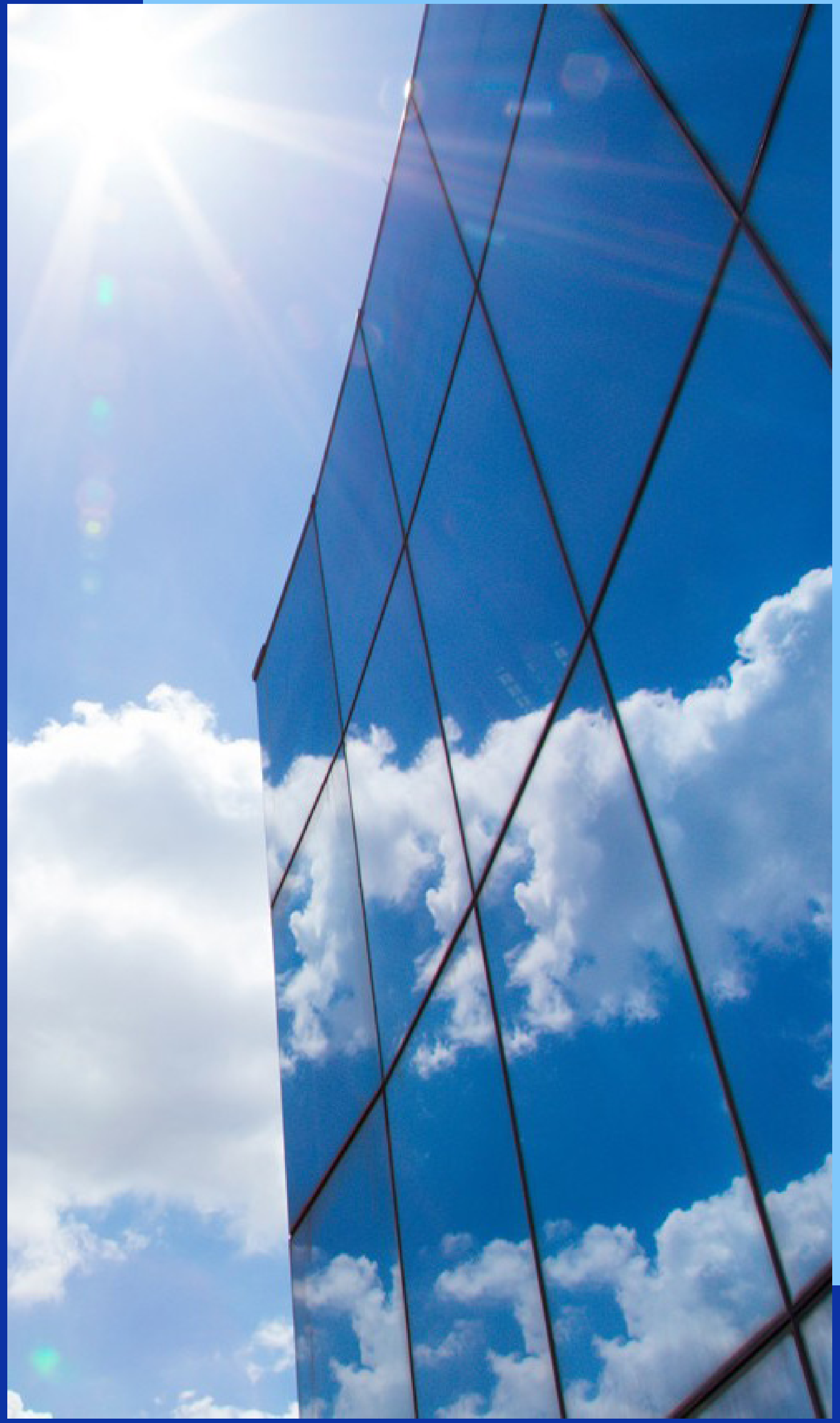
Global Data Protection Index

Cyber Resiliency Multicloud Edition

DELL Technologies

Table of contents



Introduction

In today's digitally transformed world, data's crucial role in business strategy makes it a prime target for escalating cyber threats. The rise of generative AI and expansion into hybrid, multicloud environments have heightened these risks, with cyberattacks causing significant financial harm—doubling from the previous year to an average of $1.4 million. Amidst this, organizations face challenges in protecting and securing their increasingly complex cloud assets, underscoring the vital need for robust cyber resilient data protection strategies in this ever-evolving landscape.

This eBook presents findings from Dell Technologies' 2024 Global Data Protection Index commissioned through Vanson Bourne, a survey of 1,000 IT decision makers and 500 IT security decision makers globally. Unless otherwise specified, only the results from the 1,000 IT decision makers are referenced when making historical comparisons.

The data protection risk landscape

Navigating the complex terrain of data protection remains a formidable challenge for organizations, a hurdle that directly impacts their journey toward digital transformation. The vast majority (90%) of organizations have experienced some form of disruption in the last 12 months.

This widespread disruption is not lost on IT and IT security leaders, with 79% expressing concerns about potential disruptive events in the upcoming year.

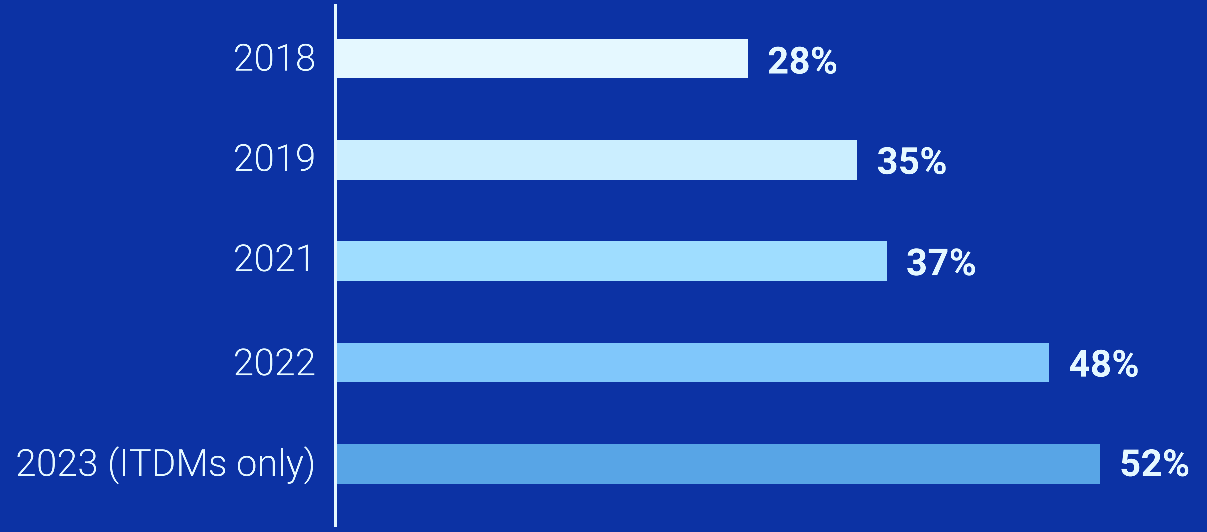
Such apprehensions are casting a shadow over their confidence in achieving backup and recovery service level objectives (SLOs), with 60% not feeling 'very confident' in their organization's capabilities in this area.

To add to these concerns, data loss events are having a significant financial impact on organizations, costing on average $2.61 million in the last 12 months (USD).

The increasing threat of cyberattacks

The threat of cyberattacks continues to grow, remaining top of the list for causes of organizational disruption for the second year running. Over half (52%) of IT decision makers report that their organization has suffered a cyberattack or incident that prevented access to data within the last 12 months.

Cyberattack or other cyber incident that prevented access to data



Cybercriminals target an array of entry points, but attacks are more likely to come from external sources. In fact, 55% of attackers' first point of entry was external - users clicking on spam or phishing emails and malicious links, compromised user credentials and hacked mobile devices.

Cost of cyberattacks

This is having a considerable financial impact on organizations, with costs associated with cyber-attacks and other cyber-related incidents over doubling in the last 12 months:

2022

$660k

↑

2023 (ITDMs only)

$1.41m

Furthermore, external security breaches are the most commonly cited causes of data loss and/or systems downtime within organizations

40%

The risk of remote working

Despite the popularity of remote and hybrid working, organizations find themselves in a precarious position. Over eight in ten (81%) now believe they have an increased exposure to data loss from cyber threats due to the growth of employees working from home.

We have increased exposure to data loss from cyber threats with the growth of employees working from home

2022

70% →

2023 (ITDMs only)

81%

Summary: Combination of “Strongly agree” and “Agree”

To add to concerns, a growing portion agree that their organization’s existing data protection measures may not be sufficient to cope with malware and ransomware threats.

I am concerned my organization’s existing data protection measures may not be sufficient to cope with malware and ransomware threats

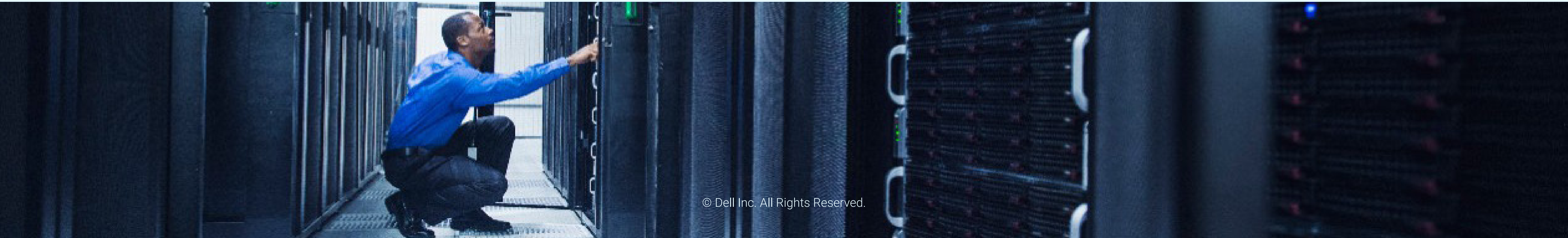
2022

67% →

2023 (ITDMs only)

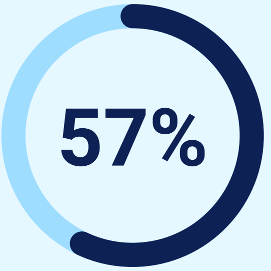
75%

Summary: Combination of “Strongly agree” and “Agree”

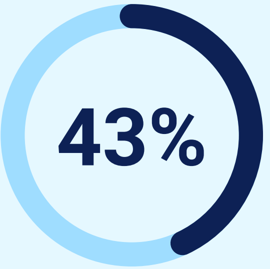


Ransomware policies

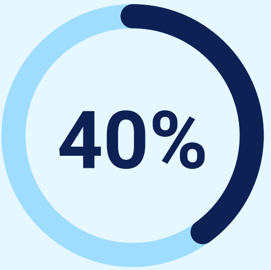
In an age where cyber threats pose an ever-present threat, insurance policies can provide organizations with reassurance. However, despite ransomware policies being commonplace (93%), they come heavily caveated:



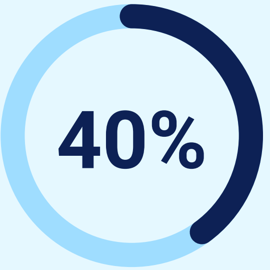
My organization must prove ‘best practice’ cyberthreat prevention activity



The policy has a limit on how much they will pay for a claim



There are particular scenarios which would make the policy void



The policy will not pay out as payment to some entities may be restricted by law

85% For those that experienced a ransomware attack, the vast majority paid to access their data.

But only just over a quarter **(28%)** were **fully reimbursed** by their **insurance policy**, leaving many **organizations financially exposed**.

Generative AI and cybersecurity

As the landscape of cyber threats expands, a significant shift is emerging towards embracing generative AI as a strategic tool for bolstering cyber defenses.

52% believe that integrating generative AI will provide an advantage to their organization's cybersecurity posture in the ongoing battle against cybercriminals.

This optimism, however, is tempered by the recognition of inherent challenges.

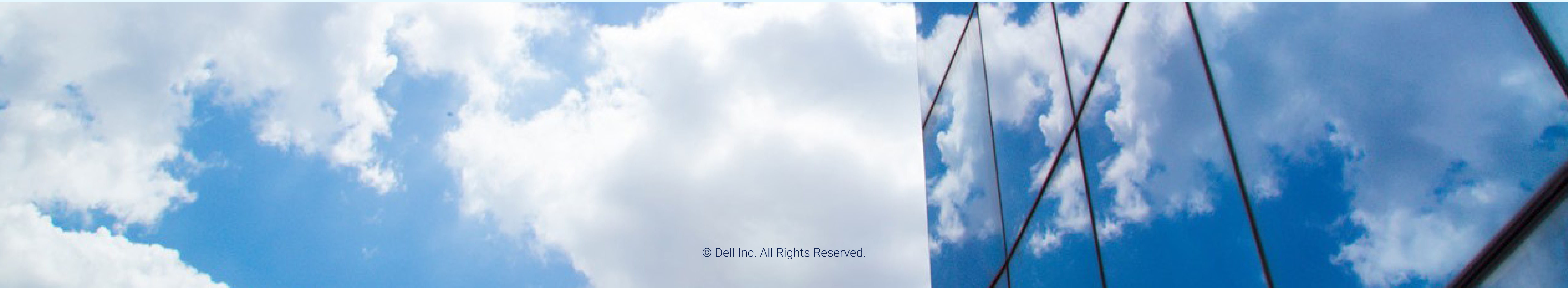
88%

of experts agree that the adoption of generative AI will generate large volumes of new data, necessitating protection and security measures.

Similarly
88%

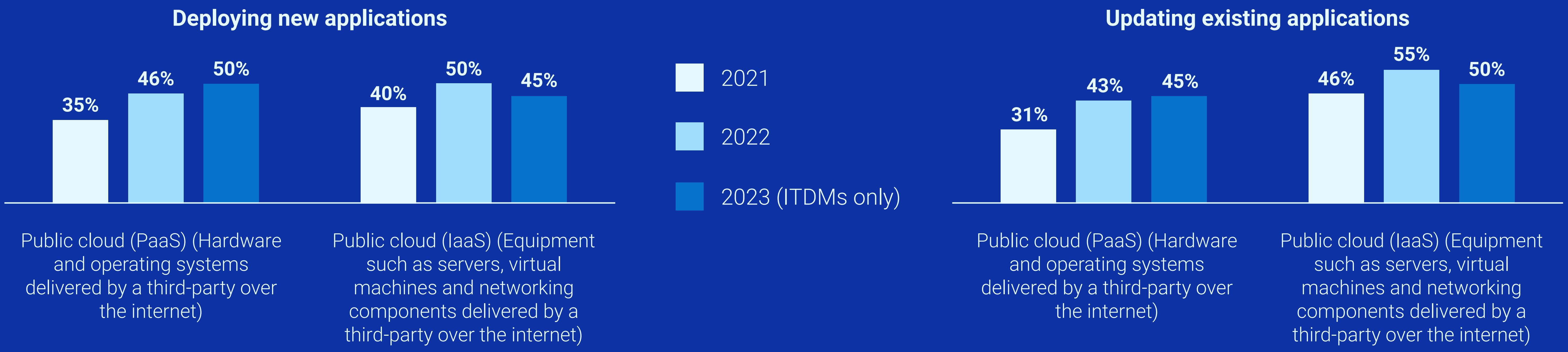
agree that generative AI will amplify the value of specific data types, thereby demanding elevated levels of data protection services.

These insights underscore the dual nature of generative AI as both a powerful defensive asset and a source of new cybersecurity complexities.



The use of multicloud

The adoption of public cloud solutions continues to be a favored strategy for organizations seeking to deploy or update applications. However, this preference also introduces an additional layer of data protection complexity.



96% of organizations encounter challenges in managing data within public, multicloud environments.

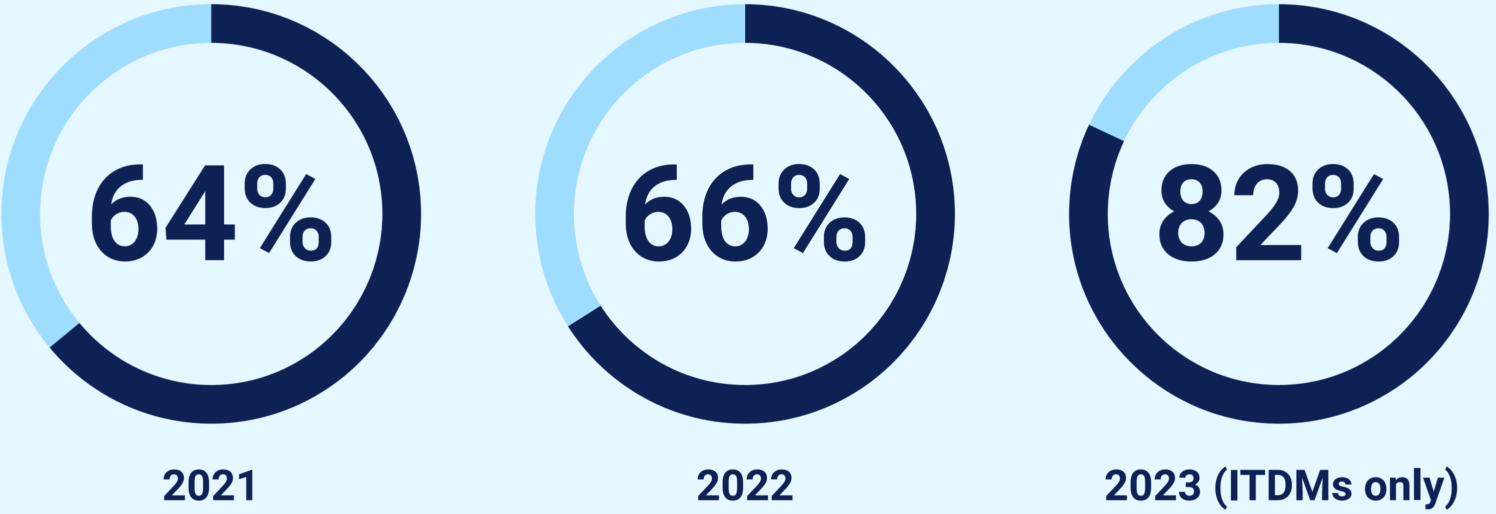
44% grapple with the complexities inherent in navigating multiple public cloud platforms, each with its unique features and requirements.

40% express concerns over securing their data across these diverse environments.

Securing a multicloud environment

With cyber threats increasing, many organizations lack confidence about keeping their data safe in the cloud, especially when deploying new applications and updating existing ones. In fact, their confidence is at an all-time low.

Percentage of respondents not 'Very confident' in their organization's ability to protect all of its data across public cloud environments



Understandably, over half of the respondents prioritize two capabilities as critical for enabling effective hybrid and multi-cloud operations:

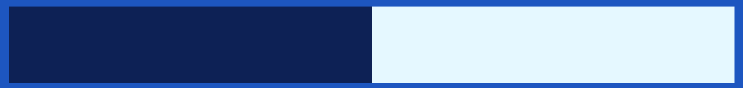
58%

The ability to protect multi-workload environments

56%

Ensuring robust cybersecurity

50%

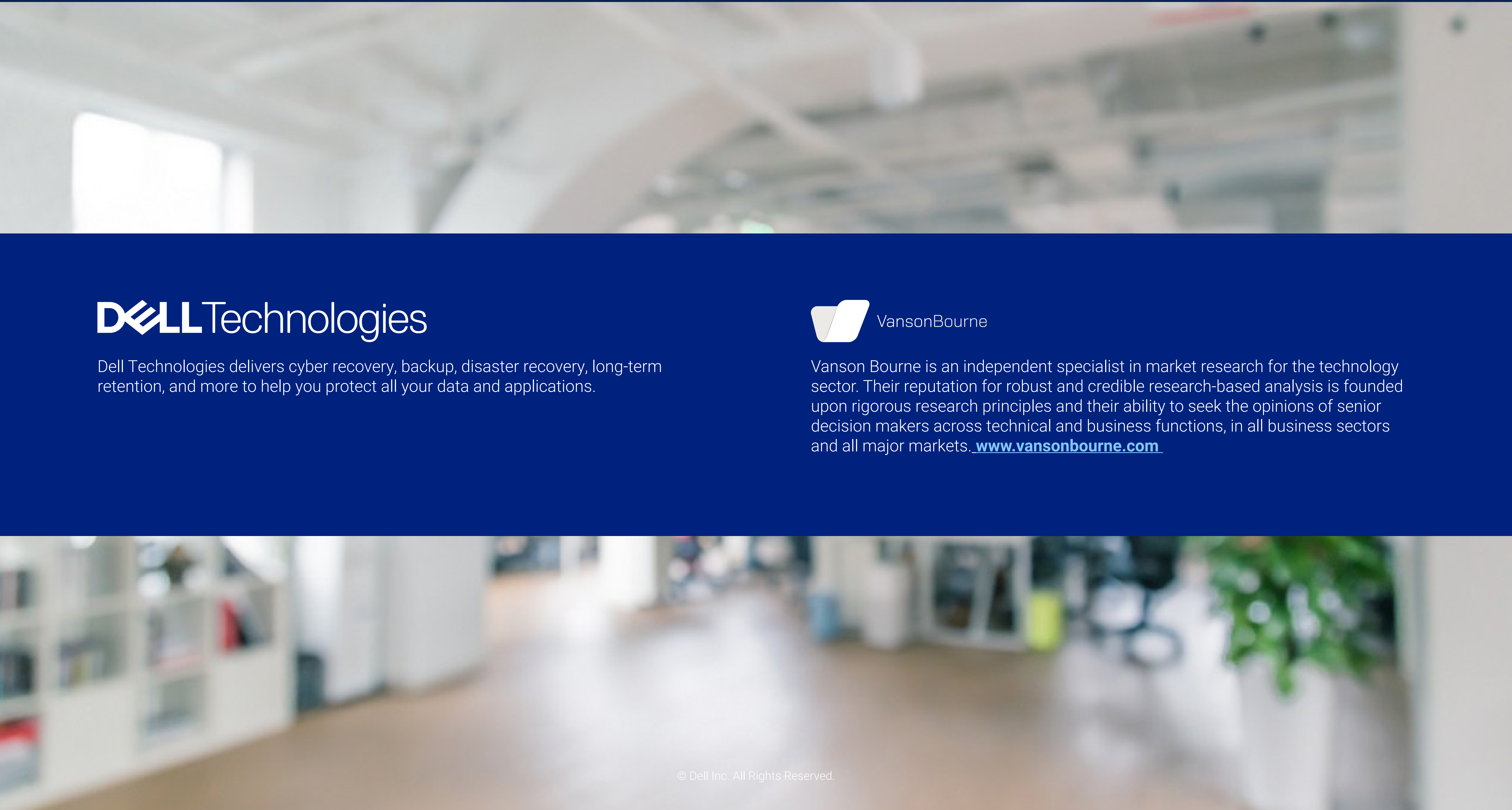


To address these challenges, half of organizations have already brought in outside support to enhance their cyber resilience.

Conclusion

As organizations increasingly turn to public cloud solutions, implement hybrid working models, and experiment with generative AI, the criticality of data protection is more evident than ever. Yet, securing and safeguarding digital assets is becoming a more complex challenge for many. In a landscape continuously threatened by cyberattacks, it is essential for businesses to adopt measures that bolster the resilience of their operations.

Learn more about Dell modern, simple, resilient multicloud data protection:
www.dell.com/dataprotection



DELL Technologies

Dell Technologies delivers cyber recovery, backup, disaster recovery, long-term retention, and more to help you protect all your data and applications.

VansonBourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. www.vansonbourne.com