Enterprise Strategy Group | Getting to the bigger truth.™

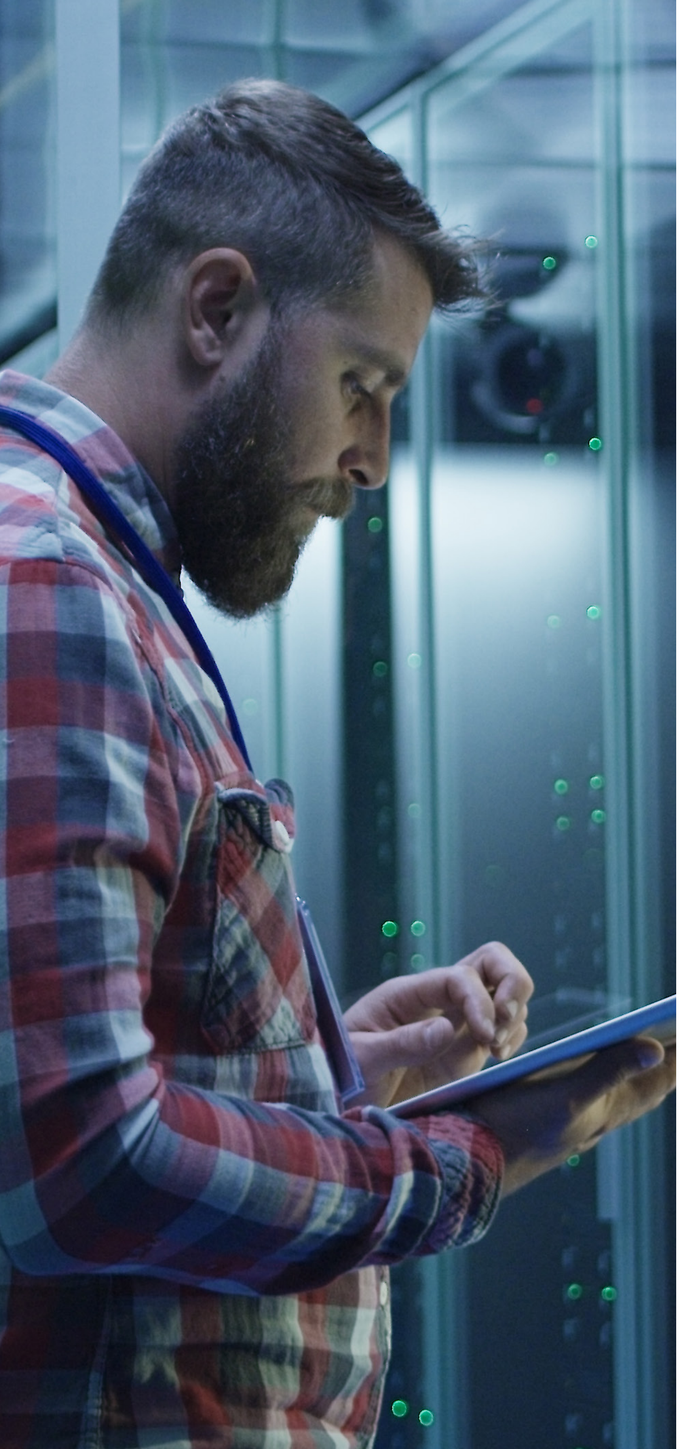
RESEARCH HIGHLIGHTS

# The Evolution of Data Protection Cloud Strategies

**Christophe Bertrand,** Senior Analyst

APRIL 2021

# TABLE OF CONTENTS





# Research Objectives

The broad adoption of public cloud services as a source and repository of business-critical data is placing the onus on data owners to deliver on data protection SLAs of applications, and their associated data, that are cloud-resident. Many users are confused about what exact data protection levels public cloud infrastructure and SaaS solutions provide, leading to potential data loss and compliance risks. Concurrently, on-premises backup and disaster recovery strategies are increasingly leveraging cloud destinations, resulting in hybrid data protection topologies with varying degrees of service levels and end-user tradeoffs and opportunities. How do IT organizations utilize cloud services as part of their data protection strategy today?

In order to gain insight into these trends, ESG surveyed 381 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 research aimed to understand cloud data protection challenges, plans, and strategies by probing how organizations are protecting data in the cloud, as well as how they are leveraging cloud services to protect data to the cloud.

## THIS STUDY SOUGHT TO:

**Determine** key challenges organizations are facing while leveraging and deploying data protection solutions to/in the cloud.

**Highlight** key trends and market requirements for data protection to the cloud and in the cloud.

**Understand** how IT organizations utilize cloud services as part of their data protection strategy today.

**Monitor** YoY trends with respect to evolving data protection cloud strategies.



Back to Contents

# Research Highlights

### CLOUD-BASED DATA PROTECTION IS THE NEW NORM.

The adoption of public cloud-based data protection services has grown significantly over the past five years. Organizations identify security, the ability to deliver against RPOs and RTOs, reduced costs, and even improved compliance as the most common benefits from using such solutions.

### CONTINUOUS DATA PROTECTION CAPABILITIES ARE KEY TO MEETING BAAS RECOVERY OBJECTIVES.

Backup-as-a-service is a very popular solution for protecting data, with security and speed of recoverability being top of mind when considering BaaS. Organizations are placing some stringent RPO requirements on their BaaS vendors, with more than one in five expecting continuous data protection-like capabilities.

### EXTENDING ON-PREMISES DATA PROTECTION ENVIRONMENTS WITH CLOUD BACKUP TARGET SOLUTIONS IS GAINING MOMENTUM.

Extending on-premises backup to cloud destinations was one of the first topologies early cloud data protection adopters leveraged. Cost-effectiveness and security top the list of key capabilities cloud backup/DR target solutions must meet while operating at scale.

### DATA TIERING IS AN INFLUENCING FACTOR ON IN-CLOUD DATA PROTECTION STRATEGIES.

New solutions and capabilities have recently emerged that focus on in-cloud data protection that often leverage hyperscalers' own new capabilities to protect data that they host. The key characteristics that organizations expect of these solutions are granular restores and tiered storage.

### THE BIG SAAS-DATA PROTECTION DISCONNECT IS NOT IMPROVING.

The previously identified "big disconnect" associated with SaaS data protection has not improved much since 2019 and more market education is needed. Organizations are looking at their backup solution for SaaS to deliver advanced protection and recovery while maintaining data protection SLAs.



Back to Contents

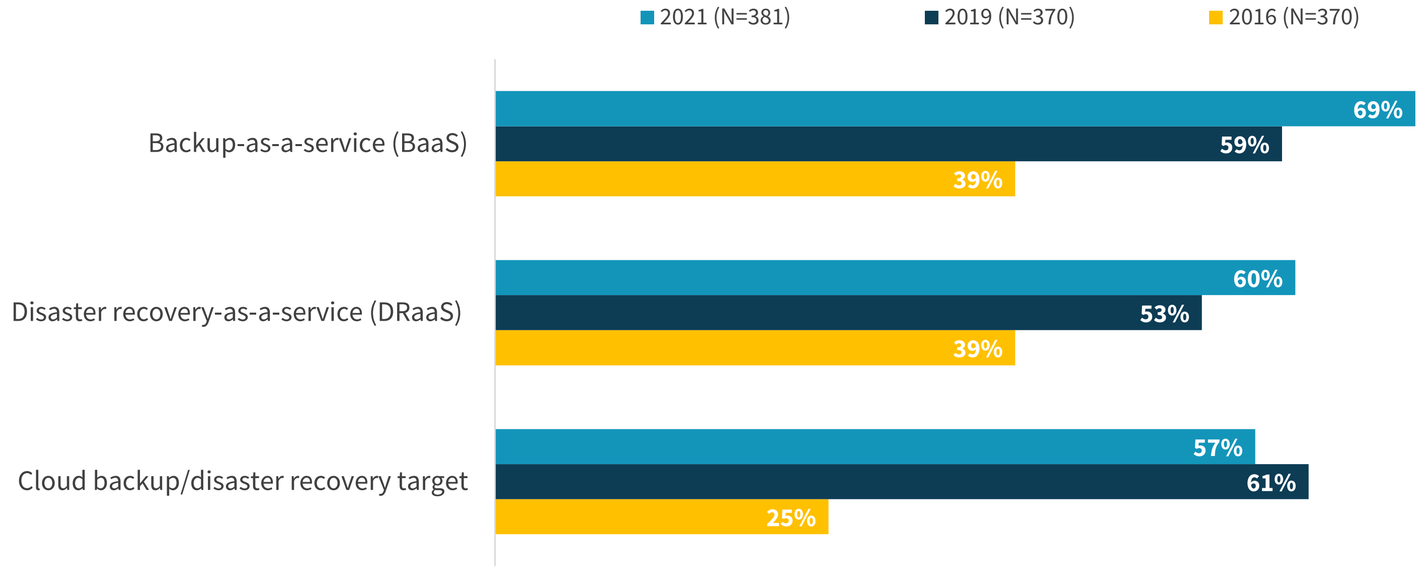
# Cloud-based data protection is the new norm.

## Cloud Data Protection Services Have Gained Significant Market Traction

In less than five years, the adoption of public cloud-based data protection services has grown significantly. While cloud backup and disaster recovery target configurations saw a strong rate of adoption over the last several years, there has been a more consistent uptick in the use of as-a-service topologies since 2016. Specifically, the adoption and use of backup-as-a-service (BaaS) is currently the most widely used approach, with more than two-thirds of organizations using these services. In time, ESG expects to see the BaaS and disaster recovery-as-a-service (DRaaS) categories merge as needs and technologies evolve to deliver shorter point-in-time intervals and more continuous data protection.

> ***The adoption and use of backup-as-a-service (BaaS) is currently the most widely used approach,*** *with more than two-thirds of organizations using these services.”*

Percentage of organizations currently using cloud-based data protection services.






Back to Contents

# Security and Reliability Are Decisive Benefits

The value proposition of cloud-based data protection is powerful in light of the many benefits organizations have derived. The perception of cloud-based data protection services is very positive. Organizations identify security, the ability to deliver against RPOs and RTOs, reduced costs, and even improved compliance as the most common benefits from using such solutions. This trend is consistent with broader cloud trends across IT. It also offers a window into how IT is evolving its focus towards modernized, cost-aware data protection solutions to better support strategic initiatives, which may explain why adoption has ramped up so quickly in the past few years.

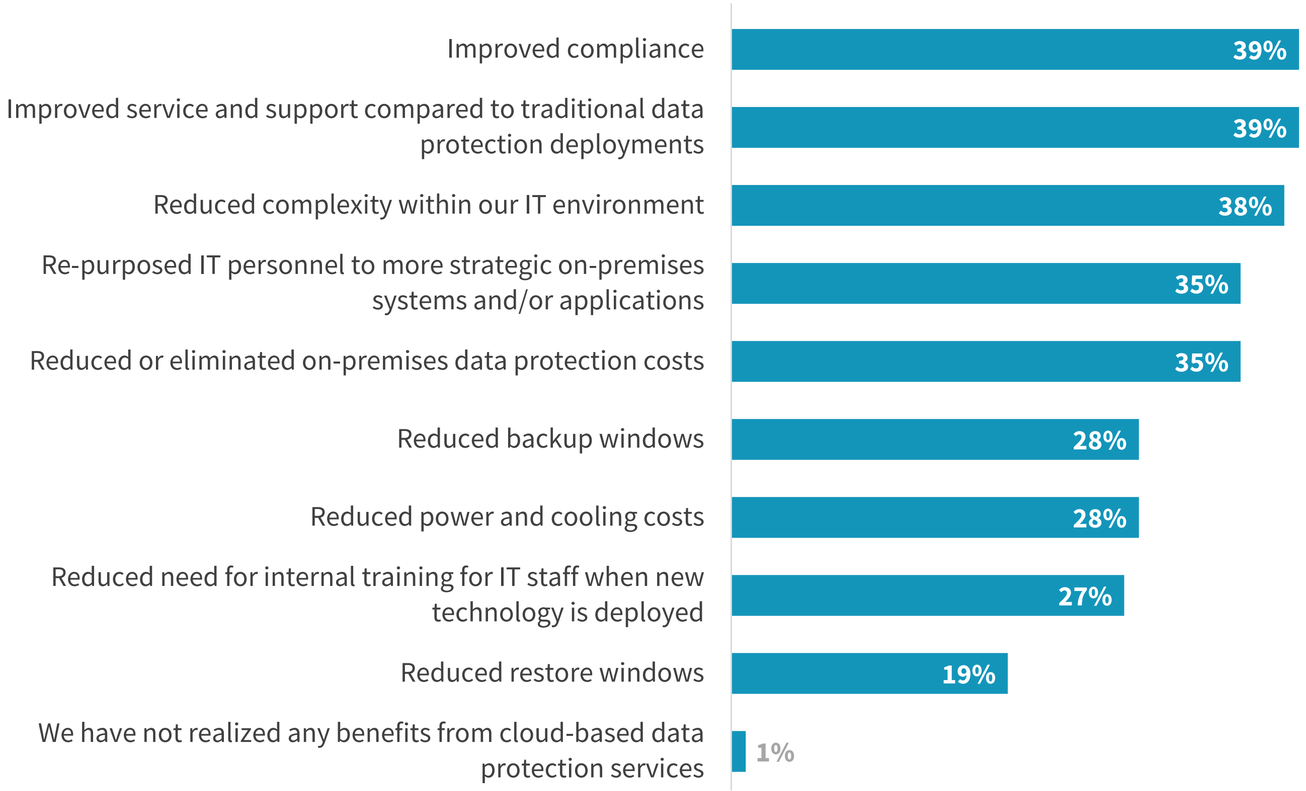
Most common benefits of cloud-based data protection services.

**52%**
Improved security

**46%**
Improved recoverability and reliability of backups

**41%**
Reduced IT personnel costs

Additional benefits of cloud-based data protection services.



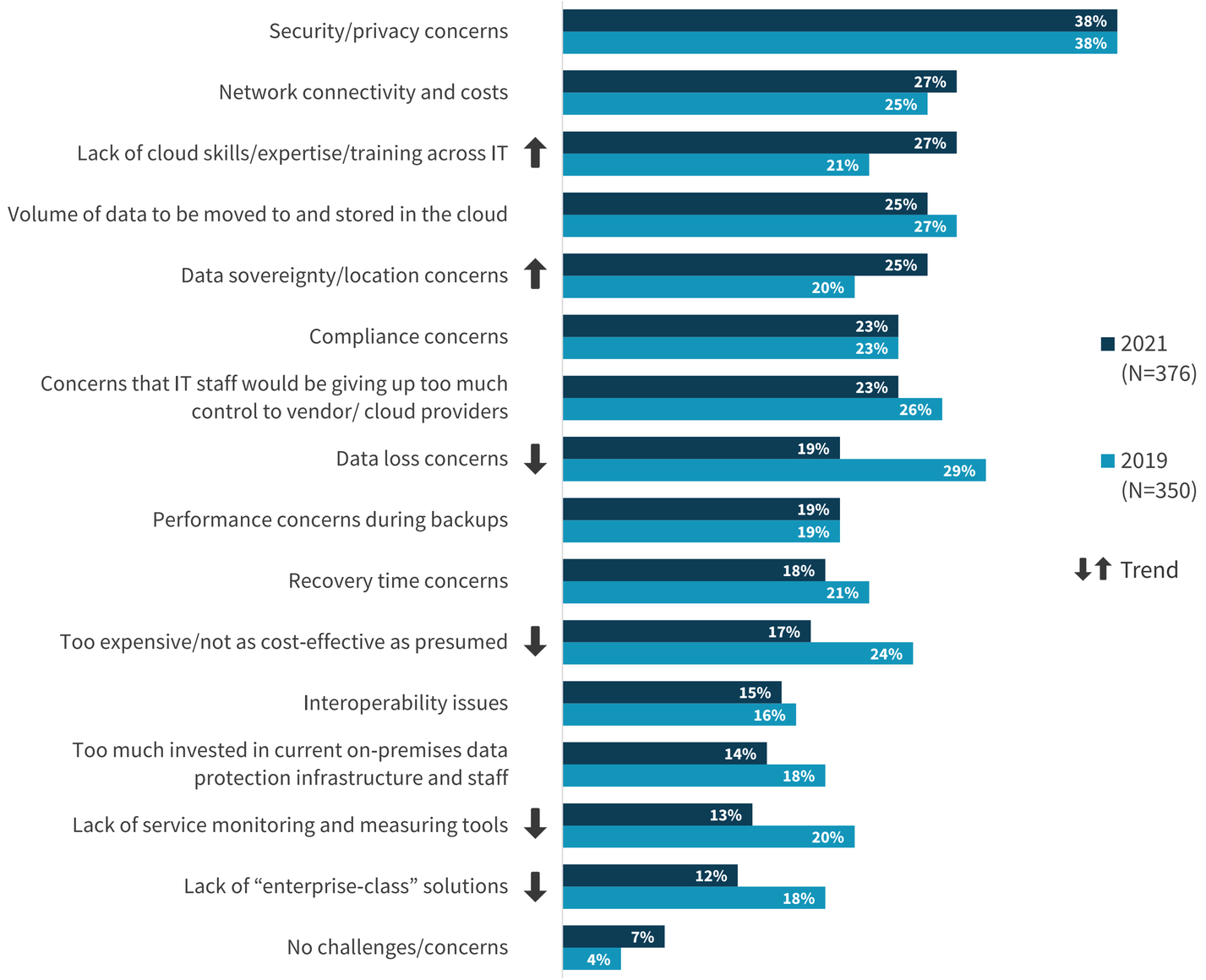



Back to Contents

# Skill Sets and Data Sovereignty Stand Out As Mounting Challenges

While the success of cloud-based data protection is undeniable and has yielded success for organizations that use it, there are still some challenges to overcome. As these services continue to gain traction, new challenges emerge and previous challenges subside, signs of a maturing market. There is still some work ahead in security and costs, two categories in which end-users express some ambivalence. In terms of security, on the one hand, users can benefit from the massive security investments that cloud providers have made in strengthening the security of their infrastructures; conversely, the level of control and the locality of data are by definition fundamentally different than when it was in the data center "under your roof." Cost is also a complex area as scale efficiencies can be gained versus doing it yourself, yet the unstoppable growth of data and intensified use of cloud and network bandwidth resources place a burden on budgets. Of note is the increasing concern around compliance and data sovereignty, which is becoming more visible, likely as a consequence of recent regulations such as GDPR.

Biggest challenges associated with cloud-based data protection services.





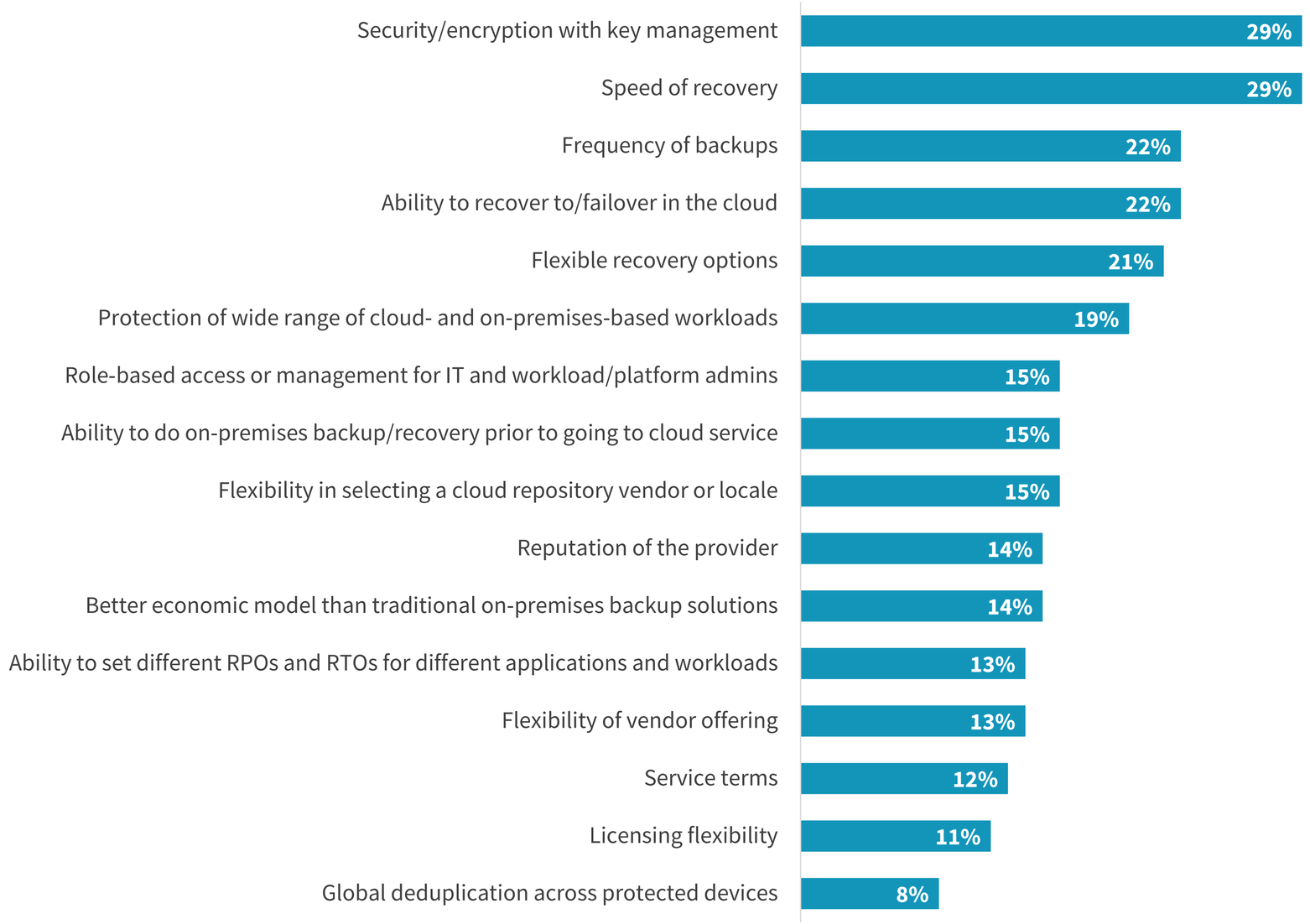

Back to Contents

# Continuous data protection capabilities are key to meeting BaaS recovery objectives.

# Security and Recovery Speed Headline BaaS RFPs

Backup-as-a-service is a very popular solution for protecting data, increasingly replacing traditional on-premises data protection technology. Not surprisingly, security and speed of recoverability are top of mind when it comes to the most important factors organizations weigh when considering BaaS. It should be noted that as BaaS is more widely leveraged, more workloads are expected to be protected by these services, another indicator of maturing backup and recovery solutions. ESG expects to see support for all the key mission-critical workloads, including applications with significant database requirements, become a table-stakes expectation among end-users and practitioners.

Top characteristics of or considerations for BaaS.



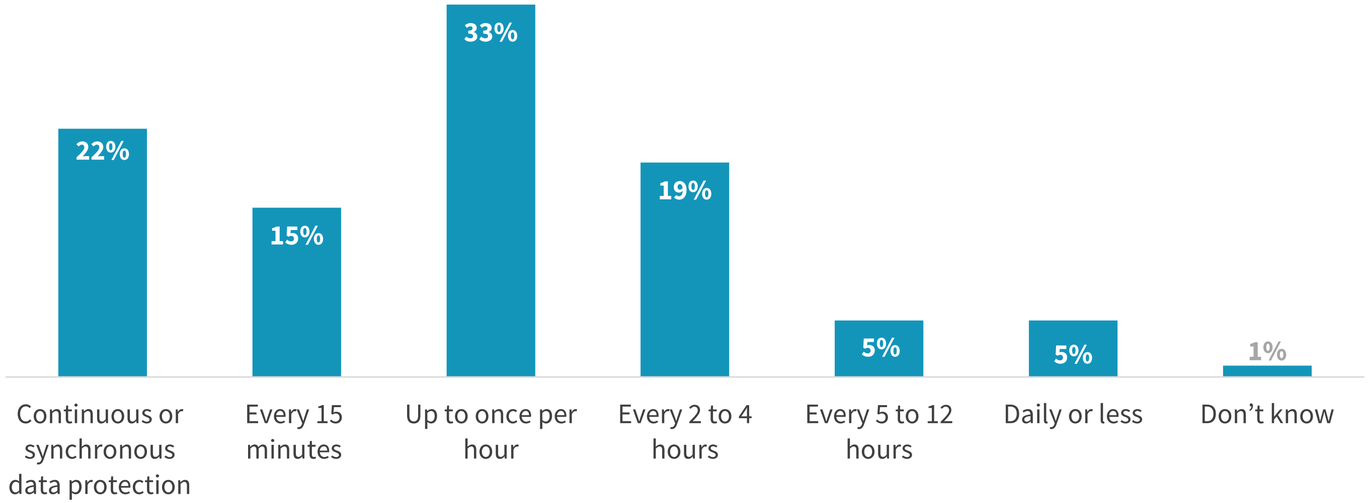



Back to Contents

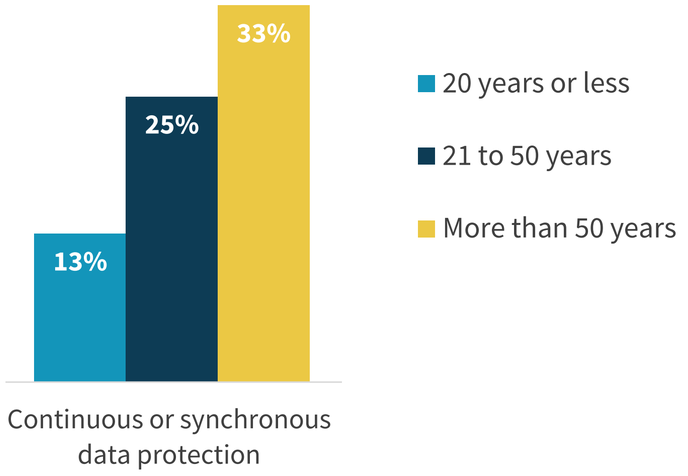
# BaaS RPOs Are Stringent, Especially with Age

Organizations are placing some stringent RPO requirements on their BaaS vendors, with more than one in five expecting continuous data protection-like capabilities, which translates to minimal data loss should anything happen. This can also be seen as a sign of the blurred line between disaster recovery-as-a-service and backup-as-a-service. It is worth noting how demographics, especially the length of time an organization has been in operation, influence this distribution. Specifically, older organizations with more established best practices for mission-critical applications and legacy habits from the on-premises world are significantly more likely to demand tougher requirements in the form of continuous protection. Digital-native companies, for their part, tend to require less stringent RPOs, likely due to a combination of data protection inexperience and potential overconfidence in all things cloud.

Average BaaS RPOs.




BaaS RPOs by age of organization.






Back to Contents

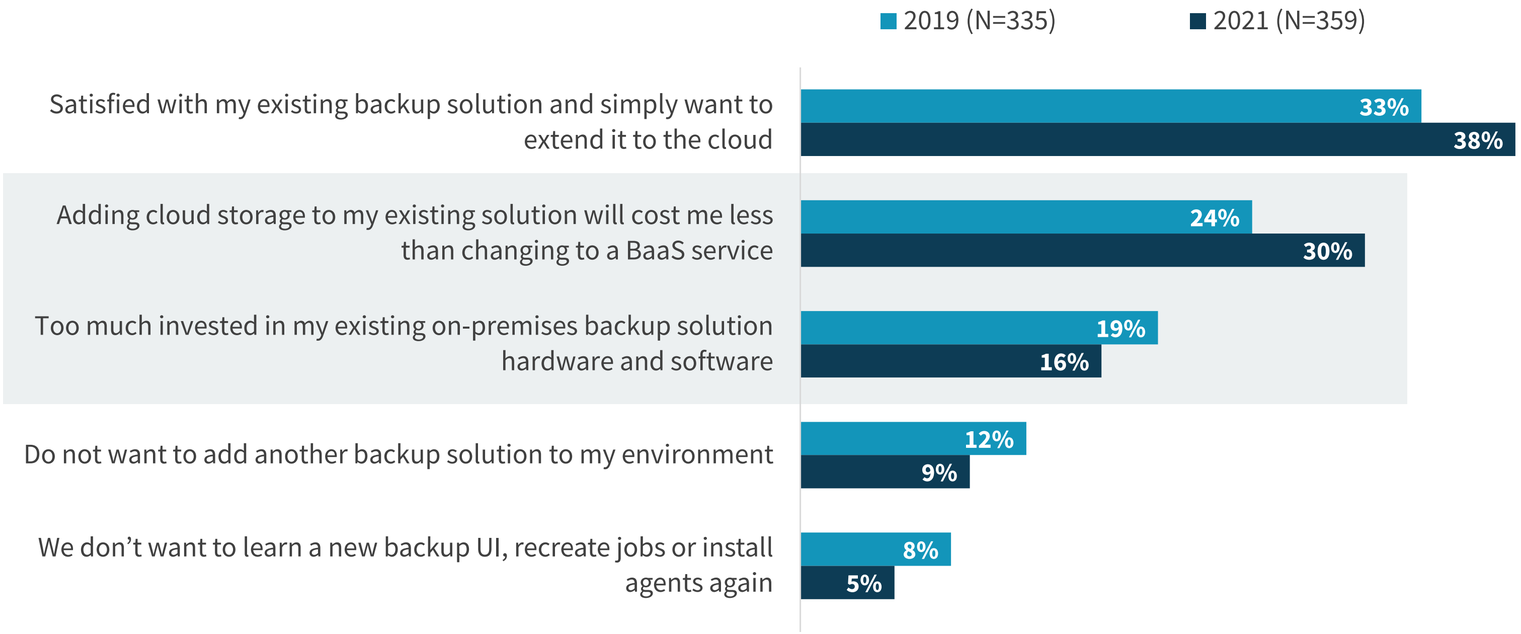
# Extending on-premises data protection environments with cloud backup target solutions is gaining momentum.

# Extending On-premises Backup Leads the Charge for Cloud Target Preference

Extending on-premises backup to cloud destinations was one of the first topologies early cloud adopters leveraged. Things have evolved quickly in the past few years with many advances to the capabilities of this option that is simply an extension of a familiar technology. Change is not always an easy thing for IT to manage, and with change often comes cost. Switching to a different data protection philosophy, and subsequently technology, is not for every organization, especially when it could be viewed as "re-inventing the wheel." There is clearly some level of resistance to extensively or exclusively switching to BaaS due to cost concerns. It is also worth noting the improved level of satisfaction organizations reported this year compared to 2019 with extending their current solution. This is likely due in part to improved vendor capabilities and usability (which we have noticed through the years) and more familiarity with the cloud destination backup and recovery workflows.

> ***There is clearly some level of resistance*** *to extensively or exclusively switching to BaaS due to cost concerns."*

Primary reason to select cloud backup/DR target instead of BaaS.



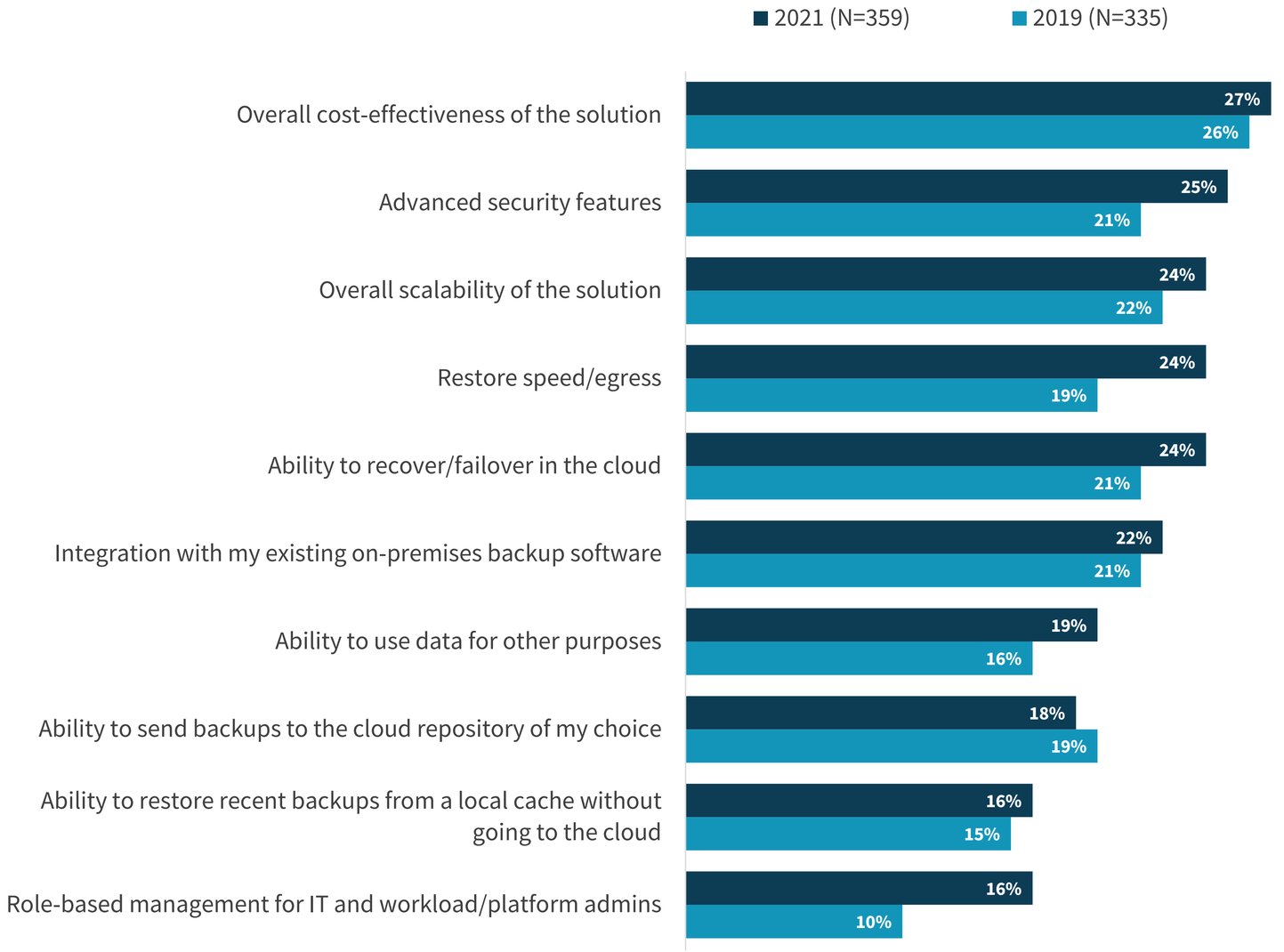



Back to Contents

# Cost and Security Most Common Cloud Backup Target RFP Inclusions

As seen previously, security and cost are both common considerations for organizations when weighing cloud-based data protection technology options. It is not surprising, therefore, that cost-effectiveness and security top the list of key capabilities cloud backup/DR target solutions must meet, while operating at scale. Scalability, restore, and cloud-based recoverability are the other common objectives users have for these services. It is worth noting that the ability to implement intelligent data management processes through data reuse is on the rise, consistent with a shift in the overall backup market.

Most important cloud backup/DR target considerations.






Back to Contents

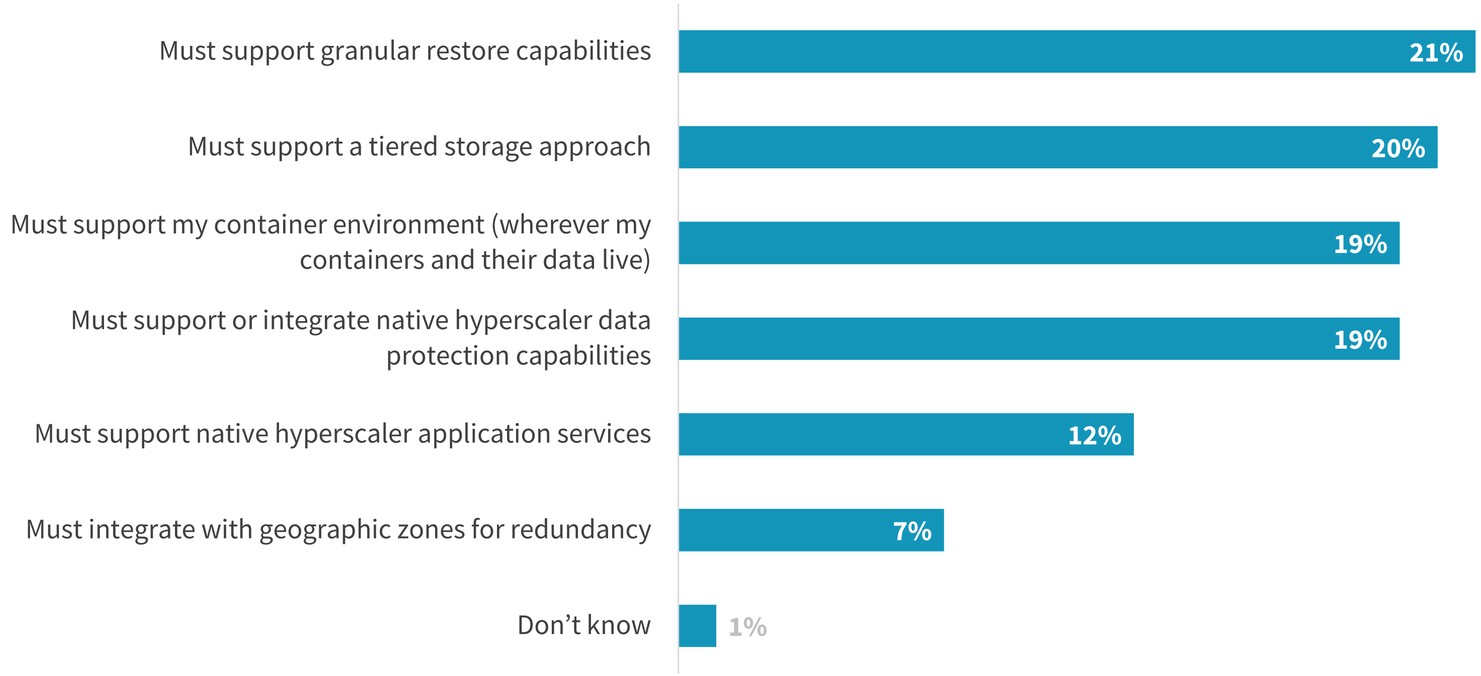
# Data tiering is an influencing factor on in-cloud data protection strategies.

# Granular Restores and Tiered Storage Prioritize In-cloud Data Protection Capabilities

New solutions and capabilities have recently emerged that focus on in-cloud data protection, which often leverage hyperscalers' own new capabilities to protect data that they host. The key characteristics that organizations expect of in-cloud solutions are granular restores and tiered storage, as well as the ability to deliver against service levels and support newer technology deployments, such as those based on container technology. Native integration into the hyperscaler platform is to be noted since it might offer challenges for vendors who will need to integrate deeply with each hyperscaler in order to deliver a consistent set of features and experience across multi-cloud environments.

> ***The key characteristics*** *that organizations expect of in-cloud solutions are granular restores and tiered storage…"*

Most important characteristic for hyperscaler data protection solutions.



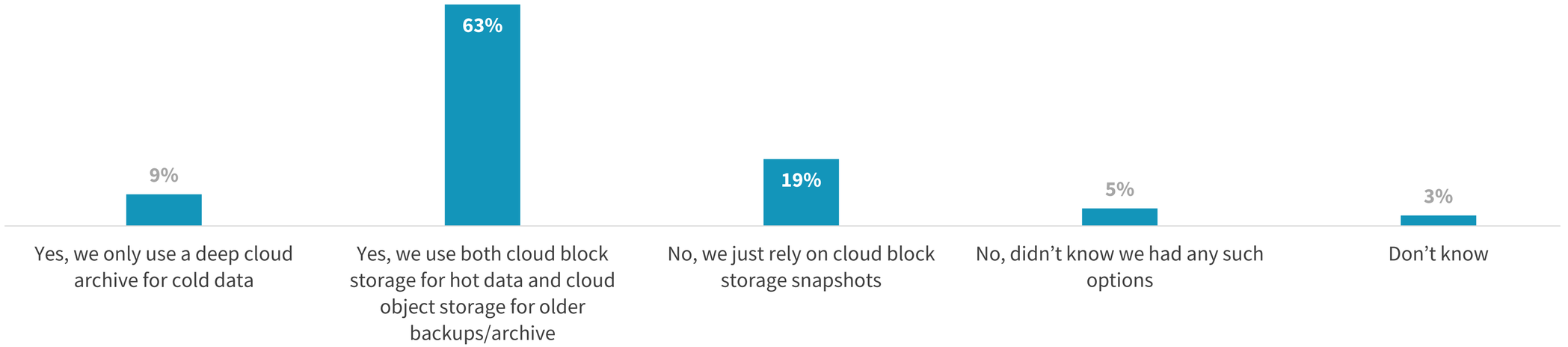



Back to Contents

> **Surprisingly, one in five** *are still leveraging more costly snapshots only.”*

Over the past few years, as they established a growing presence in organizations’ infrastructures, hyperscalers have developed different tiers of compute and storage in order to maximize their operations and match customer needs, which can vary widely based on individual situations and requirements. Cost of storage is a perennial issue in IT, so implementing data tiering for lower costs by leveraging cloud object storage, for example, is becoming the norm. Most organizations use both a “hot” layer with block storage and a cold layer of longer-term retention purposes. Surprisingly, one in five are still leveraging more costly snapshots only. ESG expects that more organizations will likely incorporate colder storage tiers into their strategies as their in-cloud data protection experience matures.

Use of cost-efficient data tiering for data protection storage supporting public cloud infrastructure-resident applications.






Back to Contents

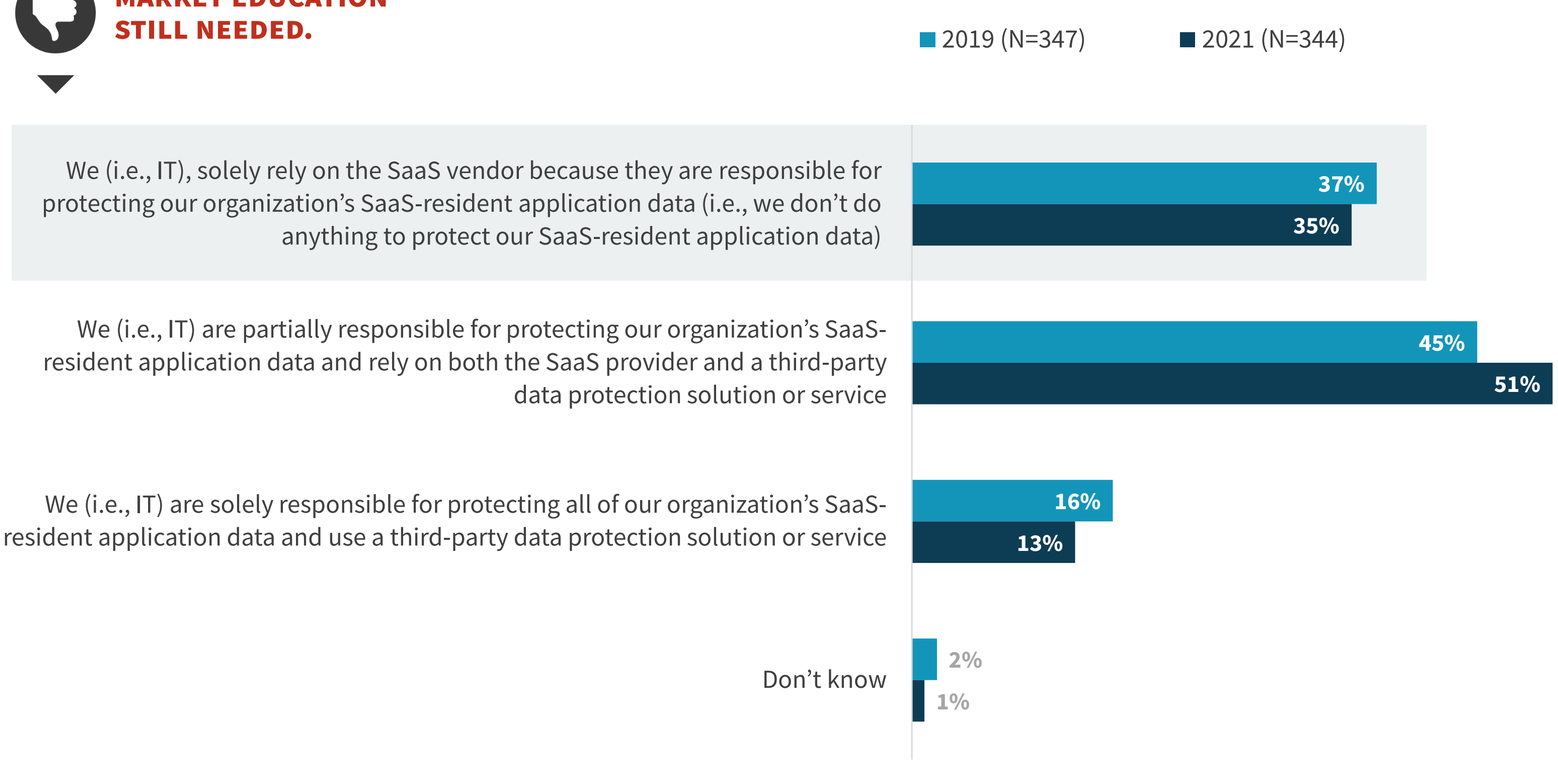
# The big SaaS-data protection disconnect is not improving.

# Many Ways to Lose SaaS Data, Starting with Dependence on SaaS Vendors

ESG has previously highlighted the "big disconnect" associated with SaaS data protection. Unfortunately, the situation has not improved much since 2019 and more market education is needed to convey or redefine best practices when it comes to protecting these cloud-resident applications. First, organizations are **always** responsible for their data and its recovery, so *solely* relying on SaaS vendors is a major mistake. Most do not offer data protection capabilities, instead promoting third-party solutions, and those that offer data protection tools tend to fall short of the scale and SLA that are needed by many organizations. It can be argued that it is a shared responsibility between IT and the SaaS vendor but, to be sure, using a third-party solution is the right answer in every case. These disconnects can lead to serious business consequences should data be lost or become irrecoverable.

Approach to protecting SaaS-resident application data.

**MARKET EDUCATION STILL NEEDED.**

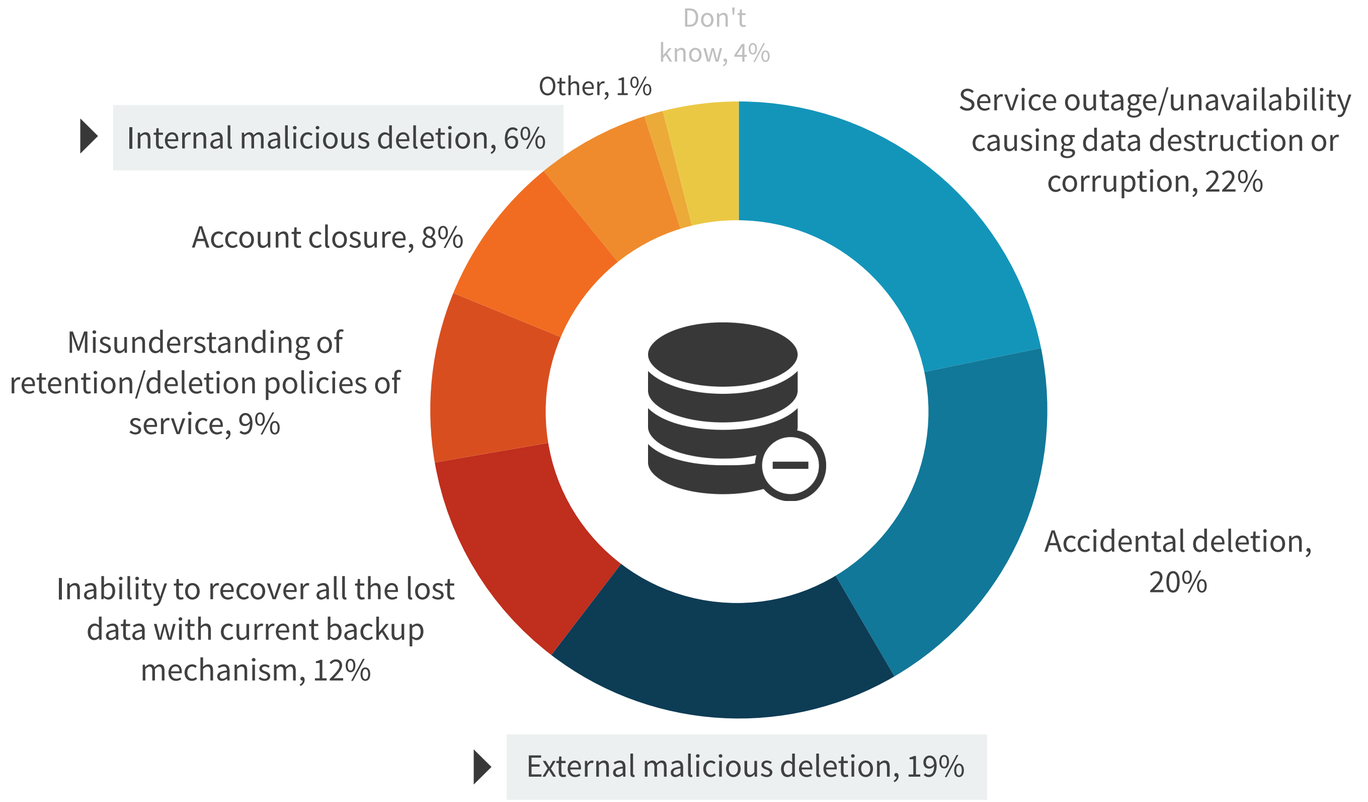





Back to Contents

In addition to not applying any data protection technologies, there are many ways to lose data in SaaS applications, with nearly half (45%) of data loss risk attributed to data deletion. It is particularly unsettling to see that malicious deletion represents one-quarter of the causes of SaaS data loss, whether external (19%) or internal (6%) in nature. These risk levels are incompatible with supporting a mission-critical environment and possibly the signs of organizations' lack of experience and controls. It is also notable that the services themselves are often the top cause of data destruction or corruption. While data corruption is not new and has always been a risk for IT, in the SaaS paradigm, the control of the data and the application is in someone else's hands in a mutually shared environment, making it much harder to control recovery efforts without a strong solution in place.

Top cause of SaaS data loss.




**25%**

of organizations say malicious deletion is their top cause of SaaS data loss.



Back to Contents

## Specific Application Protection and SLAs Top SaaS Backup RFP

Backing up SaaS applications comes with many complexities due to the diversity of these services' technical environments, platforms, and API maturity, among other things. Overall, organizations are looking at their backup solution for SaaS to deliver advanced protection and recovery while maintaining data protection SLAs. In ESG's opinion, this confirms the mission-critical nature of many SaaS applications and the subsequent necessity of the highest levels of data protection.

Top 6 backup solution features for SaaS.

**37%**
Advanced protection and recovery of specific applications

**31%**
Data protection SLAs

**26%**
Cloud-based backup requiring no on-premises hardware/software

**22%**
Industry-leading security

**21%**
Ability to restore large data sets from point-in-time snapshots

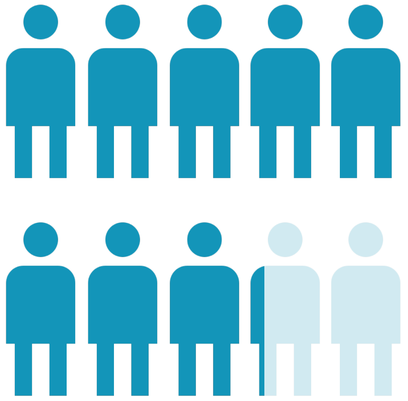
**19%**
Flexibility in selecting a cloud repository locale



Back to Contents

# O365 Recoverability Slowly Improving Overall, though 100% Still Seems Elusive for Many

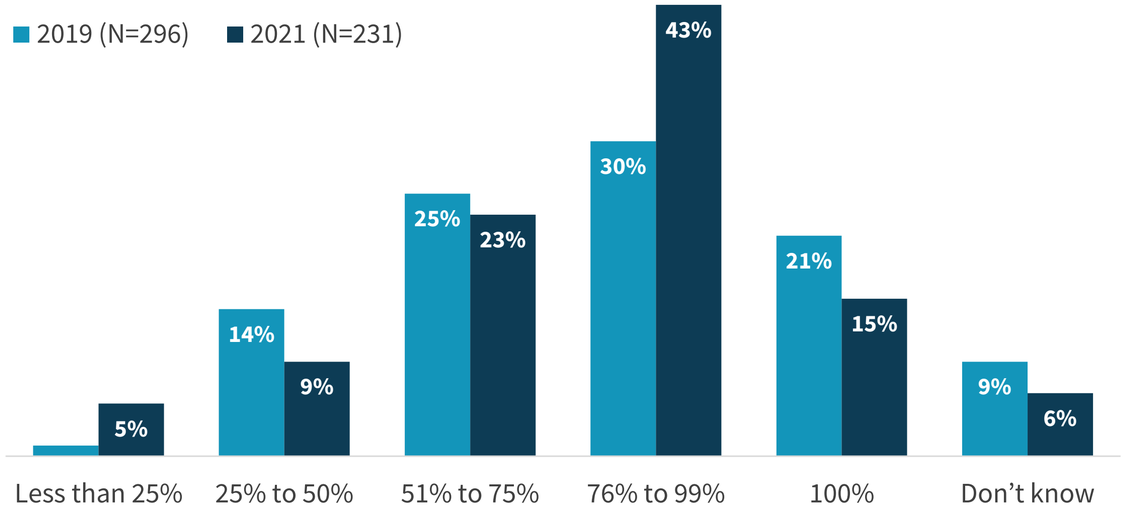
Office 365 is one of the most visible SaaS tools across all market segments and industries. Many critical communications and documents reside within this service, yet organizations are not achieving the success rates one would expect for a mission-critical environment (i.e., 100%). As a matter of fact, while ESG has seen progress overall in terms of O365 data recoveries, fewer organizations actually reported a 100% success rate compared to 2019. More adoption and other exogenous factors may be at play such as data growth, increased use by inexperienced employees due to COVID, and lack of skill sets.



**81%**

of organizations surveyed by ESG have had to recover O365 data

O365 data recovery success rate.






Back to Contents

IRON MOUNTAIN®

Iron Mountain Incorporated (NYSE: IRM) is a global business dedicated to storing, protecting and managing information and assets.

LEARN MORE

**ABOUT ESG**

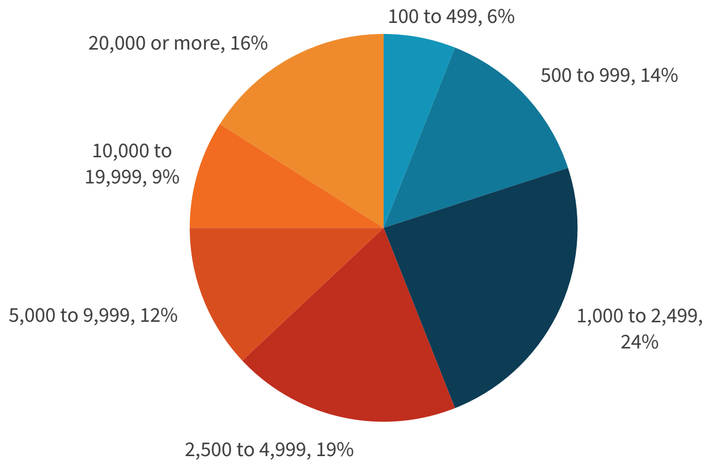
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

# Research Methodology and Demographics

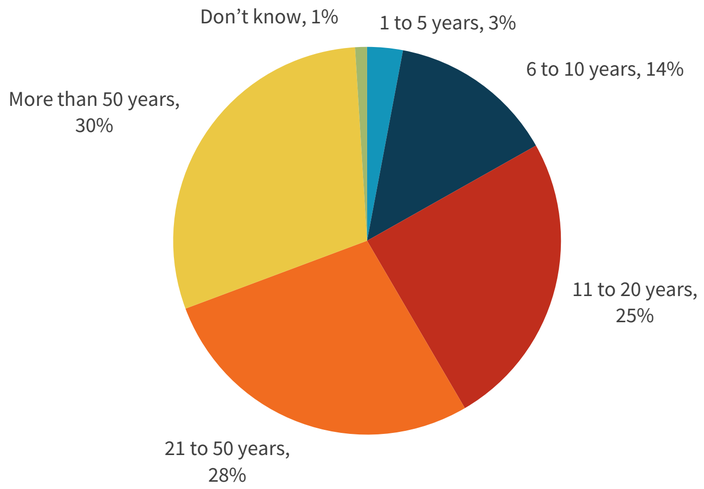
To gather data for this report, ESG conducted a comprehensive online survey of IT professionals from private- and public-sector organizations in North America (United States and Canada) between January 22, 2021 and January 30, 2021. To qualify for this survey, respondents were required to be IT professionals 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. Respondents' organizations were required to be using a cloud-based data protection service and/or protecting public cloud-resident applications or data. 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 381 IT professionals.

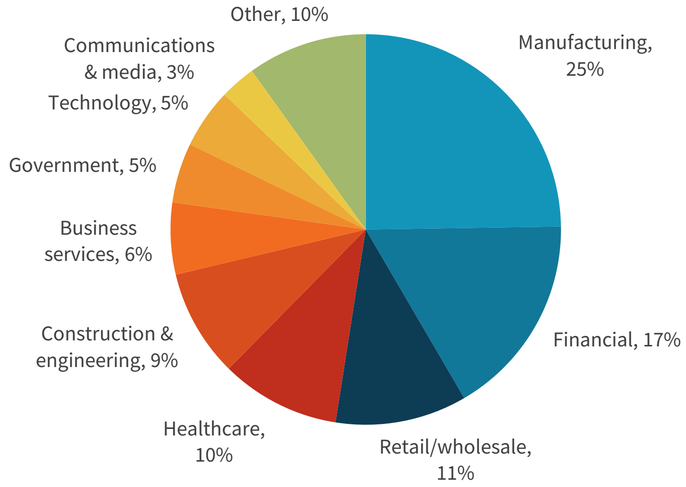
**RESPONDENTS BY NUMBER OF EMPLOYEES**




**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.