Enterprise Strategy Group™ by TechTarget

Data Protection Cloud Strategies at a CROSSROADS

Christophe Bertrand, Practice Director

APRIL 2023

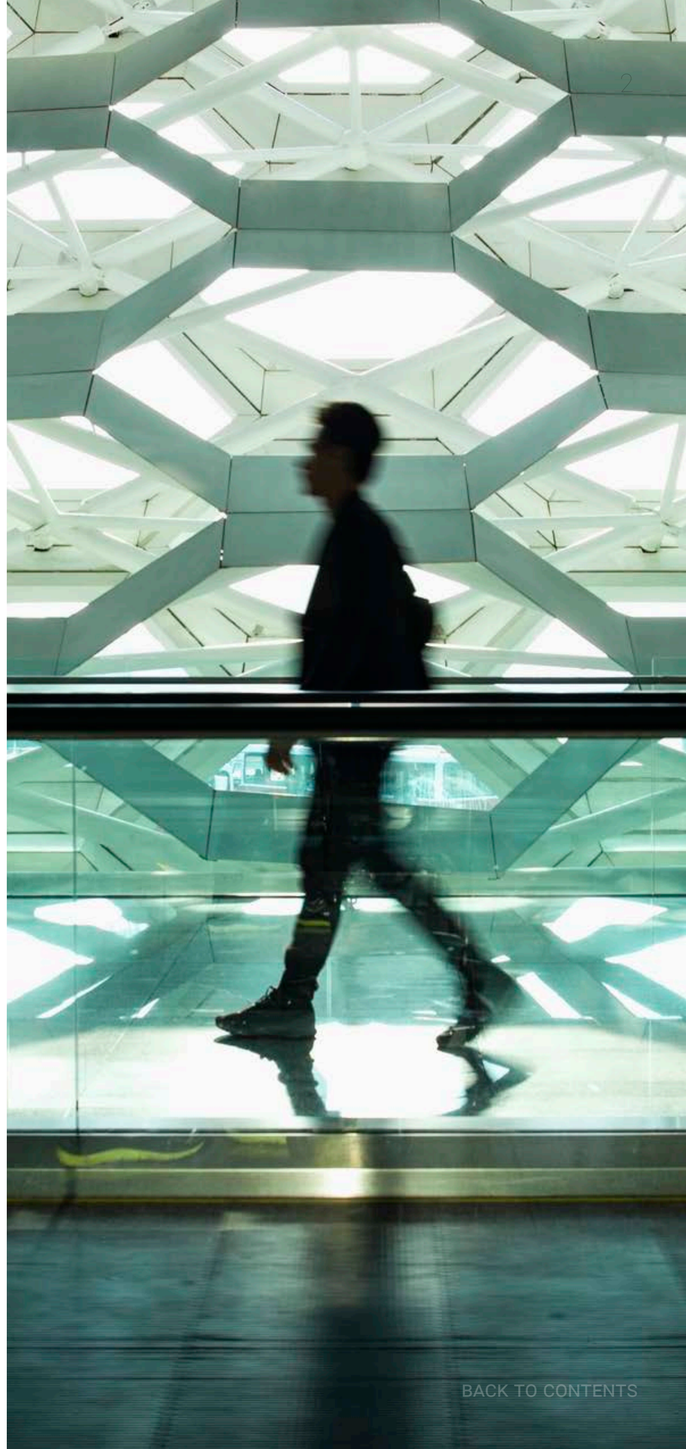
Research Objectives

The broad adoption of public cloud services and containers as sources and repositories of business-critical data puts the onus on data owners to deliver on data protection service level agreements (SLAs) for cloud-resident and container-based applications and data. Users are confused about the data protection levels that public cloud and Kubernetes environments deliver and about the changing protection options (DIY in the cloud, cloud-native third-party solutions, hyperscalers' built-in features, as-a-service offerings, etc.). As vendors and the cloud ecosystem evolve and add as-a-service consumption options, end users are making incorrect comparisons and assumptions as well as failing to select the key data protection capabilities they need to maximize their cloud technology investments. This confusion leads to lasting challenges, and the market is now at a crossroads.

In order to gain further insight into these trends, TechTarget's Enterprise Strategy Group (ESG) surveyed 397 IT professionals at organizations in North America (US and Canada) personally familiar with and/or responsible for data protection technology decisions for their organization, specifically around those data protection and production technologies that may leverage cloud services as part of the solution.

This study sought to:

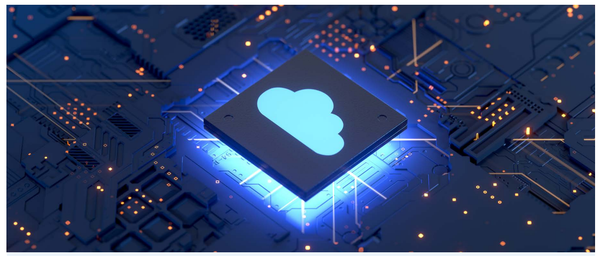
- Assess the state of cloud-based data protection and the as-a-service market (i.e., in the cloud/to the cloud, BaaS, and DRaaS).
- Establish the role of key decision makers and personas in the buying cycle.
- Explore end-user challenges and highlight requirements.
- Assess the use and impact of cloud technologies for data protection.

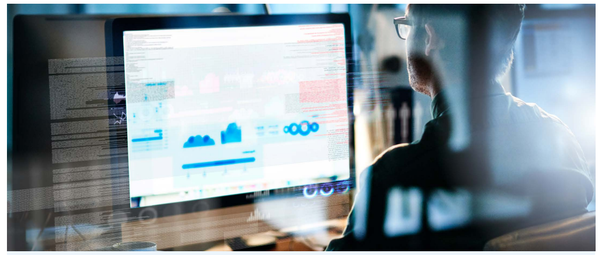


BACK TO CONTENTS

KEY FINDINGS

CLICK TO FOLLOW



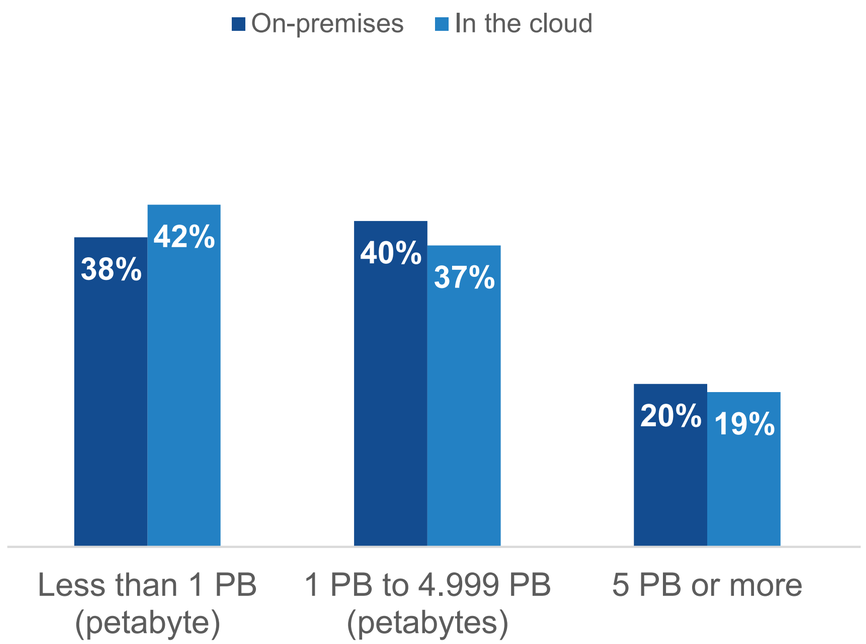


Cloud Is Exacerbating the Amount of Data that Needs to Be Protected

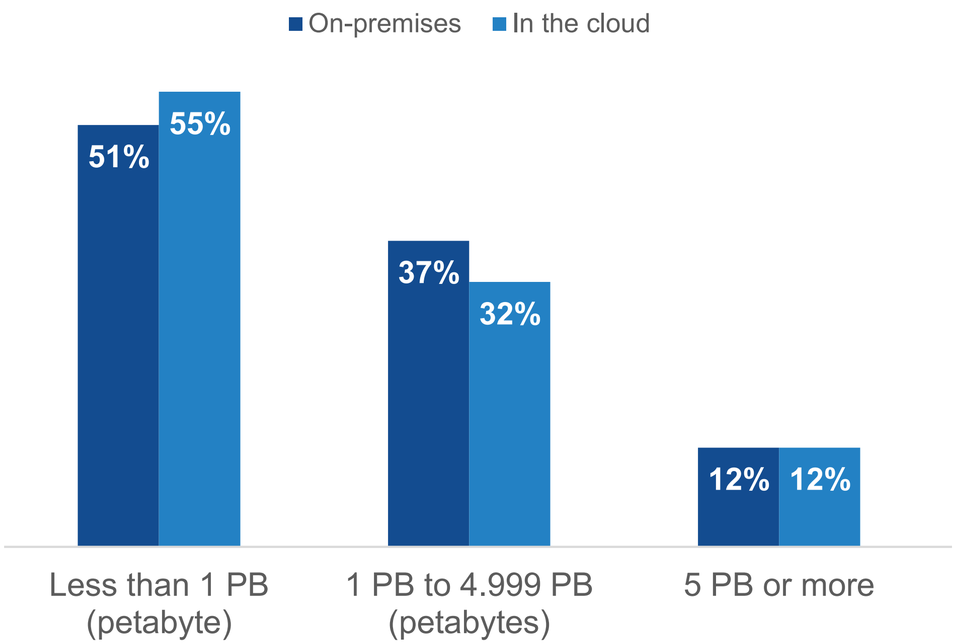
The Primary and Secondary Data Deluge

With so many applications, users, and devices, organizations are creating and managing an unprecedented amount of data today. Indeed, the majority of organizations report having more than 1 PB of total data across their on-premises (60%) and public cloud (56%) environments. Given the importance of protecting production data as well as other activities performed on secondary copies of data, such as analytics or test and development, each TB of production data has the potential to generate an additional 6 TB on average of secondary data. As a result, secondary data accounts for more than 60% of organizations' total data footprints spanning their on-premises data centers and public cloud platforms. This means that cloud backup and recovery solutions must naturally scale to meet these data volumes regardless of where production volumes live.

Approximate total volume of data
(including both production and secondary data) stored on corporate servers, storage systems, backup media, and public cloud services.

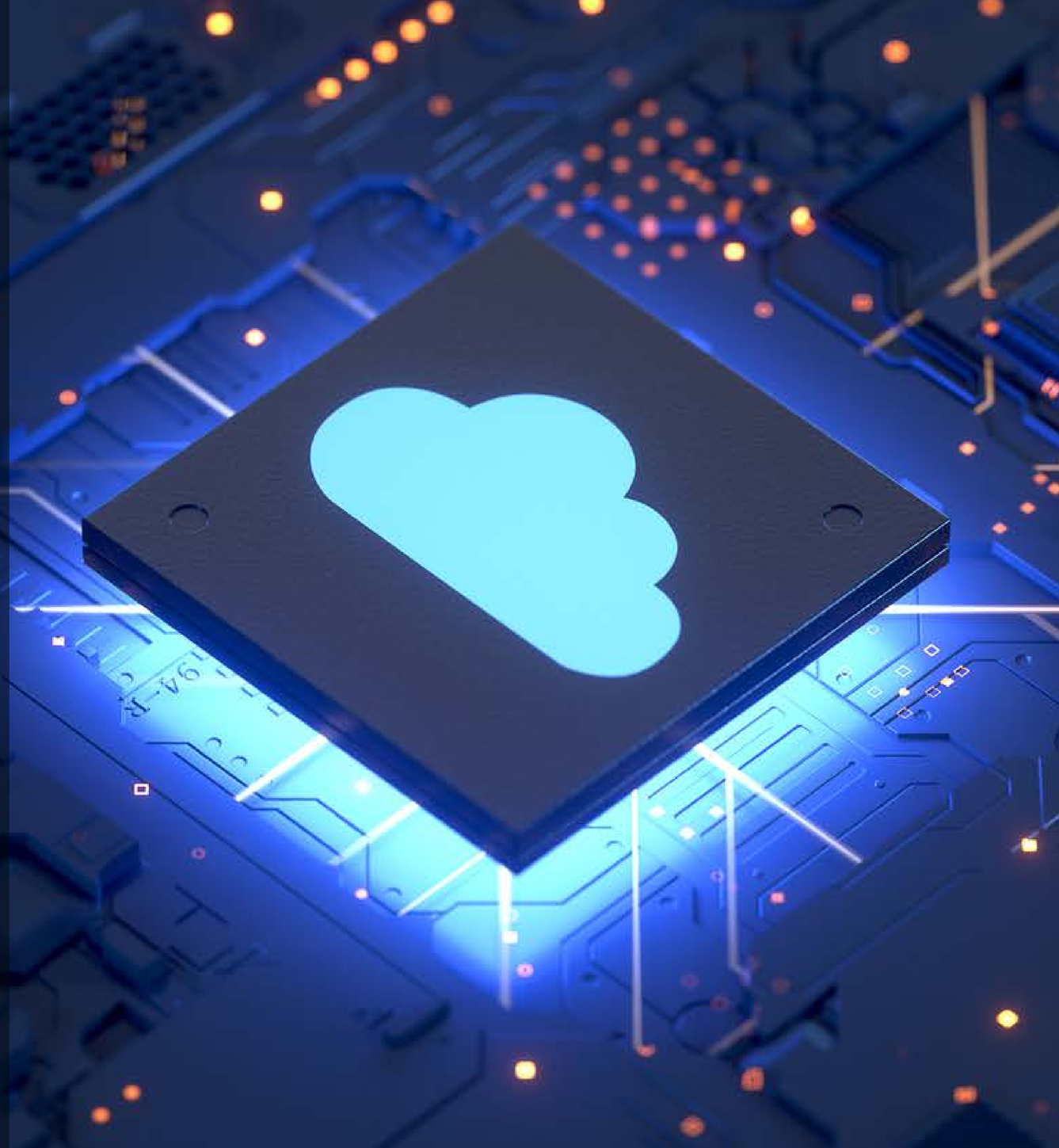


Approximate total volume of secondary data
(backup and archive) stored on corporate servers, storage systems, backup media, and public cloud services.



BACK TO CONTENTS

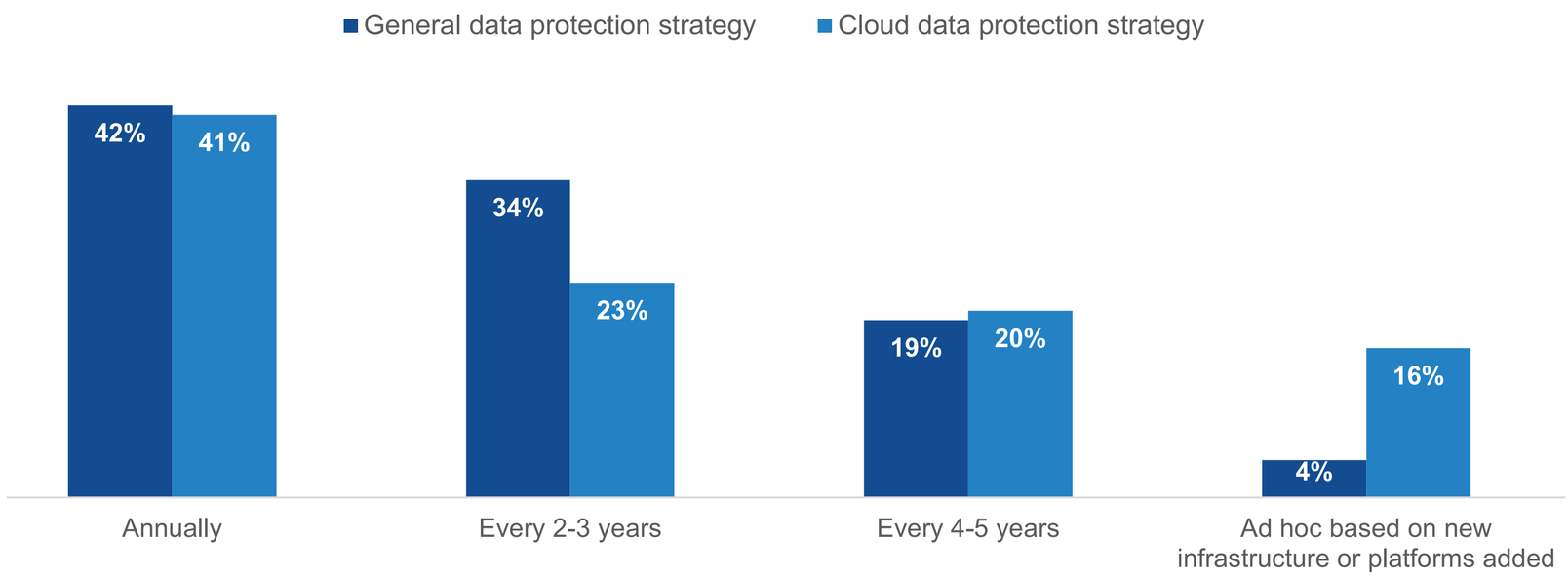
Cloud Data Protection Strategies Are Evolving Quickly with BaaS and DRaaS Leading the Charge



Data Protection Under Close Scrutiny

Data protection is a very dynamic market, with a plurality of organizations revisiting their strategy for backing up applications and data, whether on-premises or cloud-based, on an annual basis. It is interesting to note that cloud data protection strategies are four times likelier to be rearchitected on an ad hoc basis. ESG believes that this is associated with the utility nature of public cloud services that allows for faster infrastructure and application deployments having a direct impact on the associated data protection processes.

Frequency with which data protection strategy is assessed or rearchitected.



Cloud data protection strategies are

4x likelier

to be rearchitected on an ad hoc basis.

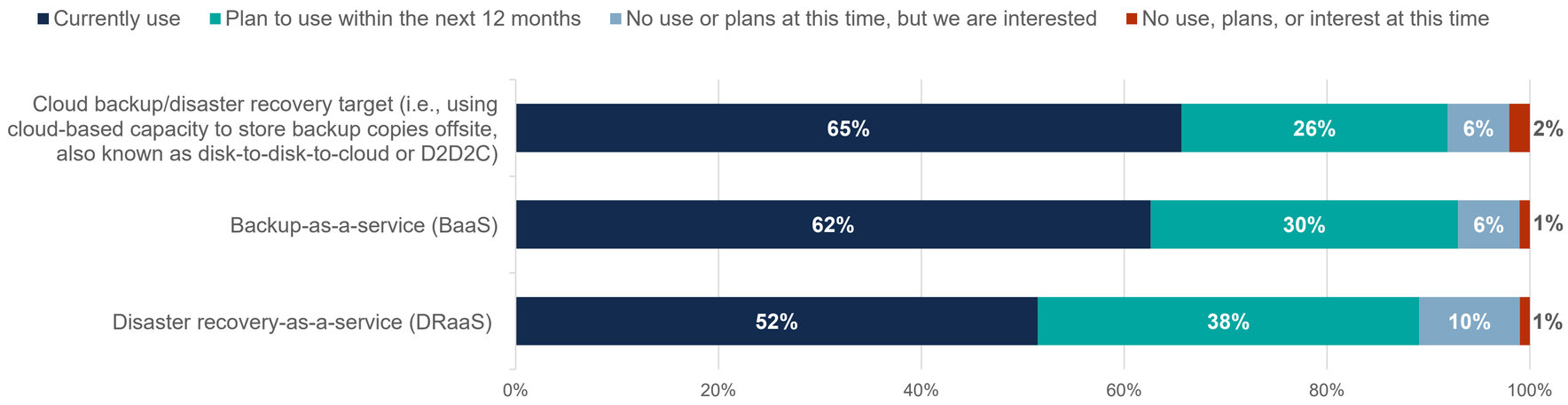
BACK TO CONTENTS

Cloud-based Data Protection Services Are the Norm

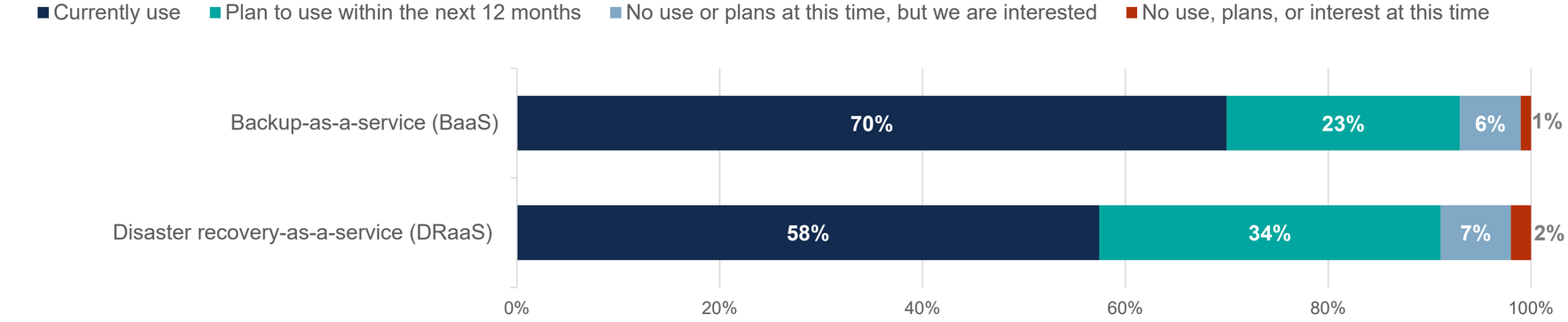
Organizations leverage a variety of topologies and "consumption" modes that leverage public cloud-based data protection services to protect their on-premises environments. The traditional topology of cloud platforms serving as backup targets is still leading the pack. However, as most organizations continue to evolve their functional application environment, using more as-a-service options, the backup and recovery space sees the same trend with 90% or more organizations currently using or planning to use BaaS or DRaaS.

In terms of applications and data that are hosted on public cloud infrastructure, the majority of organizations report using BaaS or DRaaS. While BaaS is currently more widely deployed than DRaaS, intentions indicate that both will "equalize" in the future, with almost the entirety of the market leveraging one or the other option in the future.

Public cloud-based data protection services used to protect **on-premises** applications, workloads, and data.



Public cloud-based data protection services used to protect **public cloud-based** applications, workloads, and data.



BACK TO CONTENTS

Multi-cloud Is the Norm and Impacting Data Protection Strategies

The Best Tools for the Job of Protecting Multi-cloud Environments

Multi-cloud use is pervasive, with 91% of organizations leveraging at least two unique cloud service providers (CSPs), and nearly one in five using four or more public cloud infrastructure service providers. This has a direct impact on cloud data protection strategies and tools. Data and applications must be protected wherever they live, particularly those that are deemed mission-critical.

Organizations strongly favor using specialized tools for each cloud environment. While pragmatic, it is very likely that in time this stovepipe approach will lead to complexity: People need to be trained on multiple tools, processes may differ from cloud to cloud, and capabilities may vary, all of which have the potential to negatively impact SLAs. It is worth noting that the single backup platform approach is more preferred the more CSPs an organization uses. Specifically, there seems to be an inflection point at 5 CSPs or more, in which those organizations are much likelier to favor a more unified approach.

91%
of organizations are leveraging **at least two unique CSPs.**

ONE IN FIVE
use four or more public cloud infrastructure service providers.

Preferred approach to protecting multiple unique public CSP environments.

- Using a single backup/data protection platform (i.e., “unified across all cloud services”) to protect all of our disparate cloud infrastructure environments holistically and consistently
- Using different backup/data protection tools (i.e., “best for each cloud service”) to protect unique cloud infrastructure environments separately in stovepipe fashion

A single backup platform approach is more preferred **the more CSPs an organization uses.**

Preference level based on number of CSPs

BACK TO CONTENTS

Tiered Storage Aligns with Cloud Data Protection Strategies

Tiered Storage Wins the Hyperscaler Data Protection ‘RFP’

Tiered storage support stands out as the most popular capability organizations look for in their cloud data protection tool kit. This confirms that against the deluge of data IT professionals deal with every day, optimizing for cost is necessary, which is what tiered storage can deliver in a public cloud environment.

Of note is the need to integrate well with the cloud provider’s native capabilities at the data protection level as well as for application services. Stringent data protection SLAs are also clearly top of mind with continuous backup (meaning low RPOs) cited as the second most important characteristic.

| TOP 5 most important characteristics for hyperscaler data protection solutions.

1

Support for a tiered storage approach

2

Continuous backup

3

Support for or integration with native hyperscaler data protection capabilities

4

Support for our container environment

5

Support for native hyperscaler application services

BACK TO CONTENTS

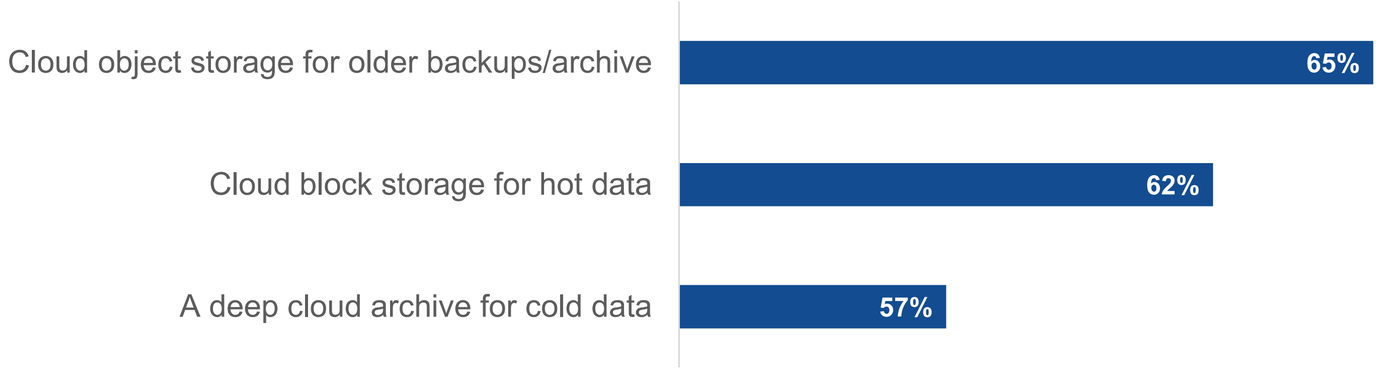
Cost-driven Tiering Is ‘a Given’

Leveraging tiered storage is one of the most popular characteristics of a cloud backup solution. Delving further into the motivations and technologies, it is clear that these tiering decisions are cost-driven for a vast majority of organizations. Matching cost, storage, performance, and use cases in full play with cloud object storage is becoming the standard for older backups or archives, while block storage is widely used for “hot” data. On the archiving front, the majority report leveraging deep cloud archives for “cold” data. The vast majority of organizations expect this process to be driven by their backup solutions.

78%

of organizations practice cost-efficient data tiering for the data protection storage supporting their public cloud infrastructure-resident applications.

Approaches organizations take to cost-efficient data tiering for the data protection storage supporting public cloud infrastructure-resident applications.



91%

of organizations say their backup software handles the appropriate tiering of the data written to object storage.

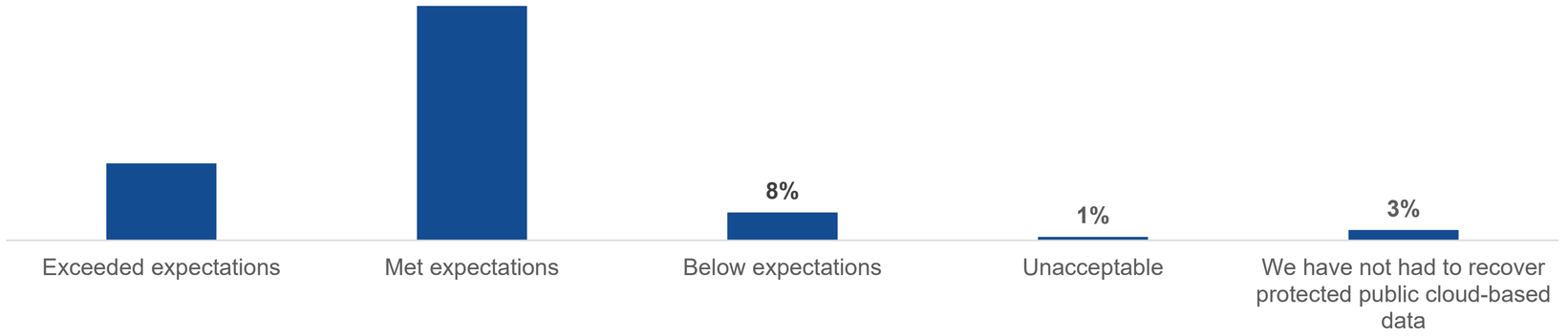
BACK TO CONTENTS

Cloud Recoverability Leaves a Lot to Be Desired

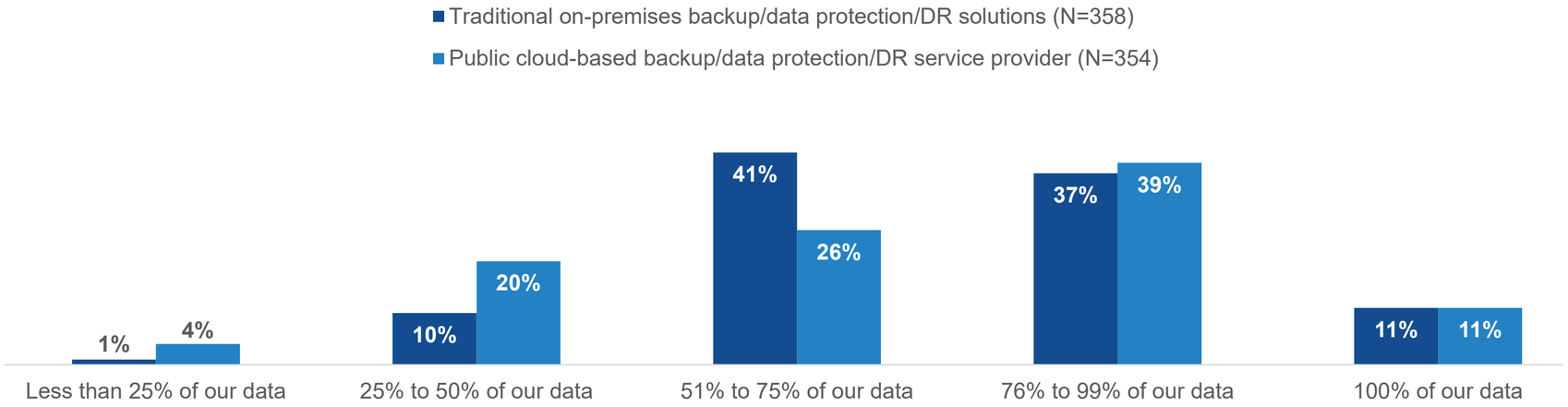
Vast Majority Are Satisfied with Public Cloud Recovery, yet Recovery Metrics Leave a Lot to Be Desired

General sentiment for public cloud-based data recoveries is positive, with two-thirds saying the recovery timeframe met their expectations, and 22% reporting their expectations were exceeded. However, there is more than meets the eye: Only 1 in 10 can recover 100% of their data, regardless of the topology, so many organizations still have work ahead to get closer to the 100% objective. Traditional on-premises backup is only marginally ahead as cloud-based data protection capabilities have vastly improved over the past few years. Overall, with these reported results, there is still significant data loss risk and therefore business risk across the board. This is an opportunity for the ecosystem of vendors, including both cloud providers and backup and recovery vendors, to work on improving recoverability through further integrations, testing, and end-user support and education. As technologies continue to mature, it is ESG's view that recoverability will, too, even if the amorphous and ever-changing threat of ransomware complicates matters.

Acceptability of **public cloud-based** data recovery timeframe.



Percentage of data organizations were able to recover on average.

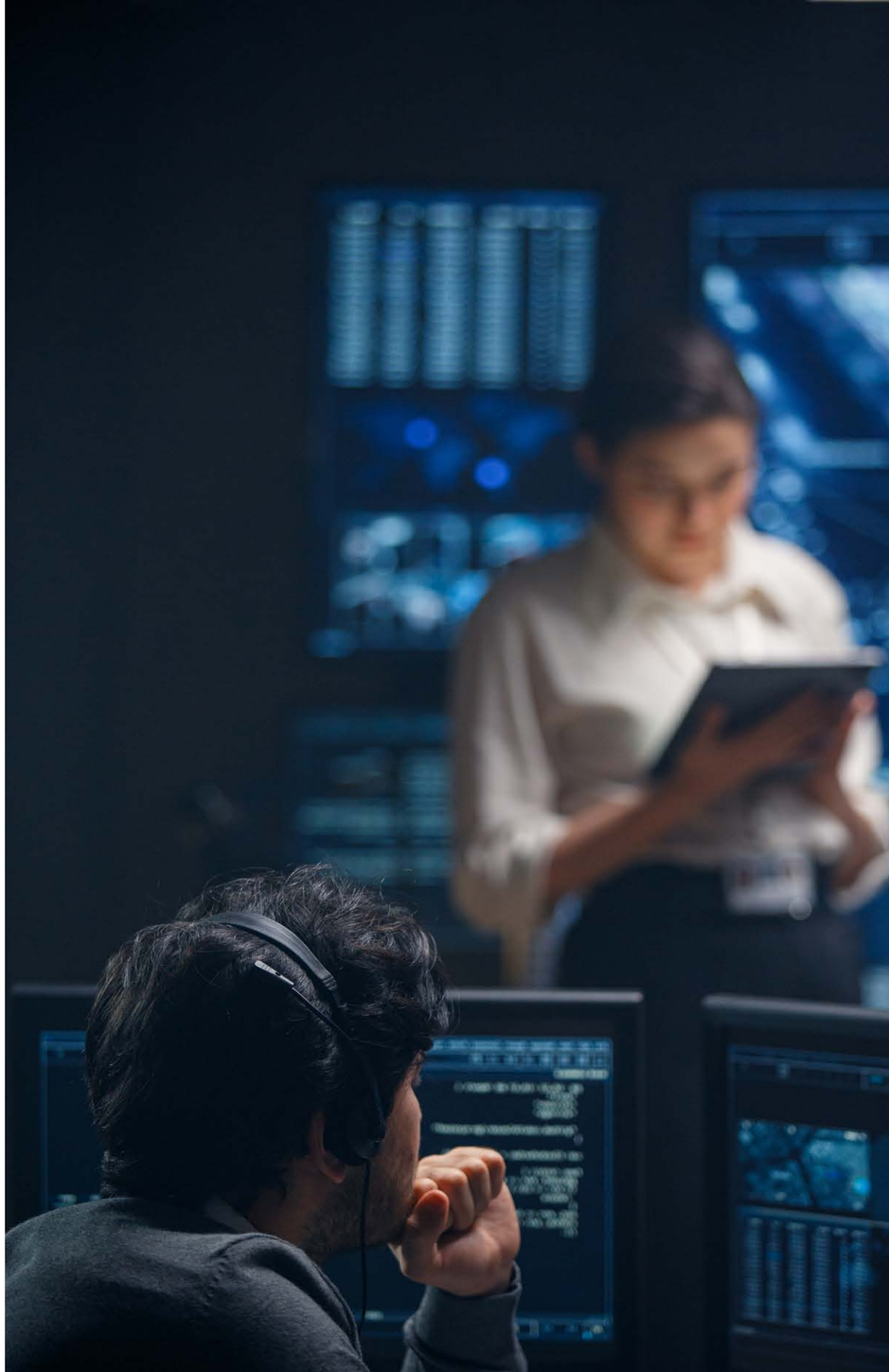


BACK TO CONTENTS

COHESITY

Cohesity is a leader in cloud data security and management solution. Cohesity Cloud Services, a portfolio of fully-managed SaaS offerings, help organizations secure and protect their most critical data and provide rapid recovery to minimize business impact. These services include backup and recovery, cyber vaulting, disaster recovery, and threat defense, which play a vital role in helping organizations enhance cyber resilience and increase IT and business agility across multicloud environments.

LEARN MORE



ABOUT ENTERPRISE STRATEGY GROUP

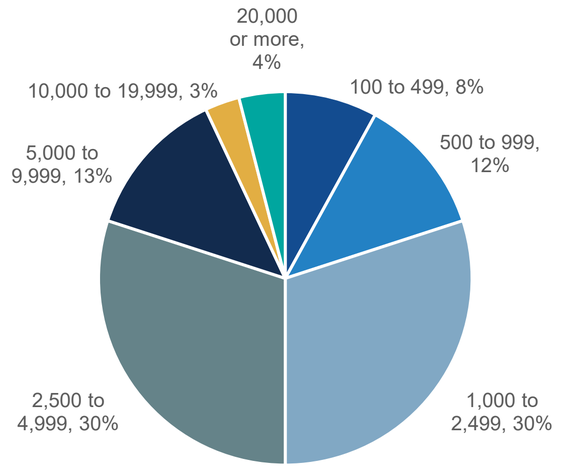
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

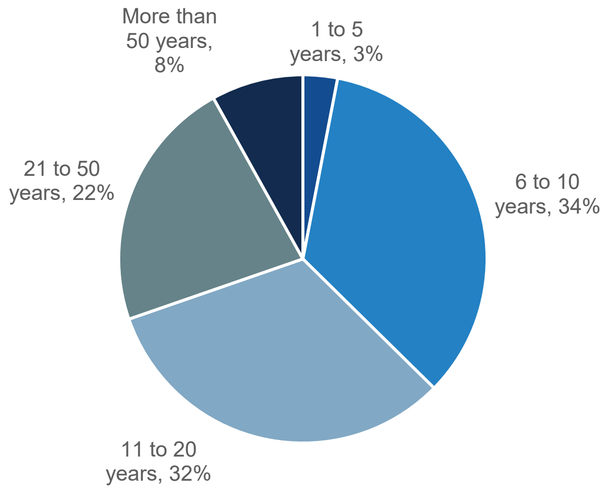
To gather data for this report, ESG conducted a comprehensive online survey of IT professionals from private- and public-sector organizations in North America (United States and Canada) between March 9, 2023 and March 15, 2023. To qualify for this survey, respondents were required to be familiar with and/or responsible for data protection technology decisions for their organization, specifically around those data protection and production technologies that may leverage cloud services as part of the solution. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 397 IT professionals.

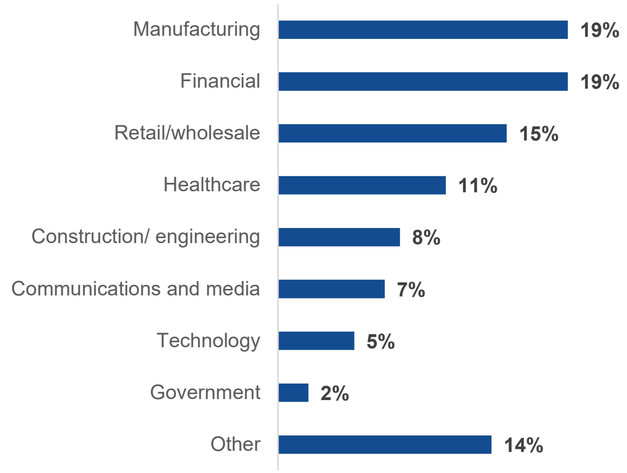
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.