their organization's primary concern is with a potential ransomware attack.

9 https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

"

Beyond the [ransom] payments, the average cost of each ransomware attack last year was over $5 million.[10]

Fisher Phillips, Ransomware Costs Businesses Record-High $1 Billion in 2023

10 Ransomware Costs Businesses Record-High $1 Billion in 2023: Your 5-Step Plan to Prevent Attacks in 2024 | Fisher Phillips

Key takeaways

Data is the foundation of business; but for many, data management isn't a priority topic. It only hits the top of the agenda when access problems manifest themselves in critical ways.

For instance, when data can't be accessed—to support collaboration or fuel innovation—or conversely when it's accessed too easily, and security breaches occur. What's clear from this survey of senior leaders is that those access issues are becoming acute. Relying on legacy, on-premises solutions isn't an option in the era of hybrid cloud.

Security and backup are indivisible from storage

Half of organizations say their data is backed-up, immutable, and easily recoverable—which leaves a worrying 50% who risk data being lost or deleted. Infrastructure teams who try to tackle security and back-up separately to storage risk drowning in complexity, thanks to the exponential growth in unstructured data. And the problem will only grow more complicated, unless firms adopt hybrid cloud storage solutions with built-in security and backup.

Recovering quickly after breaches is critical

If the worst happens and a security breach occurs, the top concern for organizations is recovering their data. The ramifications of data loss and downtime spread far and wide in a business, so the quicker the problem can be resolved, the better. It's one reason we designed a platform capable of recovering a million files within a minute. Most solutions aren't designed to recover such high volumes of data across multiple locations.

Key takeaways

Efficiency and collaboration must be baked in for growth

We all know working patterns have changed since the pandemic. Add to that the recent increase in M&A activity (up 41% in the last quarter of 2023)[11] and it's easy to see why firms need to find ways to work efficiently across disparate locations. Improving business efficiency is the top business goal for organizations' cloud infrastructure strategies. At Nasuni, we've developed our platform to support long-distance collaboration through virtual machines at the edge, synchronized with the cloud, which prevent accidental overwriting of changes.

AI-fueled innovation will rely on extracting value from data

AI offers a competitive advantage to those who manage to deploy it well. But 42% of firms say concerns around data security are hampering AI implementation. Cost-wise, relying on legacy storage in this scenario is a double-whammy: expensive to run and a brake on the increased profit margins offered by AI. Leading firms will securely break down data silos across on-premise, private, and public cloud with a single storage platform. Nasuni offers these forward-thinking firms, including the one-third (35%) lacking in-house AI expertise, support to build strong data foundations for successful AI strategies.

"

As hybrid cloud storage takes center stage, organizations need strategies to capitalize on their most valuable asset: data. In tandem, they need strategies for addressing critical IT issues including ransomware attacks and the introduction of AI integrations to the market. Legacy storage solutions cannot keep up with these demands. Nasuni's 'The Era of Hybrid Cloud Storage' report gives organizations the necessary industry and peer insights to understand and take action in a rapidly evolving cloud landscape.

David Grant, President, Nasuni

About Nasuni

Nasuni is a scalable data platform for enterprises facing an explosion of unstructured data in an AI world.

The Nasuni File Data Platform delivers effortless scale in hybrid cloud environments, enables control at the network edge, and meets the modern enterprise expectation for insight- and AI-ready data. It simplifies file data management while increasing storage access and performance. Its best-in-class file recovery protects customers against a range of cyber threats and eliminates the need for specialized backup and disaster recovery – all while cutting the cost of infrastructure by up to 65%.

Organizations worldwide rely on Nasuni, spanning across the manufacturing, construction, energy, consumer goods, and public sectors. Nasuni's corporate headquarters is located in Boston, Massachusetts, and the company delivers services to over 70 countries. For more information, visit **nasuni.com.**

About Sapio Research

Sapio Research is a full-service B2B and tech market research agency that helps businesses grow thanks to high quality, efficient and honest research solutions.

We deliver valuable insights to support our clients understand their audience, build powerful brands, cut through the noise with great content and headlines, and make vital business decisions relevant to their market. We're based in the UK and have access to over 149 million people across 130 countries, working with clients that range from top tech companies to global consultancies, Marketing/PR agencies and household name brands.

Our purpose-driven team of expert market researchers is passionate about providing data confidence for all and performing research that makes a difference. We're here to support our clients every step of the way in all areas of quantitative and qualitative research, so they can save time and thinking space, deliver with confidence, and unlock more value with their research. For more information, visit **sapioresearch.com.**

⋮ NASUNI