



Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

DATA PROTECTION CLOUD STRATEGIES

Protecting Data *To* and *In* the Cloud

Christophe Bertrand, Senior ESG Analyst

JUNE 2019



CONTENTS

Research Objectives [3](#)

Key Research Findings [4](#)

Cloud data protection has hit the stratosphere. [5](#)

BaaS is all about recovery and RTAs are improving. [8](#)

Cost and scalability are key cloud backup target considerations. [11](#)

SaaS data protection expectations are disconnected from reality. [14](#)

SLAs, support, and employee behavior are among the most common SaaS pitfalls. [17](#)

RESEARCH OBJECTIVES

The broad adoption of cloud services as a source of business-critical data is placing the onus on data owners to deliver on data protection SLAs of data and applications that are hosted in the cloud. Concurrently, on-premises backup and disaster recovery workloads are leveraging cloud destinations, resulting in hybrid data protection topologies with varying service levels, end-user tradeoffs, and opportunities. How are IT organizations utilizing cloud services as part of their data protection strategy today?

In order to get more insight into these trends, ESG surveyed 370 IT professionals at organizations in North America (U.S. and Canada) 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:

- Determine how organizations utilize cloud services as part of their data protection strategy.
- Establish users' understanding of what exact data protection levels public cloud infrastructure and SaaS solutions provide.
- Identify current business requirements driving modern and increasingly cloud-centric data protection strategies.
- Monitor year-over-year trends with respect to evolving data protection cloud strategies.

Survey participants represented a wide range of industries including manufacturing, financial services, health care, communications and media, retail, government, and business services. For more details, please see the Research Methodology and Respondent Demographics sections of this report.

KEY RESEARCH FINDINGS

- 1. Cloud data protection has hit the stratosphere.** Whether it involves using public cloud-based data protection services, backing up cloud-based applications/workloads, or some combination of the two, the vast majority of survey respondents classified cloud computing as helpful to their organization's data protection strategy. There has been significant uptake across the board in the past three years for the cloud backup target, backup-as-a-service, and disaster recovery-as-a-service topologies, making on-premises-only approaches a thing of the past for many organizations.
- 2. BaaS is all about recovery and RTAs are improving.** Nearly three-quarters of current BaaS users report that they have had to recover more than a single file within the past 12 months compared with only 59% in 2016. In addition to more organizations performing more BaaS recoveries, the success rates of these efforts are increasing. When asked about those cases in which their organization had to recover data, the number of respondents indicating that their recovery time objectives (RTOs) were always met successfully was nearly double that of three years ago.
- 3. Cost and scalability are key cloud backup target considerations.** When asked about the primary factor that would lead—or has led—organizations to add cloud storage to an existing on-premises backup solution in lieu of a BaaS solution, more than four in ten cited economic considerations. Among current and potential users of cloud backup target services, cloud destinations are preferred for offsite backup data today. Cloud targets now offer a great replacement option for tape, confirmed by the fact that more than three-quarters of current and potential cloud backup target service users are likely to replace their on-premises tape libraries with cloud.
- 4. The big expectations for SaaS data protection are disconnected from reality.** One-third of current and potential SaaS users believe these cloud-based applications do not need to be backed up. Similarly, 37% believe that the SaaS provider is actually responsible for protecting data, which is only typically true for limited periods of time, and only from an availability standpoint (versus data recoverability). The vast majority of current and potential SaaS users claim to be familiar with the data protection and recovery SLAs of their SaaS providers, with more than half asserting awareness with all SaaS SLAs.
- 5. SLAs, support, and employee behavior are among the most common SaaS pitfalls.** Many organizations have reported struggling with the quality and availability of the support provided by their SaaS providers. The most common support shortcomings include finding the right person to solve specific problems, misalignment of understanding in terms of what recovery SLAs include, inexperienced staff, and limited support hours. As far as top data loss causes for SaaS applications, nearly one in three organizations cite deletions, whether accidental or intentional in nature.

A wide-angle, high-altitude view of Earth from space, showing the curvature of the planet and the thin blue atmosphere. The sun is visible in the distance, creating a bright orange and yellow glow over the clouds. The clouds are scattered and appear as white and light blue patches against the darker blue of the atmosphere. The overall scene is a dramatic, high-contrast view of the planet from the stratosphere.

**Cloud data protection
has hit the stratosphere.**

Usage of cloud data protection services has become mainstream.

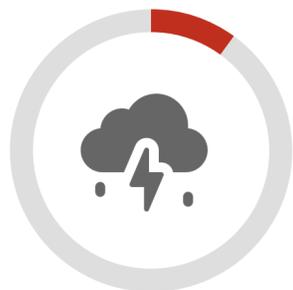
IT professionals overwhelmingly recognize the positive impact of cloud services to their data protection strategy. Whether it involves using public cloud-based data protection services, backing up cloud-based applications/workloads, or some combination of the two, the vast majority (87%) of survey respondents classified cloud computing as helpful to their organization’s data protection strategy.



87%

Helpful

Cloud computing has become an important part of our data protection strategy that has enabled us to better and/or more cost-efficiently protect our data.



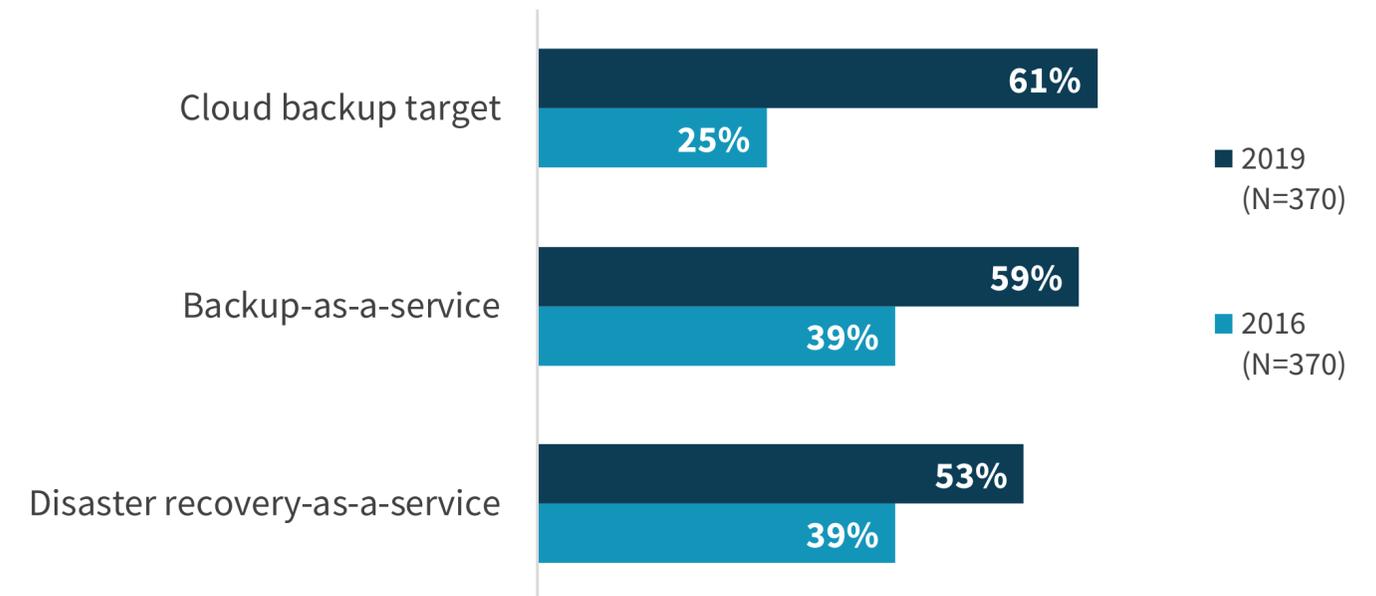
10%

Hindrance

Using cloud services as backup/DR targets and/or backing up cloud-based applications and infrastructure has only added new processes and more complexity to our data protection strategy.

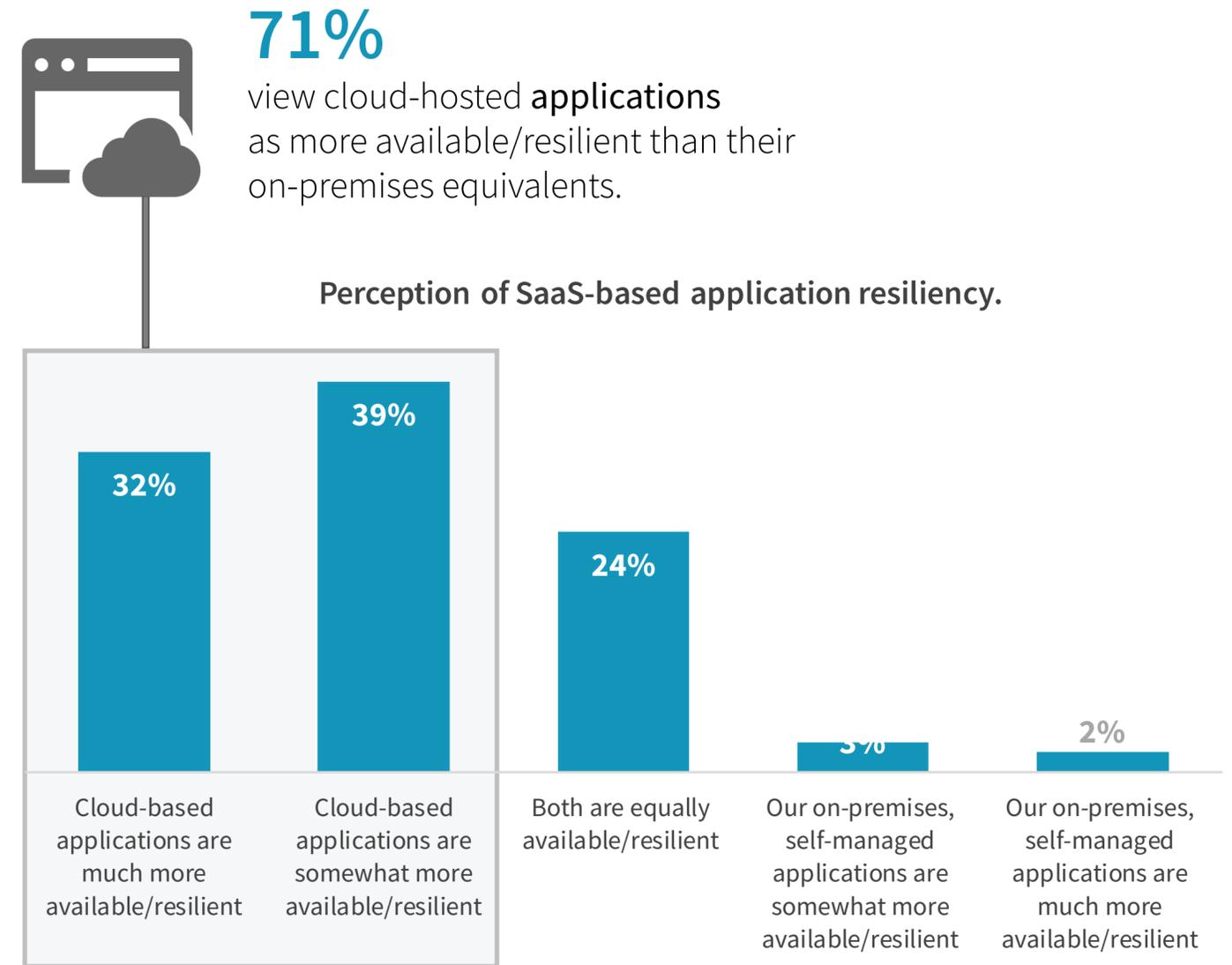
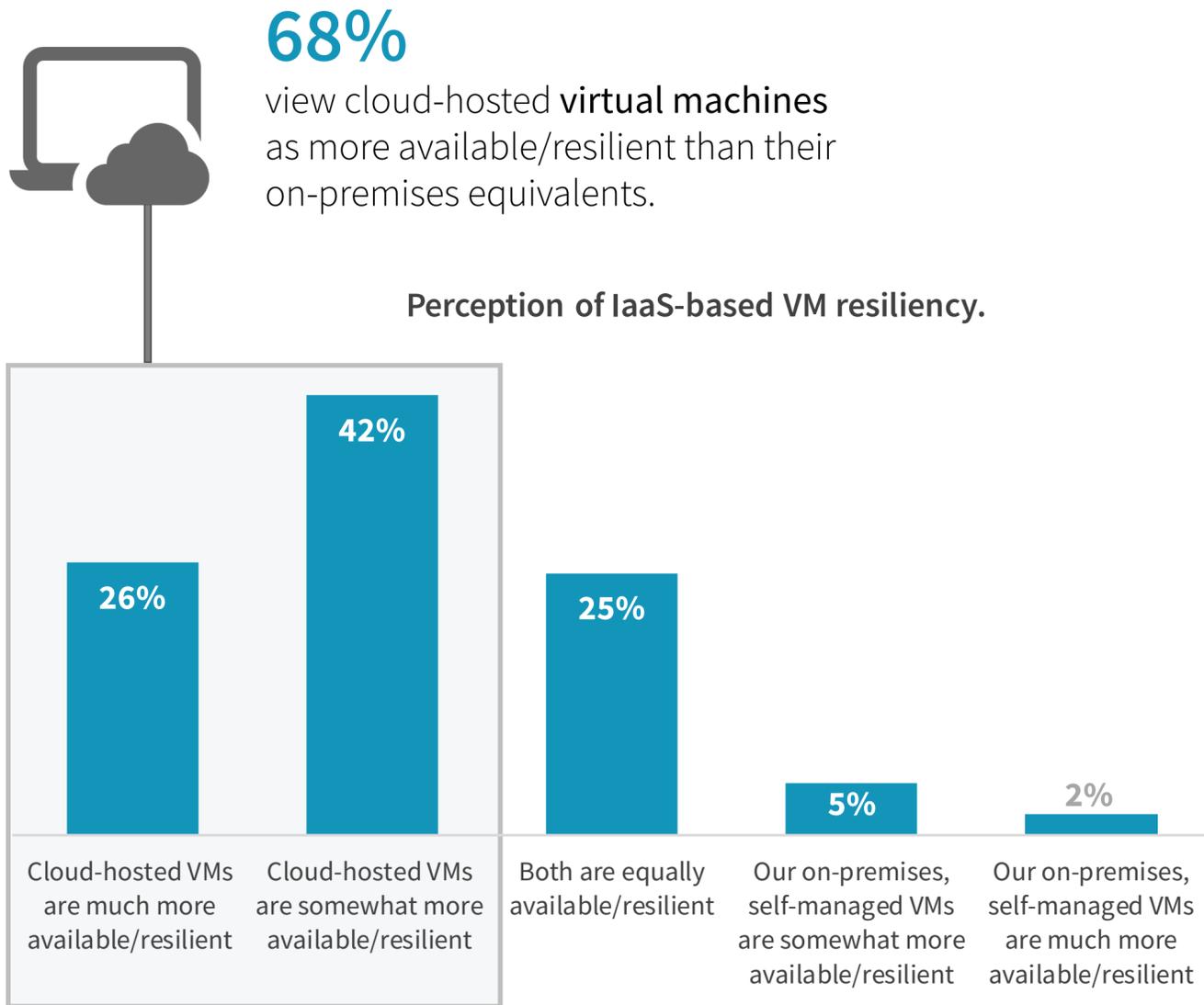
When it comes to using public cloud-based data protection services, this positive sentiment is clearly reflected in the increased usage in the main deployment models since 2016. Specifically, there has been significant uptake across the board in the past three years for the cloud backup target, backup-as-a-service, and disaster recovery-as-a-service topologies, making on-premises-only approaches a thing of the past for many organizations.

Percentage of organizations currently using cloud-based data protection services, 2016 vs. 2019. (Percent of respondents)



Cloud-based VMs and applications are perceived to be more resilient than their on-premises counterparts.

Resiliency is the name of the game in IT, since applications and associated data are the lifeblood of businesses. Cloud is king when it comes to resiliency perceptions. Indeed, the majority of respondents view both cloud-hosted virtual machines (68%) and cloud-hosted applications (71%) as more available/resilient than their on-premises equivalents.

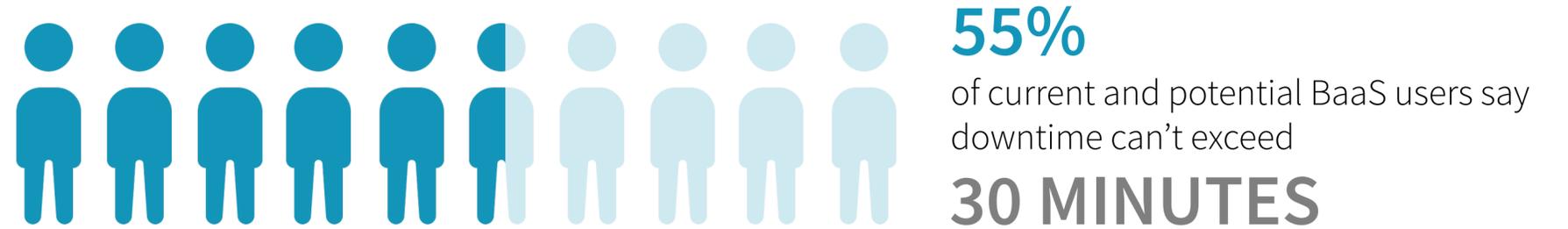




**BaaS is all about recovery
and RTAs are improving.**

BaaS: low threshold for downtime and high priority on recovery.

Organizations have a low threshold for downtime, and very stringent RTO expectations for their cloud backup services. In fact, more than half (55%) of current and potential BaaS users say downtime can't exceed 30 minutes when it comes to the applications/workloads protected by these services.



Similarly, and perhaps not surprisingly, for those using and aspiring to use cloud backup services, BaaS is about recovery, with three of the five most commonly cited characteristics involving recoverability. This means that more than half (58%) of current and potential BaaS users prioritize the speed of recovery (27%), ability to recover/failover to the cloud (25%), and/or flexibility of recovery options (22%) when it comes to considering these services.

Most commonly desired BaaS characteristics



27%

Speed of recovery



25%

Ability to recover/
failover in the cloud



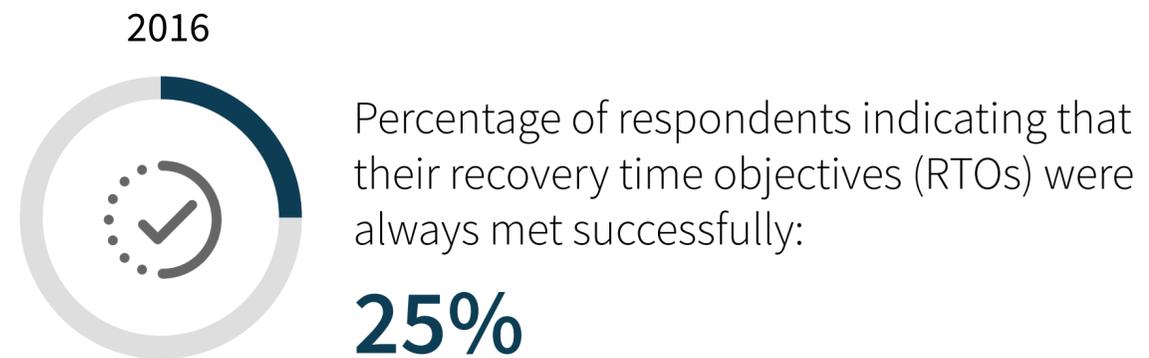
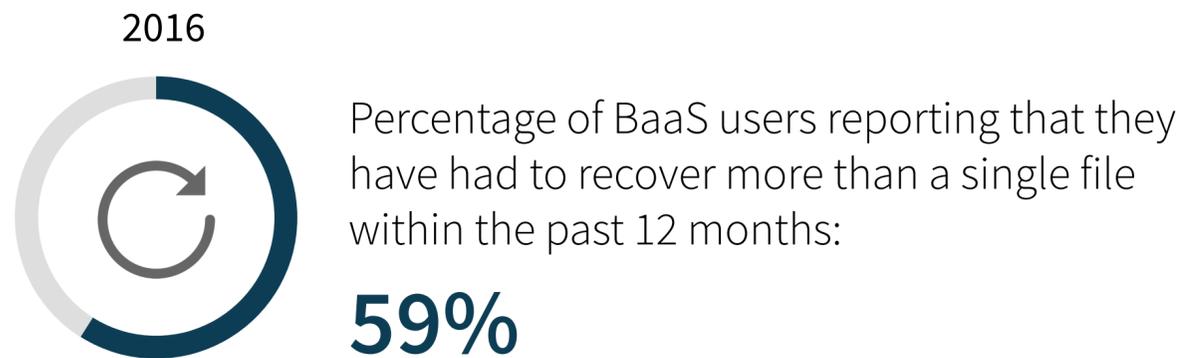
22%

Flexible recovery
options

BaaS RTAs are getting better but leave room for improvement.

When it comes to actual BaaS recovery operations, these procedures have become more frequent over the last three years. Specifically, nearly three-quarters (71%) of current BaaS users report that they have had to recover more than a single file within the past 12 months compared with only 59% in 2016, equating to an average of 1.33 recoveries in the last year.

In addition to more organizations performing more BaaS recoveries, the success rates of these efforts are increasing. When asked about those cases in which their organization had to recover data, the number of respondents indicating that their recovery time objectives (RTOs) were always met successfully was nearly double that of three years ago (25% in 2016 versus 48% in 2019). However, this means that more than half of organizations are not always having their RTOs met, so there is room for improvement.



A man with a grey beard and glasses is looking at a screen. The screen is covered with several yellow sticky notes. The background is a bright, slightly blurred office environment.

**Cost and scalability
are key cloud backup
target considerations.**

Status quo and investment protection are driving choices for cloud backup target over BaaS.

As the saying goes, if it's not broken, don't fix it! Changing backup and recovery technologies has historically been a cumbersome process and switching to a cloud solution adds an extra degree of difficulty. When asked about the primary factor that would lead—or has led—organizations to add cloud storage to an existing on-premises backup solution in lieu of a BaaS solution, more than four in ten cited economic considerations in the form of adding cloud storage simply costing less than changing to a BaaS solution (24%) or concerns that they had already invested too much in their existing on-premises backup portfolio (19%). Another third stated they were satisfied with their existing backup solution and simply wanted to extend it to the cloud.

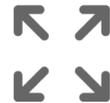
 **33%**
Satisfied with my existing backup solution and simply want to extend it to the cloud

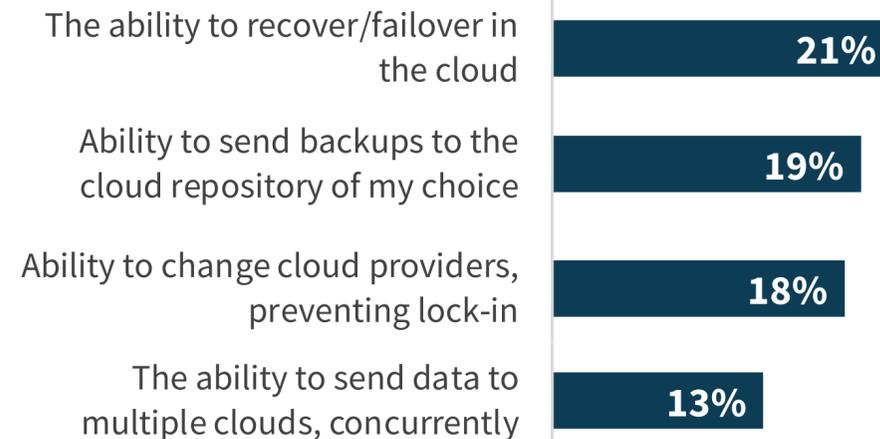
 **24%**
Adding cloud storage to my existing solution will cost me less than changing to a BaaS service

 **19%**
Too much invested in my existing on-premises backup solution hardware and software

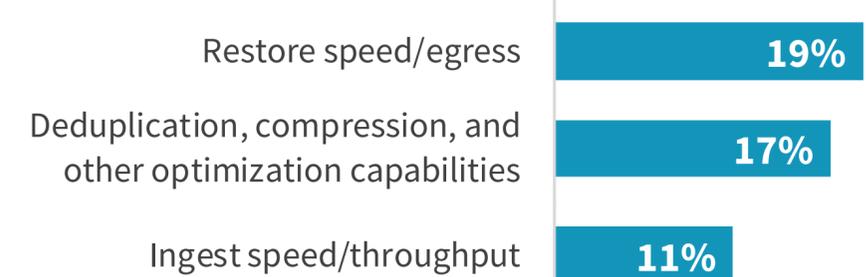
 **12%**
Do not want to add another backup solution to my environment

The promise of cloud deployments in general terms is the ability to add capacity in an elastic fashion at a great price point. For cloud backup target topologies, this expectation is no different. Organizations that have adopted or are considering a cloud backup target solution favor flexibility (58%) and performance (41%).


Flexibility

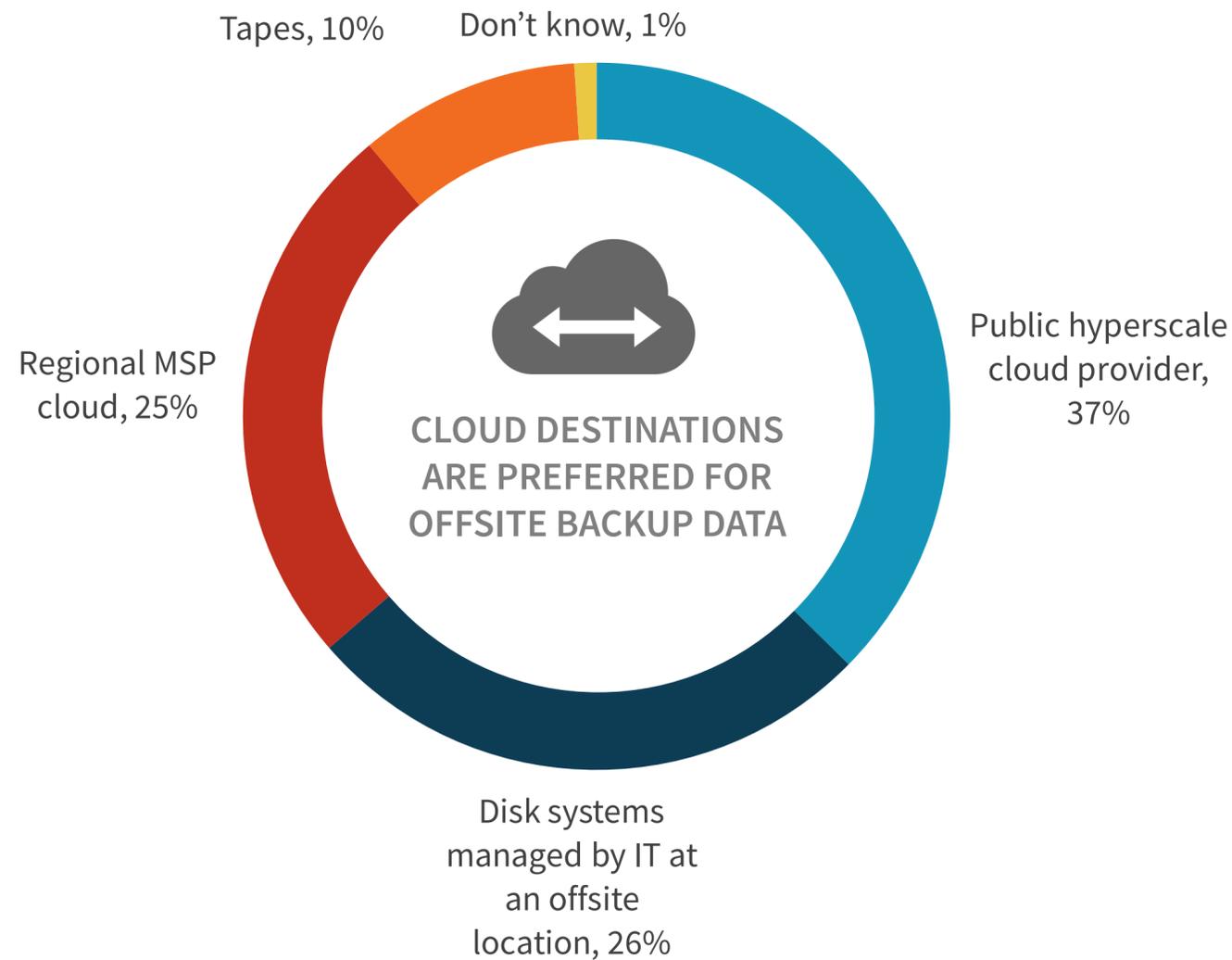


Performance-related



Cloud destinations are preferred for offsite backup data and primed to replace on-premises tape.

The world of secondary disaster recovery data centers is evolving. Among current and potential users of cloud backup target services, cloud destinations are preferred for offsite backup data today, whether by leveraging a hyperscaler (37%) or a regional MSP (25%).



The demise of tape has been expected for many years, yet it maintains a presence in many environments as both a backup and archive medium. Attitudes are changing as cloud targets now offer a great replacement option for tape, confirmed by the fact that more than three-quarters of current and potential cloud backup target service users are extremely likely (31%) or likely (47%) to replace their on-premises tape libraries with cloud. Those with at least 250 TB of cloud-resident backup data are nearly twice as likely (54% versus 29%) as those below that mark to consider themselves extremely likely to replace on-premises tape with cloud.



78%

of current and potential cloud backup target service users are extremely likely (31%) or likely (47%) to replace their on-premises tape libraries with cloud.



TWICE AS LIKELY

as those below that mark to consider themselves extremely likely to replace on-premises tape with cloud.

**SaaS data
protection expectations
are disconnected
from reality.**



SaaS and data protection misperceptions.

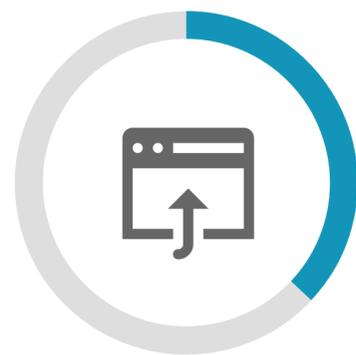
There is a big disconnect between the expectations of IT users who leverage SaaS applications and the reality of what is delivered by the SaaS providers in terms of data protection. Indeed, one-third of current and potential SaaS users believe these cloud-based applications do not need to be backed up. Users might be giving up control and residency of the data, but not data protection or governance responsibilities. Similarly, 37% believe that the SaaS provider is actually responsible for protecting data, which is only typically true for limited periods of time, and only from an availability standpoint (versus data recoverability).

The vast majority of current and potential SaaS users claim to be familiar with the data protection and recovery SLAs of their SaaS providers, with more than half (58%) asserting awareness with all SaaS SLAs. ESG believes that they might be confusing availability of the service with actual backup and recovery responsibility, which is always the data owner's concern.



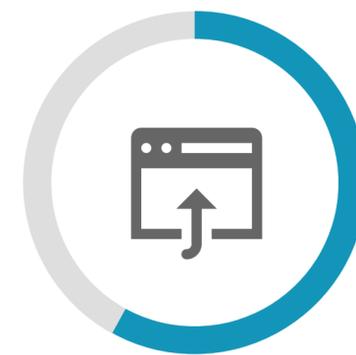
33%

of current and potential SaaS users believe these cloud-based applications do not need to be backed up



37%

believe that the SaaS provider is actually responsible for protecting data



58%

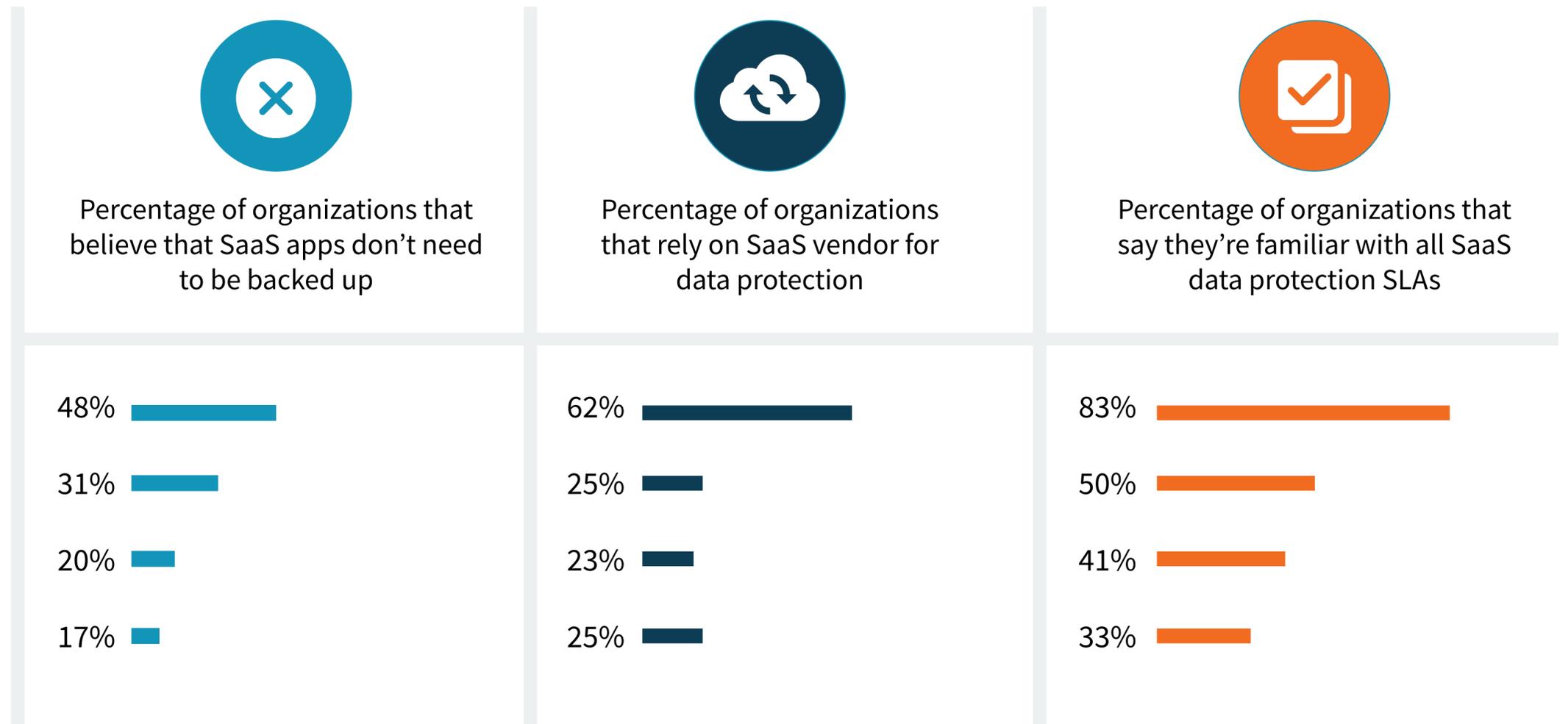
asserting awareness with all SaaS SLAs.

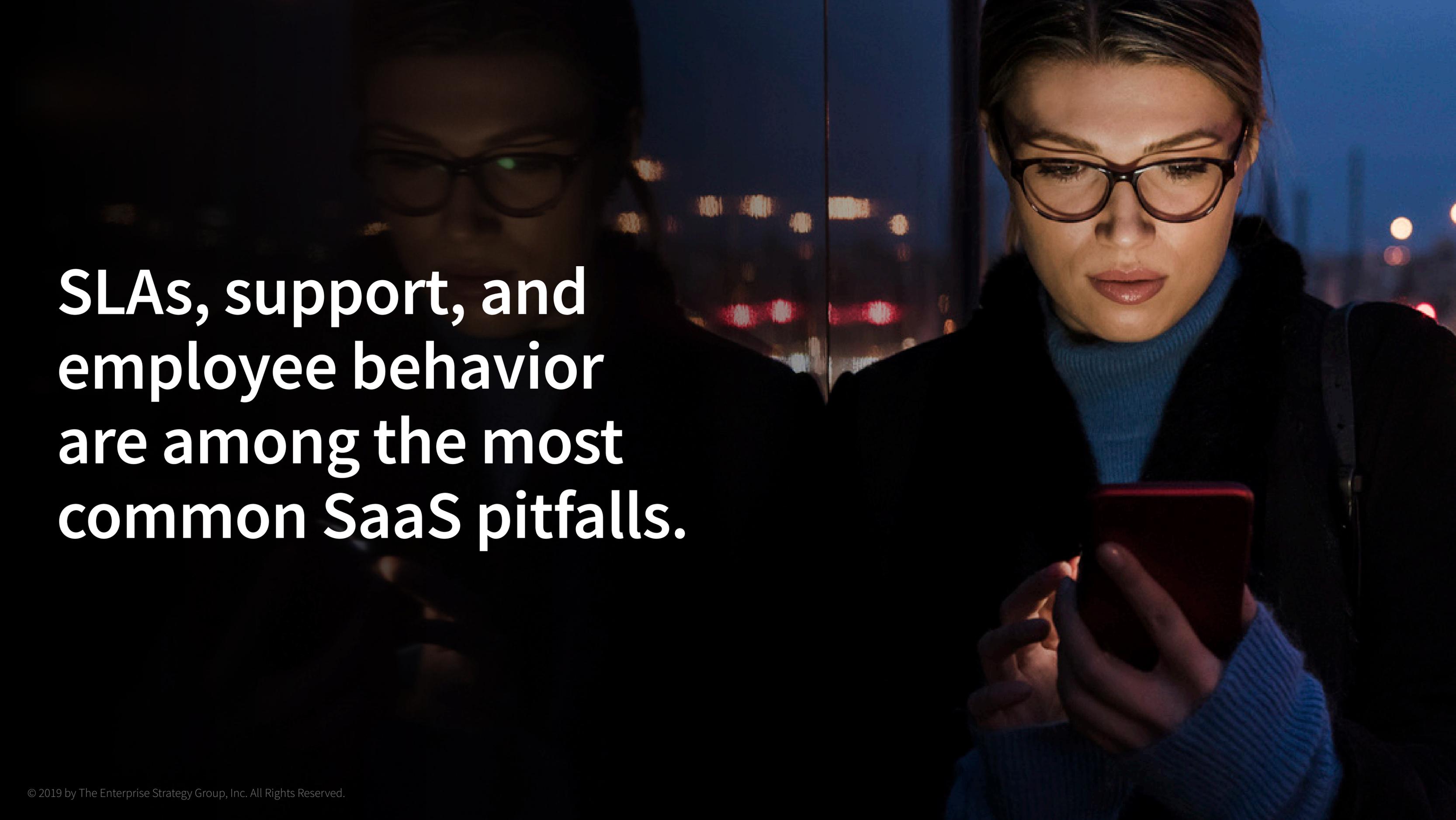
Is SaaS application resiliency being conflated with SaaS data *availability*?

SaaS applications are expected to be always on, always available...and except for rare service interruptions, they actually are. Yet this does not mean that data is backed up as is the age-old best practice in on-premises environments. Could it be that many organizations are still naïve when it comes to data protection and cloud, specifically as it pertains to SaaS? As seen earlier, nearly three-quarters of respondents believe that cloud-based applications are more resilient than those run on-premises in their own data centers, and those perceptions can affect data protection behaviors.

Specifically, the higher the level of confidence that organizations have in cloud-based application resiliency, the likelier they are to believe that SaaS apps don't need to be backed up, rely on the SaaS provider for data protection, and claim they are familiar with all SaaS data protection SLAs.

- Cloud-based apps much more resilient:
- Cloud-based apps more resilient:
- Cloud-based and on-premises apps equally resilient:
- On-premises apps more resilient:



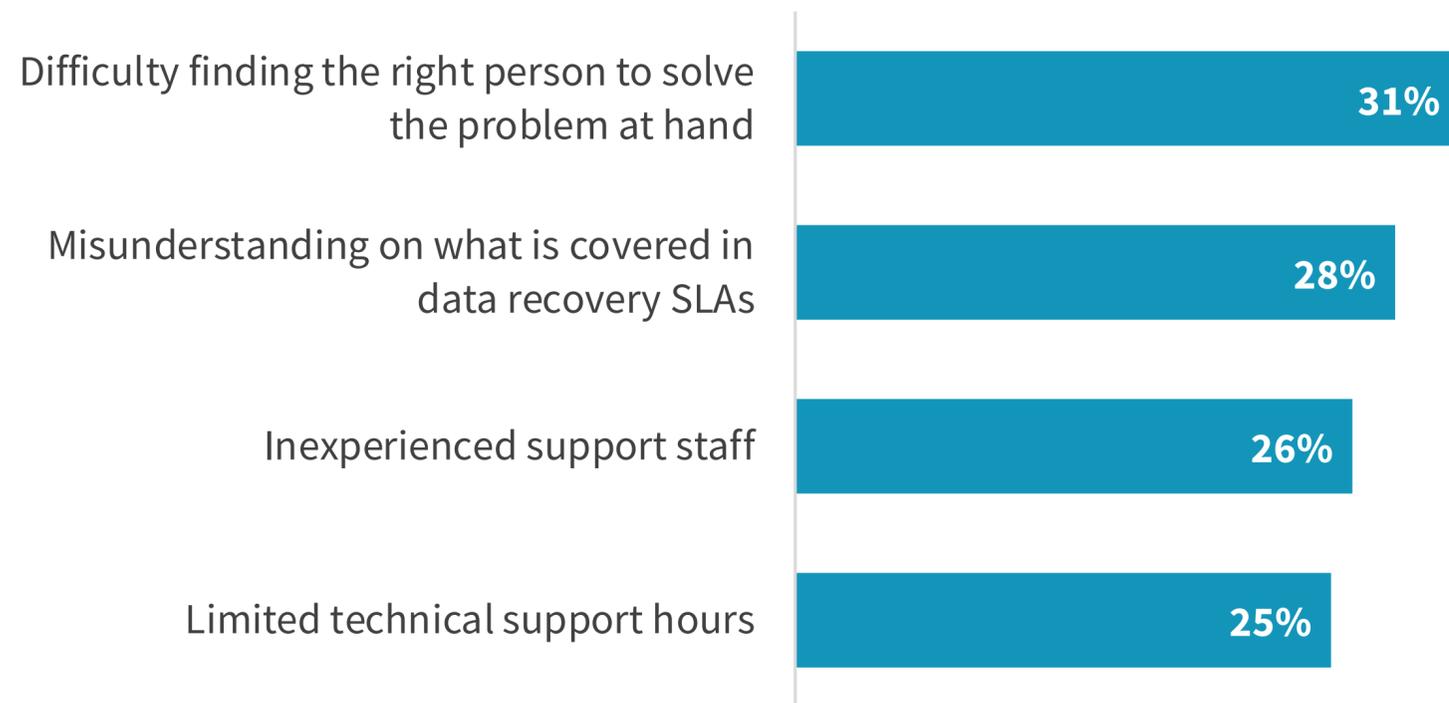
A photograph of two women at night, looking at a smartphone. The woman on the right is in focus, wearing glasses and a blue turtleneck, holding the phone. The woman on the left is out of focus, also wearing glasses. The background shows blurred city lights.

**SLAs, support, and
employee behavior
are among the most
common SaaS pitfalls.**

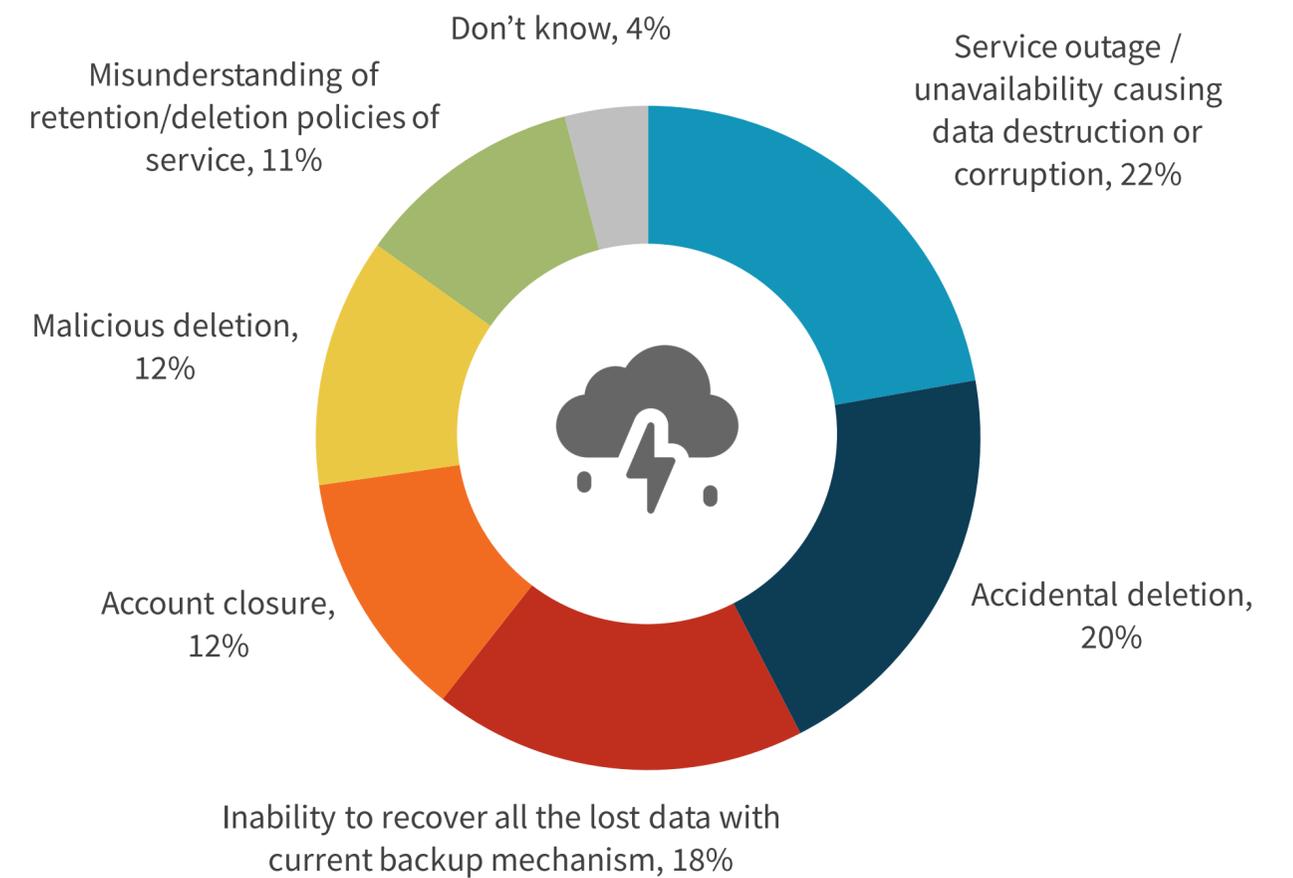
SaaS providers struggle with support and SLAs, while SaaS users contend with accidental and malicious deletion.

Many organizations have reported struggling with the quality and availability of the support provided by their SaaS providers. With many years of experience with enterprise-class support for on-premises resources setting the expectations bar high, SaaS providers will need to up-level their support capabilities. The most common support shortcomings include finding the right person to solve specific problems (31%), misalignment of understanding in terms of what recovery SLAs include (28%), inexperienced staff (26%), and limited support hours (25%).

TOP 4 service and support challenges organizations experienced with its SaaS providers, as it relates to data protection and recovery?



As far as top data loss causes for SaaS applications, nearly one in three organizations cite deletions, whether accidental (20%) or intentional (12%). More than one in five report losing data to service outages or unavailability, an unacceptable level of risk (in terms of compliance and RPOs/RTOs) for most modern enterprises.



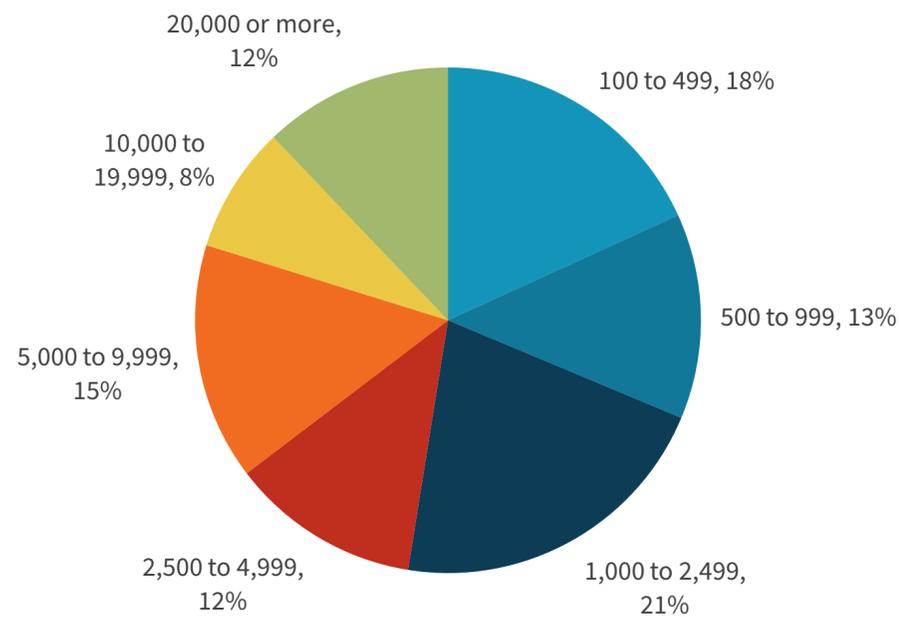
Research Methodology

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 February 6, 2019 and February 21, 2019. 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. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

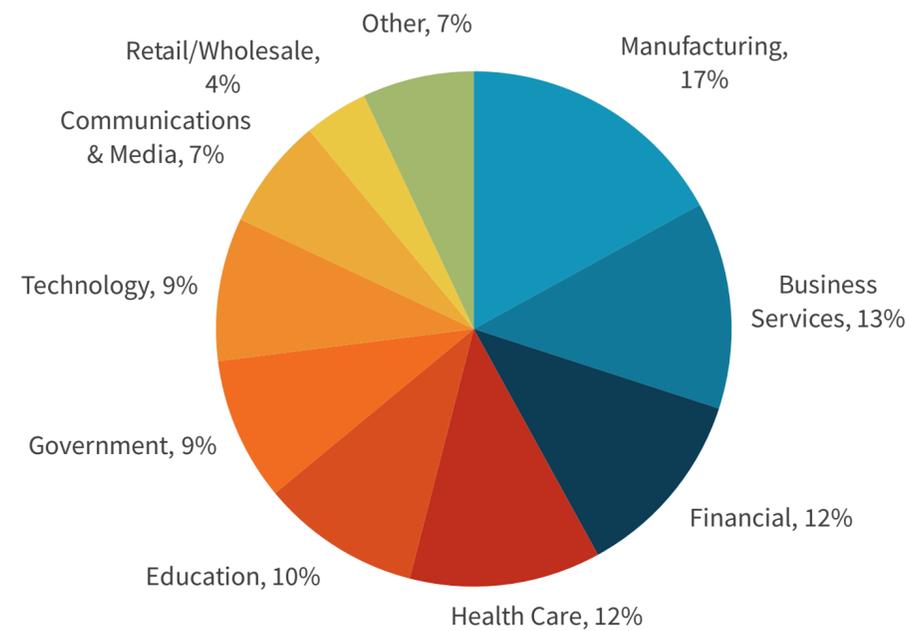
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 370 IT and cybersecurity professionals.

Respondent Demographics

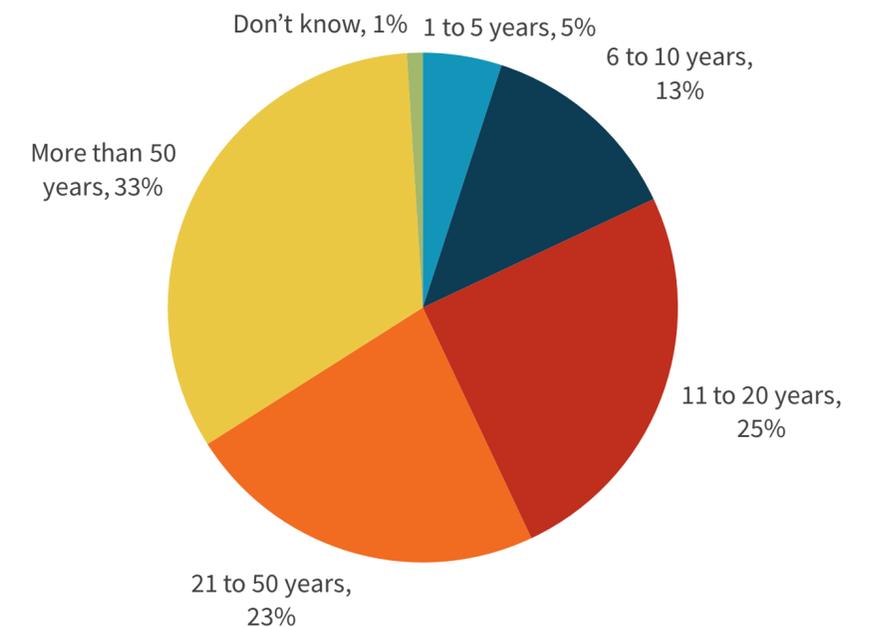
Respondents by Number of Employees



Respondents by Industry



Respondents by Age of Organization





Spanning Cloud Apps, a Kaseya company, is the leading provider of backup and recovery for SaaS applications, helping organizations around the globe protect their information in the cloud. The company provides powerful, enterprise-class data protection for Microsoft Office 365, G Suite, and Salesforce. With data centers located in North America, the EU, and Australia, Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of companies and millions of users around the world.

Learn more at www.spanning.com. Follow Spanning on Twitter [@spanningbackup](https://twitter.com/spanningbackup).

LEARN MORE



All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.
© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.