Enterprise Strategy Group | Getting to the bigger truth.™

SaaS Data Protection: A Work in Progress

Christophe Bertrand, ESG Practice Director

AUGUST 2022

Research Objectives

Organizations are increasingly reliant on SaaS for many of their mission-critical applications and workflows. This means that a significant amount of business-critical data associated with these applications is now also cloud-resident. As a result, it is more important than ever that this data is available or at least recoverable. However, there is (still) a problematic misunderstanding about the responsibility for protecting SaaS data. While maintaining application uptime is the responsibility of individual SaaS providers, the onus for the availability and protection of data typically falls on IT organizations. This data protection gap exposes organizations to potential data loss, compliance and governance violations, and general operational risks.

In order to gain further insight into these trends, ESG surveyed 398 IT professionals at organizations in North America (US and Canada) personally familiar with and/or responsible for SaaS data protection technology decisions, specifically around those data protection and production technologies that may leverage cloud services as part of the solution.

THIS STUDY SOUGHT TO:

Determine key challenges organizations face deploying and leveraging data protection mechanisms for their SaaS environments.

Gain insights into key trends and requirements for successful high availability and data protection strategies for SaaS environments.

Understand the education and best practices gaps in protecting SaaS environments, with specific focus on key capabilities and data protection SLAs.

Gauge end-users' data protection knowledge and challenges for specific key SaaS environments.

BACK TO CONTENTS

KEY **FINDINGS**

CLICK TO FOLLOW

The SaaS Backup Disconnect Persists and Is Causing Data Loss

PAGE 4

SaaS Data Protection Presents Challenges but Offers Substantial Benefits

PAGE 8

Leading SaaS Applications Are Mission-critical, and so Are Their Data Protection SLAs

PAGE 12

SaaS Data Protection Is a Top Priority Overall and Budgets Will Increase

PAGE 16

The SaaS Backup Disconnect Persists and Is Causing Data Loss

> “Solely relying on the SaaS vendor **is not a viable strategy.”**

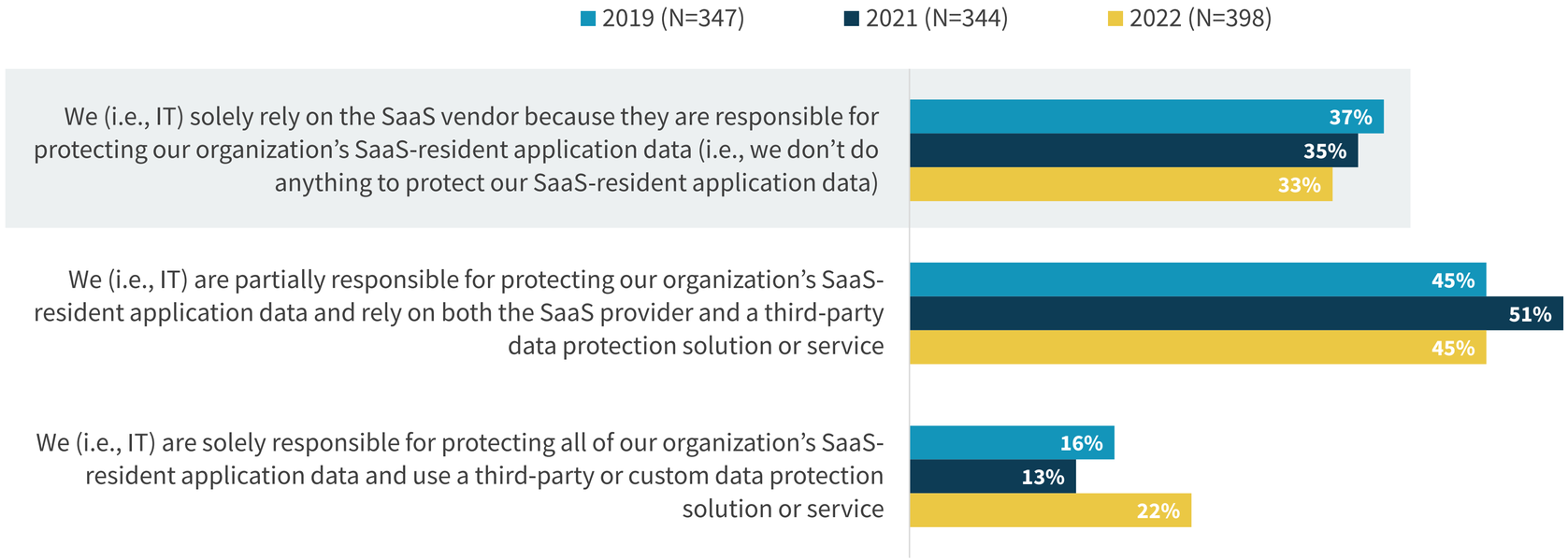
ONE-THIRD

of IT professionals are confused about their responsibility to protect SaaS data.

The SaaS Backup Disconnect Persists

One-third of IT professionals are confused about their responsibility to protect SaaS data. SaaS vendors will take many protective and availability measures to protect *their service,* but organizations are always responsible for their data. Solely relying on the SaaS vendor is not a viable strategy. In some cases, organizations may be able to recover some data with the help of the SaaS vendor, but unless expressly possible and contracted for, there is typically no built-in individualized enterprise-class data backup capability included in services. The disconnect is still significant overall and has not improved much in the past three years, which means that many organizations are still exposed and not doing anything about it. A majority of respondents accept partial responsibility for the protection of their data, commonly known as the “shared responsibility model.” This “middle of the road” position has remained relatively stable over the past three years; however, it only works if SLAs, roles, and responsibilities are clearly understood by each party. But there is a glimmer of hope: In 2022, more than one in five (22%) respondents understand their organization is solely responsible for protecting its own SaaS-resident data, up from 2019 and 2021.

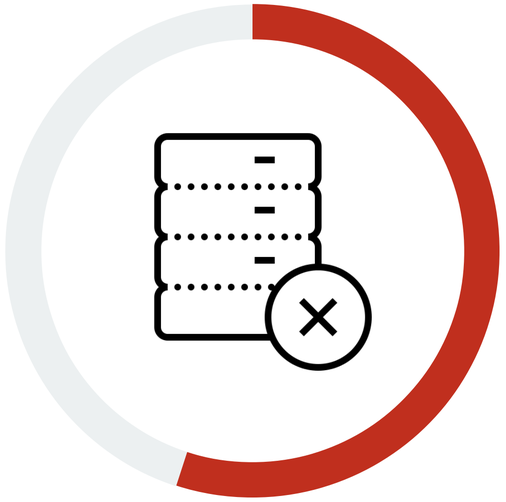
Approach to protecting SaaS-resident application data.



BACK TO CONTENTS

SaaS Applications Are Not Immune to Data Loss, Especially Those Relying on SaaS Providers

The problem with the data protection disconnect is that it can lead to data loss. As a matter of fact, a majority (53%) of organizations reported having lost SaaS-resident data in the last year. This should be a red flag for IT professionals! This propensity to lose SaaS data is even more pronounced among those who **solely rely on** the SaaS vendor, while those who report that they are fully responsible for their SaaS data protection are faring better. IT professionals should take this into account and immediately review their current policies and processes when it comes to SaaS data protection.



55%

Yes, we've experienced SaaS data losses/corruption in the last 12 months.

Percentage of organizations that have experienced data losses or corruption with any of the SaaS applications they use over the last year, based on approach to protecting SaaS-resident application data.

We don't do anything to protect our SaaS-resident application data.

59%

We (i.e., IT) are partially or solely responsible for protecting our organization's SaaS-resident application data.

50%

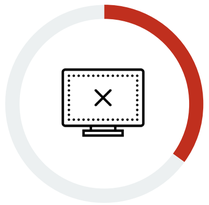
BACK TO CONTENTS

The Many Ways to Lose SaaS Data

Causes of data loss in SaaS applications are important to understand in order for IT professionals to mitigate the issue. More than a third (35%) of organizations report that the service itself is the primary cause of data loss or corruption, the most common issue cited. This is a key point to understand, especially since over a third of respondents rely on the service itself for data protection. This is not necessarily a new IT phenomenon; applications have always involuntarily participated in data corruption, including issues with software, operators, APIs, and more. Why would it be different with SaaS? This should justify taking measures such as acquiring a third-party data recovery or high availability solution.

There are many more ways to lose SaaS data, among which a salient one is related to malicious and voluntary data destruction, whether external with cyber-attacks or internal with malicious deletions by employees. Again, this alone should be more than enough to justify advanced data protection and recovery mechanisms. One can also see the impact of poorly understood SLAs, with data loss being credited to a misunderstanding of retention/deletion policies, and account closures (with closed account data being deleted by the SaaS vendor). Many recognize they need better (less deficient or insufficient) backup and recovery mechanisms, which is clearly an important step to understand to improve the data protection posture of an organization.

Most common causes of SaaS data loss.



35%
Service outage/ unavailability

34%
Malicious deletion from cyber-attack

33%
Accidental deletion

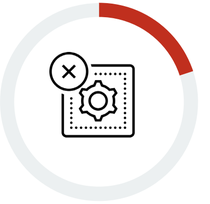
29%
Account closure

28%
Insufficient or deficient backup mechanism

26%
Our backup vendor does not support the specific SaaS application(s) for which we lost data

24%
Misunderstanding of retention/deletion policies of service

23%
Malicious deletion by employee



20%
Schema misconfiguration/ bad schema update

BACK TO CONTENTS

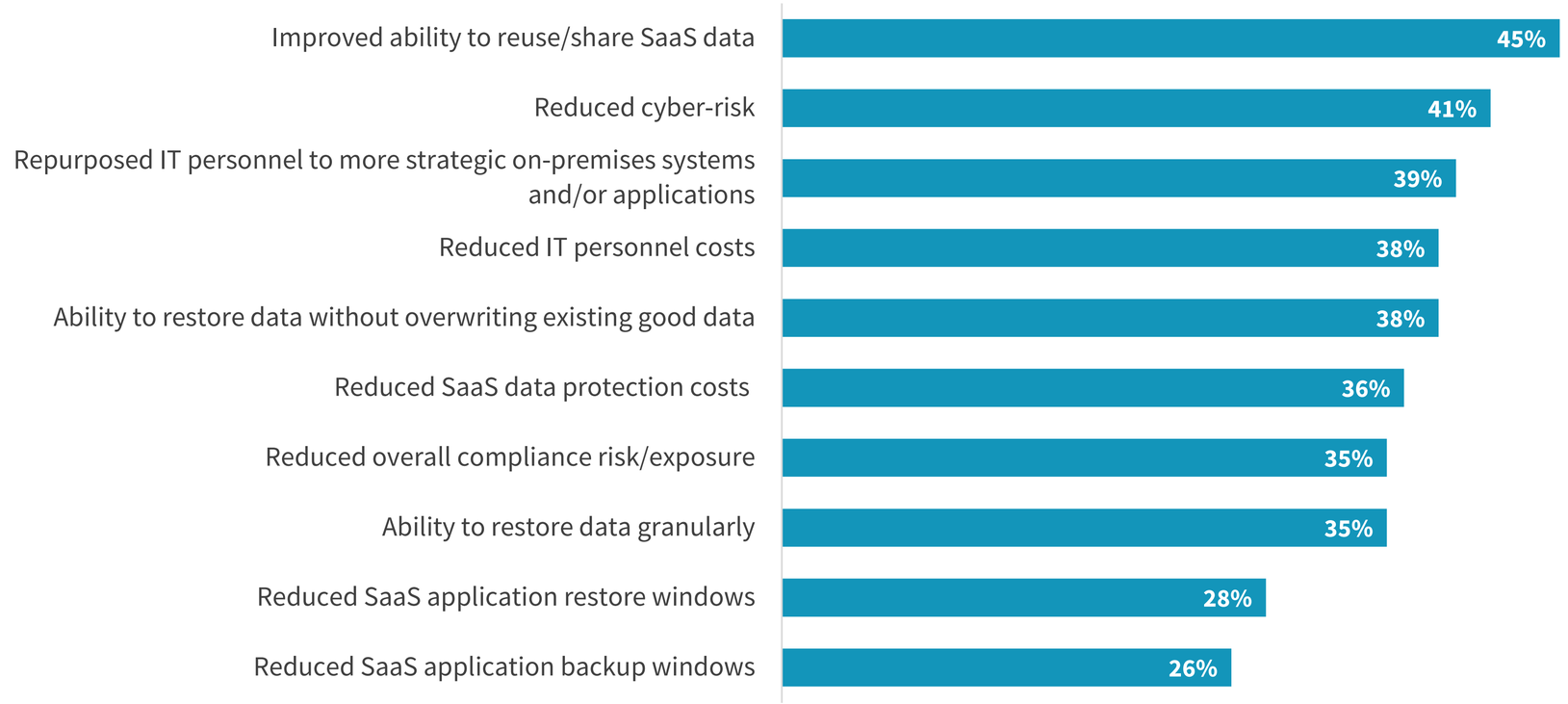
SaaS Data Protection Presents Challenges but Offers Substantial Benefits

“In line with other intelligent data management ESG research, **the ability to reuse or share SaaS data is the most common benefit realized.**”

SaaS Data Reuse/Portability Is a Key Backup Benefit

Many organizations are trying to effectively protect SaaS data in order to mitigate data loss. In doing so, they reported reaping a number of benefits that go far beyond traditional recovery. In line with other intelligent data management ESG research, the ability to reuse or share SaaS data is the most common benefit realized. This is a significant finding in that it confirms the evolving nature of data protection mechanisms, and signals to IT professionals and vendors that more than traditional data recovery is expected. This is also true of reduction in cyber-risk (or improved cyber-resilience posture). SaaS data is a target of cybercrime and needs to be protected accordingly. In addition, IT professionals attribute operational efficiencies, reduced costs, and improved compliance risk to their SaaS data protection efforts.

Benefits of using a solution to protect SaaS applications.



BACK TO CONTENTS

Challenges Abound in Protecting SaaS Environments

While organizations can realize many benefits by using SaaS data protection mechanisms, there are also obstacles to overcome. The fact that the applications are consumed as a service clearly does not make them immune to the newer challenges of cyber-resiliency and the common hurdles associated with data recoverability and compliance.

One set of major challenges lies in the complex topic of security and privacy. Data must be secure and privacy must be implemented in order to meet exacting compliance and governance standards. Not surprisingly, data loss is the second most common challenge among IT professionals as many likely realize that their SaaS backup solutions are just not cutting it. This may be related to the fact that nearly one-quarter of respondents believe that backup solutions aren't sufficiently integrated into SaaS applications and/or the deluge of SaaS data that has to be protected is a significant challenge. While other data recoverability and compliance challenges are mentioned, it is clear that SaaS environments are not immune to common, and historical, IT and data protection challenges.

Top 10 challenges experienced using a solution to protect SaaS applications.

31%
Security/privacy concerns

27%
Data loss concerns

24%
Backup solutions are not integrated into enough SaaS applications

24%
Volume of data to be protected

24%
Concern that IT staff would be giving up too much control to SaaS vendor

24%
Network connectivity and costs

24%
Recovery time concerns

23%
Technical support availability concerns

21%
Performance concerns during backups

20%
Number of SaaS platforms to be protected

For IT professionals, this means that the same best practices that apply to other workloads and associated data sets should apply to SaaS. Given the existing levels of data loss and disconnects identified, this may not be an easy task as organizations struggle to protect their current SaaS environments, especially with many disparate SaaS applications to be protected.

BACK TO CONTENTS

SaaS Data Protection ‘RFP’

Among the most important characteristics of data protection solutions for SaaS applications, security capabilities top the requirements list. This should not be surprising as organizations continue to struggle with cyber-attacks and ransomware, which are increasingly targeting SaaS environments. It is also significant to note that organizations need both speed and flexibility of recovery to support mission-critical processes increasingly found in SaaS applications (e.g., collaboration, CRM, etc.).

Overall, modern data protection requirements that could apply to other topologies are well-represented in the list of what could be considered high-focus capabilities. While the consumption of the application has changed, its data protection requirements are overall the same. After all, if it’s data that is important or critical to the business, so is its protection. However, SaaS applications are not run or owned by IT anymore, but rather by a service provider. This means less control and more reliance on APIs (when they exist). That’s why backup vendors can play a significant role.

In addition, there is one specific and important requirement that is worth highlighting:

The need to protect multiple SaaS applications, which is going to become more central over time as organizations become unable to handle many different backup solutions successfully.

Eventually, backup vendors will be expected to support most, if not all, “popular” SaaS applications (just like they did in the days of on-premises IT). This creates a potential challenge for both end-users and backup vendors: which applications, which APIs, and in what order of priority?

Key characteristics of solutions protecting SaaS applications.

32% Security capabilities

30% Speed of recovery

25% Flexible recovery options

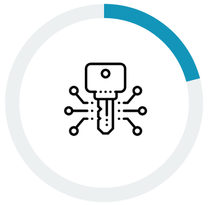
24% Quality of solution development

24% Flexibility in selecting a cloud repository vendor/service or locale

23% Data migration capabilities

22% Ability to recover to /fail over to another location in the cloud

22% Ransomware protection/detection



21% Protection of multiple SaaS applications or workloads

BACK TO CONTENTS

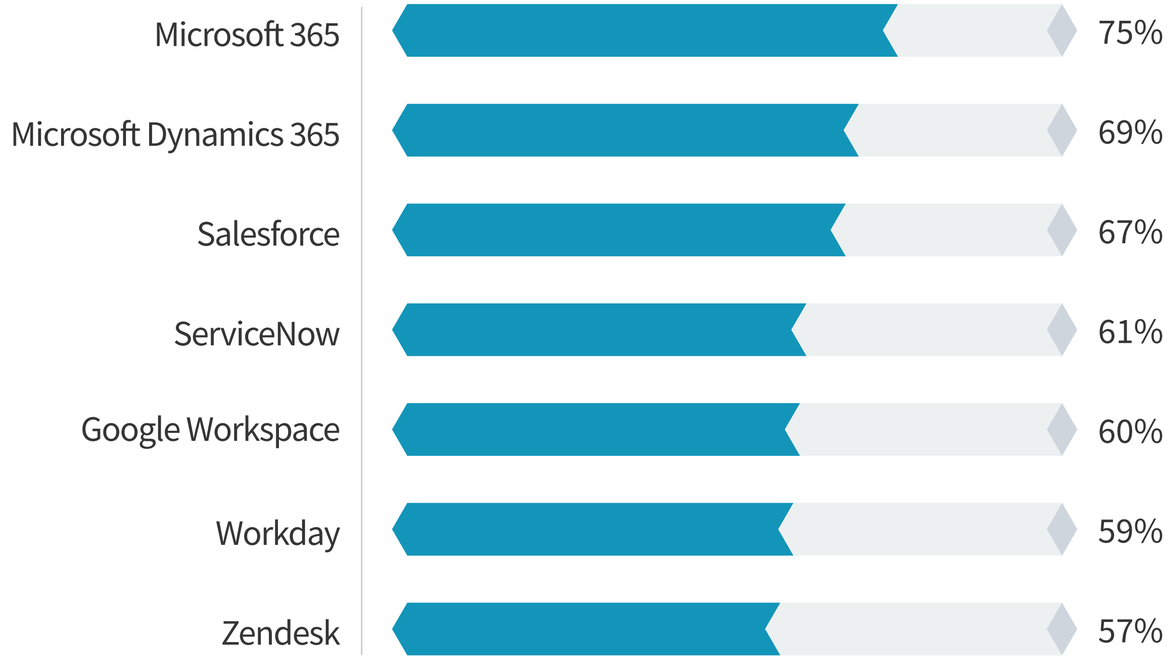
Leading SaaS Applications Are Mission-critical, and so Are Their Data Protection SLAs

“Overall, the research confirms that **the most widely used SaaS applications are mission-critical for most organizations.**”

Key SaaS Applications Are Mission-critical for Most

As traditional on-premises applications continue their move to the cloud, the emergence of ready-made replacements in the form of SaaS application has led to massive adoption across industries and functions. Many enterprises now heavily rely on SaaS applications for business-critical functions, making them mission-critical. This comes with many consequences from a service-level and data protection standpoint. While ideally these applications should always be up and running (though some outages are inevitable), their associated data sets should be protected accordingly (ideally, never lost or always recoverable). Overall, the research confirms that the most widely used SaaS applications are mission-critical for most organizations. This means that stringent SLAs or objectives should be identified from a data protection standpoint, and the appropriate solutions put in place to meet these requirements.

Percentage of organizations that consider certain SaaS applications mission-critical.

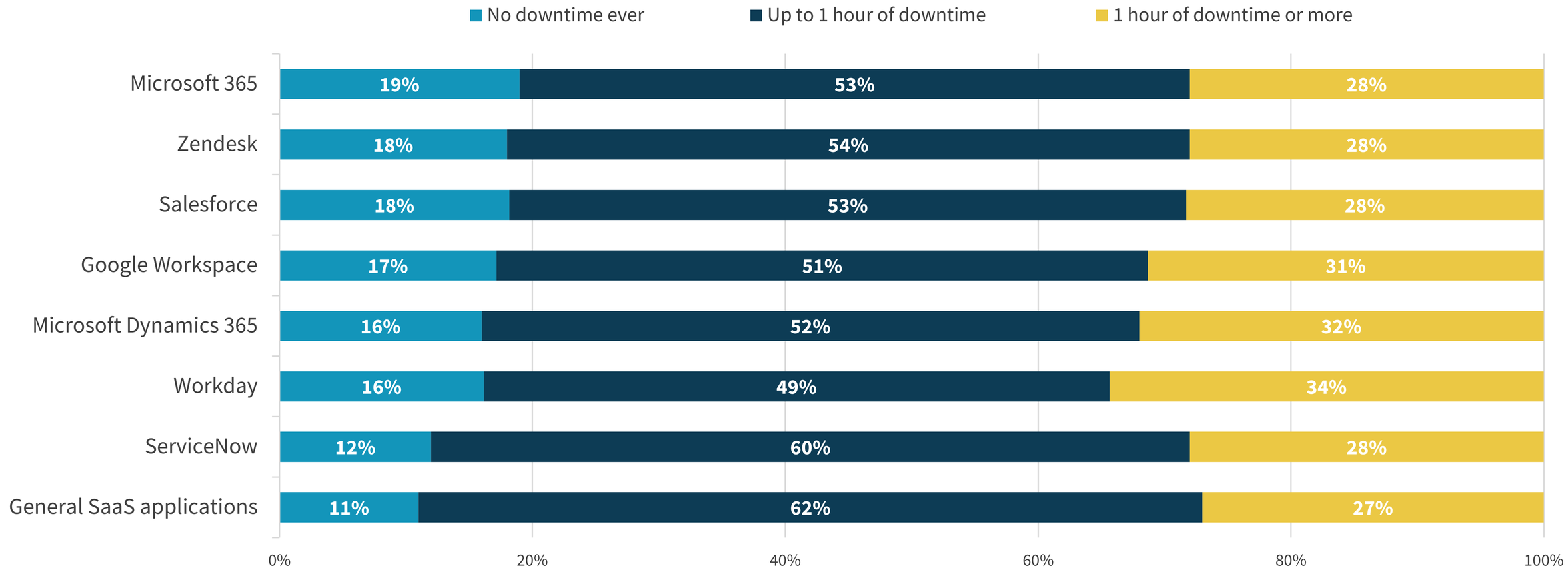


BACK TO CONTENTS

Stringent RTOs in Place for SaaS Environments Align with Mission-criticality of Services

IT professionals report having stringent recovery time objectives in place for their SaaS environments, including requirements for no downtime at all. Across the board, the vast majority of organizations expect their SaaS applications to be back up and running in under an hour. While there are variations by individual SaaS applications, these are stringent RTOs that are in line with other real-world SLA research ESG has conducted.

Downtime tolerance (RTO) for SaaS applications protected today.

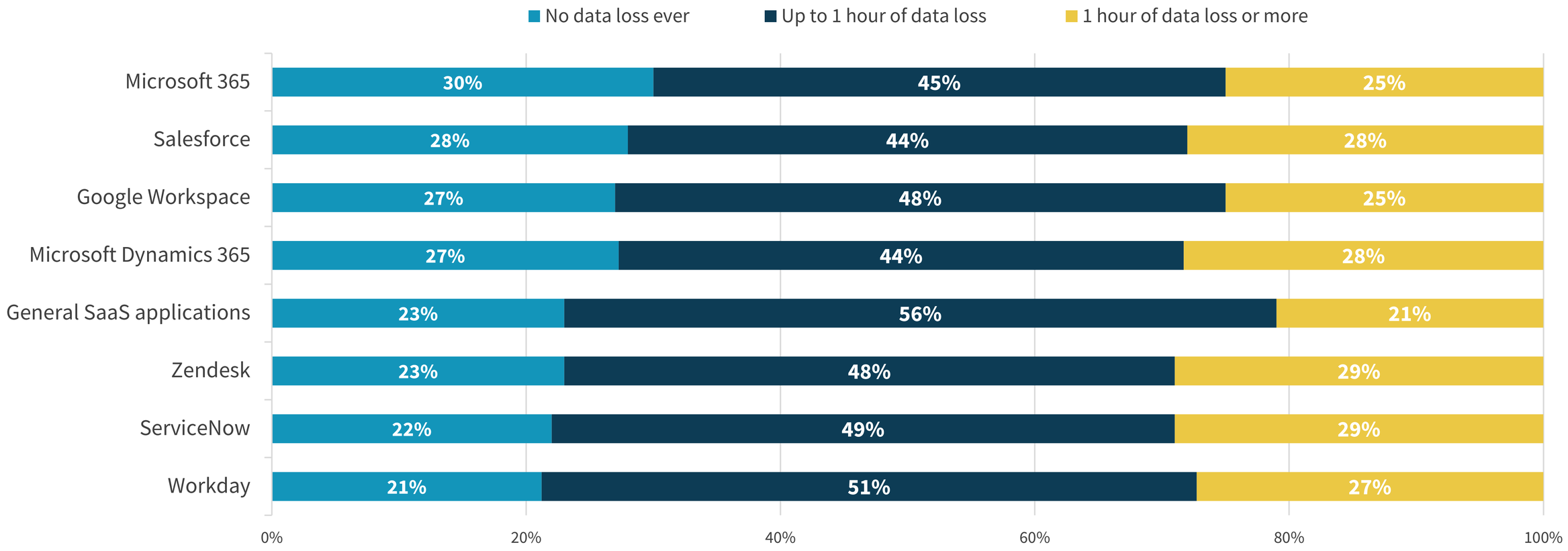


BACK TO CONTENTS

Little Tolerance for SaaS Data Loss

Data loss tolerance is very limited across the board for SaaS applications. Specifically, the requirements for no data loss at all are particularly stringent, with nearly one-third (30%) of organizations citing this as their RPO for Microsoft 365. Overall, at least 70% of organizations report wanting no more than 1 hour of data loss across all SaaS applications. These uptime and data loss requirements are laudable, but it's questionable whether they are realistic to achieve on the basis of previously stated data loss reports (i.e., 53% report losing SaaS data). There is also a likely conflation of service availability versus uptime versus data loss. The fact that the SaaS service is up does not mean someone is not deleting data. It could even be happening automatically at scale with poorly designed and automated scripts or unsuccessful data integrations that wipe out "good" data.

Data loss tolerance (RPO) for SaaS applications protected today.



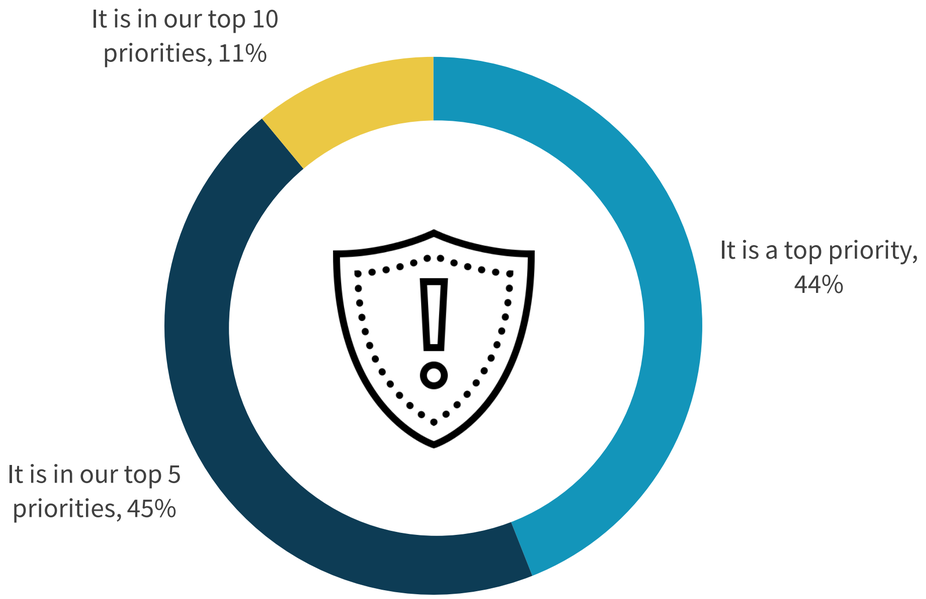
BACK TO CONTENTS

SaaS Data Protection Is a Top Priority Overall and Budgets Will Increase

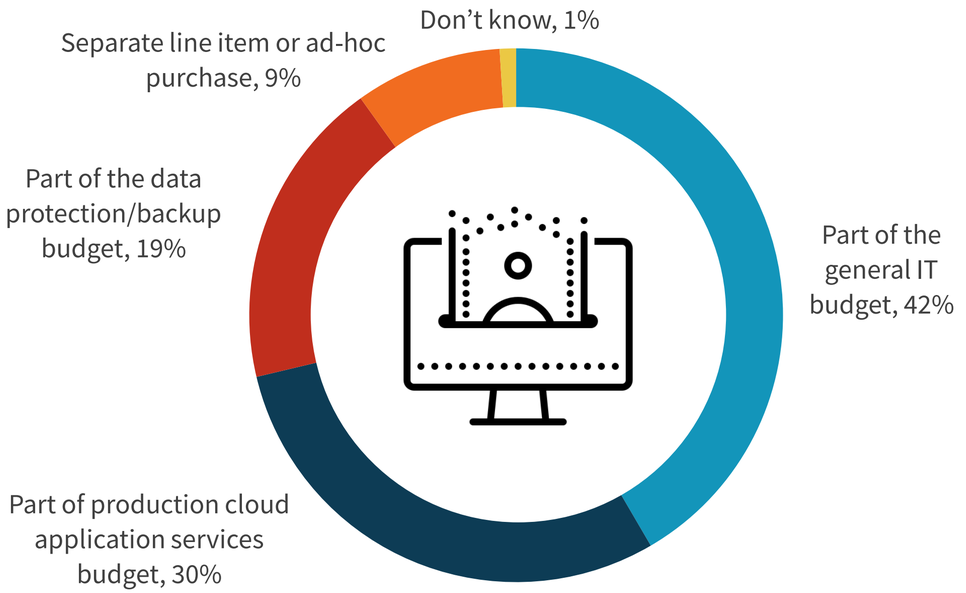
Protecting SaaS Applications Is a Key Priority for IT, with a Diverse Group of Funding Providers

As organizations continue to struggle with data loss and overall need a better understanding of the shared responsibility model, the good news is that IT organizations are prioritizing efforts to improve, and the requisite investments are going to be made to protect SaaS applications in the next 12 to 24 months. Indeed, protecting SaaS applications is a top IT priority for 44% of organizations, and another 45% report it is in their top five priorities. The funding to support these improvements is not necessarily a one-time investment: Building a resilient SaaS data protection infrastructure for all mission-critical data and applications takes time. Protecting SaaS applications is not funded exclusively out of the backup budget. Multiple IT personas are in the mix, reflecting the changing nature of the infrastructure, and it should be noted that the internal SaaS owners are key in funding and influencing purchasing decisions for the backup and recovery components. Vendors in the data protection space should take note: This is a big problem to solve with IT budget that is earmarked to solve it, so backup and recovery vendors should expand their capabilities and coverage of SaaS applications, which will benefit end-users.

Priority level for protecting SaaS apps and data.



Funding data protection solutions for SaaS-based applications.

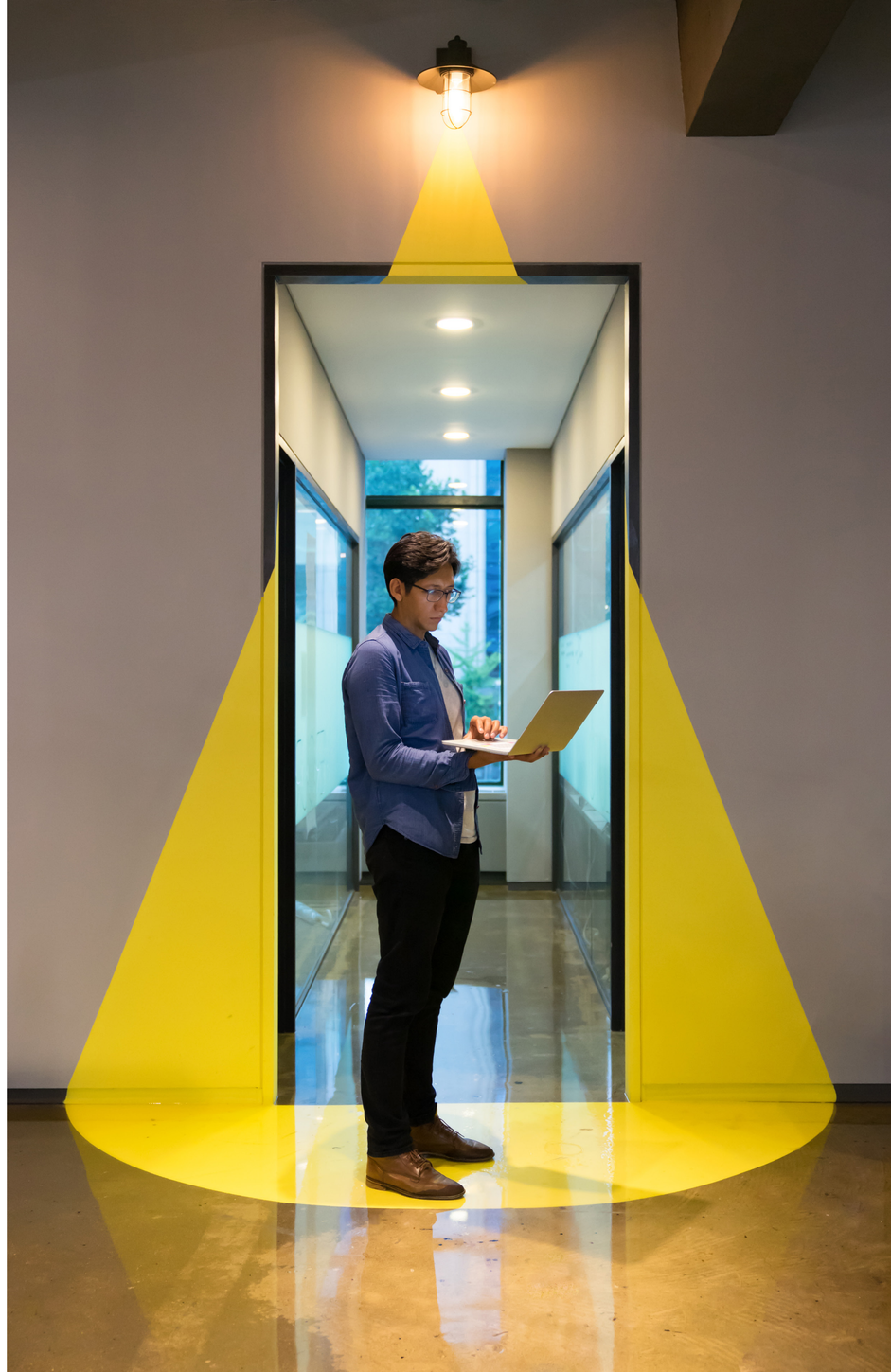


BACK TO CONTENTS

COHESITY

Cohesity radically simplifies data management. We make it easy to protect, manage, and derive value from data — across the data center, edge, and cloud. We offer a full suite of services consolidated on one multi cloud data platform: backup and recovery, disaster recovery, file and object services, dev/test, and data compliance, security, and analytics — reducing complexity and eliminating mass data fragmentation. Cohesity can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

LEARN MORE



ABOUT ESG

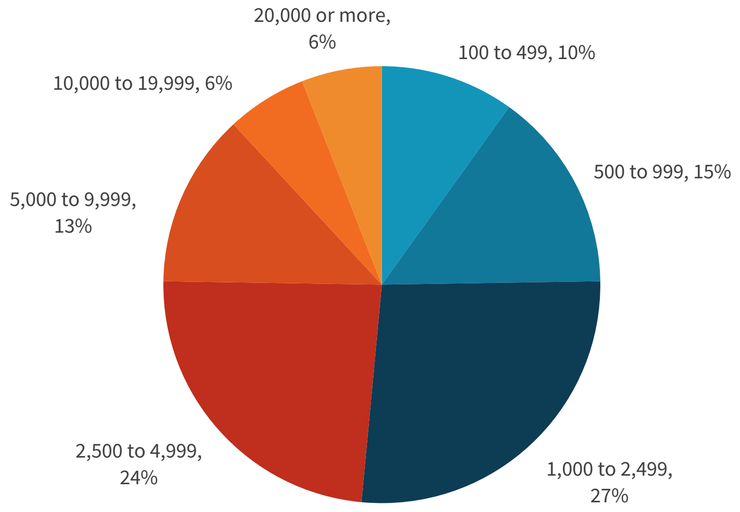
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology

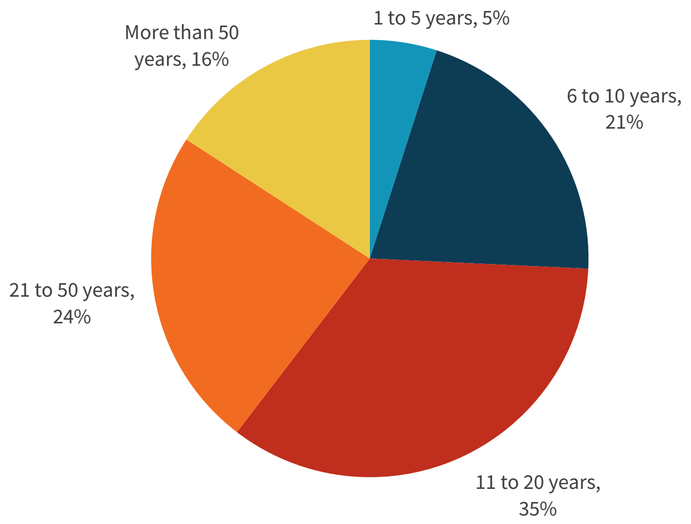
To gather data for this report, ESG conducted a comprehensive online survey of IT professionals from private- and public-sector organizations in North America (United States and Canada) between June 10, 2022 and June 22, 2022. To qualify for this survey, respondents were required to be IT professionals personally familiar with and/or responsible for SaaS 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 SaaS applications and/or protecting the associated 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 398 IT professionals.

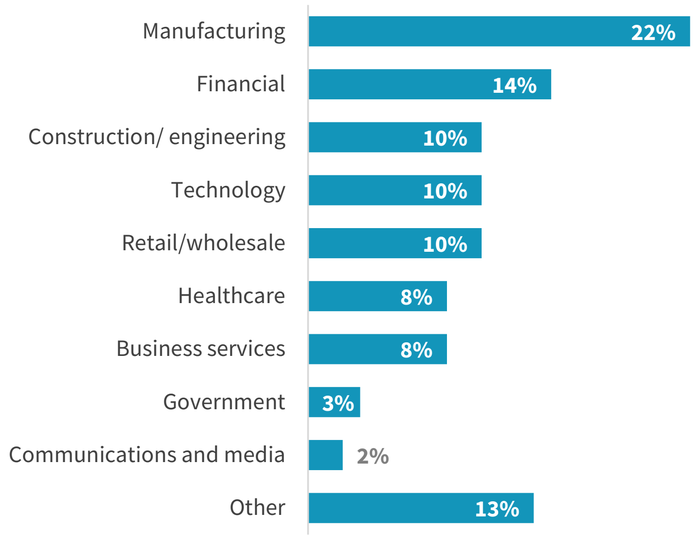
RESPONDENTS BY NUMBER OF EMPLOYEES



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.