



Enterprise Strategy Group | Getting to the bigger truth.™

A Successful Cloud Data Protection Blueprint

Christophe Bertrand, Senior Analyst

OCTOBER 2021

The Evolving Data Protection Landscape

The adoption of cloud infrastructure technology in the past few years has generated a mass migration of data and applications to the cloud. A significant number of these now cloud-based applications are mission-critical for the organizations that leverage them, as are the associated data sets. This broad adoption of cloud services as a source of and repository for business-critical data does not absolve organizations/data owners from delivering on stringent data protection SLAs as impacts of downtime can be significant and damaging.

Cloud-based solutions are clearly gaining favor with IT professionals when it comes to data protection mechanisms, and many organizations have the highest level of confidence in public cloud infrastructure applications to meet recovery SLAs. At the same time, a disconnect exists for SaaS application data protection: Many organizations wrongly believe that such protection comes with the service, in turn leaving popular solutions such as Microsoft 365 and Salesforce.com potentially exposed to data loss.

Research Methodology

In order to understand how organizations are evolving their approach to data protection SLAs and to what extent these efforts are affected—both positively and negatively—by the use of public cloud services, ESG surveyed IT professionals at organizations in North America (US and Canada) responsible for their organization's data protection technology decisions. All respondents were provided an incentive to complete the surveys in the form of cash awards and/or cash equivalents. Please see the Respondent Demographics sections of the reports below for more information on the profiles of these respondents.

Sources:

ESG Research Reports:

Real-world SLAs and Availability Requirements, October 2020.

2021 Technology Spending Intentions Survey, January 2021.

The Evolution of Data Protection Cloud Strategies, May 2021.

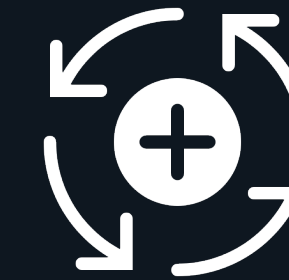
KEY FINDINGS

CLICK TO FOLLOW



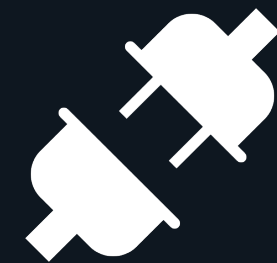
Downtime is a business problem—not just an IT problem—for which organizations have a low tolerance... especially in the cloud.

PAGE 4



Data protection and BC/DR processes are becoming increasingly intertwined with the cloud.

PAGE 10




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

PAGE 15



Druva and AWS: Protecting your cloud workloads for business success.

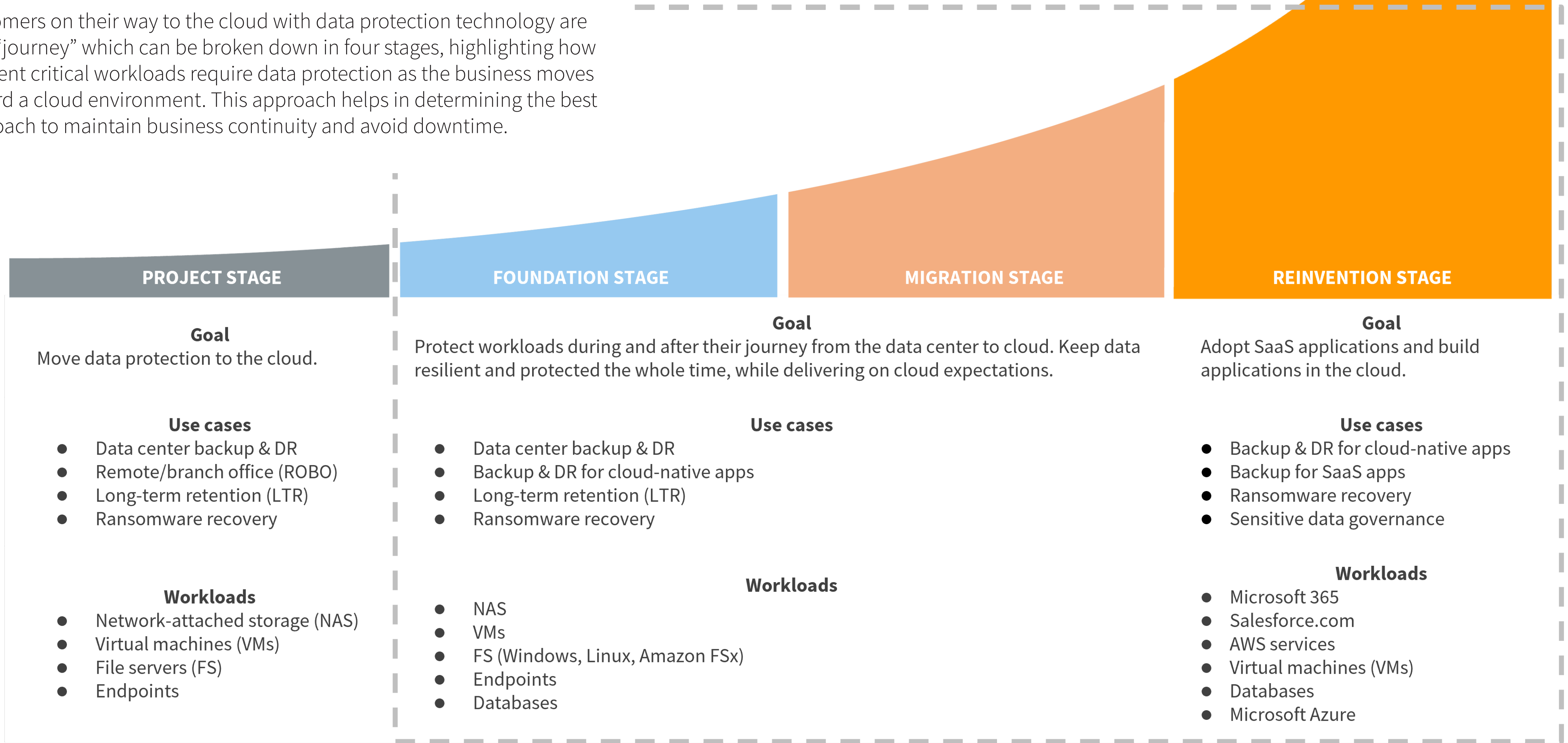
PAGE 20

A photograph of three IT professionals in a server room. One person is in the foreground, another is in the middle ground working on a laptop, and a third is in the background near server racks. The scene is dimly lit with a strong red glow from the server equipment. The text is overlaid on the left side of the image.

Downtime is a business problem—not just an IT problem—for which organizations have a low tolerance...especially in the cloud.

The Journey to the Cloud

Customers on their way to the cloud with data protection technology are on a “journey” which can be broken down in four stages, highlighting how different critical workloads require data protection as the business moves toward a cloud environment. This approach helps in determining the best approach to maintain business continuity and avoid downtime.



Most Concerning Impacts of Application Downtime

Organizations report that downtime has significant impact. Among the most visible are the direct operational efficiency consequences of an outage on IT, with 1 in 5 citing the diversion of resources from other business-critical projects as the most concerning impact. Effects more obvious to the bottom line are evident. While IT is directly affected by and responsible for downtime, it's really the whole business that suffers.

“1 in 5 cite the diversion of resources from other business-critical projects as the most concerning impact.”

| Most concerning impact of application downtime.



Mission-critical Applications Are on the Rise, especially in the Cloud

Data and applications run the business, but not every application is equally important. Organizations report that 1 in 3 applications are essential to the business, which in turn means more stringent SLAs.

The prevalence of public cloud services for hosting vital workloads is evident in the fact that the average organization says 58% of their mission-critical applications run in a cloud environment spanning public cloud infrastructure or in SaaS environments.

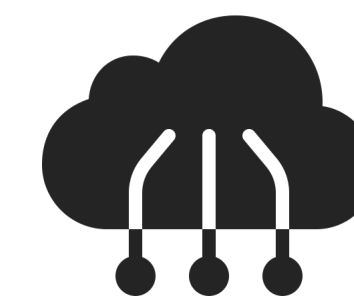
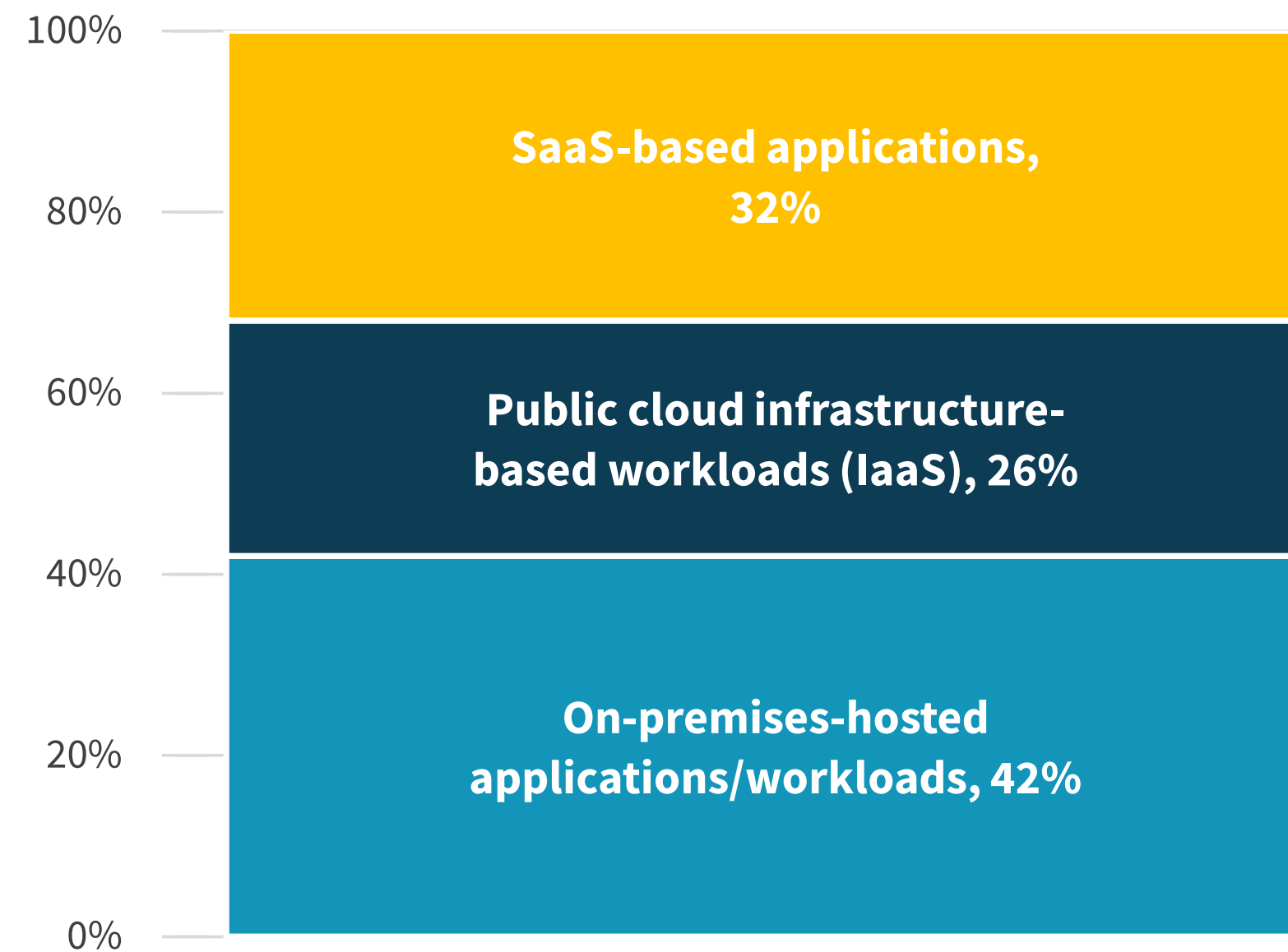
This leads to a number of challenges for the data protection infrastructure: Can the solutions in place credibly deliver mission-critical SLAs for applications running on public cloud infrastructure or in SaaS environments?



33%

of production applications are mission-critical.

| Percentage of “mission-critical ” applications/workloads currently operated/run in each environment.



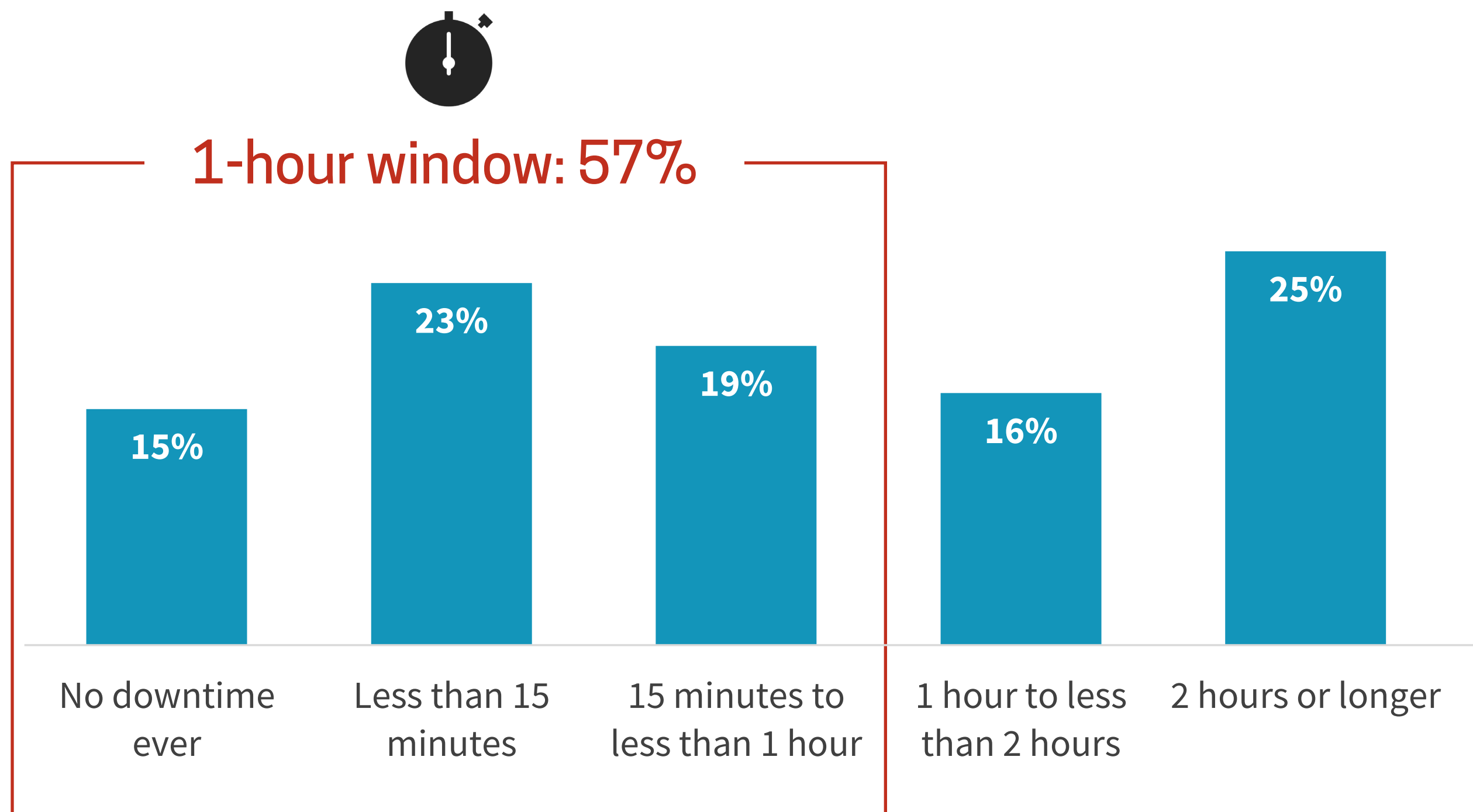
58%

of their mission-critical applications run in a cloud environment spanning public cloud infrastructure or in SaaS environments.

Most Can't Handle More than an Hour of Downtime for Mission-critical Applications

Time flies when systems are down or data is unavailable. The “one-hour window” is the crucial time objective in which mission-critical systems must be back up and running for the majority (57%) of organizations. It is also worth noting that 15% can tolerate no downtime for their mission-critical applications. Looking at all organizations collectively, the estimated mean for acceptable downtime for mission-critical applications is 2 hours, meaning that solutions that are deployed for recovery or failover must meet stringent requirements in a timely manner.

| Amount of downtime mission-critical applications/workloads tolerate before making the decision to “failover/recover” to a BC/DR secondary site.

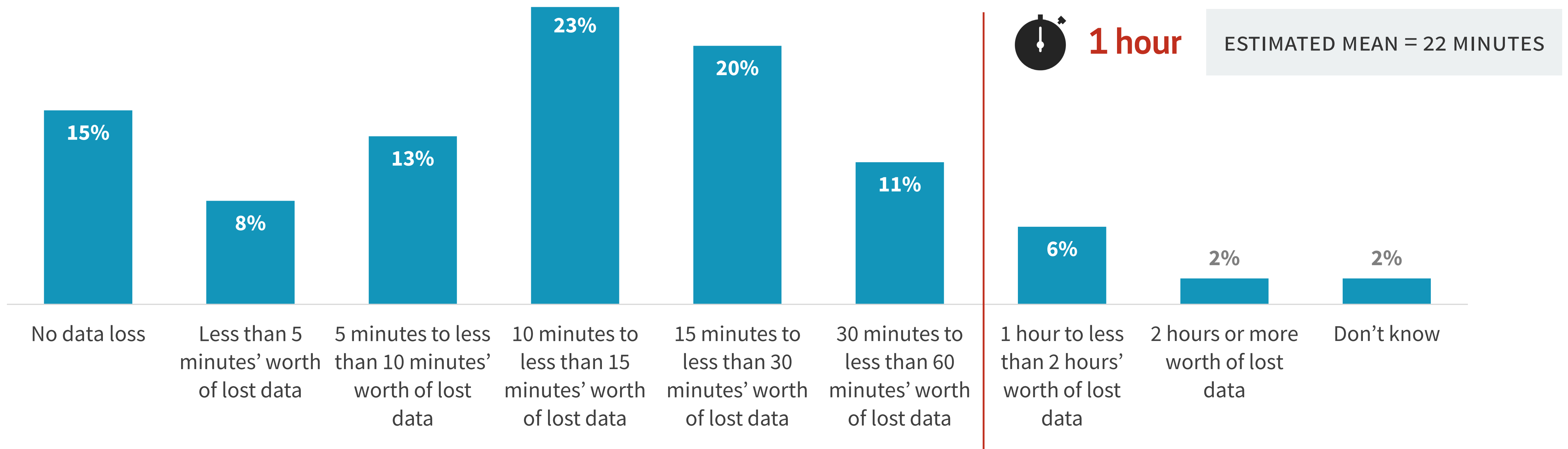


“ The ‘one-hour window’ is the crucial time objective in which mission-critical systems must be back up and running for the majority (57%) of organizations.”

Mission-critical Data Loss Tolerance Is (Understandably) Low

Mission-critical data loss tolerance is, not surprisingly, low. Indeed, 90% of respondents reported their organization could not withstand in excess of an hour's worth of lost data before experiencing significant business impact, equating to an estimated mean RPO of 22 minutes. It is worth noting that 15% of organizations actually report objectives of no data loss at all, which means putting in place availability technologies and highly redundant infrastructure and solutions that support this objective.

| Amount of mission-critical data that can be lost without significant impact to the business.



**Data protection and BC/DR processes
are becoming increasingly intertwined
with the cloud.**



Cloud Adoption Is Ubiquitous and Extent of Usage Continues to Grow

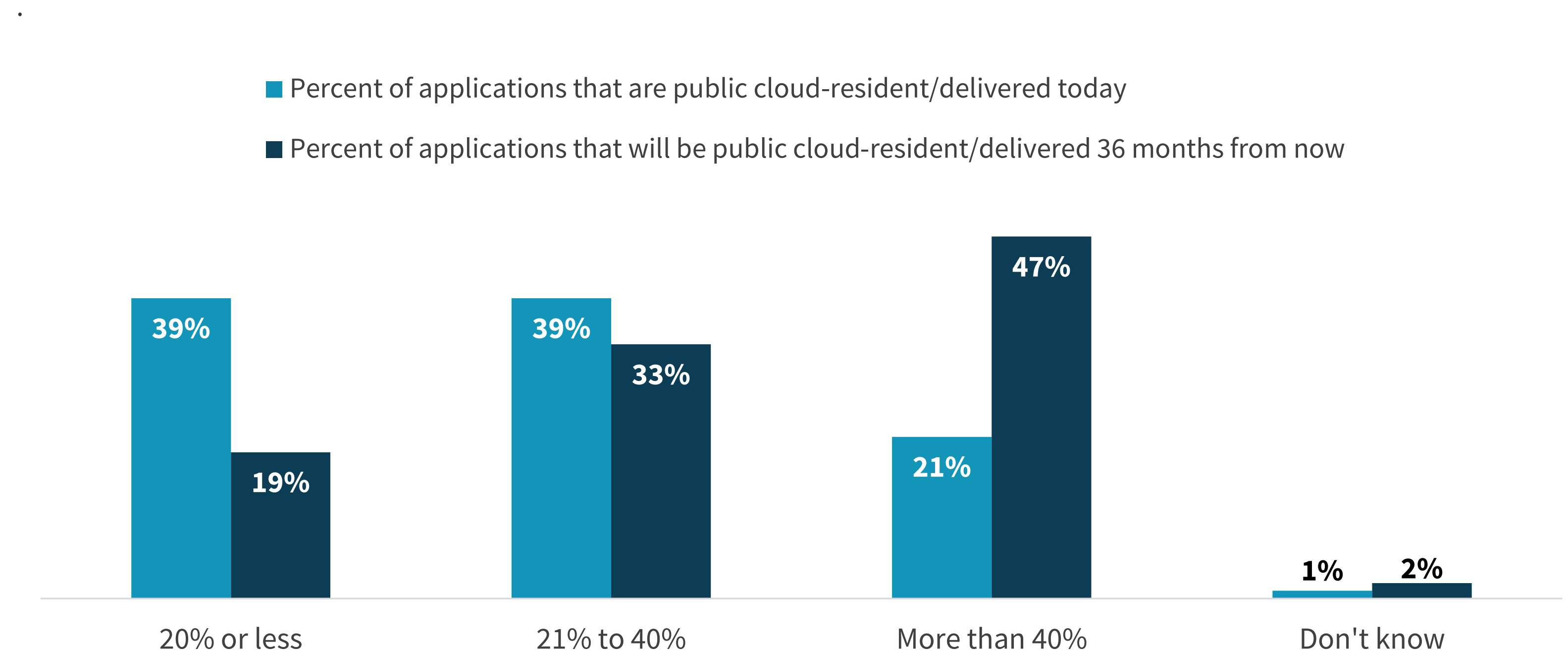
The market trends are very clear: Cloud adoption is continuing at an accelerated pace. As more applications shift to a cloud infrastructure, the need to adjust data protection processes will only increase whether for IaaS or SaaS. This ties directly to the stages of foundation and migration outlined in the model on page 5.



94%

currently use public cloud services.

| Amount of applications that are public cloud-resident/delivered.

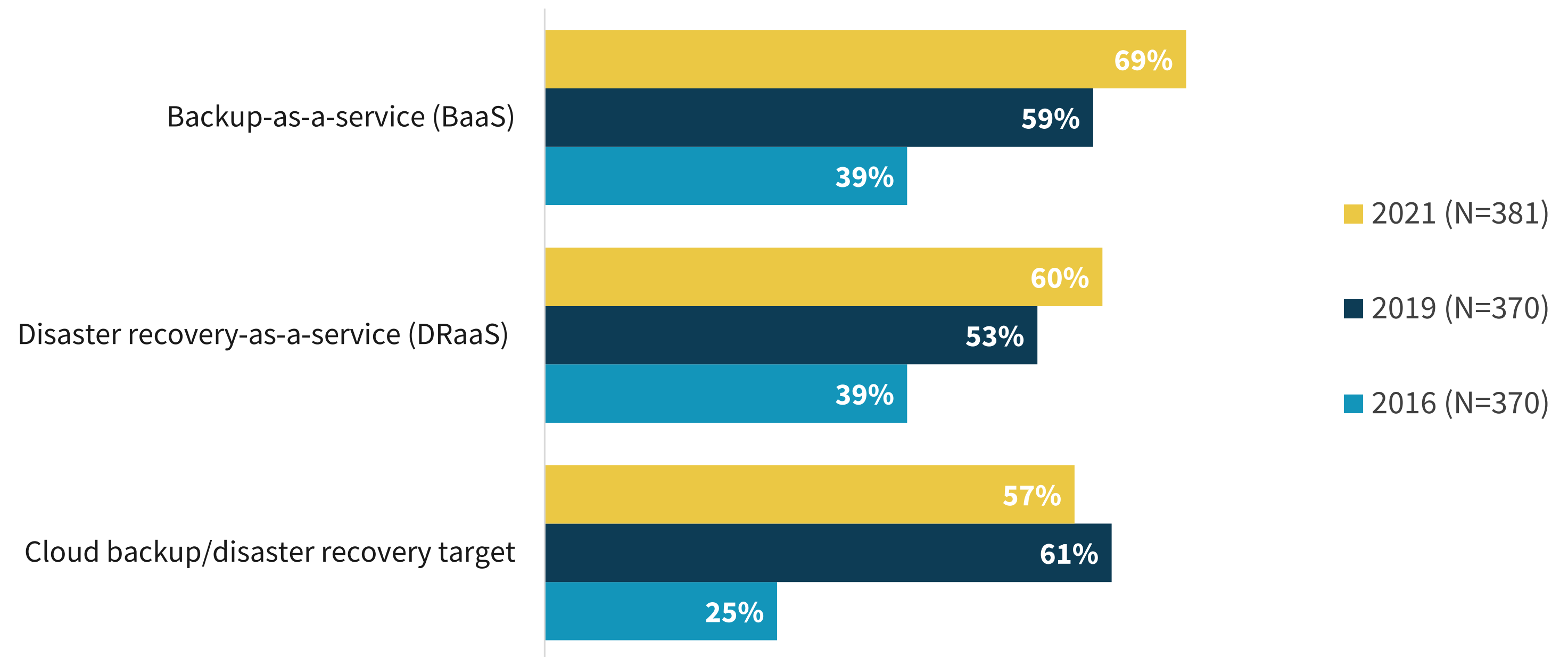


Usage of Cloud Data Protection Is The New Norm

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. This is a good example of the market evolving into the migration stage highlighted in the journey to the cloud model.

“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.



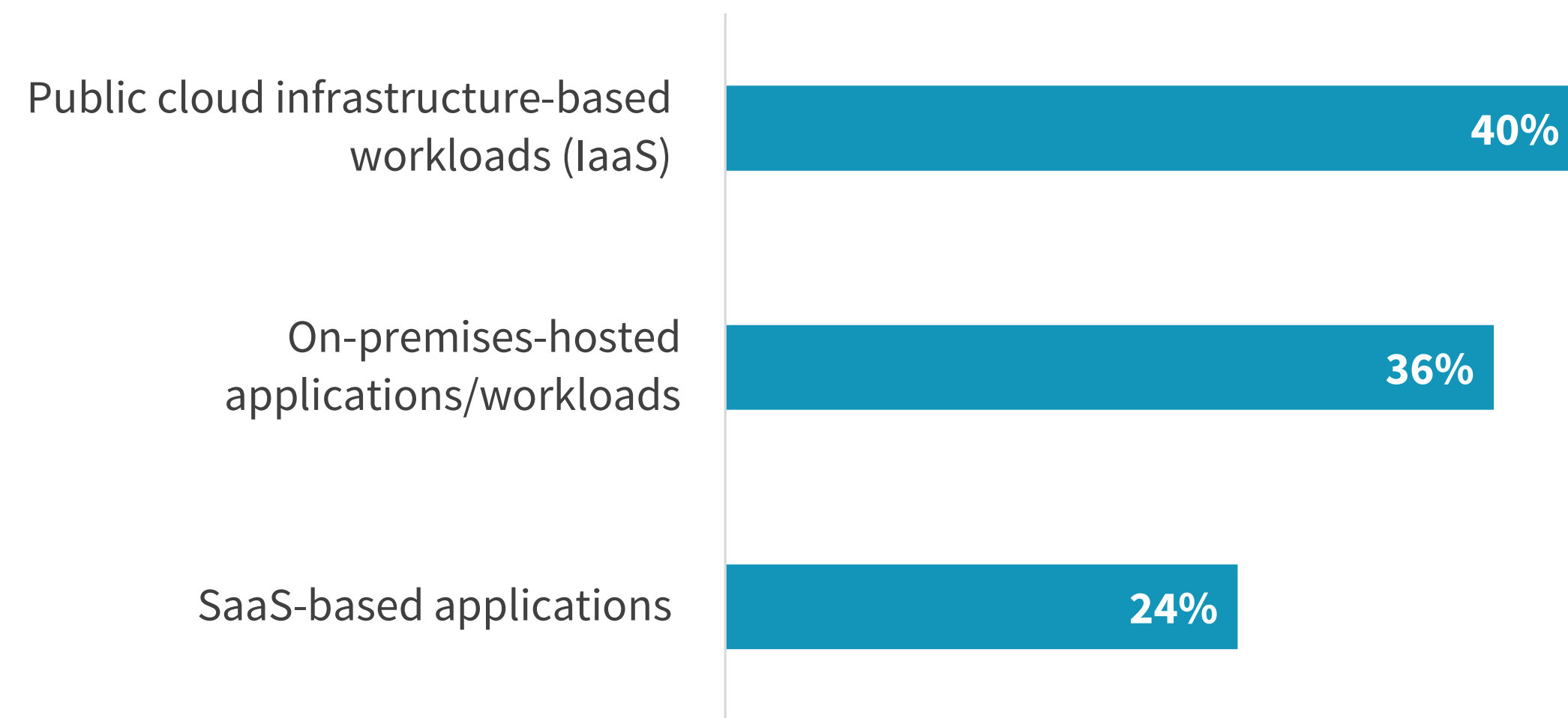
Confidence Matters...and Favors Cloud

Confidence, or perceived confidence, is a major influencer in buying decisions, and this is especially true when it comes to data and application recoverability. And while on-premises applications tend to have better recovery times, 40% of organizations state they have the highest level of confidence in public cloud infrastructure applications when it comes to meeting recovery SLAs. This is a likely reason why more organizations are moving to cloud environments (e.g., IaaS and SaaS workloads) to support recovery from incidents like ransomware, disasters, and accidental deletion.

This also raises the question of what will happen with on-premises applications if the general availability and recoverability sentiment keeps favoring cloud platforms.

The reinvention stage highlights the importance of data protection for virtual machines (VMs) hosted in the cloud. Very different philosophies are at play based on ESG’s research, leading to a potential for confusion. These different philosophies can also cause complexity at scale, with geographically distributed data or multiple business units for example.

| Application model in which organizations have the highest level of confidence in meeting recovery SLAs.

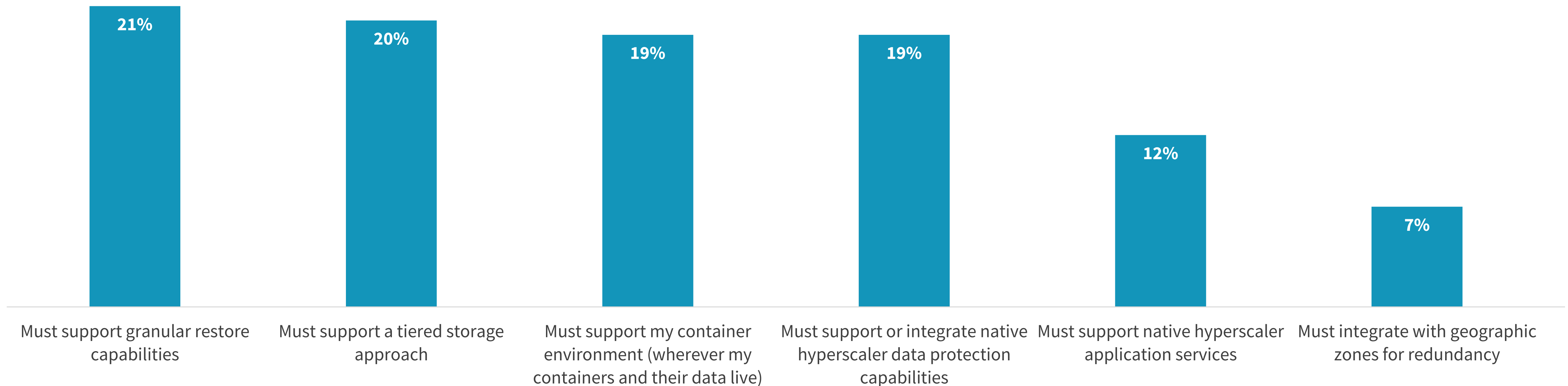


When protecting data stored within virtual machines (VMs) running on public cloud infrastructure, **45% said they leverage built-in data protection mechanisms (e.g., snapshots) within the same infrastructure cloud service (e.g., AWS).**

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. 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 notable since it might offer challenges for vendors that will need to integrate deeply with each hyperscaler in order to deliver a consistent set of features and experiences across cloud environments. This corresponds to the migration/reinvention stages of Druva's journey to cloud data protection. The highlighted capabilities exemplify organizations' needs to not only support "lift and shift" workloads and cloud-native workloads, but also modern workloads, like containers, to future proof cloud data protection and lower costs with tiered storage for long-term retention.

| Most important characteristic for hyperscaler data protection solutions.





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

Many Ways to Lose SaaS Application Data, Starting with Relying on SaaS Application Vendors

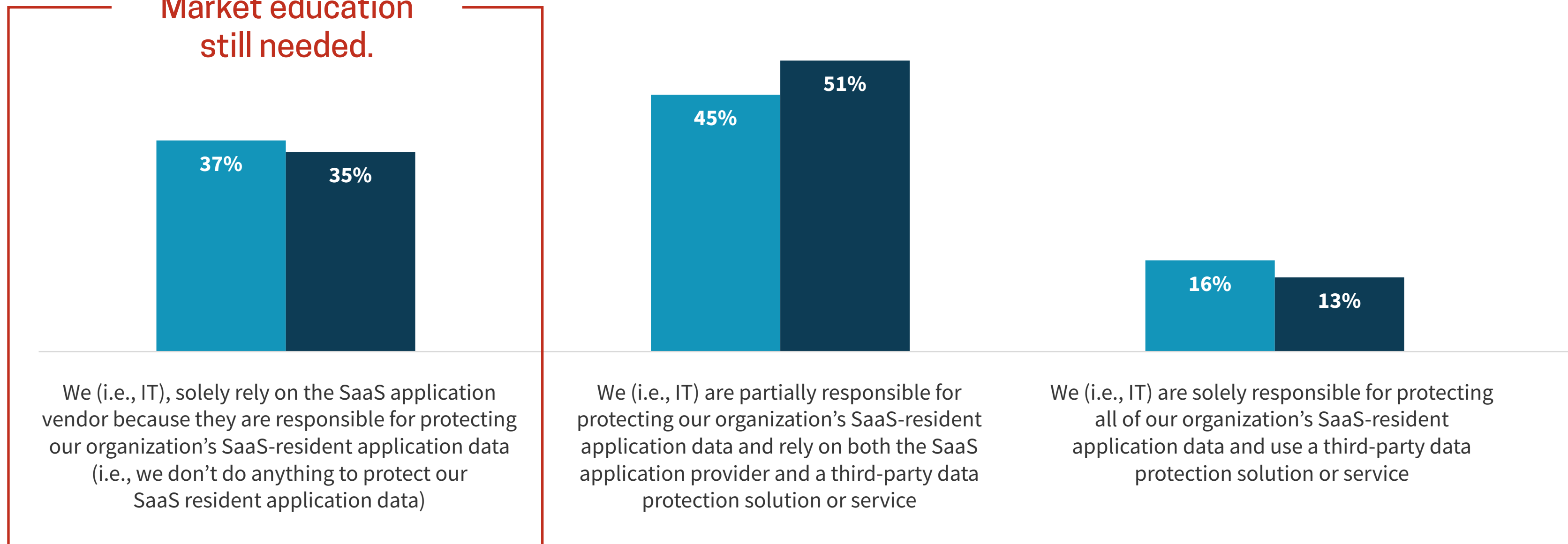
In the stage of reinvention, a key characteristic highlighted by Druva is the adoption of SaaS applications and the creation of applications in the cloud. In this context, it is important to remember that organizations are **always** responsible for their data and its recovery, so solely relying on SaaS application 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 SLAs many organizations need. It can be argued that it is a shared responsibility between IT and the SaaS application 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.

■ 2019 (N=347) ■ 2021 (N=344)



“It is important to remember that organizations are always responsible for their data and its recovery, so solely relying on SaaS application vendors is a major mistake.”

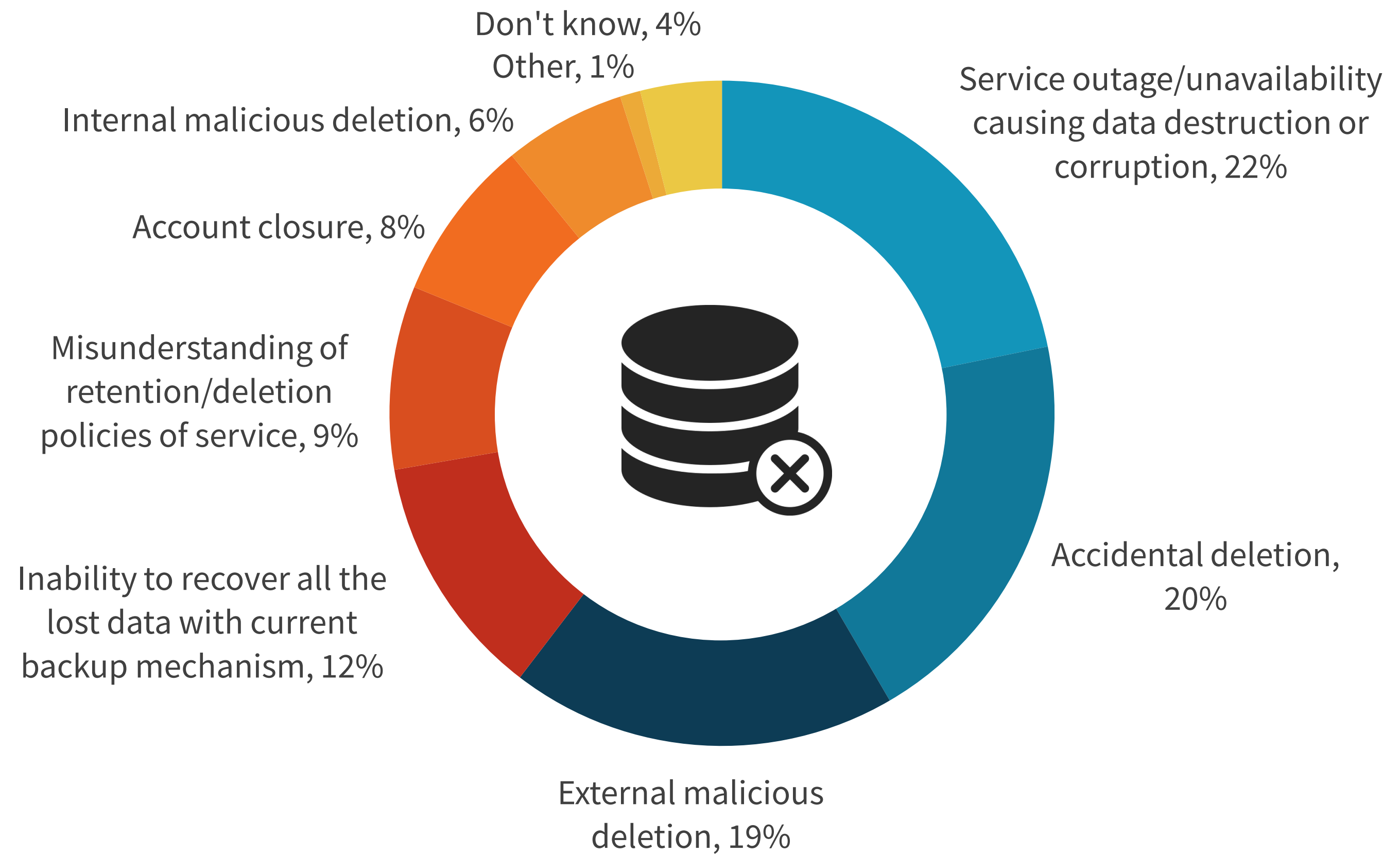
Various Causes of SaaS Application Data Loss

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—one-quarter being malicious external (19%) or internal (6%) deletion.

These risk levels are incompatible with supporting a mission-critical environment, **which is what SaaS applications have become over time.**

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.

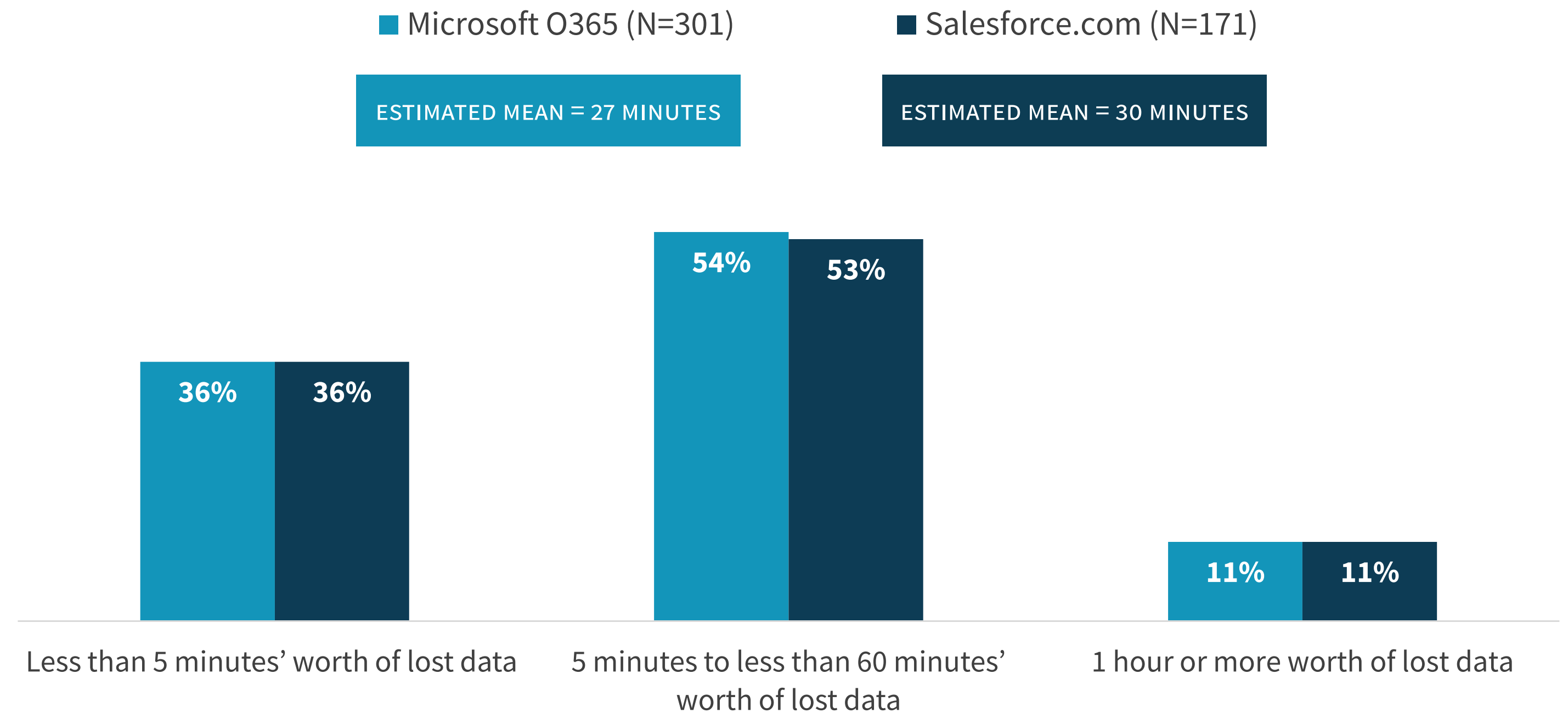


SaaS Recovery Point Objective (RPO) Tolerance

SaaS workloads have become critical in many organizations, and for this reason, organizations have high Recovery Point Objective (RPO) expectations for these cloud-based applications. It is important to distinguish that availability of the service itself and what the provider does for their own backup purposes should not be conflated with the need and responsibility for organizations to perform their own backups to ensure the recoverability of their data. Microsoft 365 and Salesforce.com top the list of most stringent SLAs, with more than one-third of these users reporting RPOs of less than five minutes' worth of lost data. These RPO requirements are not achievable with native Microsoft 365 or Salesforce.com backup offerings, highlighting the need for third-party offerings instead.

“ Microsoft 365 and Salesforce.com top the list of most stringent SLAs, with more than one-third of these users reporting RPOs of less than five minutes' worth of lost data. ”

| Amount of acceptable data loss for different SaaS applications.



Microsoft 365 Recoverability Slowly Improving Overall, though 100% Still Seems Elusive for Many

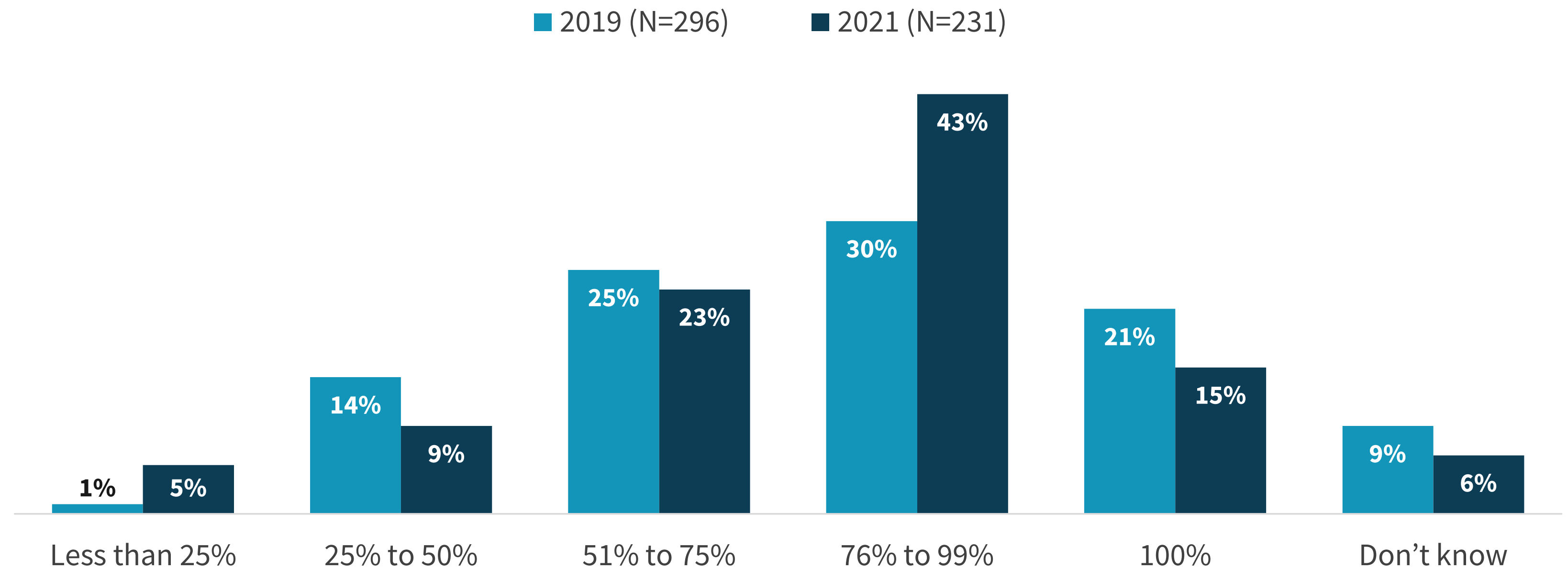
Microsoft 365 is one of the most visible SaaS tools across all market segments and industries. Many critical communications and documents reside within this service, yet organizations are not achieving the success rates one would expect for a mission-critical environment (i.e., 100%). As a matter of fact, while ESG has seen progress overall in terms of Microsoft 365 data recoveries, fewer organizations actually reported a 100% success rate compared with 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 have had to recover Microsoft 365 data.

| Microsoft 365 data recovery success rate.

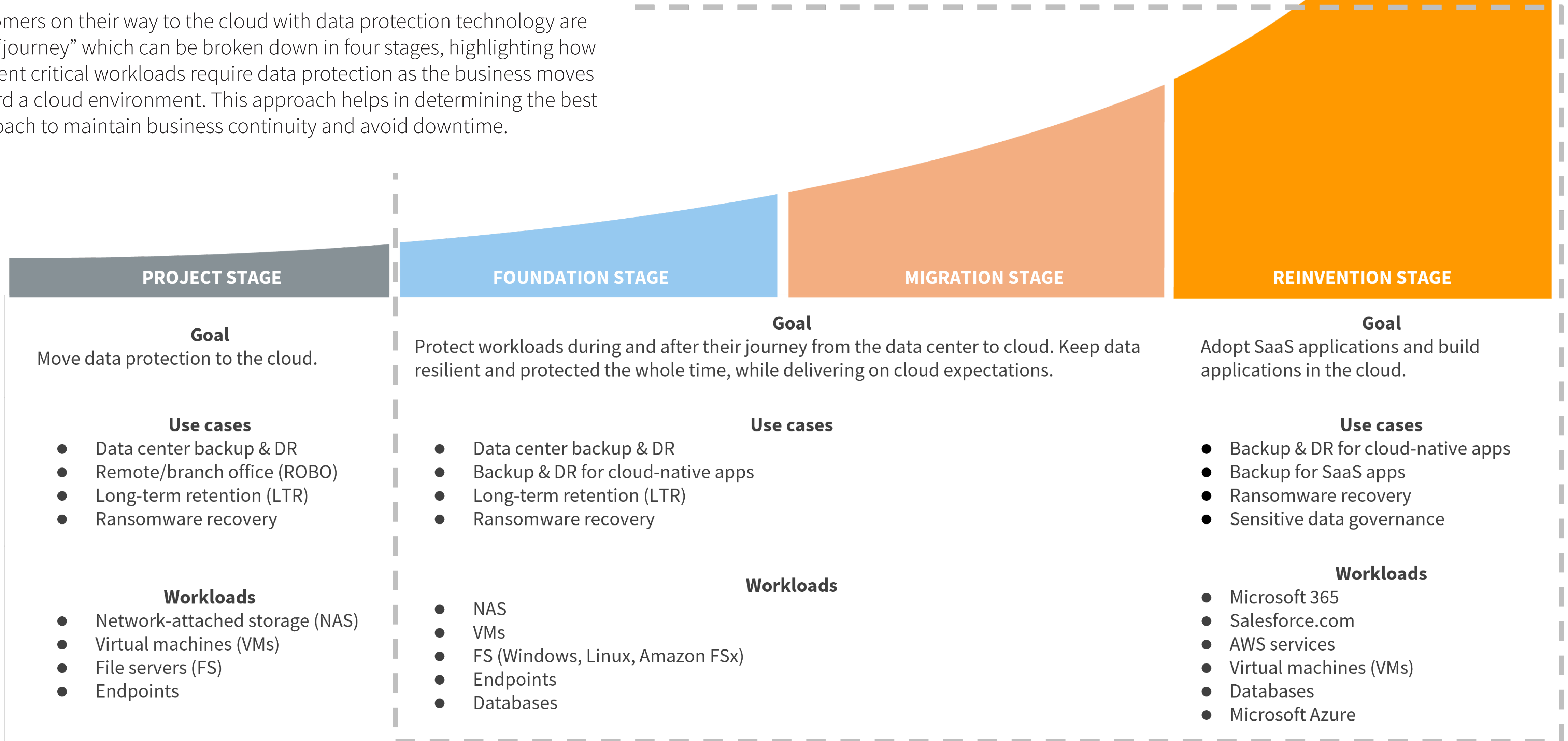


An aerial view of a city skyline at dusk or dawn, with a warm orange and yellow glow. Overlaid on the city are several glowing blue digital network structures, consisting of interconnected nodes and lines, resembling a data mesh or cloud architecture. A prominent blue line connects a central point to several other points across the city. A small red horizontal bar is located above the text.

**Druva and AWS:
Protecting your cloud workloads
for business success.**

The Journey to the Cloud

Customers on their way to the cloud with data protection technology are on a “journey” which can be broken down in four stages, highlighting how different critical workloads require data protection as the business moves toward a cloud environment. This approach helps in determining the best approach to maintain business continuity and avoid downtime.





Druva and AWS, Driving the Evolution of Cloud Data Protection

Druva offers a cloud-native SaaS platform, built on AWS, to protect all aspects of your cloud infrastructure including lift-and-shift, cloud-native, and SaaS applications. Druva and AWS provide the security, cost efficiency, and unified experience you expect at every stage of your cloud journey. Druva and AWS innovate together to bring customers a resilient data protection solution based on best practices and the latest cloud technologies.

Together, Druva and AWS are driving the evolution of cloud data protection. To learn more, watch this webinar to discover how Katz Media Group, the largest media representation company in America, successfully executed their cloud transition with Druva and AWS by incrementally identifying and shifting new workloads to the cloud.

[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.



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, 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 TechTarget, 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 Client Relations at cr@esg-global.com.



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.

© 2021 TechTarget, Inc. All Rights Reserved.