SPANNING
A Kaseya COMPANY

REPORT

THE STATE OF SAAS BACKUP AND RECOVERY REPORT 2025:

NAVIGATING THE FUTURE OF CLOUD DATA PROTECTION

OBJECTIVE

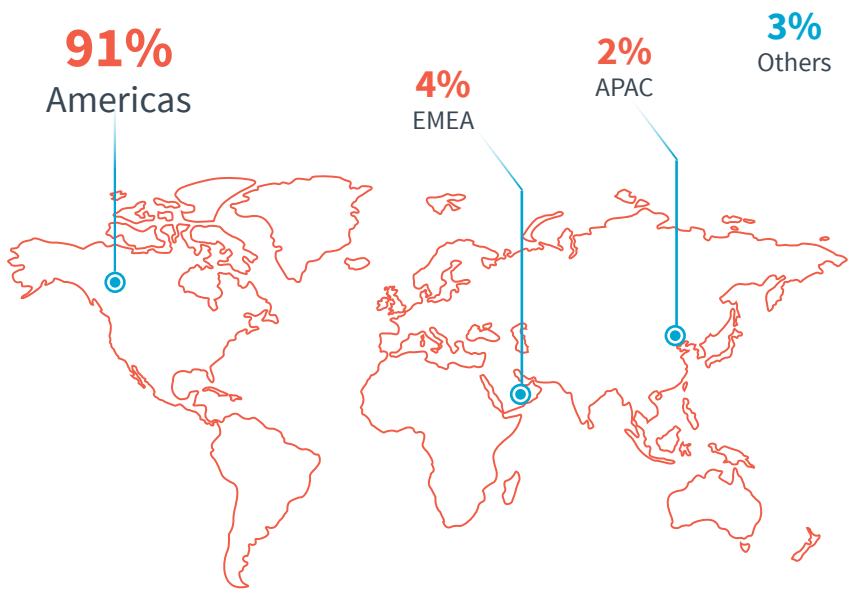
Through September and October 2024, more than 3,000 IT professionals from around the world participated in an online survey aimed at uncovering key trends, challenges and opportunities shaping the landscape of SaaS backup and cloud data protection. The result is a wealth of data and insights to offer actionable intelligence for IT professionals, business leaders and industry experts to inform strategic decision-making and strengthen operational and organizational resilience.

DEMOGRAPHICS

The survey gathered responses from a diverse group of 3,051 IT professionals, security experts and administrators worldwide. Respondents spanned a wide range of industries and company sizes, offering a comprehensive view of global data protection trends.

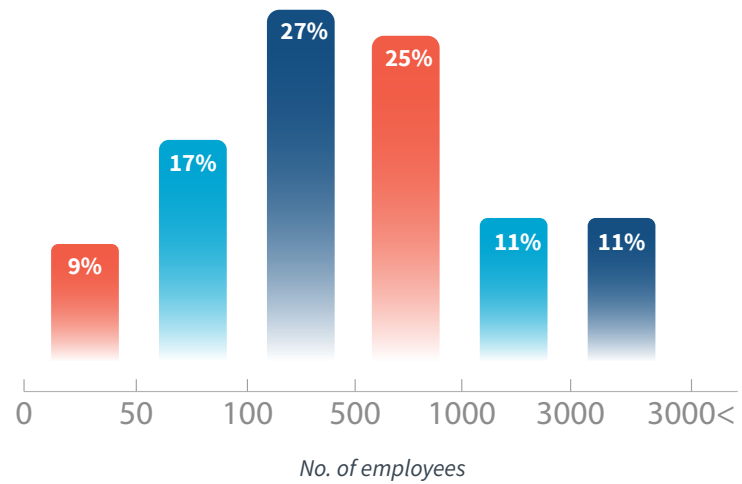
GEOGRAPHIC REPRESENTATION

The majority of respondents are from the **Americas (91%)**, reflecting strong engagement from North and South America. Contributions from **EMEA (4%), APAC (2%)** and **other regions (3%)** provide valuable perspectives from organizations operating in varied economy and regulatory environments.



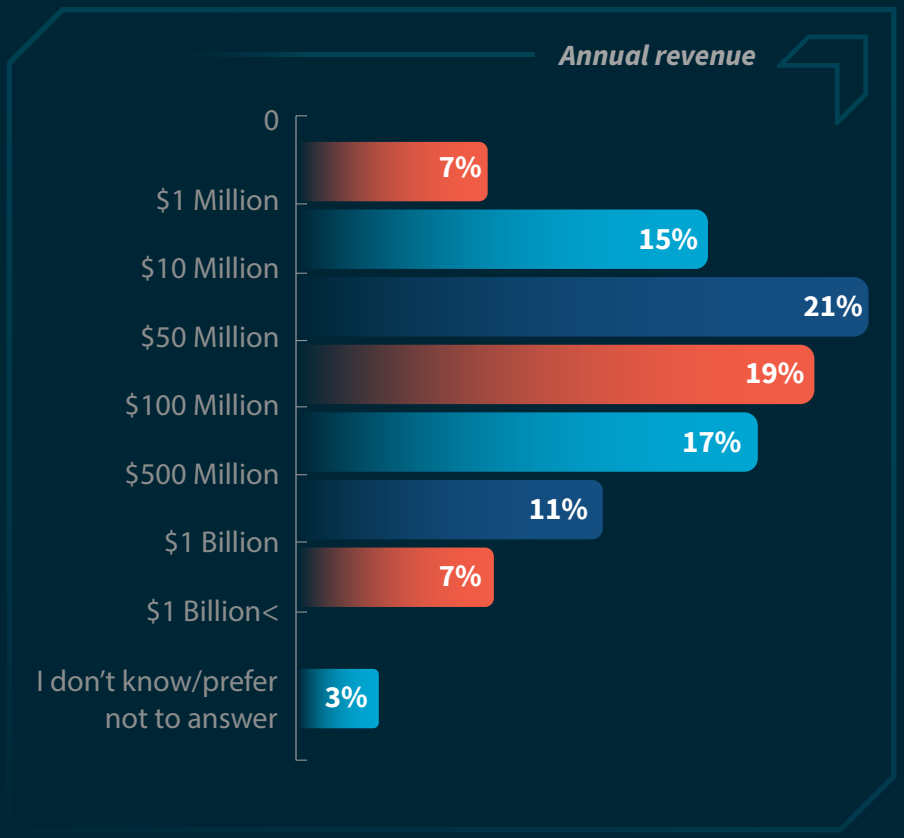
COMPANY SIZE

Participating organizations ranged in size from fewer than 50 employees to more than 3,000 employees. The majority of respondents (52%) represented organizations with 101 to 1,000 employees, showcasing trends within organizations balancing scalability with cost efficiency. Of the 3,051 respondents, 53% represent small and medium-sized businesses (SMBs) with 500 or fewer employees, and 47% represent large organizations or enterprises with 501 or more employees.



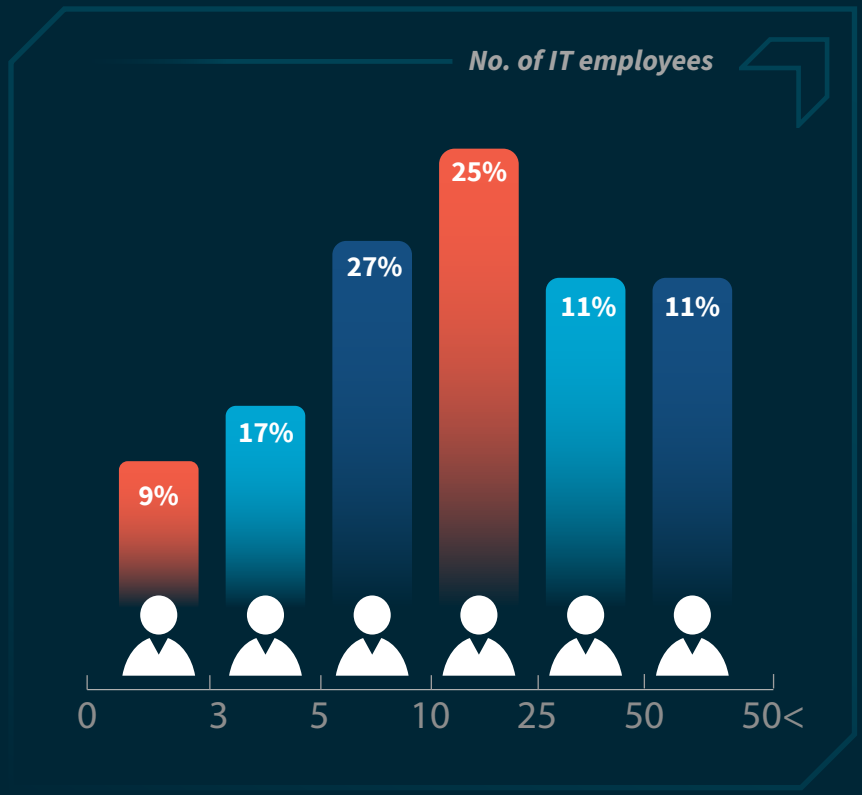
REVENUE DISTRIBUTION

Respondents represented organizations with annual revenues ranging from under $1M to over $1B, with the majority of participants (57%) representing organizations with $10M to $500M in annual revenue.



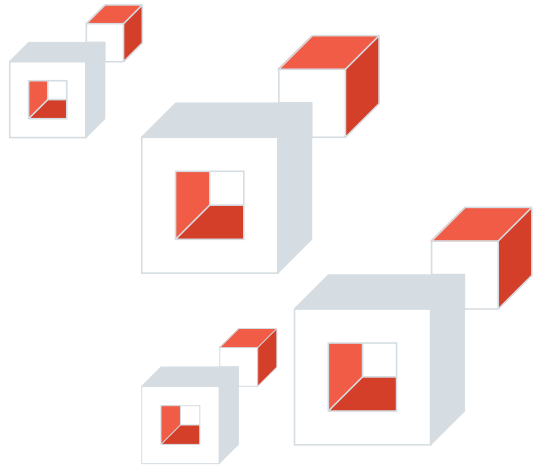
IT TEAM COMPOSITION

The majority of respondents employ more than 10 IT staff members, highlighting the vital importance of IT roles in managing data protection, cloud migration, and backup and disaster recovery strategies in today's increasingly digital business environments.



This diversity of respondents ensures a rich dataset reflecting the realities of modern data protection practices.

INDUSTRY TRENDS SHAPING DATA PROTECTION STRATEGIES

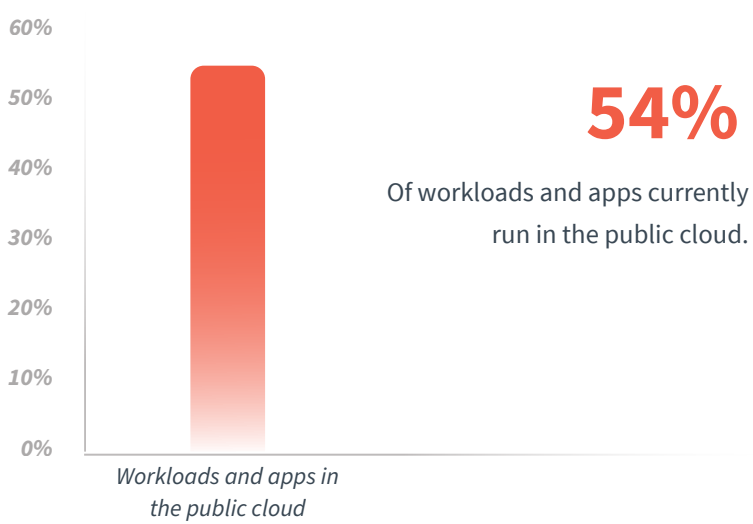


As businesses delve into new technologies, their data protection strategies evolve in turn. To better understand the shifts in today's technology landscape, we explored how organizations deliver workloads and how they back up, manage and recover their data. Key trends shaping data protection include:

CLOUD WORKLOADS ON THE RISE

The use of public cloud computing platforms has revolutionized modern business for the scalability, flexibility and wide range of use cases they offer. More than 50% of workloads and applications run in public cloud environments, and this figure is projected to grow to 60% over the next two years.

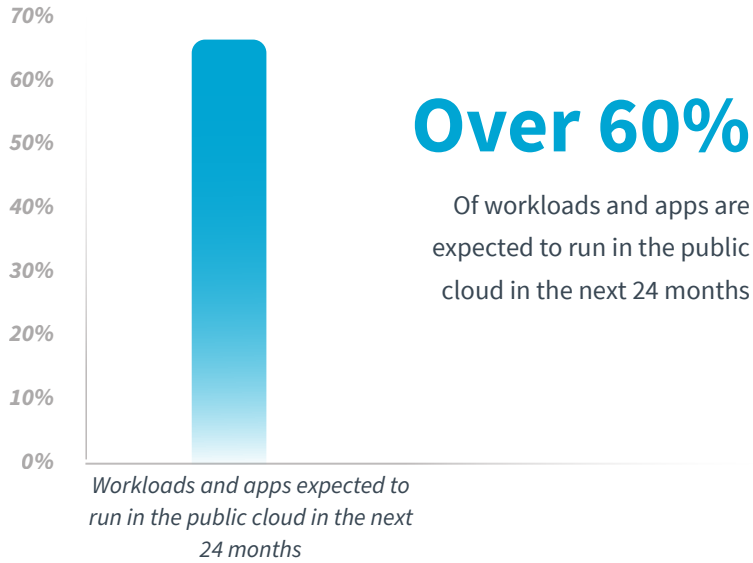
What percentage of your workloads and applications currently run in the public cloud (be sure to include IaaS, PaaS, SaaS in your calculation)?



54%

Of workloads and apps currently run in the public cloud.

In the next 24 months, what percentage of your workloads and applications do you anticipate running in the public cloud (be sure to include IaaS, PaaS, SaaS in your calculation) ?



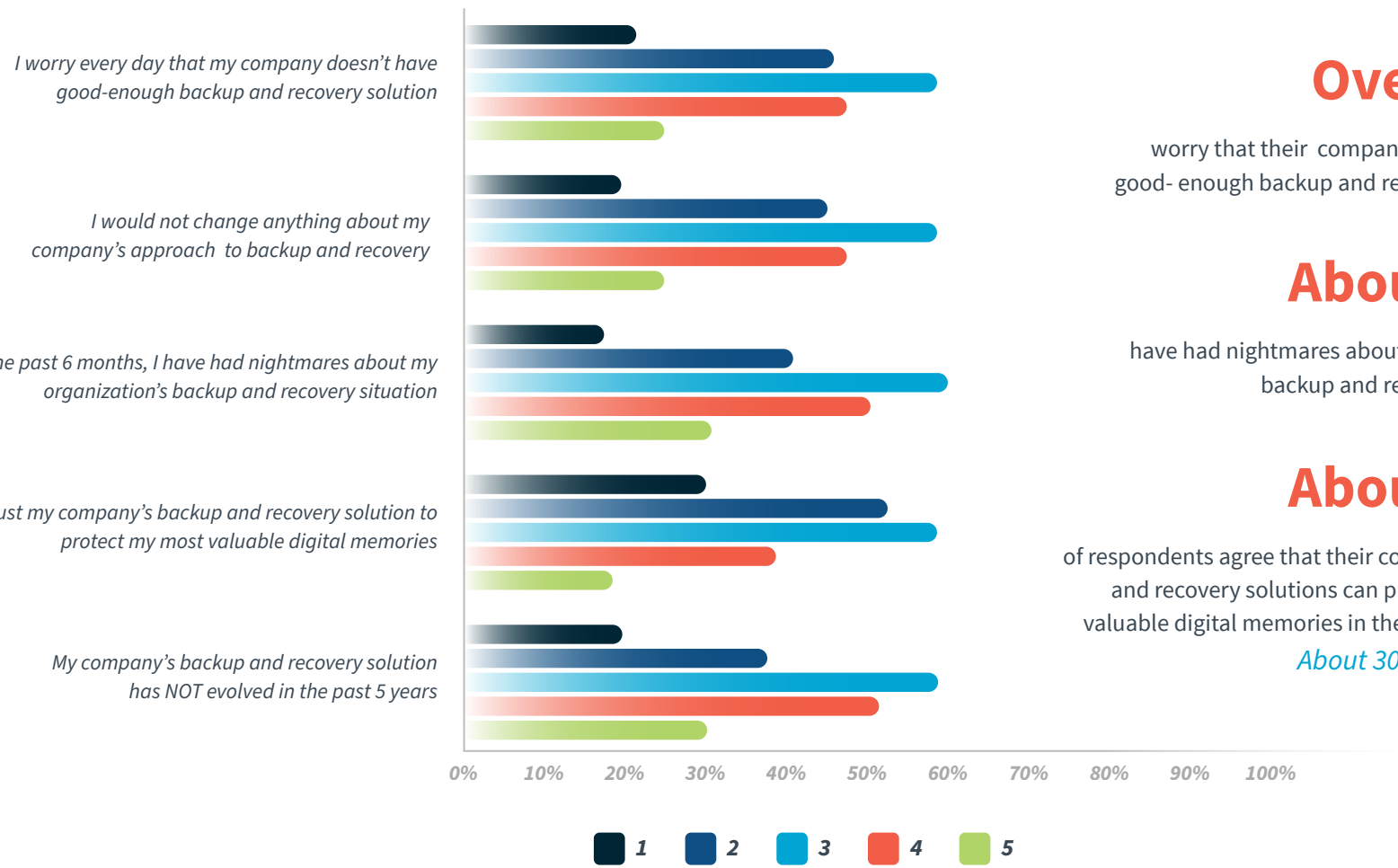
Over 60%

Of workloads and apps are expected to run in the public cloud in the next 24 months

CONFIDENCE IN CURRENT BACKUP SYSTEMS REMAINS A CHALLENGE

Only 40% of respondents expressed confidence in their backup systems' ability to protect critical data in the event of a crisis. Low confidence stems potentially from a lack of technological evolution, as more than 28% of respondents cited their backup and recovery solution has not evolved in five years. Alarmingly, 30% worry their organization doesn't have a good enough backup and recovery solution. Fewer than 10% of respondents said they would not change anything about their organization's approach to backup and disaster recovery.

Score the following statements on a scale of 1-5 (1=strongly agree; 2=agree; 3=neutral; 4=disagree; 5=strongly disagree)



Over 30%

worry that their company doesn't have a good- enough backup and recovery solution.

About 30%

have had nightmares about their company's backup and recovery situation.

About 40%

of respondents agree that their company's backup and recovery solutions can protect their most valuable digital memories in the event of a crisis.

About 30% don't agree.

MANY ORGANIZATIONS PLAN TO SWITCH BACKUP PROVIDERS

Respondents expressed dissatisfaction with their current backup and recovery providers, with more than half of respondents indicating plans to switch their primary backup solution in the next year. The cohorts responding “Definitely,” “Very Likely,” and “Somewhat Likely” to switch vendors cited the top three challenges as:

Cost

Disaster recovery execution

Backup and/or disaster recovery testing

This trend emphasizes the need for vendors to address pain points such as cost, limited automation and orchestration and ease of use.

Likely to switch primary backup solutions

5% of respondents

said their organization will not switch

12% of respondents

said their organization will definitely switch

33% of respondents

said their organization is somewhat likely to switch.

22% of respondents

said their organization is very unlikely to switch

27% of respondents

said their organization is very likely to switch

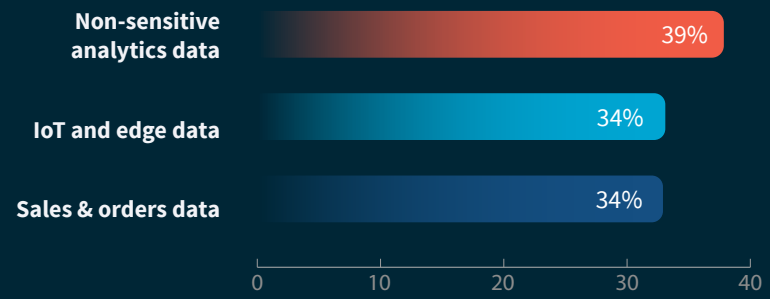
CLOUD & SAAS APPLICATION ADOPTION

The scalability, flexibility and efficiency offered by cloud-based technology has led to increased adoption in recent years. However, the shift to cloud-native platforms introduces complexities around migration, data protection and cost optimization. The survey uncovers critical insights with regards to how organizations navigate their journey to the cloud.

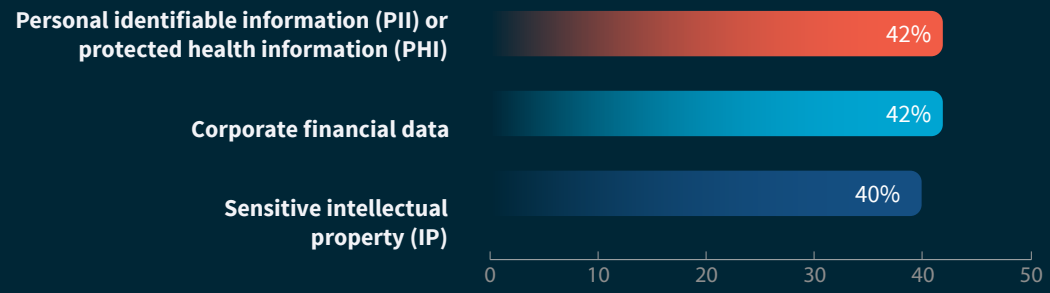
APPROACH TO DATA MIGRATION

Organizations worldwide are firmly entrenched in hybrid cloud environments, with 54% of workloads and applications cloud-hosted today. Cloud workloads are projected to grow by an additional 11% over the next two years, as respondents anticipate on average 61% of their workloads and applications will be cloud-hosted by 2026. In examining the top data types slated for migration and those unlikely to migrate, our findings suggest a growing but measured confidence in cloud solutions, with an emphasis on leveraging cloud solutions to improve operational efficiency and strategic analytics while carefully navigating concerns about data sensitivity and compliance.

Top data types likely to migrate:



Top data types unlikely to migrate:

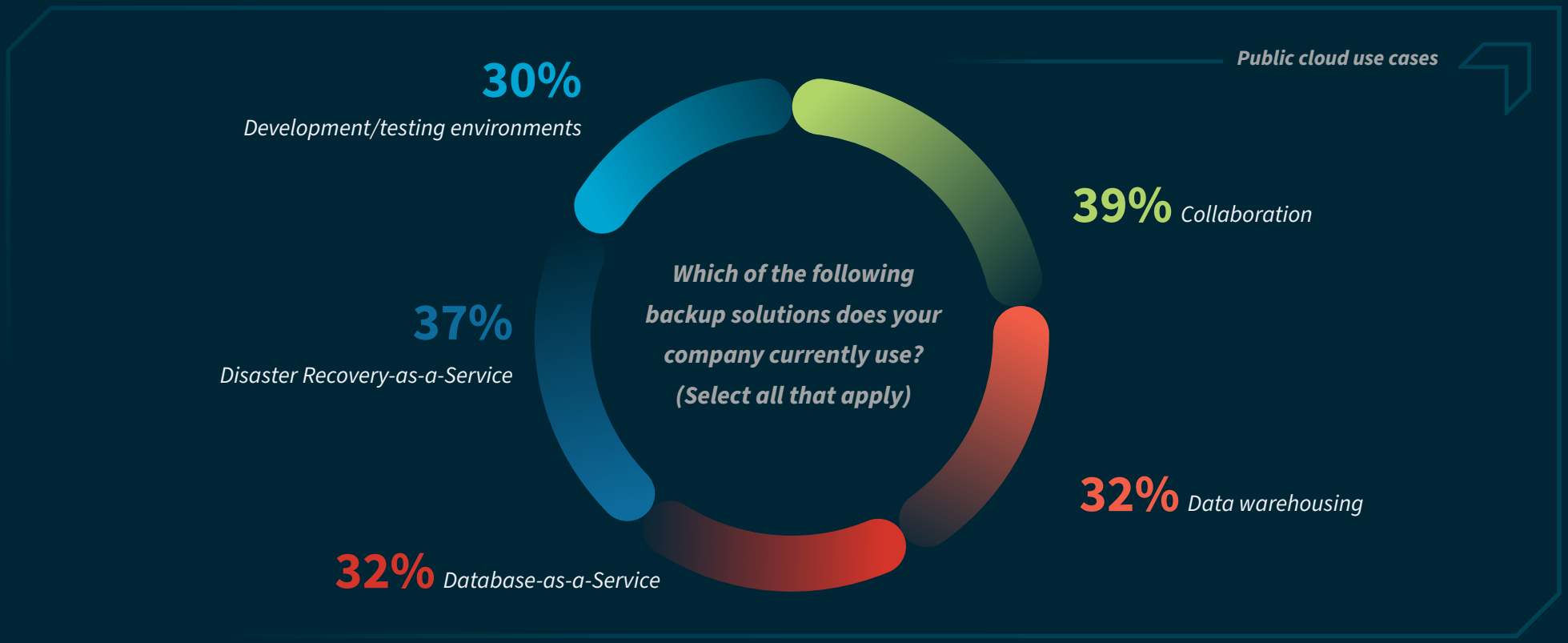


The highest percentage of migration involves non-sensitive analytics data, suggesting some hesitancy entrusting highly sensitive data to the cloud, while the inclusion of IoT and edge data reflect growing confidence in the cloud's ability to handle diverse, high-velocity data sets to enable real-time analytics and integration at scale.

The reluctance to migrate more sensitive data underscores that notion that while cloud solutions are seen as valuable for scalability and innovation, security, compliance and control concerns remain critical barriers. Data such as PII and PHI is heavily regulated by law. Organizations leery of migrating this data suggests doubt remains with regards to the cloud's ability to meet strict regulatory requirements. Despite projections of increased cloud migration, there remains hesitancy amongst organizations to entrust their most sensitive data to third-party environments, whether fear of breaches, unauthorized access, or compliance violations.

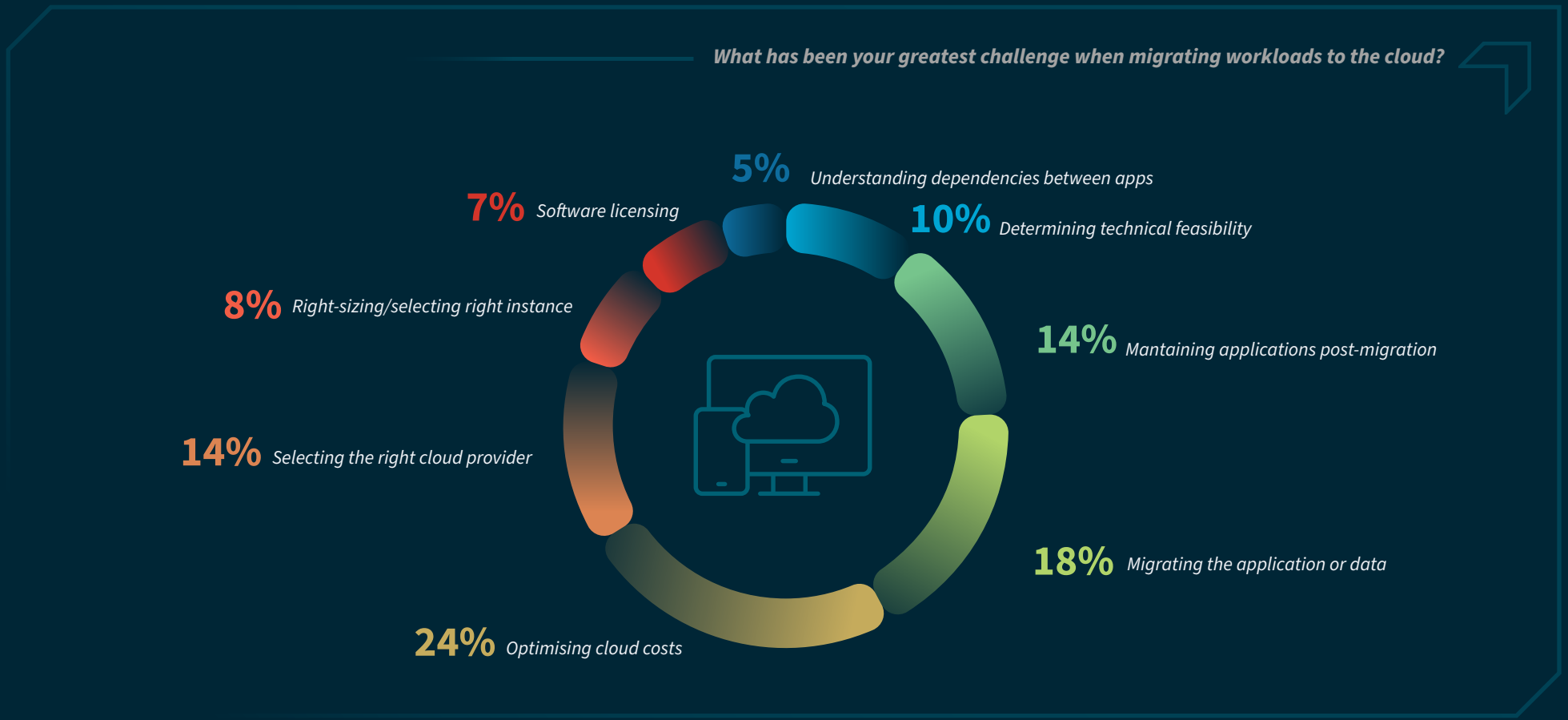
USE CASES FOR PUBLIC CLOUD ADOPTION

Collaboration (39%) is the primary driver for adopting a public cloud solution, followed by disaster recovery (37%), data warehousing (32%) and Database-as-a-Service (32%). Cloud usage today suggests the primary driver of adopting cloud services is the seamless scalability and flexibility of tools to support remote and hybrid working environments. Similarly, the emphasis on data warehousing and Database-as-a-Service underscores the cloud's ability to facilitate data-driven operations at scale. Organizations also value the cloud's ability to provide fast recovery, data redundancy and protection from downtime or data loss through use of disaster recovery services.



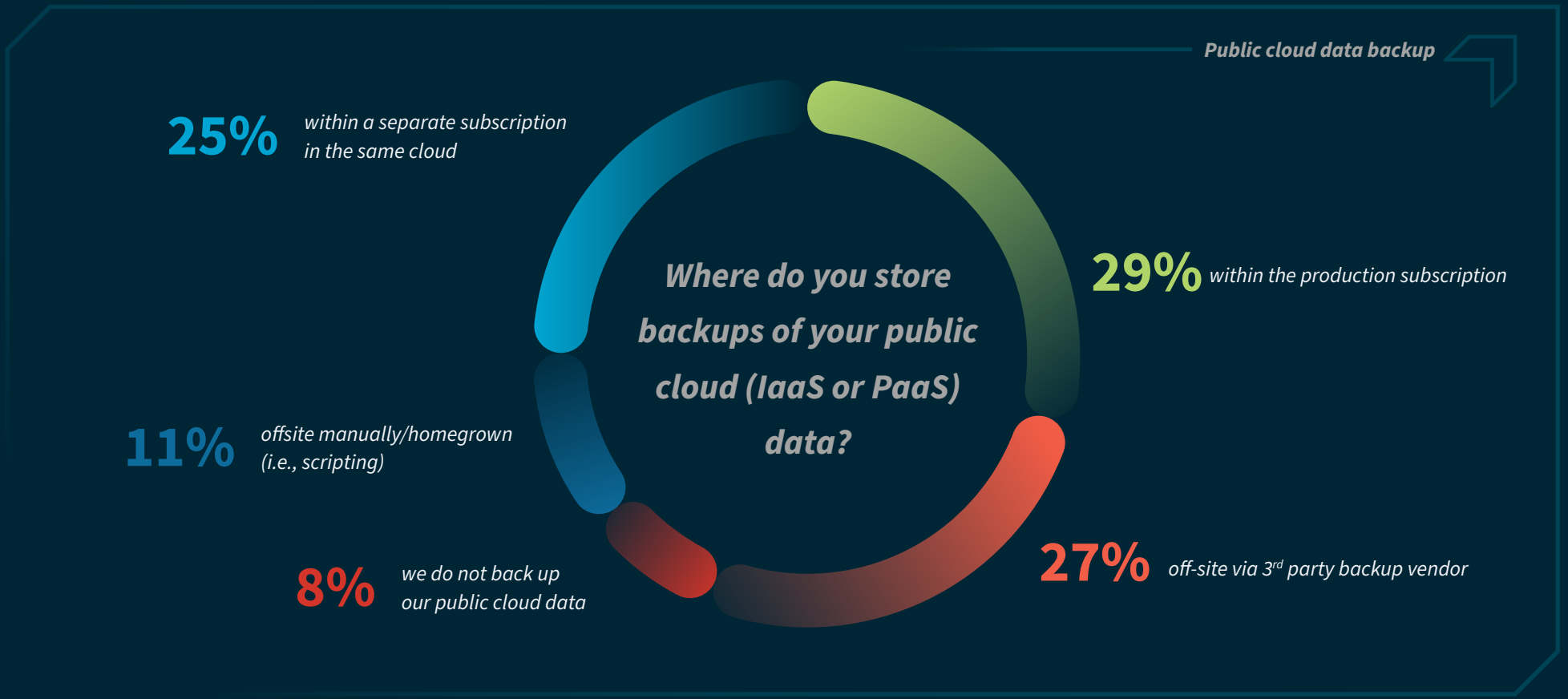
CHALLENGES WHEN MIGRATING WORKLOADS TO THE CLOUD

Cloud migration presents numerous challenges, including technical, financial and operational complexities. Optimizing cloud costs, cited by 24% of respondents, emerged as the leading challenge in migrating workloads and data to the cloud. For nearly 20% of organizations, workload migration remains a significant concern due to compatibility and performance issues during the transition. Around 15% of respondents indicated finding the right cloud service provider for their use case or determining technical feasibility (10%) a major challenge. Post-migration, maintaining applications in the cloud also poses difficulties for 14% of organizations. Right-sizing cloud instances (8%), licensing (7%) and understanding the dependencies between applications (5%) presented challenges for a small minority of organizations.



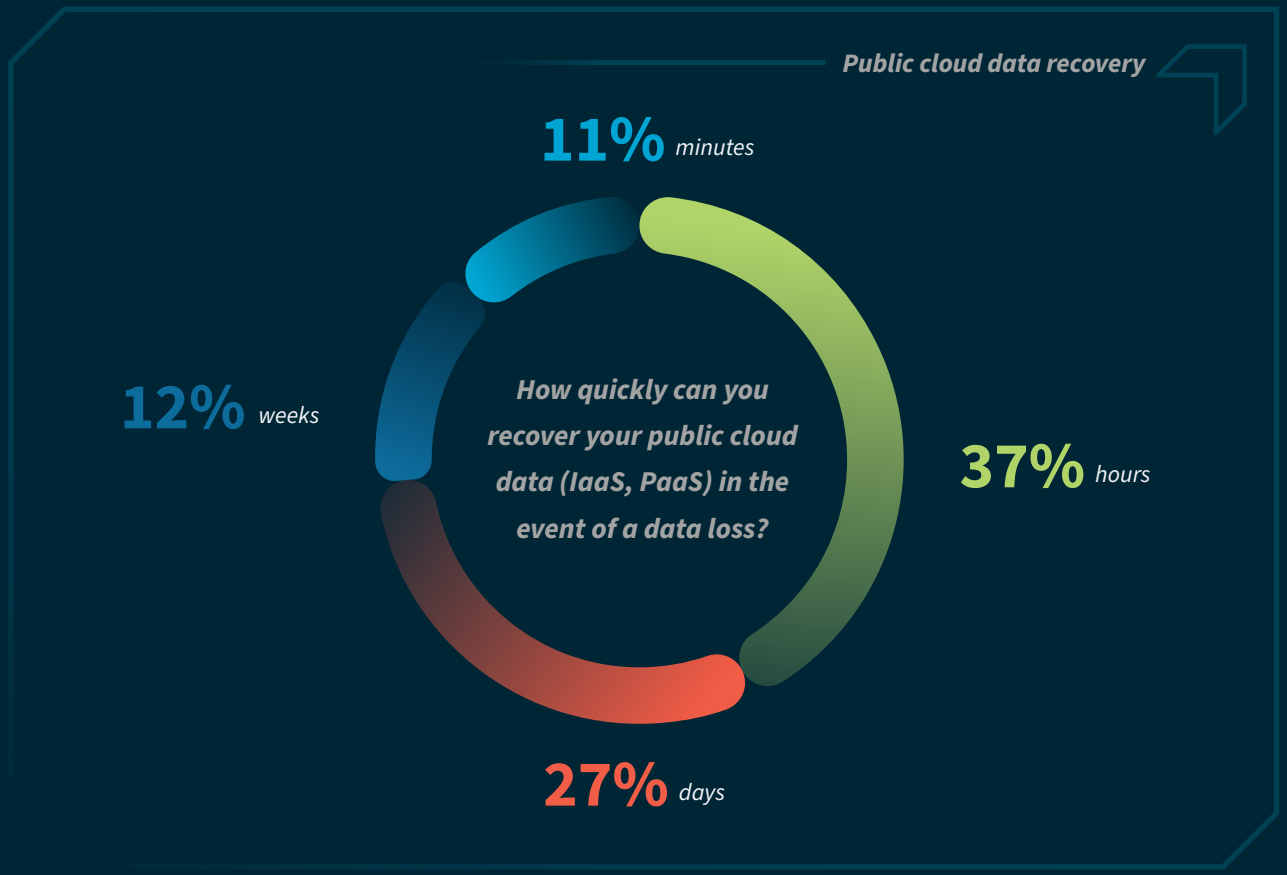
HOW ORGANIZATIONS STORE BACKUPS OF PUBLIC CLOUD DATA

Data protection remains a key concern of those migrating to the cloud, and organizations utilize a variety of strategies to store backups of their public cloud data. Nearly 30% of respondents report storing cloud backups within the production subscription, a choice that offers simplicity but raises concerns about the risks of a single point of failure. More than a quarter (27%) of respondents opt for redundant backups through third-party vendors for additional protection. Another 24% of respondents maintain backups in a separate subscription account within the same cloud provider, providing some level of isolation without relying on external providers. Alarmingly, 8% of organizations do not back up their public cloud data at all, leaving themselves highly vulnerable to potential data loss.



RECOVERY OF PUBLIC CLOUD DATA

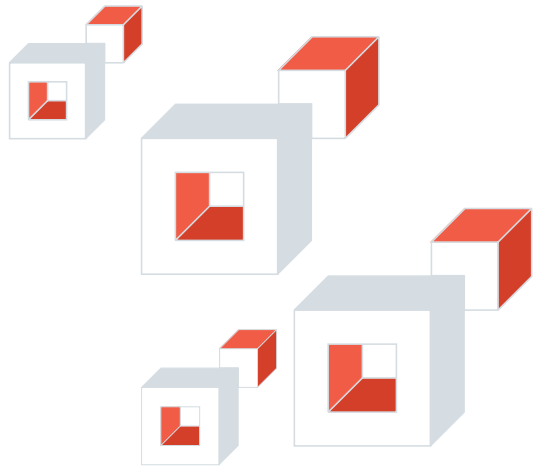
Our survey revealed varying levels of preparedness with regards to cloud data recovery. A large minority (37%) of organizations indicated they would be able to recover public cloud data within hours, while 11% reported being able to recover within minutes. However, nearly 30% of respondents reported their organizations would require days to recover and 10% would need weeks, potentially leading to significant operational disruptions and prolonged downtime.



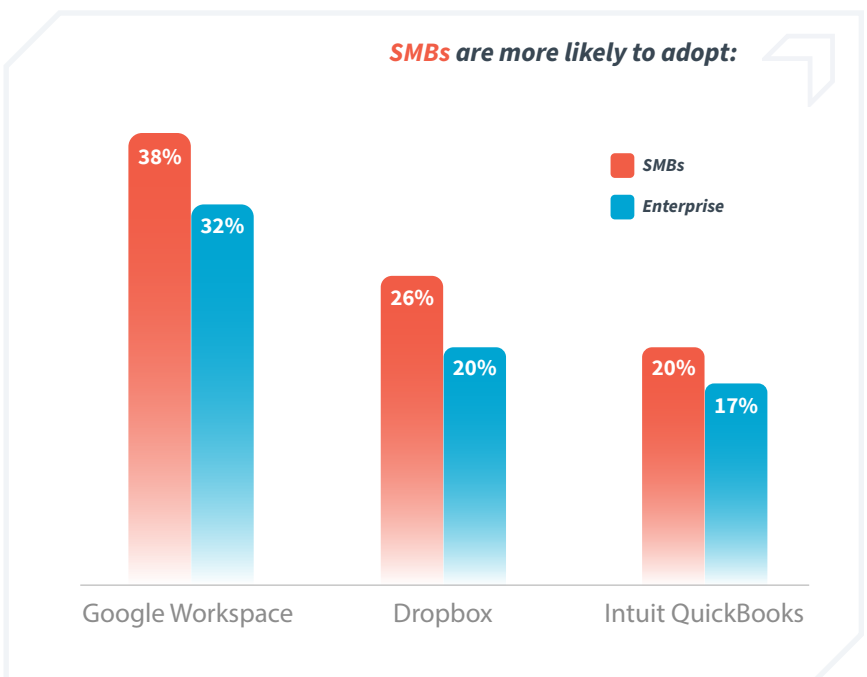
ADOPTION OF SAAS APPLICATIONS

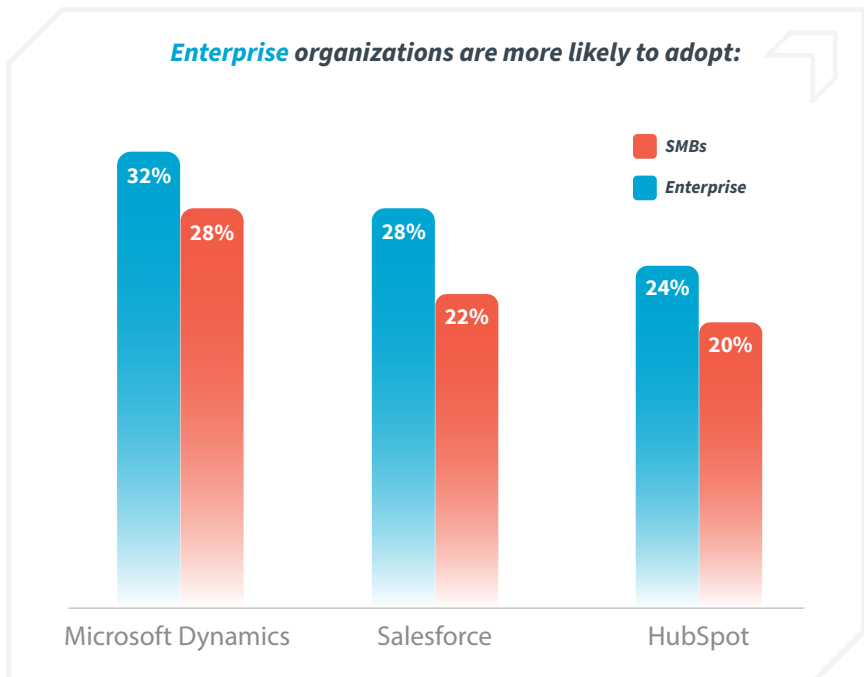
With regards to collaboration solutions (commonly delivered via SaaS model), Microsoft 365 remains the leader with a 53% adoption rate amongst respondents but has seen a decline in market share compared to 2022 adoption rates, which saw a 71% adoption of Microsoft 365 amongst our respondents. Microsoft 365 adoption remained steady amongst both SMB and enterprise cohorts.

The adoption of Google Workspace (35%) has risen steadily in the last two years (25% in 2022), driven in part by growing adoption by SMBs. SMBs (500 employees and under) reported higher usage of Google Workspace (38%) compared to enterprise adoption (32%).



SAAS ADOPTION RATES PER COHORT





IMPLEMENTATION OF SAAS BACKUP SYSTEMS

As organizations increasingly rely on SaaS applications to drive productivity and collaboration, the importance of data protection has never been greater. While awareness of the Shared Responsibility Model (SRM) — which clarifies that businesses, not SaaS providers, are responsible for protecting their data — has grown, adoption of robust backup strategies remains uneven.

Among organizations who have adopted a SaaS application(s), those adopting Microsoft 365 (70%) and Google Workspace (66%) most frequently report having a backup strategy in place. Salesforce trails with only 53% of organizations having a dedicated backup strategy — a concerning gap.

Surprisingly, the adoption of backup strategy lags for other critical applications. SaaS applications least likely to be backed up included Zapier (38%), Slack (42%) and Zendesk (49%), leaving organizations vulnerable to data loss risks.

Sentiment on how to best protect SaaS application data remains mixed:

7% *Backup not required for SaaS apps*

19% *Rely on vendor for availablity*

22% *3rd Party Backup Solution*

28% *Native Vendor Tools*

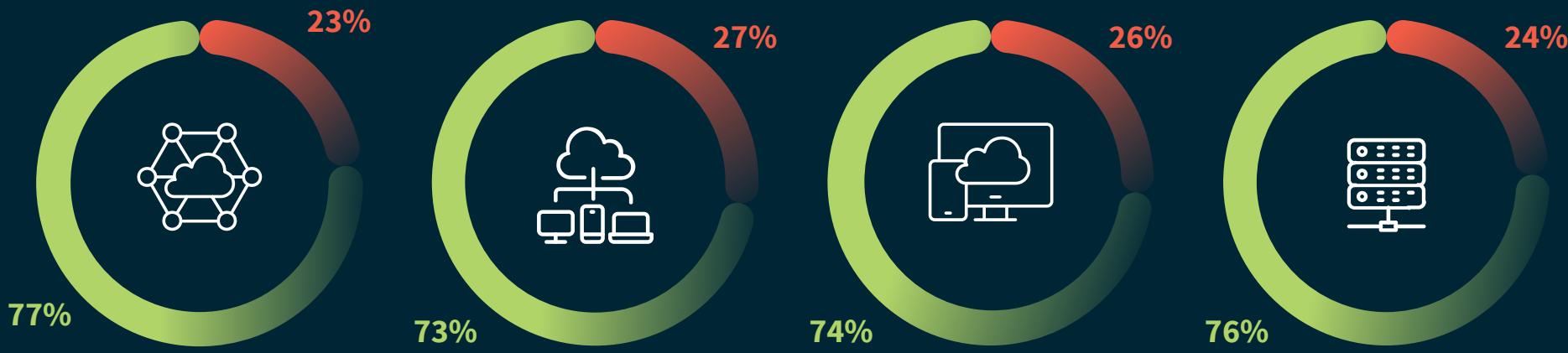
SECURITY OF BACKUP SYSTEMS AND DATA

As reliance on cloud-native applications and the volume of sensitive business data within them grows, the need for robust security measures to protect backups from unfettered and malicious access becomes critical.

POLICIES AND CONTROLS TO SECURE BACKUP WORKLOADS

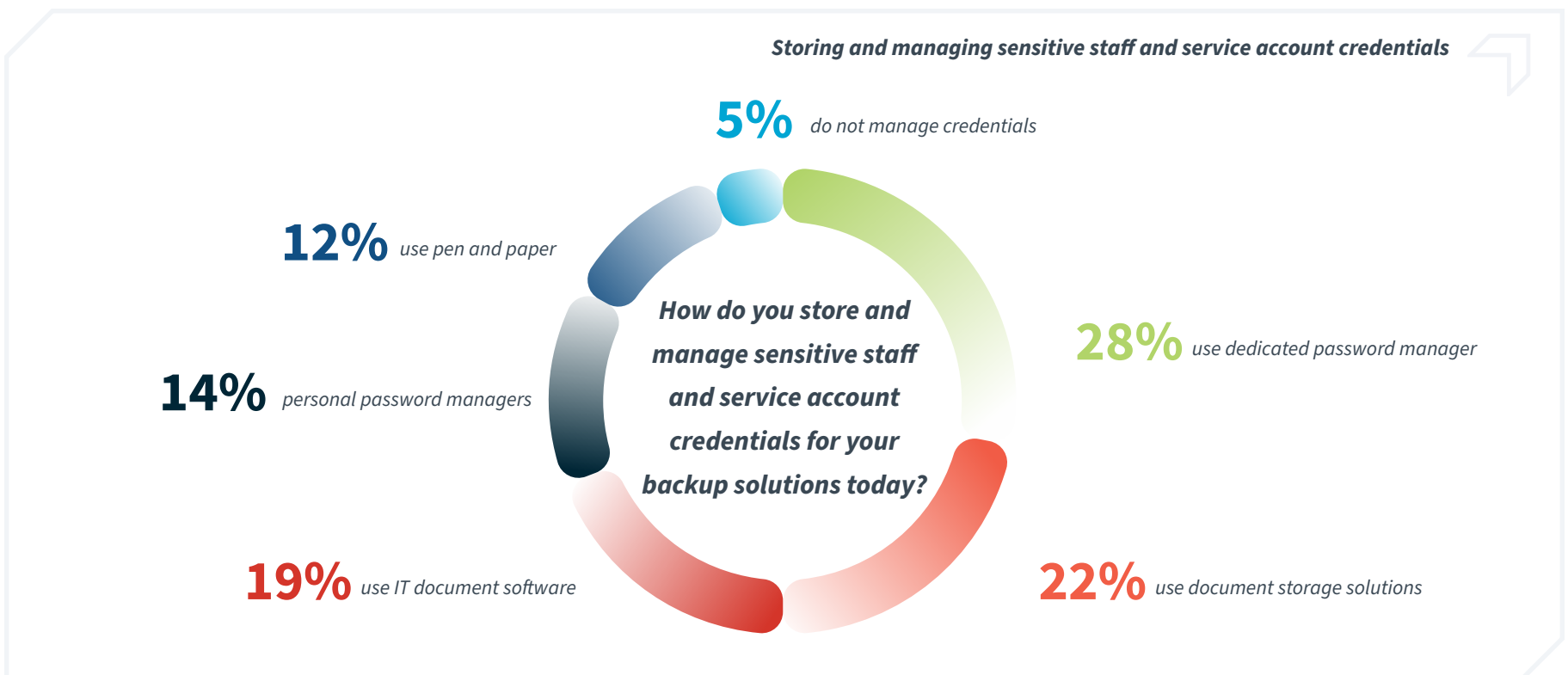
Overall, organizations have a strong posture to secure backups, given their vital role in data protection and business continuity. About 75% of respondents report having policies and controls in place to secure access to backup data across cloud, SaaS applications, endpoints and servers/VMs. However, 25% of organizations still lack these essential safeguards. The gap presents a significant risk, particularly as organizations continue to operate in increasingly hybrid and multicloud environments.

For which of the following protected workloads do you have policies and controls in place to limit and detect malicious access to your backups?



HOW ORGANIZATIONS STORE SENSITIVE CREDENTIALS

The security of sensitive staff and service account credentials is vital to maintaining backup system integrity. However, the methods employed vary greatly with regards to both adoption and efficacy. More than a quarter (28%) of respondents utilize a dedicated password manager, a widely accepted best practice for security sensitive credentials. Document storage solutions, such as SharePoint and Confluence, are used by 22% of respondents. However, relying on such solutions could introduce security risks due to limited access controls and potential vulnerabilities in these platforms, including account compromise and privilege escalation, common techniques in user-based cyberattacks. IT Documentation software is a tool used by nearly 20% of organizations, enabling easy access to information with credentials stored in a secure, centralized location. About 14% indicate using personal password managers or browser-based password managers, which offer convenience but lack the advanced security features of a dedicated password manager. About 12% store passwords with pen and paper, leaving credentials susceptible to physical security risks, damage and insider threats. Physical password storage lacks the protection provided by encryption and does not offer remote access. About 5% of organizations report they do not manage credentials for their staff and service accounts.



USER LIFECYCLE MANAGEMENT

Managing the data lifecycle of SaaS application users is an ongoing challenge for organizations, particularly when employees depart the organization. About 40% of respondents report archiving ex-employee data within their backup tool. Nearly 30% create shared mailboxes or sites to maintain access to critical information. Smaller cohorts leverage alternative methods, such as a third-party archival tool (14%) or keeping licenses active on the tenant or domain for ex-employees (14%), inviting operational risk with unmanaged credentials. Less than 10% of organizations revealed they do not maintain ex-employee data at all, increasing the risk of loss of institutional knowledge and critical records as well as non-compliance.

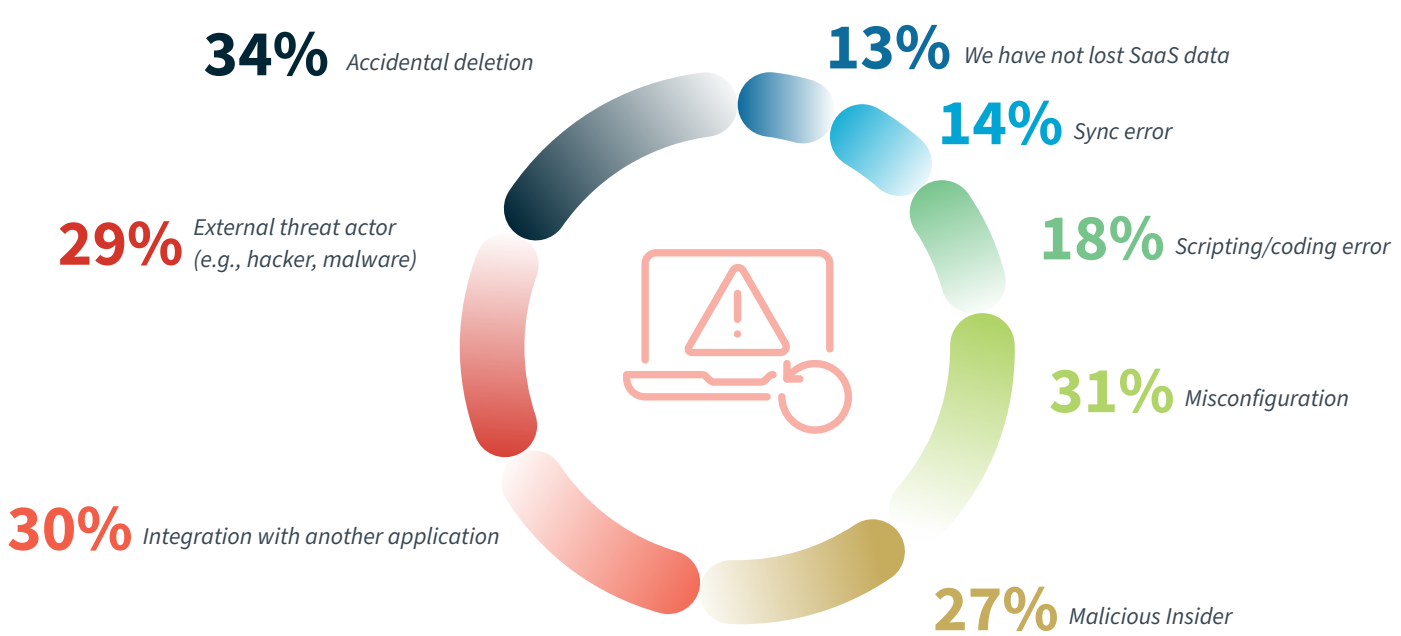
Strategies for user lifecycle data management

DATA LOSS & DATA RECOVERY

SAAS APPLICATION DATA LOSS

Data loss in SaaS applications occurs due to a variety of factors. Malicious deletion impacted more than 50% of respondents, with 29% of organizations experiencing deletion at the hands of an external threat actor and 27% by a malicious insider. Accidental deletion or human error, cited by 34% of respondents, remains a prominent cause of SaaS data loss. Misconfiguration, caused by mistakes during setup or maintenance, impacted more than 30% of organizations. Integrations, where conflicts or overwrites were caused by a third-party application, compromised data for 30% of respondents. Technical errors, such as scripting or coding errors (18%) and sync errors (14%) impacted organizations less frequently. Only 13% of respondents cited they did not suffer SaaS data loss in the last 12 months.

In the past 12 months, which of the following caused SaaS data loss in your organization? (Select all that apply)

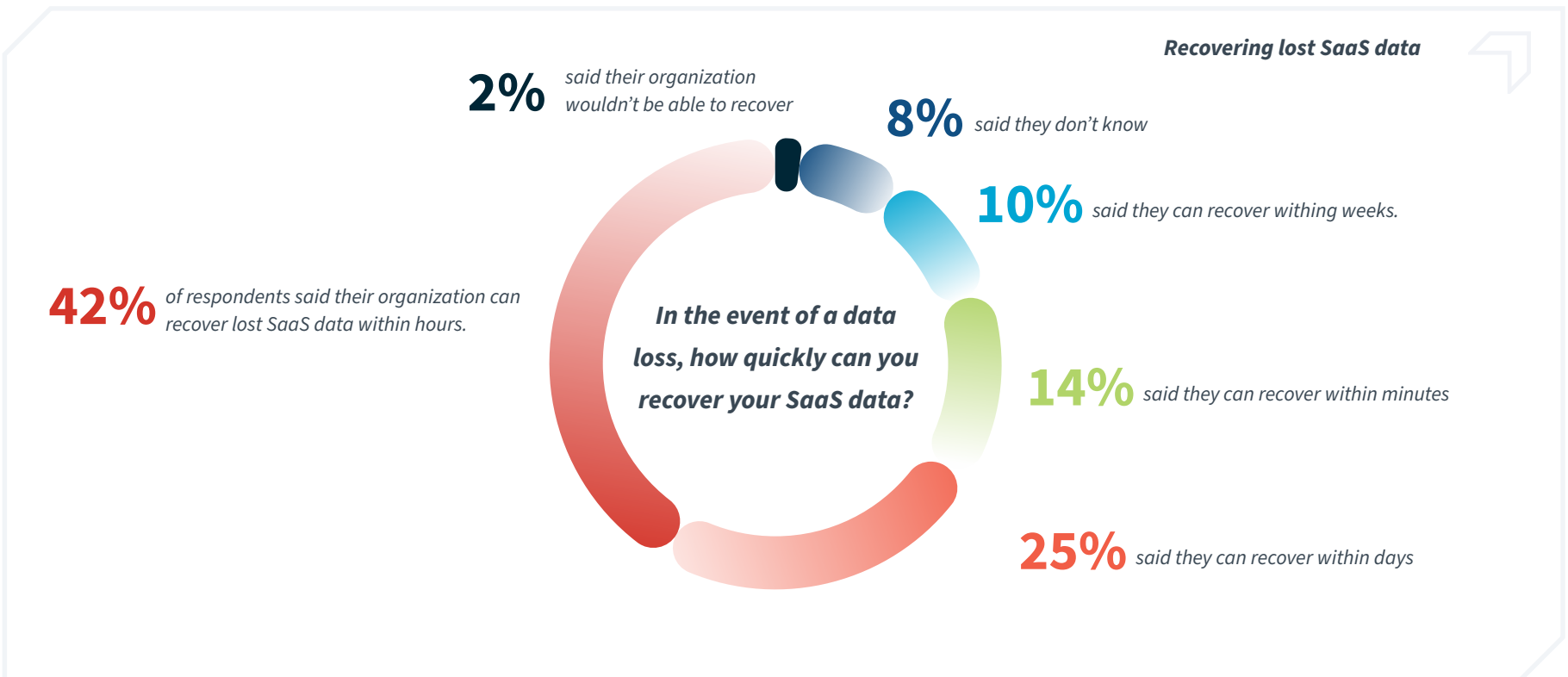


SAAS APPLICATION DATA RECOVERY

Whether it's restoring a single email, a collaborative document or an entire site, organizations need precision, speed and flexibility to recover specific data objects to maintain continuity and compliance. Without robust recovery capabilities and controls, recovery efforts can become time-consuming, error-prone and disruptive, underscoring the importance of having a robust and customizable recovery strategy for SaaS environments.

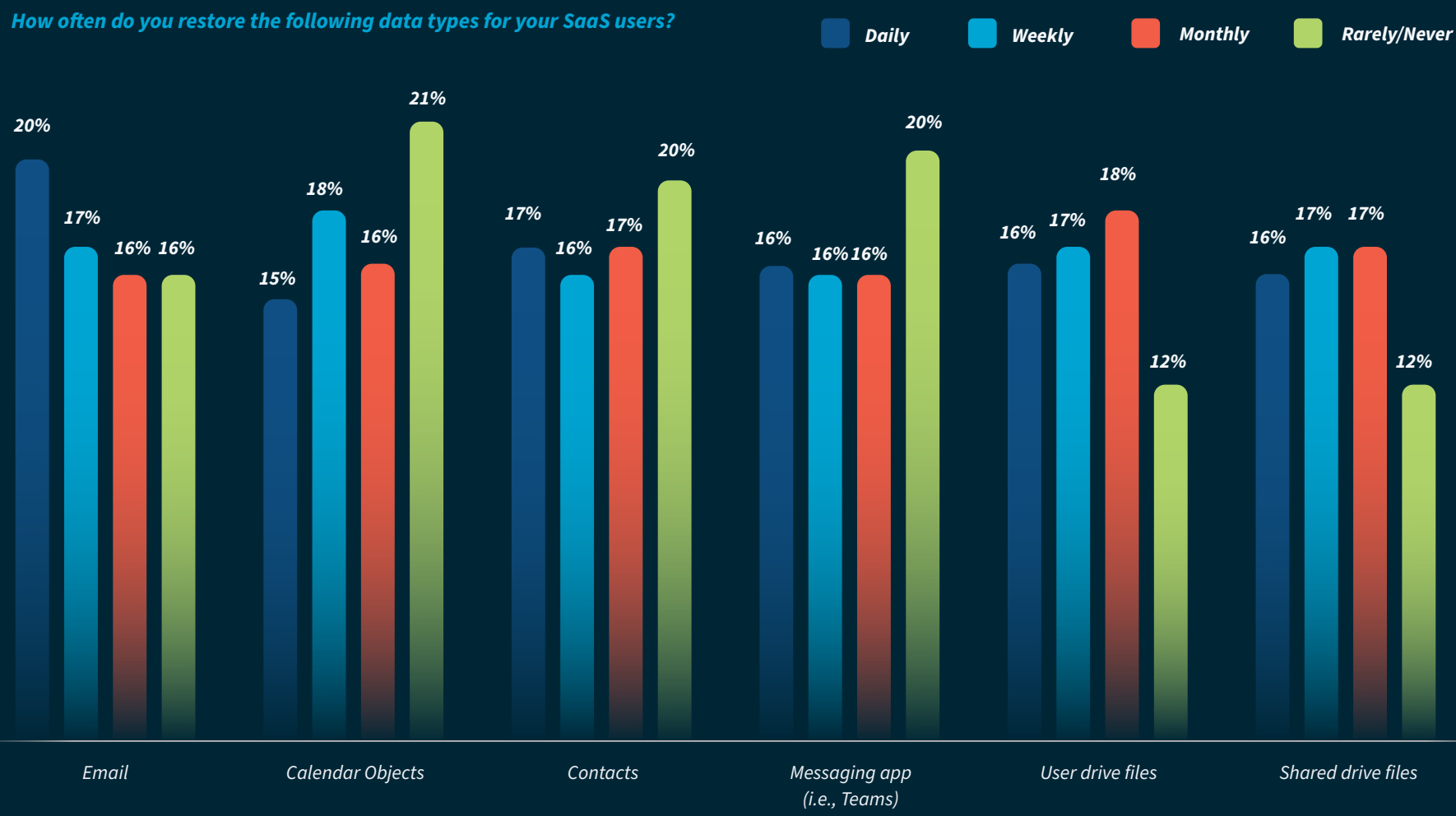
How quickly can organizations recover lost SaaS data

Quick recovery of lost SaaS data is essential for minimizing downtime and meeting industry regulations. Just over 40% of organizations report being able to recover lost SaaS data within hours while another 14% report being able to recover within minutes. Other organizations struggle with recovery times, with 35% requiring days or even weeks to recover. More concerning is the 8% of respondents who were unsure of their recovery times and the 2% of organizations that expressed that they could not recover lost SaaS data at all.



RECOVERY OF SAAS DATA OBJECTS

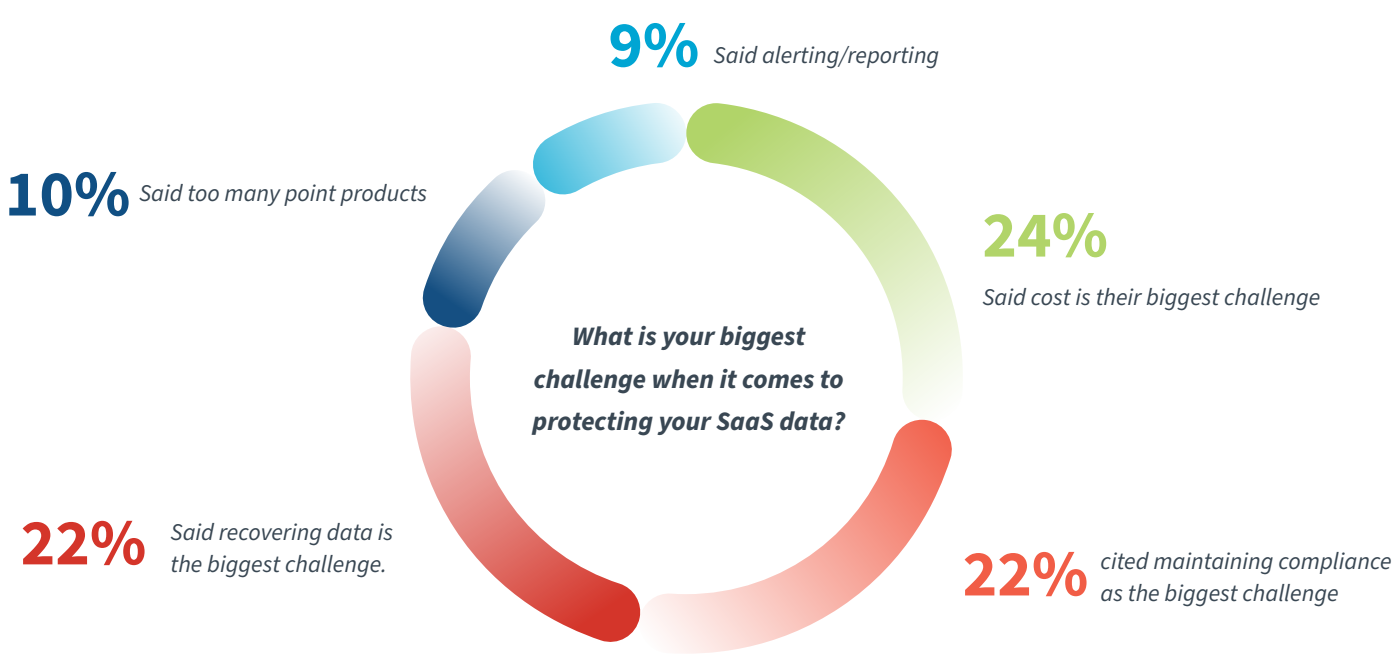
The recovery of SaaS data objects varies depending on their usage and criticality to an organization's daily operations. Email (20%) and mail contacts (17%) were most frequently recovered daily, underscoring their essential role in communication and business continuity. Conversely, calendar objects (21%) and messaging app data (20%) are the objects least likely to need to be restored, reflecting either less frequent loss or a lower immediate impact on operations. These trends highlight the importance of tailoring recovery strategies to prioritize swift recovery of frequently used and essential data while ensuring comprehensive protection across all SaaS platforms.



CHALLENGES PROTECTING SAAS DATA

As both the volumes of data within and reliance upon SaaS applications grows, protecting this data has become a critical priority. IT professionals face numerous challenges in ensuring their data remains safe, secure and recoverable. For nearly 25% of organizations, cost is their greatest challenge when it comes to protecting SaaS data. With industry regulations, compliance mandates and cyber liability insurance terms constantly evolving, 22% of respondents cited maintaining compliance as their top challenge. An equally pressing issue for 22% of respondents is the recovery of data itself. Notably, 10% of respondents cited that the use of too many backup tools creates inefficiencies and increases operational challenges. About 10% of respondents said alerting and reporting is their organization's biggest challenge, as a lack of actionable insights and visibility into backup systems makes it difficult to identify risks and missed backups.

Biggest challenge for SaaS data protection

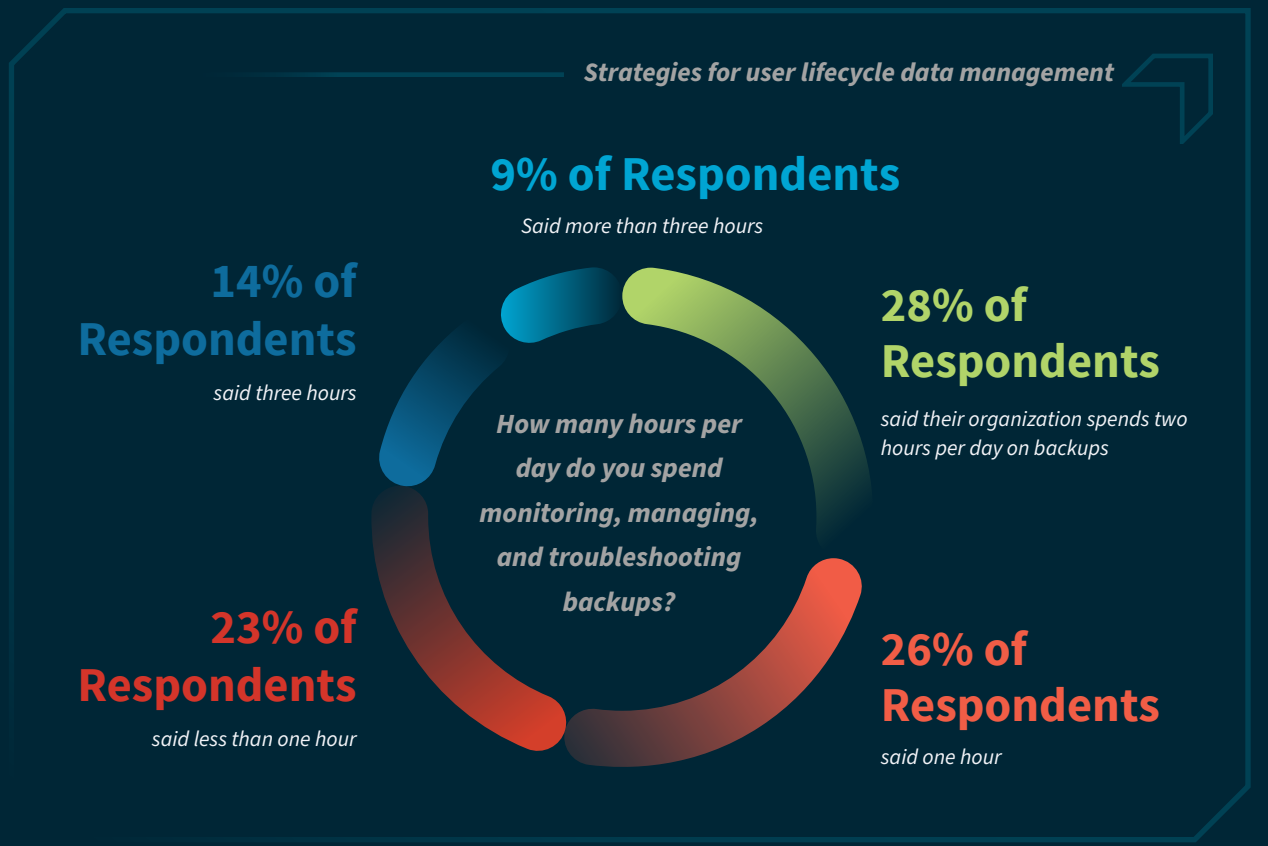


CHALLENGES AMONG SPECIFIC SAAS APPLICATIONS

When examining the challenges cited by respondents by individual product user cohorts, the data remained directionally accurate, but unique challenges emerged among Microsoft 365, Google Workspace and Salesforce users. Notably, Google Workspace (23%) and Salesforce (23%) cited the highest rate of challenge with data recovery compared to Microsoft 365 (20%). Google Workspace users (11%) reported alerting and reporting as their greatest challenge compared to 8% of Microsoft 365 users and 8% of Salesforce users. Perhaps, given the sensitivity of data, Salesforce users (24%) most frequently cited maintaining compliance as their greatest challenge, compared to 23% of Google Workspace users and 21% of Microsoft 365 users.

TIME SPENT MONITORING, MANAGING AND TROUBLESHOOTING BACKUPS

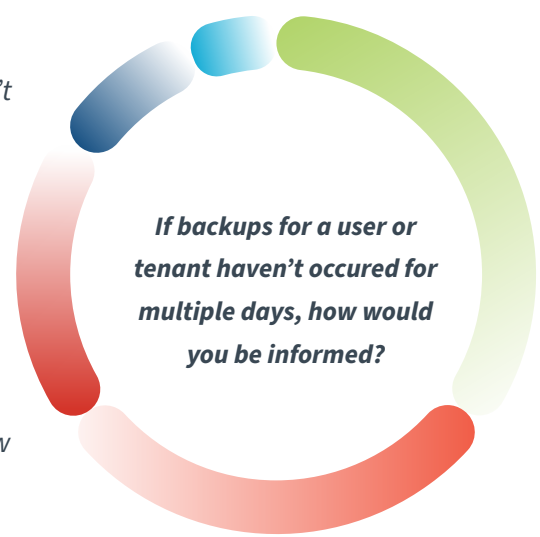
Backup management remains a time-consuming process for IT teams. Over half of the organizations surveyed said their IT team spends more than two hour per day, or more than 10 hours per week monitoring, managing and troubleshooting backups. A smaller cohort spends less time, with 23% reporting less than one hour and 26% averaging one hour daily. Since our 2022 survey, the time spent managing backups has steadily increased. The cohort spending less than one hour per day dropped by 42% (39% in 2022, 23% in 2024) and the largest increase was among those spending three hours or more daily, increasing from 5% in 2022 to 23% in 2024.



RESPONDING TO MISSED OR SKIPPED BACKUPS

When backups fail or are missed, timely detection is crucial to minimizing potential data loss and future business disruptions. A majority of respondents (65%) indicated they rely on email alerts or automatic ticketing systems to identify missed backups. However, 19% of organizations wouldn't realize there's something awry unless a backup failed — an oversight that could lead to data loss and hindered productivity. Surprisingly, 10% of respondents said they wouldn't be informed at all, and another 6% don't employ any mechanisms to monitor missed backups, leaving their organizations at significant risk.

Notification for missed backups



6% *said they don't monitor*

10% *said they wouldn't be informed*

35% *said they get email or UI alerts*

19% *said they wouldn't know unless backups failed*

30% *said they receive automatic ticket notification via PSA*

KEY TAKEAWAYS

As organizations navigate the complexities of hybrid IT environments, emerging cyberthreats and rapid cloud adoption, the importance of data protection has never been greater. The survey responses underscore the need for robust backup and recovery strategies to address current and future challenges with confidence.

RECAP OF KEY FINDINGS

The survey revealed several important insights into the state of data protection today:

Cloud reliance is growing:

Over 50% of workloads and applications run in the public cloud today, and this is projected to rise to more than 60% over the next 24 months.

Backup dissatisfaction is widespread:

More than half of organizations plan to switch their primary backup solution in the coming year, highlighting challenges in performance, cost, reliability and ease of use.

Human error and malicious deletion remain top risks:

Accidental deletion, external threat actors and malicious insiders remain leading causes of data loss in SaaS environments, emphasizing the need for stringent security controls and rapid recovery capabilities.

Security and cost are top challenges:

Securing backup systems against internal and external threats and managing the cost of data protection solutions were consistently cited as major pain points for organizations of all sizes.

The findings of this report emphasize the importance of continuous investment, innovation and vigilance to achieve complete data protection. As data volumes grow and threats evolve, organizations that prioritize data protection will not only safeguard their critical assets but also unlock the confidence to innovate and thrive in a hybrid technology landscape.

YOUR NEXT STEPS?

Use this report as a blueprint to evaluate your current backup and disaster recovery practices and take action to fortify your organization's resilience.

VISIT OUR WEBSITE

or

TAKE A TOUR

to discover how our industry-leading solutions protect your critical SaaS data, whether it lives in Microsoft 365, Google Workspace or Salesforce.

SPANNING
A Kaseya COMPANY

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. Spanning provides powerful, enterprise-class data protection for Microsoft 365, Google Workspace 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 organizations and millions of users around the world.

17012025