UNITRENDS
A Kaseya COMPANY

eBook

The State of Backup and Recovery Report 2025: Navigating the Future of Data Protection

Contents

Executive summary

The phrase “data is the new oil,” coined by British mathematician Clive Humby in 2006, resonates now more than ever.[1] It is arguably the most valuable asset for modern businesses, driving innovation, decision-making and customer engagement. Ensuring the security of this asset is critical to a business’s survival. Without a robust backup and recovery strategy, organizations risk significant data loss, workflow disruptions, reputational damage and costly consequences like fines, lawsuits and other unforeseen ramifications.

Amid the quickly shifting business landscape fueled by increasing cyberthreats, hybrid work and rapid cloud adoption, how are organizations protecting their critical digital assets? To gain deeper insights into the current backup and recovery trends and how businesses are preparing for future challenges, we surveyed over 3,000 IT professionals, security experts and administrators worldwide from various organizations.

Our findings reveal key trends and challenges that are shaping data protection strategies for businesses of all sizes:

Native backup solutions offered by cloud service providers are widely adopted but often lack robust disaster recovery (DR) capabilities.

Over **50% of businesses plan to switch primary backup solutions** in the next year, highlighting dissatisfaction with current offerings.

Accidental deletion, misconfiguration, server hardware failure and human error were the top causes of data loss in the past 12 months.

A concerning gap exists between expectations and reality when recovering from downtime events.

From emerging industry trends to data protection challenges, this report is packed with actionable insights and best practices to help organizations build a resilient data protection strategy for 2025 and beyond.

Demographics

The State of Backup and Recovery Report 2025 is based on insights 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.

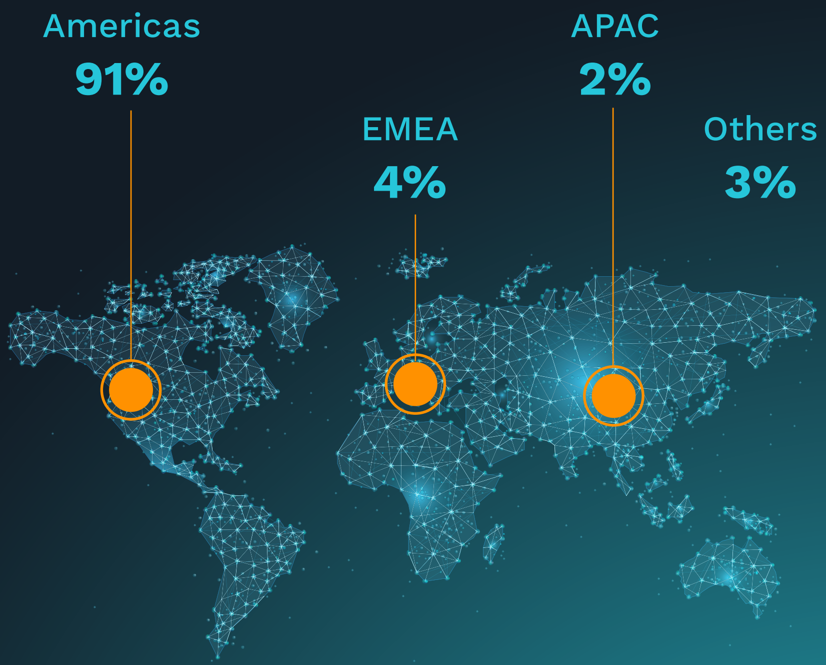
Geographic representation

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%)** add valuable perspectives from businesses operating in varied economic and regulatory environments.

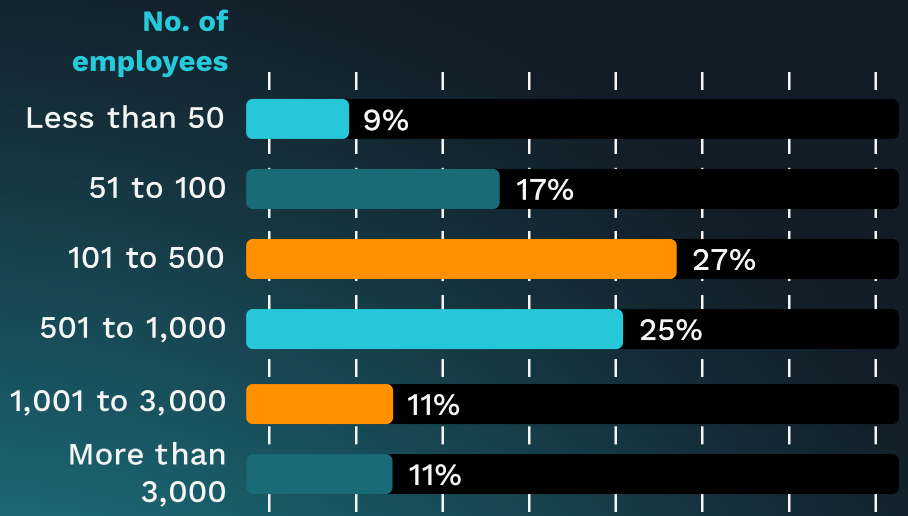
Company size and revenue

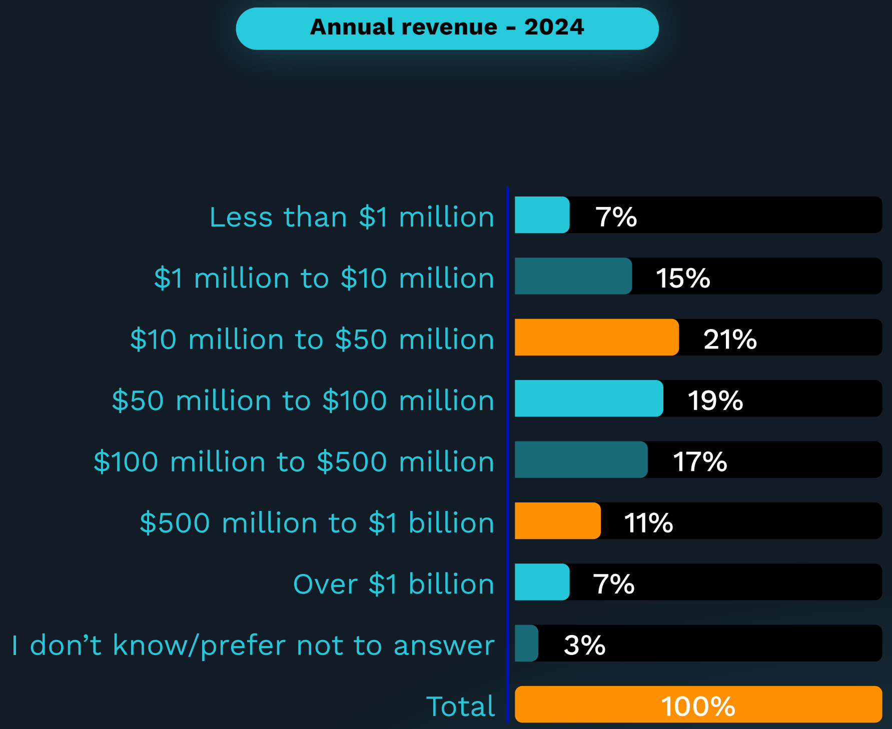
The vast majority of participants represented midsized businesses, with most reporting revenues between $10 million and $500 million. Over 50% of participants work at companies employing 101 – 1,000 people, showcasing trends within organizations balancing scalability with cost efficiency.

Demographics



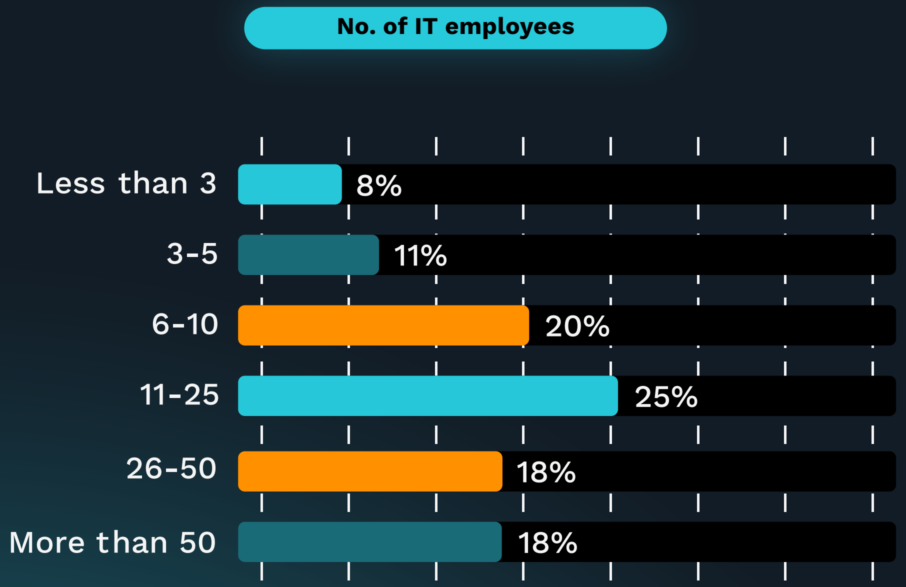
Company size





IT team composition

Most organizations employ more than 10 IT staff members, highlighting the increasing importance of IT roles in managing data protection, cloud migration and backup strategies in today's increasingly digitized business environment.



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

Industry trends shaping data protection strategies

As businesses evolve, so do the data protection strategies. To better understand the evolving landscape, we explored how organizations back up, manage and recover their data. Below are the key trends shaping the industry:

Multicloud strategies dominate

The era of a single backup solution is over. Most businesses now implement multicloud strategies to enhance resilience and flexibility. On average, organizations today use more than three backup solutions, which also shows the complexity of managing diverse IT environments.

While nearly 90% of respondents said they use native data protection tools for Azure, many are unprepared for major disasters, **with 60% of these setups lacking true disaster recovery capabilities for their Azure virtual machines (VMs).**

Cloud workloads on the rise

The use of public cloud services is surging. Over 50% of workloads and applications are currently run in public cloud environments, and this figure is projected to grow to 61% within the next 24 months.

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

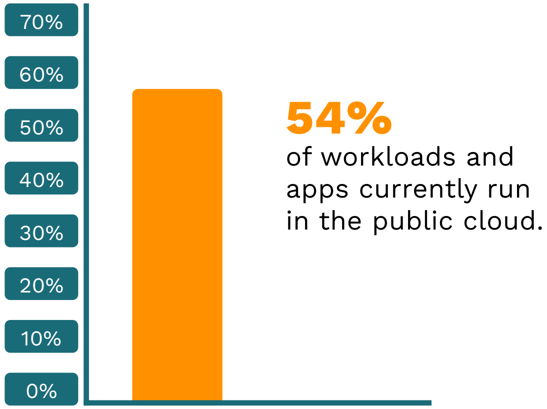


Figure 1. Workloads and apps in the public cloud

Nearly half of the organizations surveyed back up copies to the public cloud using platforms like Azure Blob, further highlighting the critical role of the cloud in modern data protection strategies.

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 and SaaS in your calculation)?

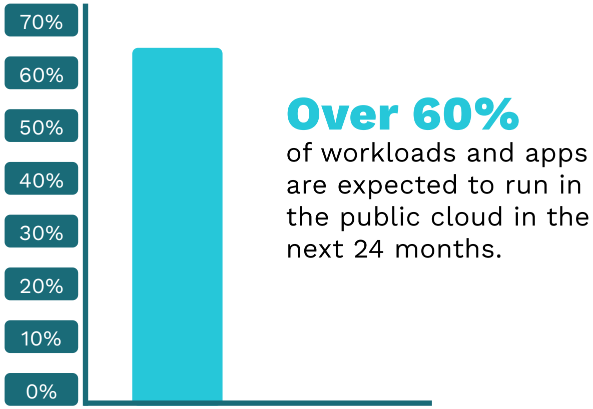


Figure 2. Workloads and apps expected to run in the public cloud in the next 24 months

Most organizations plan to switch backup solutions

The responses to the survey showed dissatisfaction with existing backup solutions as more than half of businesses surveyed plan to switch their primary backup solution in the next year. When combining responses of “Definitely,” “Very Likely” and “Somewhat Likely” the top three challenges to switching cohorts are:

Cost

Disaster recovery execution

Backup and/or disaster recovery testing

This trend emphasizes the need for vendors to address pain points, such as cost, ease of use and disaster recovery capabilities.

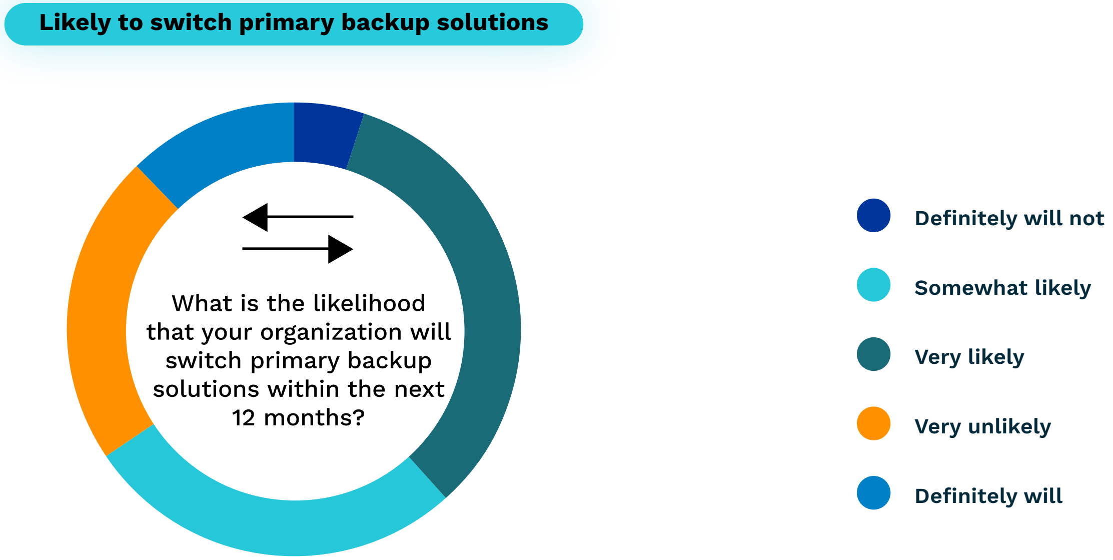
5% of respondents said their organization will not switch

12% of respondents said their organization will definitely switch

22% of respondents said their organization is very unlikely to switch

33% of respondents said their organization is somewhat likely to switch

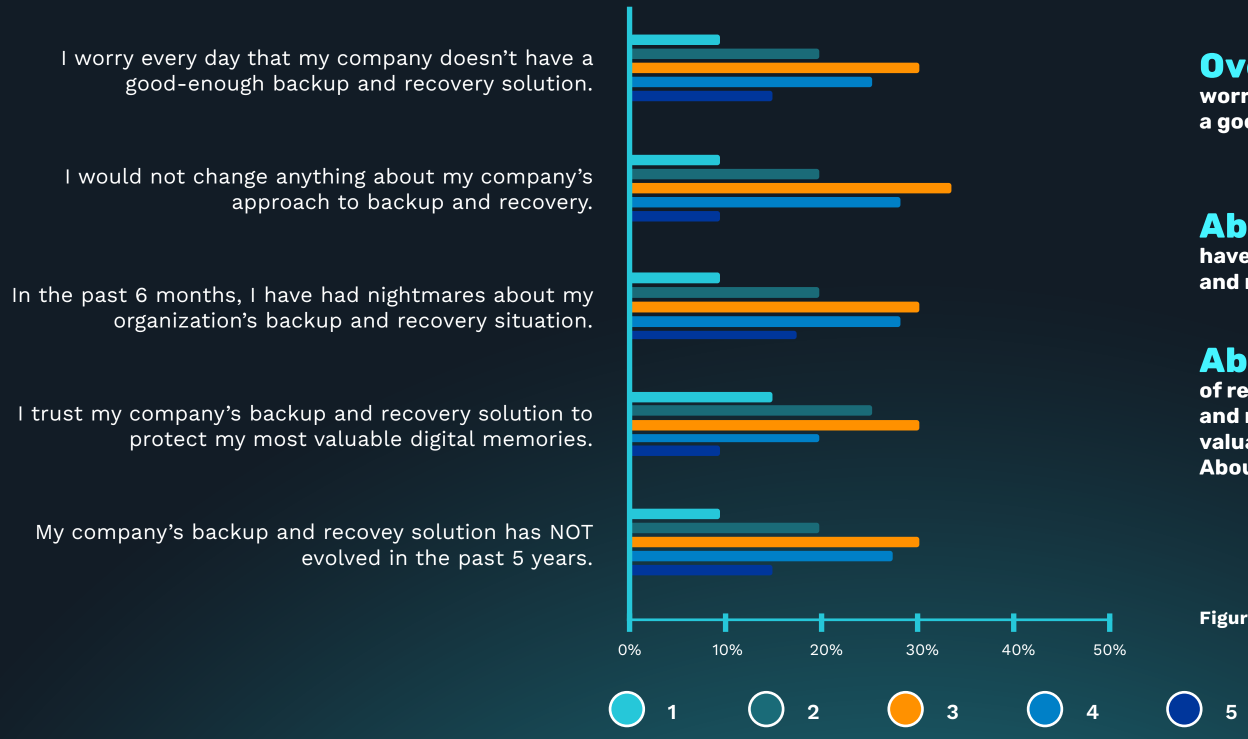
27% of respondents said their organization is very likely to switch



Confidence in current backup systems remains a challenge

Just 40% of respondents feel confident in their backup systems' ability to protect critical data in the event of a crisis. Alarmingly, 30% admitted to having nightmares about their organization's backup and recovery preparedness. Another 30% worry that their company doesn't have a good enough backup and recovery solution.

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.

Figure 3. Confidence in backup and recovery solutions

The biggest challenge in data protection is cost

The cost of protecting data — whether in Software-as-a-Service (SaaS) applications or on-premises environments — emerges as the most significant hurdle. As IT budgets tighten, businesses are forced to balance cost efficiency with robust data protection strategies.

Security of backup systems

As the volume of sensitive business data grows, the need for robust security measures to protect backups becomes critical. The survey decodes how organizations are securing their backup systems and addressing vulnerabilities.

Policies and controls for protected workloads

Overall, organizations are doing a much better job of protecting sensitive data, with 75% of respondents reporting having policies and controls in place to secure workloads across public cloud, endpoints, SaaS apps and servers/VMs. However, 25% of workloads still lack these essential safeguards. This gap represents a significant risk, especially as businesses 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?

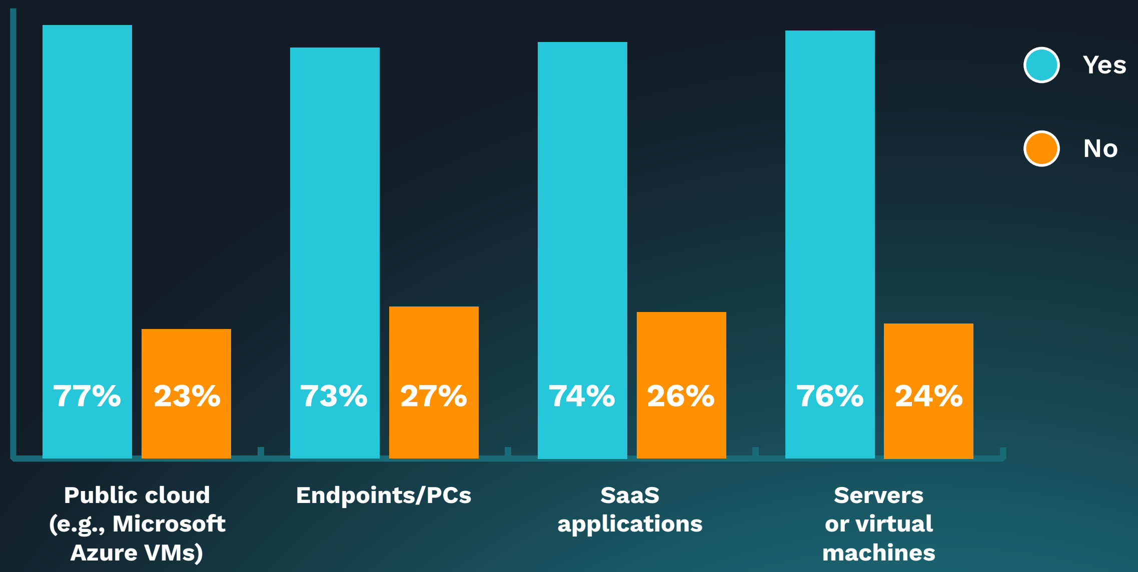
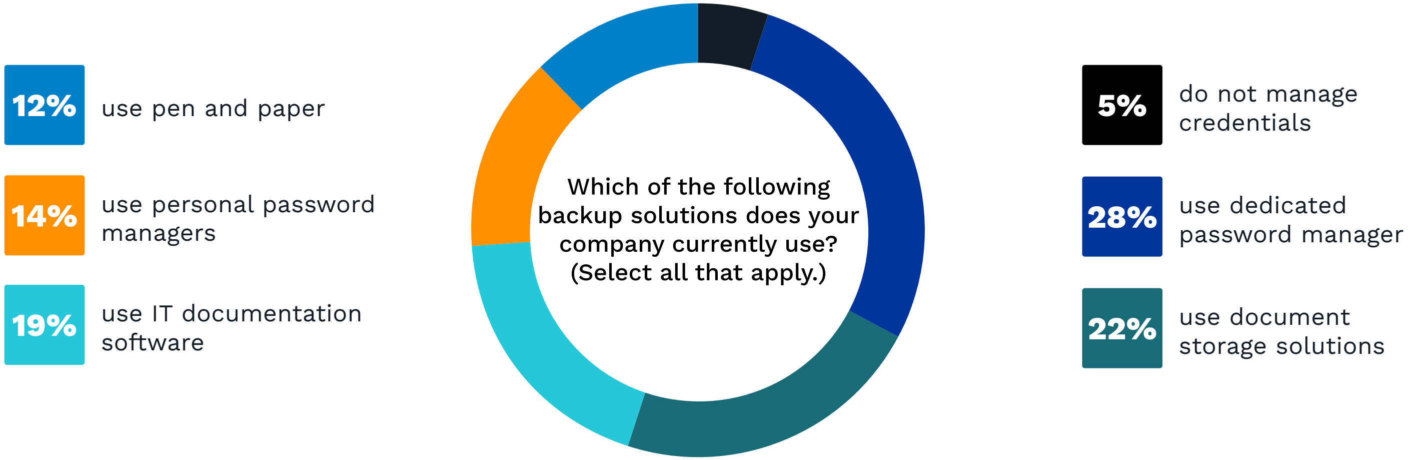


Figure 4. Policies and controls for protected workloads

How businesses store sensitive credentials

The security of sensitive staff and service account credentials is a critical aspect of backup system integrity. However, the methods employed vary widely. Nearly one-third (33%) of businesses use dedicated password managers, which is a widely accepted best practice for securing sensitive information. Document storage solutions, such as SharePoint or Confluence, are used by 22% of respondents. Relying on such solutions could introduce security risks due to limited access controls and potential vulnerabilities in these platforms. IT documentation software is another common tool used by nearly 20% of businesses, allowing easy access to information since all credentials are stored in one centralized location. About 15% indicate using personal password managers or browser-based password managers, which offer convenience but lack advanced security features like dedicated password managers.

Storing and managing sensitive staff and service account credentials

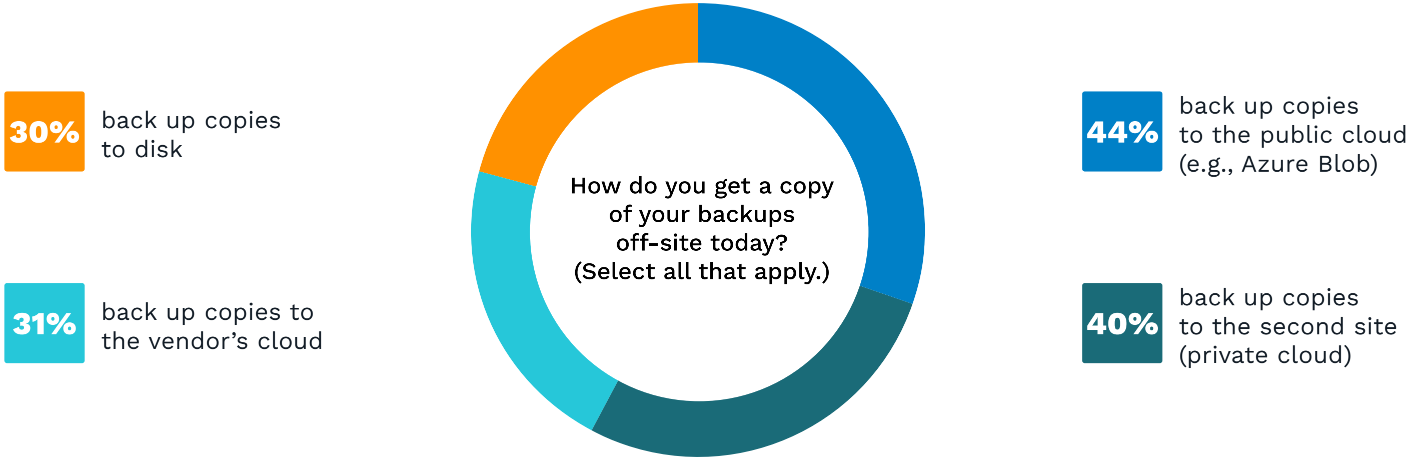


How backup copies are maintained

The survey found organizations leverage both cloud and on-premises solutions to store backup copies. The public cloud dominates as a storage option, with 44% of respondents backing up data to public cloud services, such as Azure Blob. Around 40% use a second site or private cloud to physically separate backup data to enhance resilience. Just over 30% of businesses rely on the vendor's cloud for backup storage. While this shows trust in integrated solutions provided by backup vendors, outages on the vendor's end due to technical glitches or hardware/software failure could prove to be fatal without a third-party backup solution. About 30% still rely on traditional disk storage, which, while reliable, lacks the flexibility and scalability of cloud-based options.

Alarmingly, ~2% of respondents fail to take backups off-site, leaving their data highly vulnerable to localized disasters such as fires, floods or ransomware attacks.

How backup copies are stored



[Respondents selected all that applied]

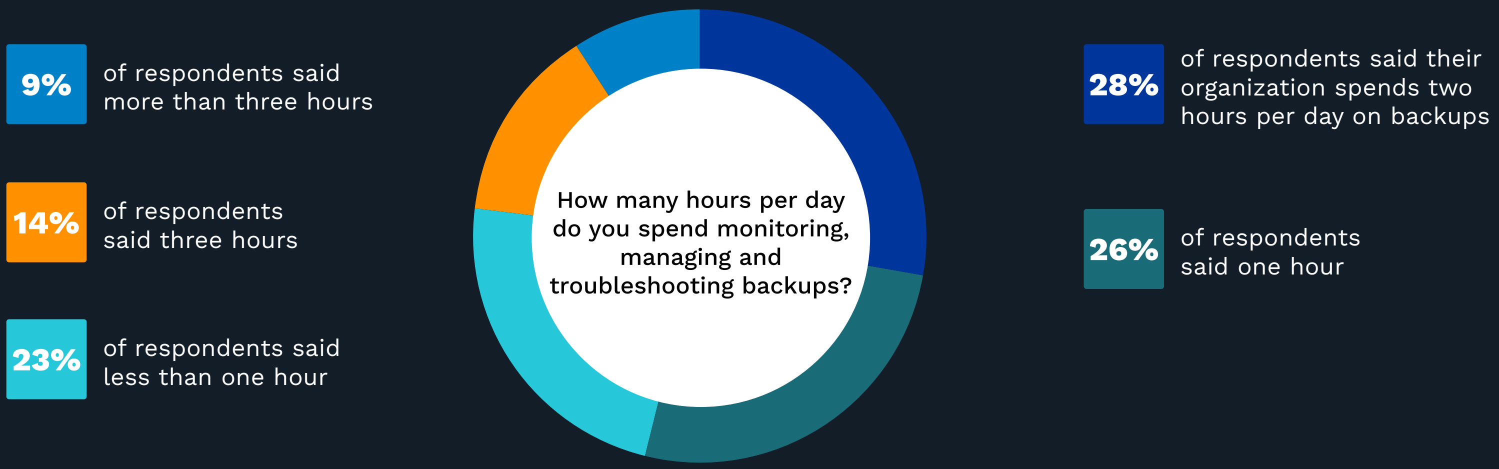
Challenges in backup and recovery

Backup and recovery play a critical role in ensuring data availability and business continuity, yet organizations face significant challenges in managing and optimizing these processes. The State of Backup and Recovery Report 2025 revealed several obstacles hindering effective backup and recovery strategies — from time-intensive management tasks to infrequent testing practices and response inefficiencies.

Time-intensive processes

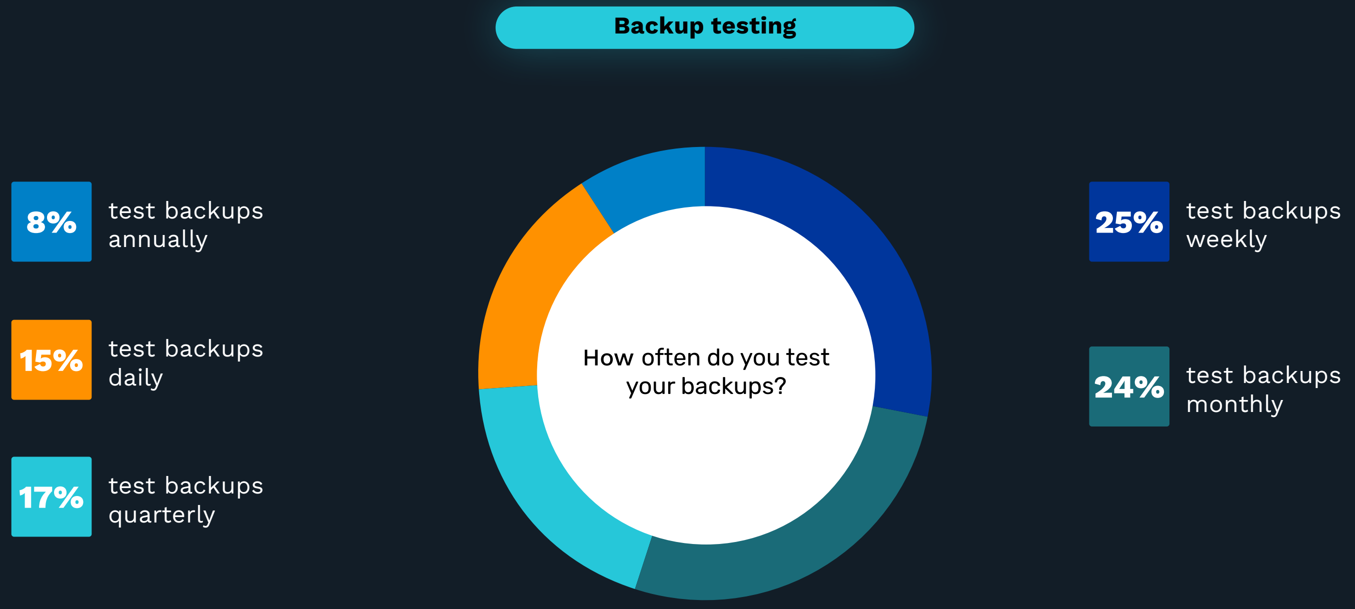
Backup management remains a time-consuming process for IT teams. Over half of organizations surveyed said their IT teams spend more than two hours per day or more than 10 hours per week monitoring, managing and troubleshooting backups. A smaller segment spends less time, with 23% reporting less than one hour and 26% averaging one hour daily.

Time spent on backups



Backup testing practices

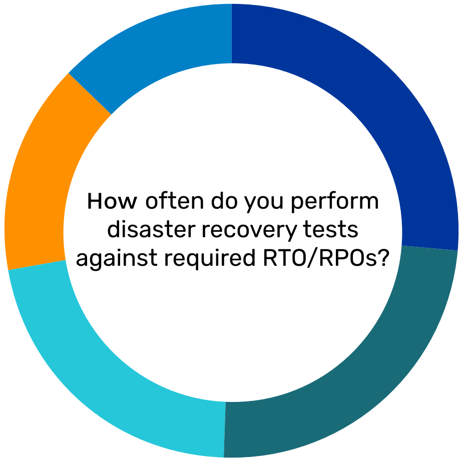
Regularly testing backups is critical to maintaining data integrity and ensuring recovery readiness in the event of a disaster. However, a large majority of organizations surveyed seem to fall short in this area. Only 15% of respondents said their organizations conduct backup tests daily. Around 25% test weekly, and 24% test monthly, suggesting that most businesses operate with a level of risk that could jeopardize recovery in the event of a disaster.



Disaster recovery testing

Disaster recovery (DR) testing is an important factor in meeting recovery time objectives (RTOs) and recovery point objectives (RPOs). However, the frequency of testing varies significantly, with only 11% of businesses performing DR tests daily. About 20% of businesses reported conducting DR tests weekly, with 23% testing on a monthly basis. A significant minority have longer DR testing cycles — 21% quarterly and 13% annually — indicating that these organizations may not be fully prepared to recover from an unexpected downtime event. Additionally, about 12% of businesses test DR capabilities on an ad hoc basis, or do not test at all, leaving them highly vulnerable to prolonged outages.

DR testing



How often do you perform disaster recovery tests against required RTO/RPOs?

11% of respondents said daily

13% of respondents said annually

19% of respondents said weekly

23% of respondents said their organization performs disaster recovery tests monthly

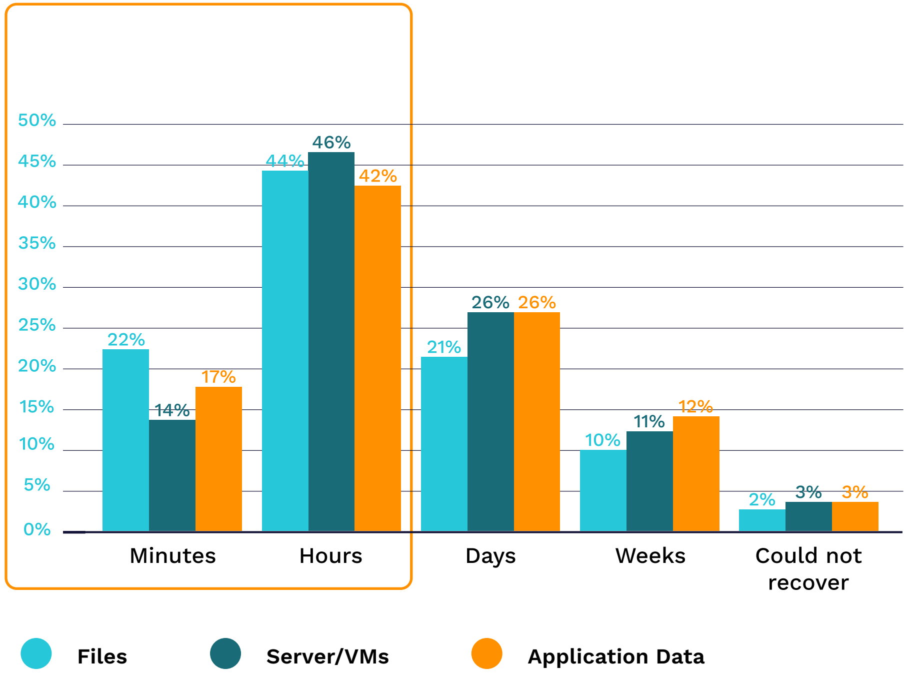
21% of respondents said quarterly

Perception vs. reality

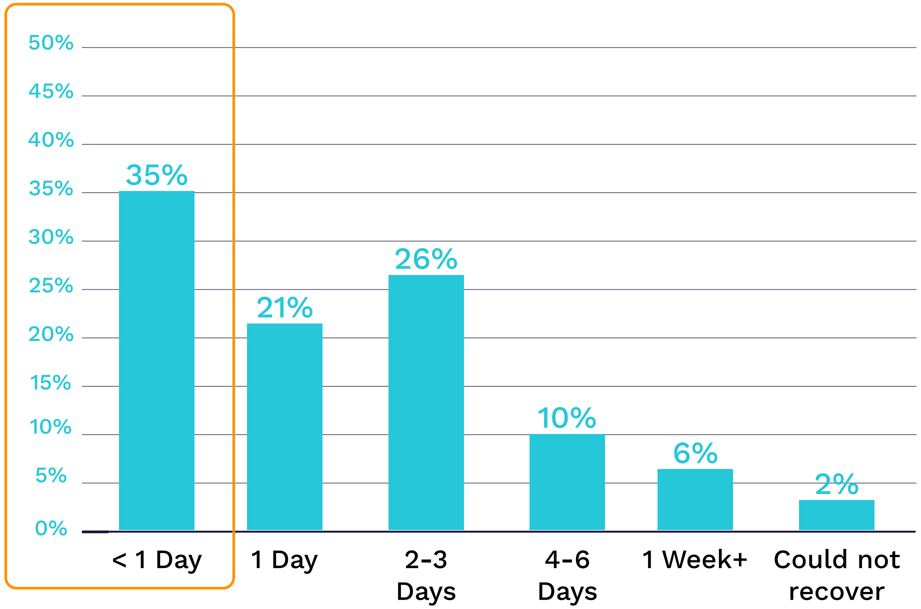
The reality of recovery falls short of respondents' perceived capabilities, revealing a striking gap between expectations and actual outcomes during downtime events. In the survey, **more than 60% respondents believed they could recover in under a day; however, in reality, only 35% could.**

Perception vs. reality

How quickly can you recover files, servers/VMs and applications in the event of an outage or data loss?



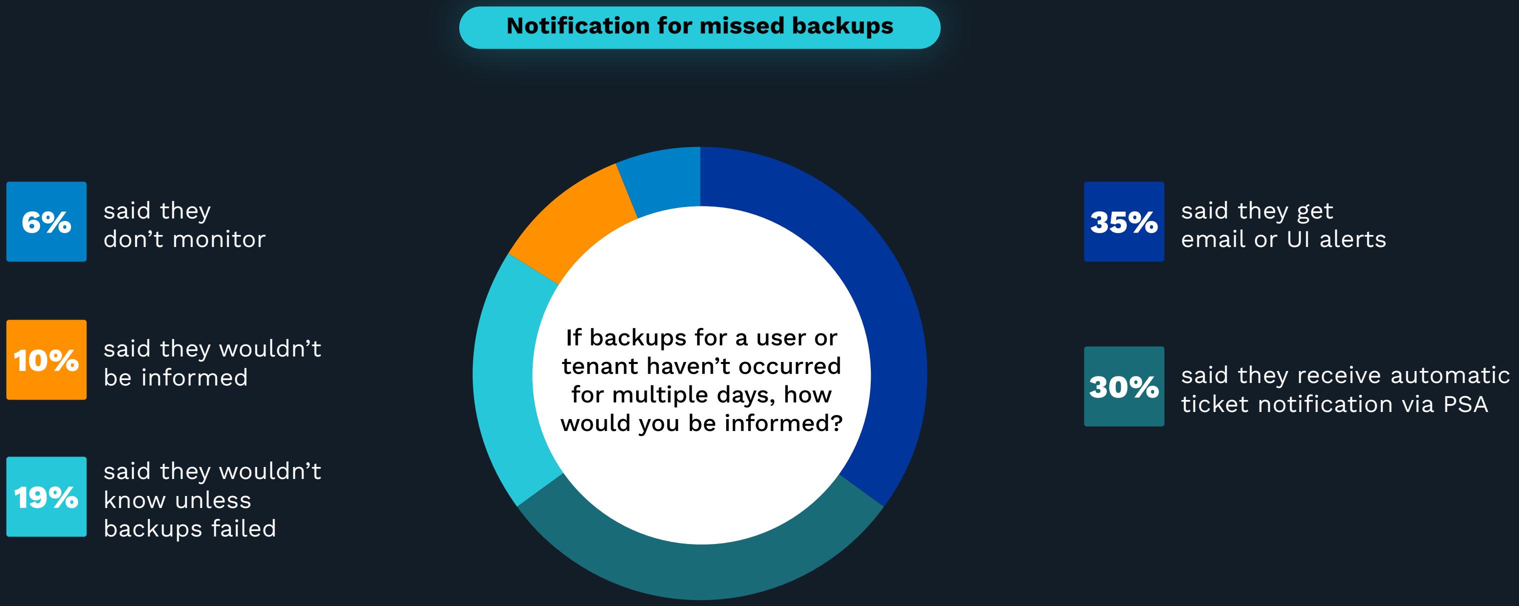
If you experienced an on-premises outage in the last 12 months, what was your total downtime?



One of the key requirements for qualifying for cyber insurance is having an incident response plan that demonstrates an organization's readiness to detect, respond to and recover from cybersecurity incidents. As such, businesses must provide evidence to insurers that they conduct regular tests and are well prepared to meet the RTO goals. Failing to meet this requirement or misrepresentation of capabilities could result in denied claims or reduced payouts.

Responding to missed backups

When backups fail or are missed, timely detection is crucial to minimizing data loss and business disruptions. A majority of respondents (65%) said they rely on email alerts or automatic ticketing systems to identify missed backups. However, 19% of businesses wouldn't know unless backups failed — a critical vulnerability that could lead to data loss and hinder 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, putting their organizations at significant risk.



Most frequently restored data types for SaaS users

SaaS applications facilitate smooth communication and collaboration. They require reliable backup and recovery processes to protect valuable information stored in them. In the survey, email and calendar items emerged as the most commonly restored data types, followed by mail contacts and messaging app data.

Email: Restored daily by 22% of respondents and weekly by 25%.

Calendar items: Restored daily by 17% and weekly by 26%.

Mail contacts and messaging app data follow similar patterns, with nearly 20% restoring them daily and 23% weekly.

Biggest challenges to SaaS and on-premises data protection

A large portion of respondents cited the cost of protecting data in SaaS and on-premises environments as the most significant challenge. Budget constraints and availability of resources often force businesses to compromise on the frequency of testing, the robustness of backup solutions or the scope of their data protection strategies.

On-premises backup and recovery

While cloud adoption grows, on-premises systems continue to play a vital role. From endpoint devices to servers, protecting these systems is essential to minimizing downtime and ensuring the business runs smoothly. However, many businesses face significant challenges in managing on-premises backups and mitigating downtime risks.

Endpoint/PC devices in scope for backup

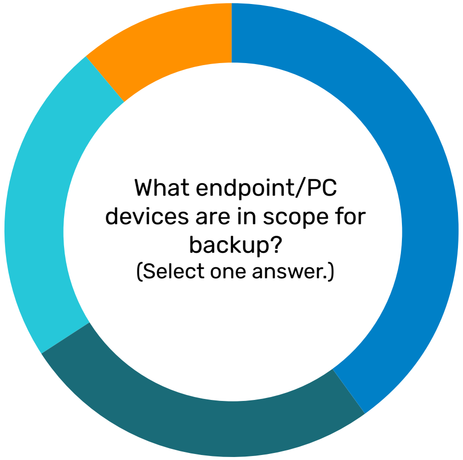
Endpoint devices play a critical role in business operations, particularly with the rise of remote work and hybrid environments. The good news is many organizations are taking endpoint protection seriously. Around 40% of respondents said their organizations plan to back up all endpoint/PC devices, including those used by remote workers, in-office staff and executives. A little over 25% focus only on remote users' devices, while 23% plan to back up only in-office devices. Another 11% limit backups to executive (C-suite) devices. This approach prioritizes high-value or sensitive data but leaves broader organizational assets exposed.

These variations in backup approaches highlight the need for more comprehensive endpoint backup strategies that address the full spectrum of devices in modern workplaces.

Endpoint/PC devices are in scope for backup

11% of respondents said only executive (c-suite) devices are in scope for backup

23% of respondents said only in-office devices are in scope for backup



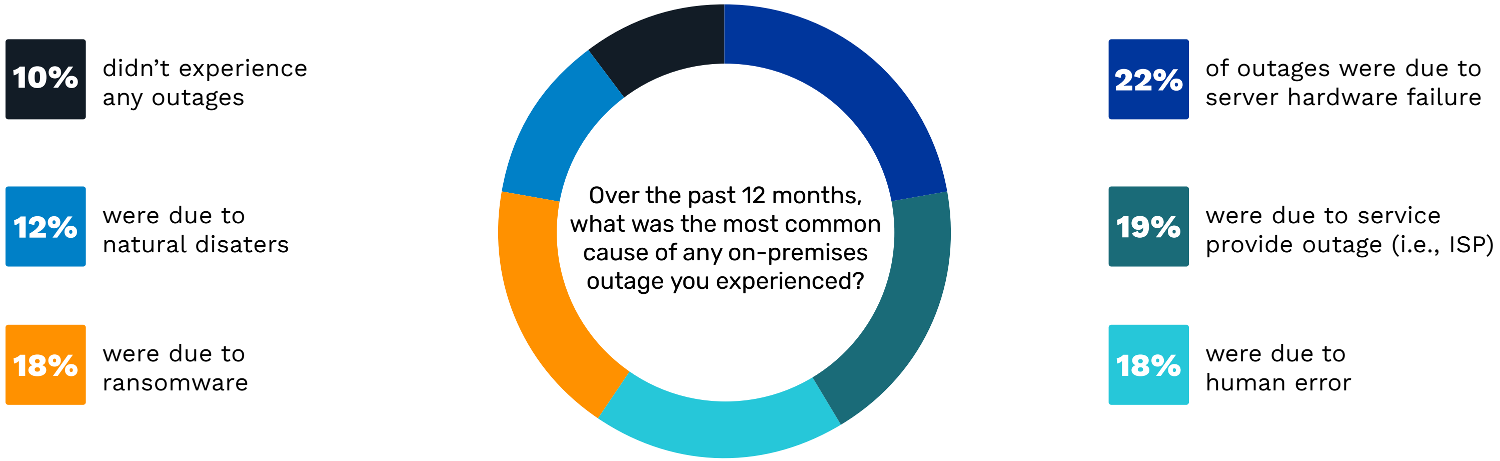
40% of respondents said all users' endpoint/PC devices are in scope for backup

26% of respondents said only remote users' endpoint/PC devices are in scope for backup

Main causes of on-premises outages

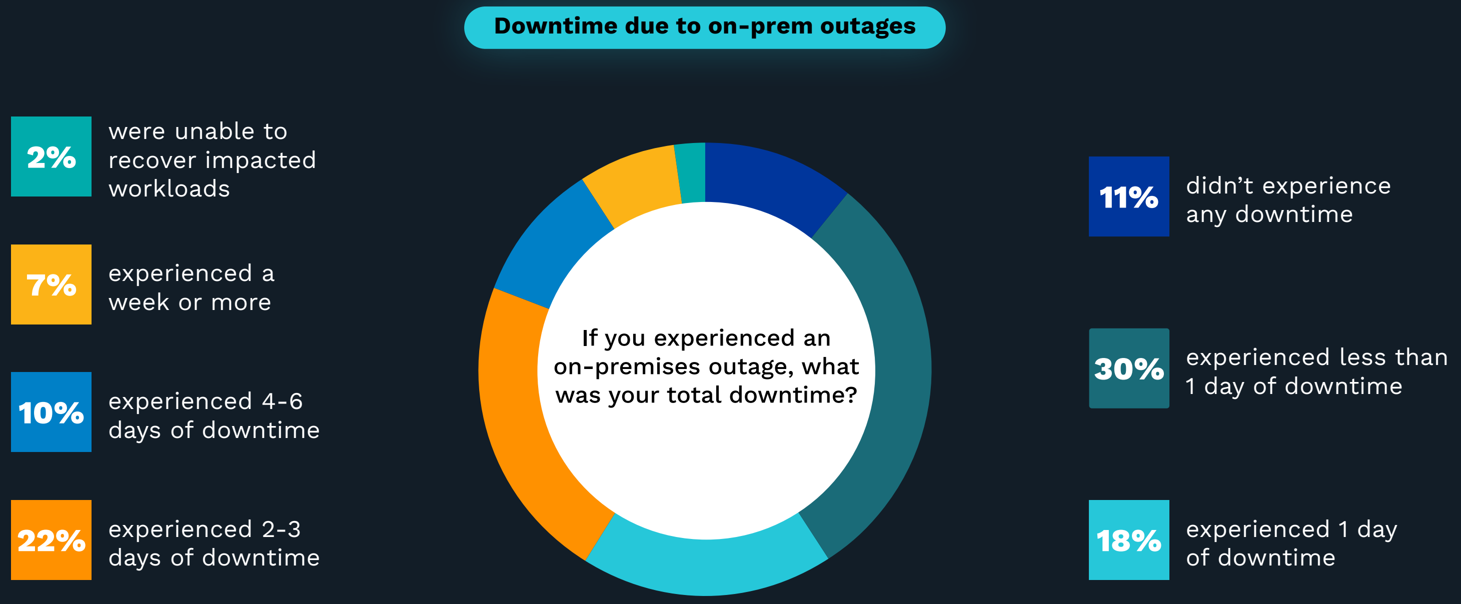
Outages in on-premises environments remain a significant challenge for businesses large and small. For more than 20% of organizations, server hardware failure was the leading cause of on-premises outages over the past year. Service provider outages (e.g., ISP disruptions) accounted for 19% of disruptions. Closely behind are human error and ransomware attacks, each causing 18% of outages. Natural disasters contributed to 12% of outages. Only 10% of respondents reported no outages, a positive indicator for organizations with well-maintained systems or robust redundancies in place.

Most common causes of any on-premises outages



Downtime due to on-premises outages

The impact of on-premises outages is often measured in downtime, which can severely impact productivity and lead to significant financial losses. On the bright side, 30% of businesses reported experiencing less than a day of downtime. However, more than 20% of respondents reported experiencing 2-3 days of downtime. Close to 20% reported a full day of disruption. Only a little over 10% of respondents said their organizations did not experience any downtime. This indicates that only a minority are fully equipped to minimize the impact of outages.



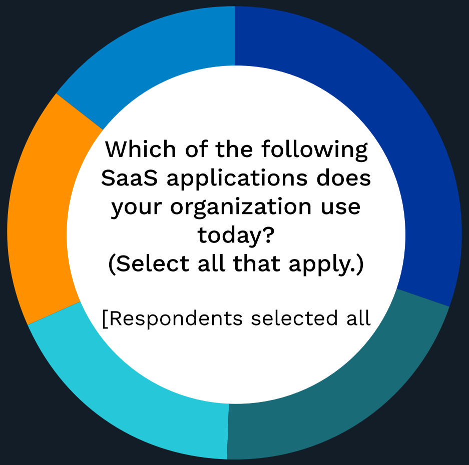
SaaS backup and recovery

As organizations increasingly rely on SaaS applications for day-to-day operations, protecting the data generated and stored within these platforms has become a critical priority. The State of Backup and Recovery Report 2025 reveals key trends, tools, challenges and gaps in how businesses approach SaaS backup and recovery.

Key SaaS applications businesses use today

Microsoft 365 is the most widely used platform, with more than 50% of respondents reporting using the tool for collaboration and productivity. Google Workspace (35%) is another popular choice for email, storage and collaboration. Interestingly, specialized Microsoft products, such as Microsoft 365 Entra ID (31%) and Microsoft 365 Dynamics (30%) are also heavily adopted. Salesforce (25%) rounds out the top five, demonstrating its importance for customer relationship management (CRM) and sales data.

SaaS apps businesses use today

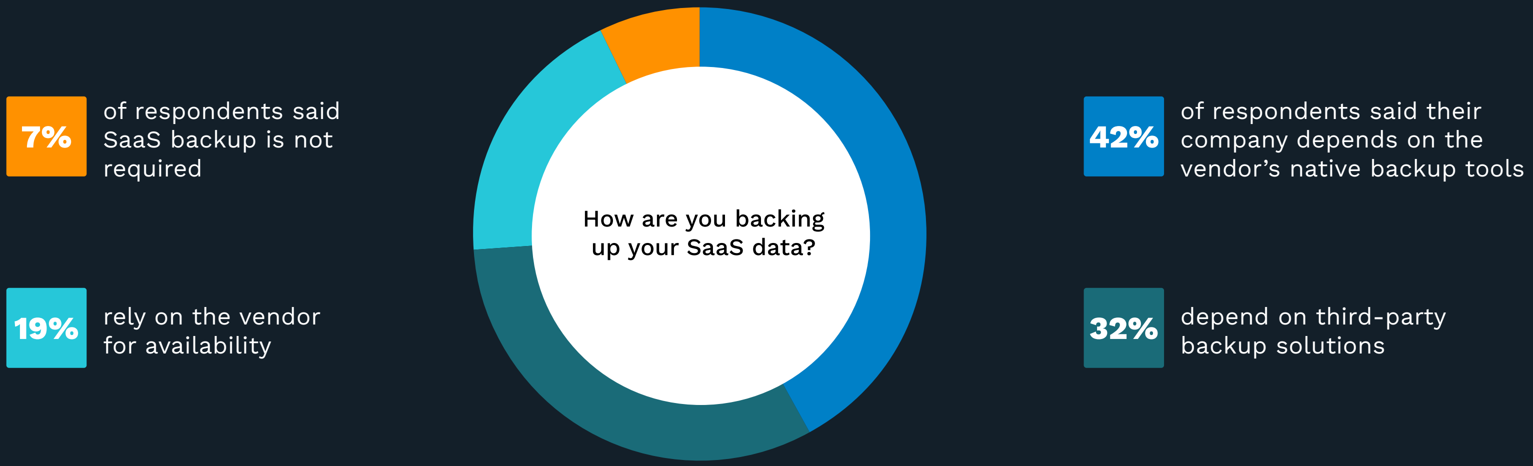


25%	of respondents said their organization uses Salesforce
30%	of respondents said their organization uses Microsoft 365 Dynamics
31%	of respondents said their organization uses Microsoft 365 Entra ID
53%	of respondents said their organization uses Microsoft 365
35%	of respondents said their organization uses Google Workspace

Tools businesses use to back up SaaS data

Today, SaaS platforms hold large volumes of sensitive business information, making data protection in these environments a strategic priority. Over 40% of IT professionals said their organizations use native backup tools provided by the SaaS vendor to back up their cloud data. In contrast, 32% depend on third-party backup tools for enhanced features, flexibility and control over their data. Nearly 20% of businesses rely solely on the vendor's service availability, risking downtime or data loss if the vendor experiences any outages. Additionally, about 10% of respondents believe SaaS backup isn't required, likely due to a potential misunderstanding of the shared responsibility model for cloud data protection.

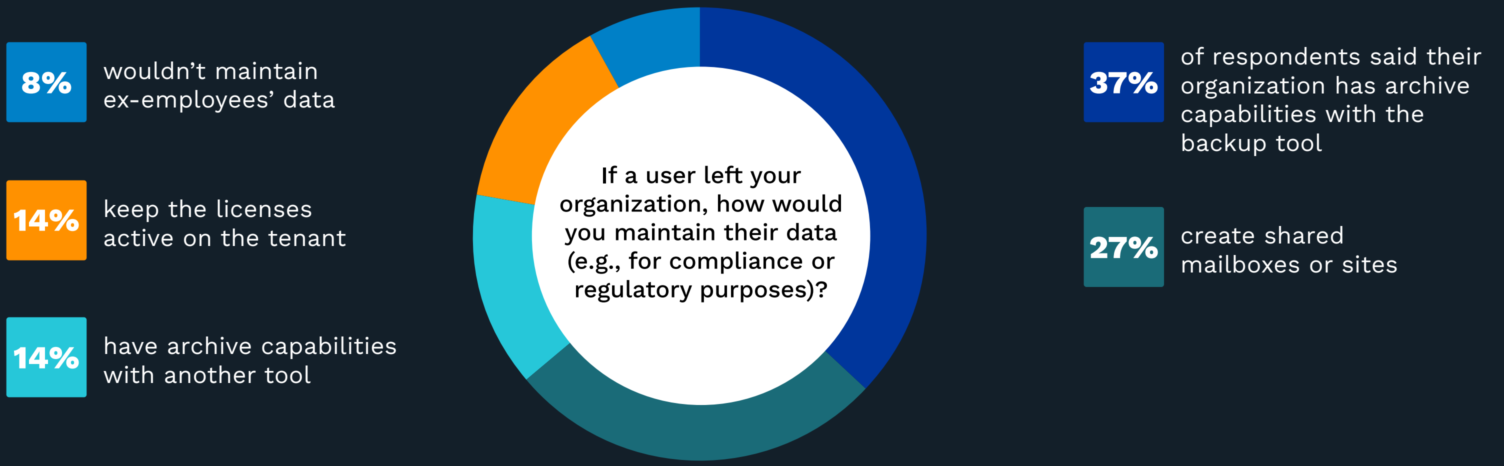
SaaS data backup



SaaS data lifecycle management

Managing the data lifecycle is an ongoing challenge for businesses, particularly when employees leave the organization. About 40% of respondents said their organization uses archive capabilities within their backup tools to retain ex-employee data. Close to 30% create shared mailboxes or sites to maintain access to critical information. A smaller portion uses alternative methods, with 14% leveraging other archive tools and another 14% keeping licenses active for departing employees. Around 10% of IT professionals revealed they don't maintain ex-employees data at all. This can result in businesses losing institutional knowledge and critical records.

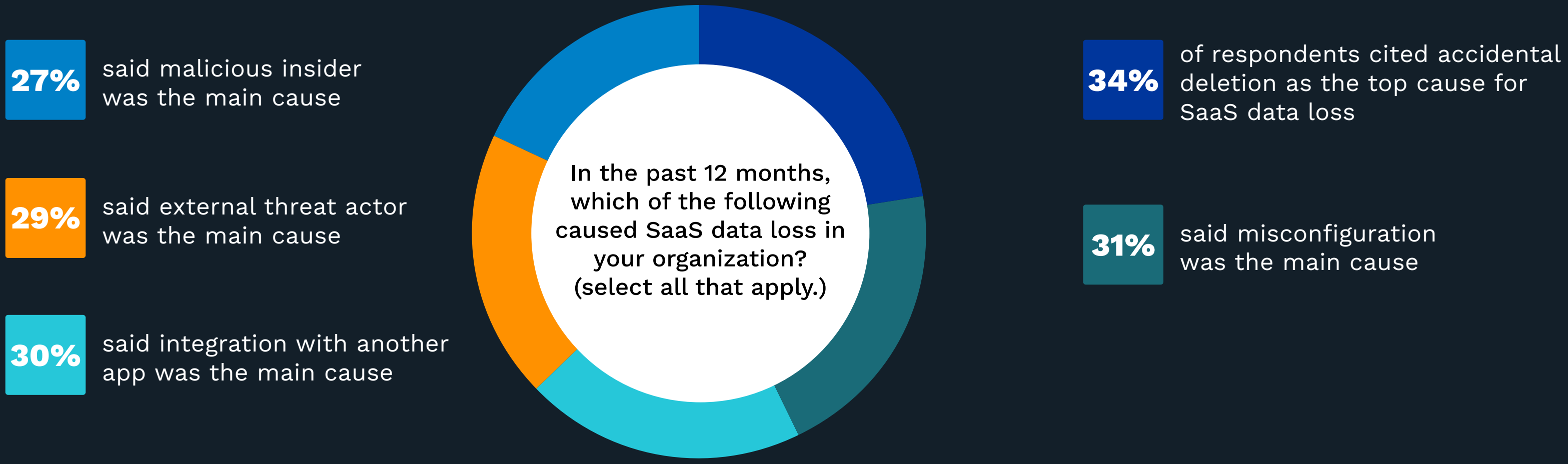
How organizations maintain ex-employees' data



Top causes of SaaS data loss

Data loss in SaaS applications can happen due to several factors. Accidental deletion or human error, cited by 34% of respondents, remains the leading cause of SaaS data loss. Misconfiguration, caused by mistakes during setup or maintenance, was responsible for over 30% of SaaS data loss incidents. Integration issues account for 30% of cases, where conflicts or overwrites caused by third-party application integrations compromise data integrity. External threat actors, such as cyberattacks targeting SaaS platforms, were identified by 29% of respondents as a growing concern. Malicious insiders, including intentional sabotage or theft by employees, pose an additional risk, with 27% of respondents acknowledging this challenge.

Top causes for SaaS data loss

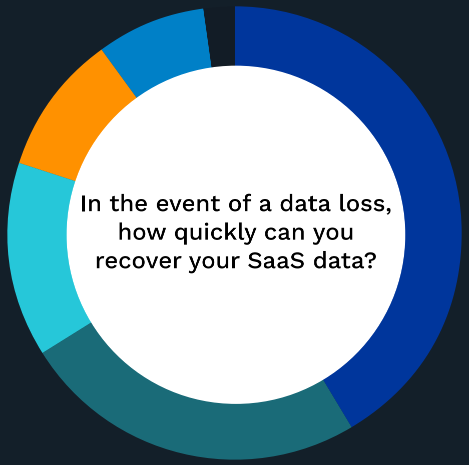


[Respondents selected all that applied]

How quickly can businesses recover lost SaaS data

Quick recovery of lost SaaS data is essential for minimizing downtime and meeting industry regulations. Just over 40% of respondents said their organizations can recover lost data within hours, while 14% reported being able to recover it within minutes. However, recovery times are significantly slower for 35% of organizations, with some requiring days or even weeks to recover. What's more concerning is that 8% of respondents were unsure of their recovery times, and 2% indicated their organization would not be able to recover lost SaaS data at all.

Recovering lost SaaS data



2% said their organization wouldn't be able to recover

8% said they don't know

10% said they can recover within weeks

42% of respondents said their organization can reccover lost SaaS data within hours

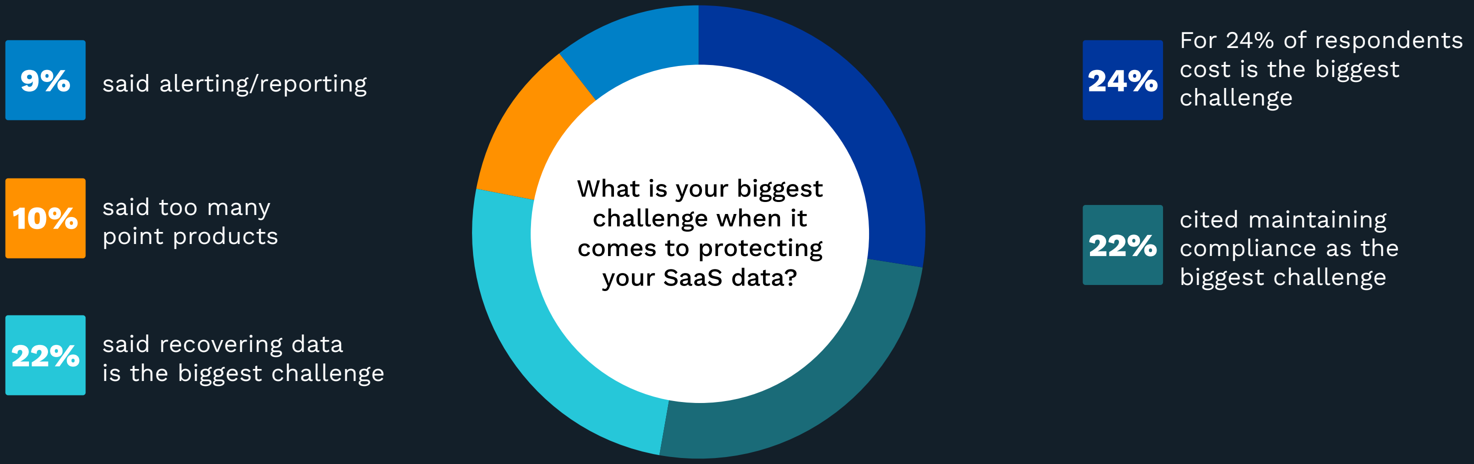
25% said they can recover within days

14% said they can recover within minutes

Biggest challenges to protecting SaaS data

As the volume of data stored in SaaS applications continues to grow, protecting this data has become a critical priority. IT professionals face numerous challenges in ensuring their organization's data remains safe and secure. For nearly 25% of businesses, cost is the biggest challenge when it comes to protecting SaaS data. With industry regulations constantly evolving, 22% of respondents cited maintaining compliance as a major challenge for their organization. An equally pressing issue for 22% of respondents is recovering data. Additionally, 10% of respondents noted that using too many backup tools creates inefficiencies and increases management challenges. About 10% of respondents said alerting and reporting is their organization's biggest challenge, as a lack of actionable insights and visibility from backup systems makes it difficult to identify risks and missed backups.

Biggest challenge for SaaS data protection



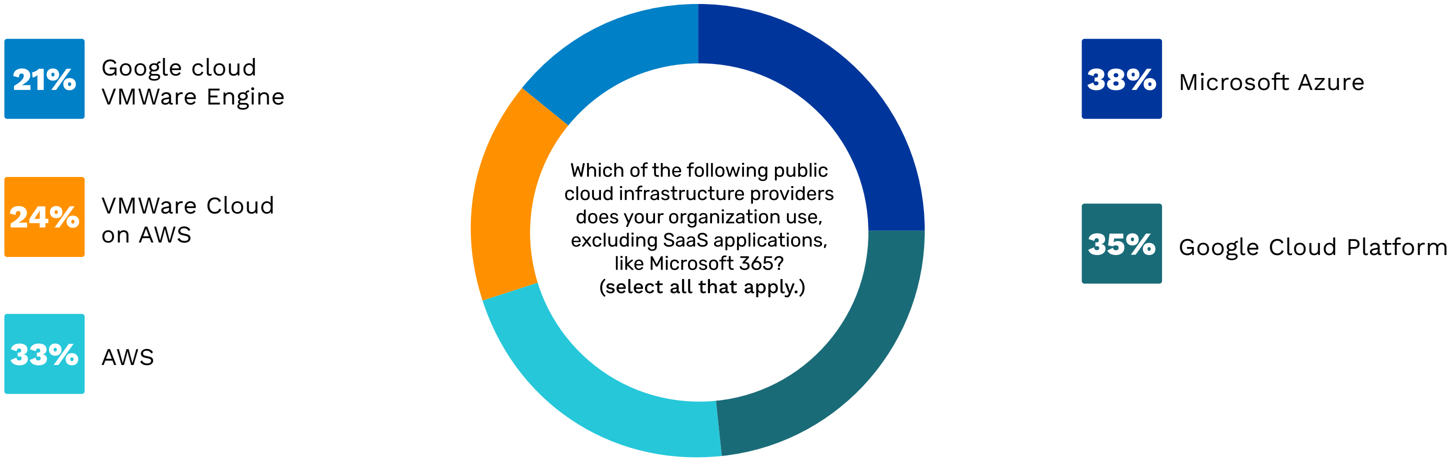
Current state of cloud adoption

Cloud technologies offer greater scalability, flexibility and efficiency, leading to increased adoption in recent years. However, this shift also introduces complexities around migration, cost optimization and data protection. The survey uncovers critical insights into how organizations are navigating their cloud adoption journey.

Top public cloud infrastructure businesses use today

Public cloud platforms are now a critical component of modern IT environments. Nearly 40% of businesses rely on Microsoft Azure for its robust and integrated cloud ecosystem, making it the top public cloud infrastructure businesses use today. Close behind are Google Cloud Platform (35%) and AWS (33%), offering a broad range of services to support diverse workloads. Additionally, platforms like VMware Cloud on AWS (24%) and Google Cloud VMware Engine (21%) are gaining popularity, indicating the growing reliance on hybrid and multicloud strategies to achieve operational resilience and flexibility.

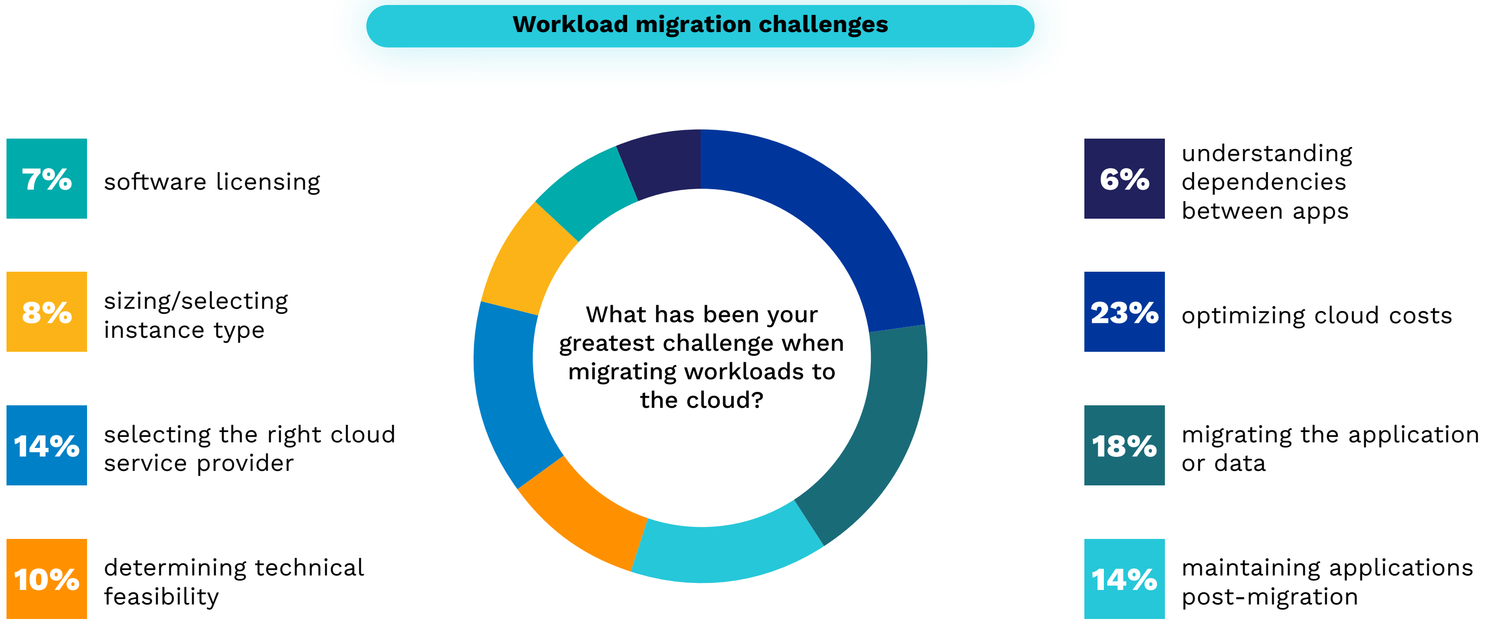
Public cloud infrastructure usage



[Respondents selected all that applied]

Greatest challenges when migrating workloads to the cloud

Migrating workloads to the cloud involves numerous challenges, including technical, financial and operational complexities. Optimizing cloud costs, cited by 23% of respondents, emerged as the greatest challenge when moving workloads 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 businesses report finding the right cloud service provider as a major challenge. Post-migration, maintaining applications in the cloud also poses difficulties for 14% of organizations.



Approach to data migration

Organizations are increasingly adopting a hybrid approach to data migration, balancing on-premises and cloud storage based on their business priorities. About 40% of respondents plan to keep most of their data on-premises, driven by concerns over security, compliance and the handling of sensitive information. On the other hand, 30% have already moved or plan to migrate most of their data to the cloud or SaaS applications. When it comes to the types of data being migrated, non-sensitive analytics data (24%) leads the way due to their high demand for scalable compute resources. Following closely are IoT and edge data (21%), and sales and orders data (21%), which are ideal for cloud environments to enable faster processing and enhanced customer experiences.

However, not all data is migrating to the cloud. Sensitive data, such as intellectual property and research (18%), is often retained on-premises due to concerns about data sovereignty and security. Similarly, customer data such as personal identifiable information (PII) and protected health information (PHI) (18%) is kept in-house to meet strict regulatory requirements, while corporate financial data (17%) remains on-premises to mitigate the risk of breaches and unauthorized access.

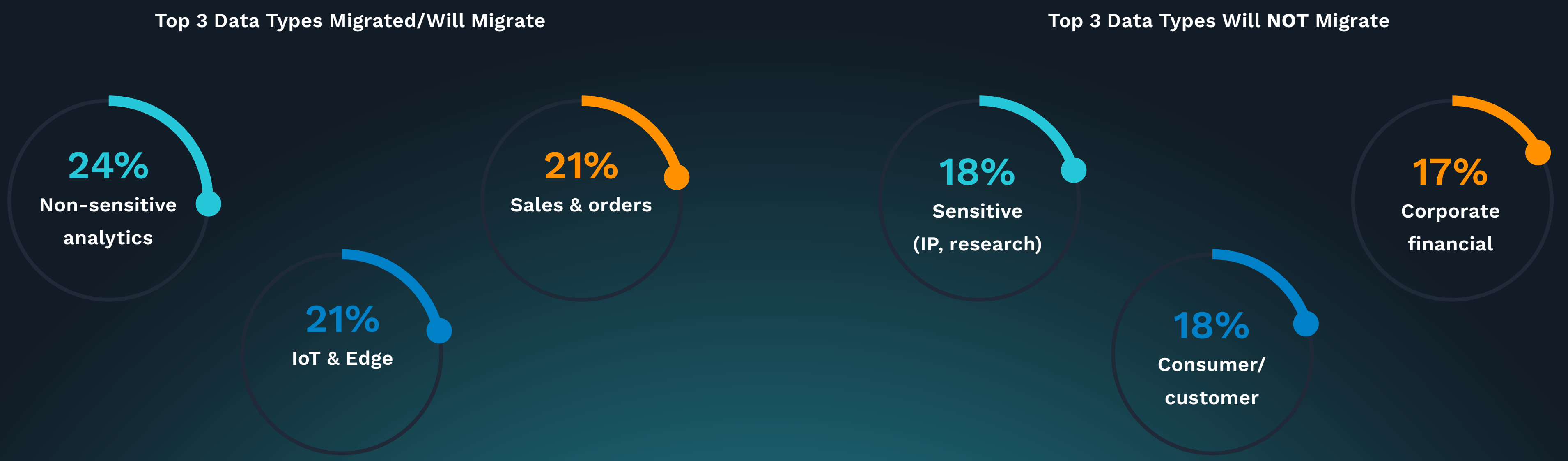
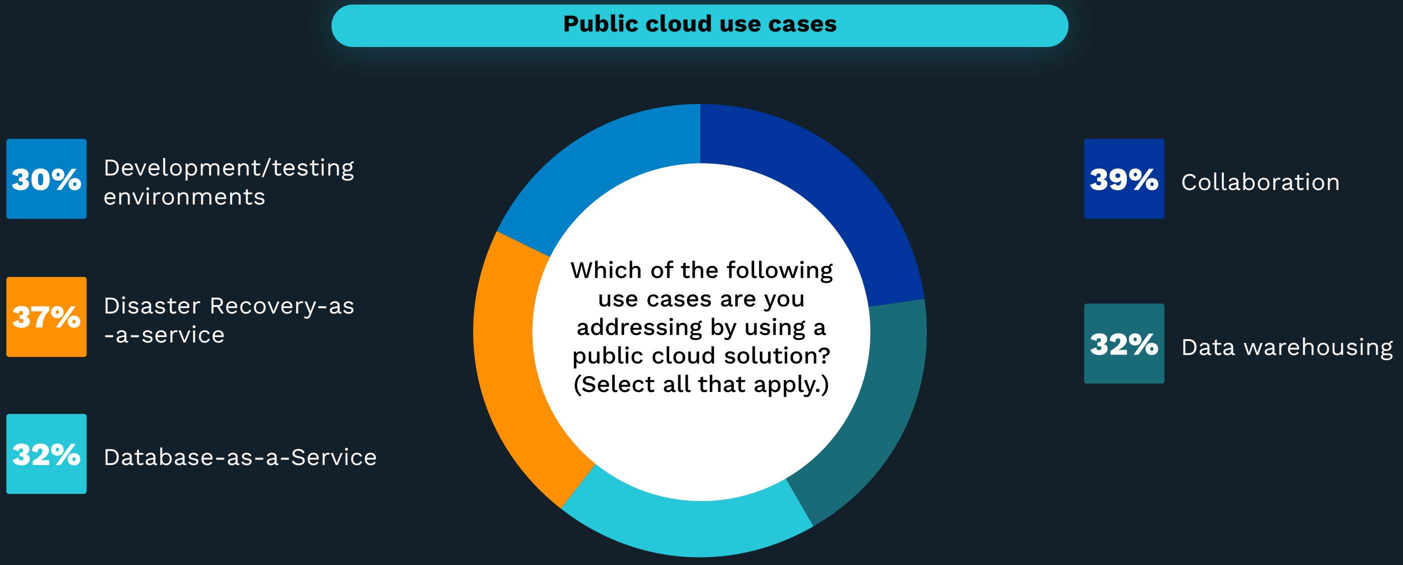


Figure 5. Approach to data migration

Public cloud solutions use cases

Businesses are leveraging public cloud solutions for a variety of use cases that drive collaboration and operational efficiency. About 40% of businesses use collaboration tools to support remote work and boost productivity. Data warehousing and Database-as-a-Service, each cited by 32% of respondents, are key priorities for modernizing data architectures and optimizing data management. Around 40% of businesses use cloud-based Disaster Recovery-as-a-Service to ensure continuity during unexpected disruptions. Development and testing environments (30%) highlight the cloud's ability to accelerate innovation and reduce time to market for new applications and services.

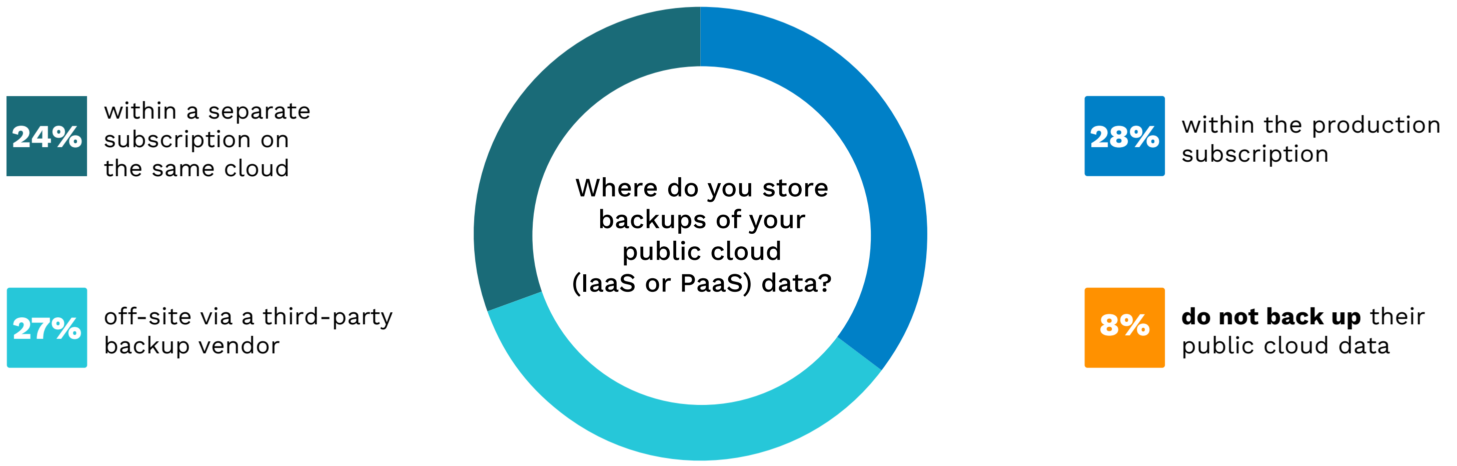


[Respondents selected all that applied]

How businesses store backups of public cloud data

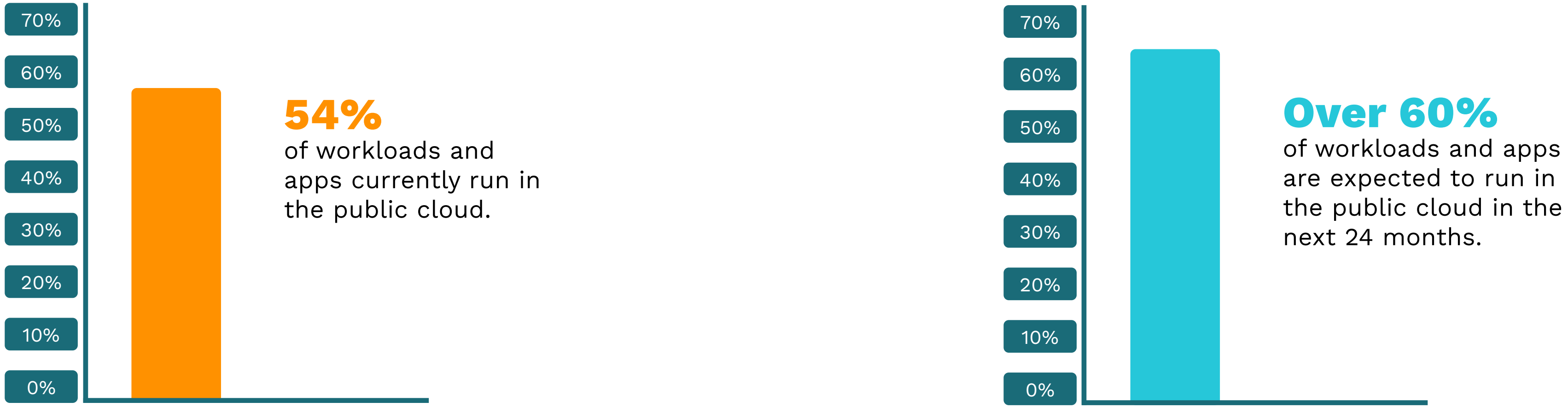
Data protection remains a key concern, and businesses are utilizing diverse strategies to store backups of their public cloud data. Nearly 30% of respondents said their organizations store backups within the production subscription, a choice that offers simplicity but raises concerns about the risks of single-point failure. Close to 30% of businesses opt for off-site backups through third-party vendors for redundancy and additional protection. Another 24% maintain backups in a separate subscription within the same cloud, providing some level of isolation without depending on external providers. However, an alarming 8% of businesses do not back up their public cloud data at all, leaving themselves highly vulnerable to potential data loss.

Public cloud data backup



Workloads and applications in the public cloud

The ongoing trend toward cloud-first strategies is gaining momentum. Over 50% of workloads and applications currently run in the public cloud and the volume of workloads and applications in the cloud is expected to increase to over 60% within the next 24 months.



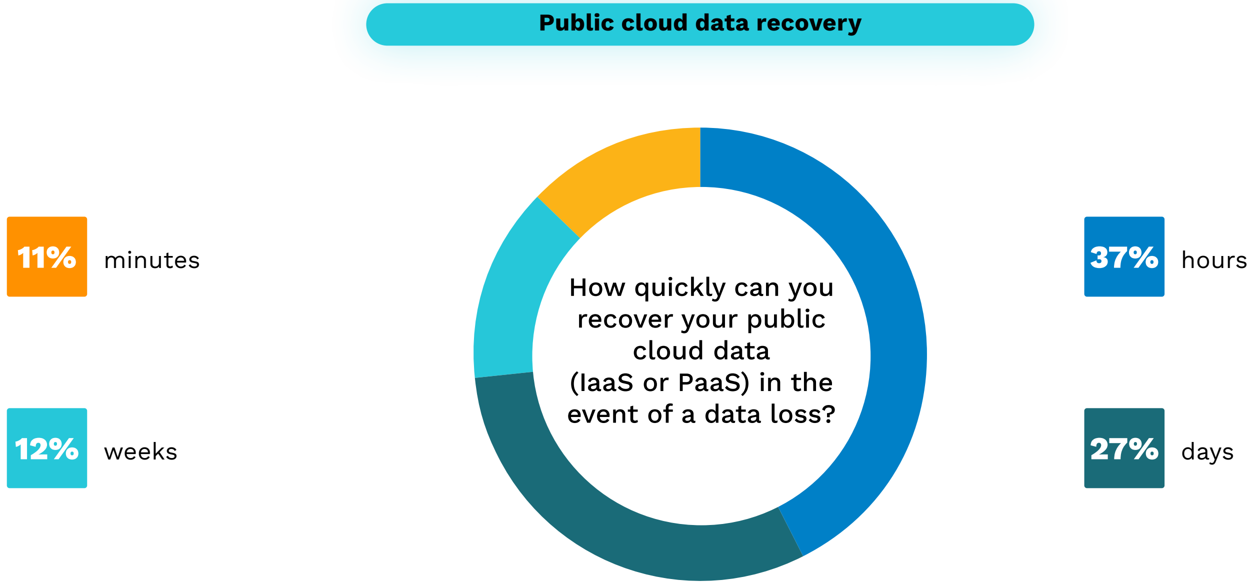
54%
of workloads and apps currently run in the public cloud.

Over 60%
of workloads and apps are expected to run in the public cloud in the next 24 months.

Figure 6. Workloads and applications in public clouds

Recovering lost public cloud data

Our survey revealed varying levels of preparedness among businesses for data recovery. About 40% of respondents indicated that their organizations could recover lost public cloud data within hours, while 11% reported being able to recover within minutes. However, around 30% of respondents said their organizations would require days to recover, and 10% would need weeks, potentially leading to significant operational disruptions and prolonged downtime.



Recommendations and best practices

As data protection becomes more complex and critical in today's hybrid IT environments, businesses must adopt robust strategies and tools to safeguard their data across on-premises, cloud and SaaS platforms. Below are actionable recommendations and best practices to address the challenges highlighted in the survey:

Strategic planning

A comprehensive data protection strategy is critical for ensuring the reliability and efficacy of backup and recovery processes. Businesses should:

Assess and prioritize workloads: Identify business-critical data and applications to ensure they are adequately protected and recoverable.

Set clear RTOs and RPOs: Ensure the RTO and RPO goals align with business continuity plans to minimize downtime and data loss during disruptions.

Standardize processes: Implement consistent backup policies across on-premises, cloud and SaaS environments to reduce gaps and redundancies.

Plan for scalability: As data grows, ensure the strategy can evolve to accommodate new technologies, workloads and storage needs.

Review and update policies: Strategic planning also requires businesses to regularly review and update their data protection policies to reflect changes in technology, regulations and organizational priorities.

Enhance the security of backup systems

Cybercriminals are increasingly targeting backup systems to disrupt recovery efforts and maximize ransomware effectiveness. To fortify backup systems, businesses should:

Implement multilayered security measures: Encrypt data at rest and in transit, enforce strong access controls and enable multifactor authentication (MFA) for backup tools.

Protect against ransomware: Use immutable backups and air-gapped storage to ensure data integrity in the event of an attack.

Regularly audit systems: Conduct periodic security assessments of backup infrastructure to identify and address vulnerabilities.

Train staff: Equip employees with the knowledge to identify potential threats, mitigate risks and adhere to security best practices.

Leverage advanced technologies

Modernizing backup and recovery processes with advanced technologies and scalable solutions can improve efficiency and reliability. Businesses should:

Utilize behavioral analytics and machine learning (ML): Leverage smart, intelligent tools to predict failures, optimize backup schedules and automate recovery processes for improved efficiency.

Adopt cloud-native solutions: Take advantage of scalable, purpose-built cloud backup solutions that align with multicloud and hybrid strategies.

Enable real-time monitoring: Use advanced backup and DR solutions that provide real-time visibility into backup performance and alert IT teams to potential issues before they escalate.

Automate testing: Automate testing for backups and disaster recovery to validate data integrity, gain recovery confidence and ensure adherence to RTOs and RPOs.

Vendor partnerships

Selecting the right backup and disaster recovery vendor is critical since it can significantly impact the effectiveness of an organization's data protection strategy. To select the right partners:

Gauge vendor capabilities: Assess providers based on their ability to integrate solutions to support on-premises, cloud and SaaS environments.

Evaluate DR features: Ensure the solutions they offer provide advanced backup and DR capabilities, including automation, failover options and data replication across regions.

Look for scalability: Choose vendors with solutions that can grow alongside your organization's data and workload needs.

Examine support and compliance: Partner with vendors who provide technical support 24/7/365 and meet industry-specific compliance standards.

Key takeaways

As businesses 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 underpin the urgent need for robust backup and recovery strategies to confidently address current and future challenges.

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 already run in the public cloud, and this is expected to rise to 60% in 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 gaps in performance, reliability and ease of use.

Human error and misconfiguration are top risks: Accidental deletion, integration errors and misconfigurations remain leading causes of data loss in SaaS and on-premises environments.

Security and costs are top challenges: Securing backup systems and managing costs were consistently cited as major pain points for businesses.

The findings of this report send a clear message: data protection requires continuous investment, innovation and vigilance. As data volumes grow and threats evolve, businesses that prioritize data protection will not only safeguard their critical assets but also unlock the confidence to innovate and thrive.

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 to discover how our industry-leading solutions protect your data no matter where it lives.

Redefine data backup and recovery with Unitrends

Don't Leave Your Data's Fate to Chance! Protect what matters most with seamless backup and recovery solutions from Unitrends. Keep data safe, secure and always recoverable.

SCHEDULE A DEMO

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over 30 years of focusing on backup and recovery with next-generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

UNITRENDS
A Kaseya COMPANY

[1] https://www.corelogic.uk/news/data-is-the-new-oil-so-to-speak/#:~:text=In%202006%2C%20British%20mathematician%20Clive,it%20cannot%20really%20be%20used.