eBook

datto
A Kaseya COMPANY

The State of BCDR 2025: Future-Proof Your Data Protection Strategies

Contents

Executive summary

Data is the backbone of every business, driving innovation, decision-making and customer engagement. Whether you're an MSP protecting client environments or an internal IT professional securing your organization's infrastructure, ensuring data availability and security is both a critical responsibility and a strategic advantage.

Without a robust business continuity and disaster recovery (BCDR) strategy, organizations face the risk of data loss, workflow disruptions, reputation damage and costly consequences such as fines, lawsuits and operational downtime. Yet, in an era of rising cyberthreats, hybrid workforces and accelerated cloud adoption, many organizations still struggle with gaps in their data protection strategies. For MSPs, this represents an opportunity to strengthen service offerings and reinforce their role as trusted advisors. For internal IT teams, it underscores the urgent need to evaluate existing backup and recovery strategies to ensure business resilience.

To uncover market gaps and opportunities in backup and recovery, we surveyed over 3,000 IT professionals, security experts and administrators worldwide. Our findings provide IT pros and MSPs with critical insights into the biggest pain points, emerging trends and areas for improvement including:

Shortcomings in native cloud backup solutions that leave businesses vulnerable due to limited disaster recovery capabilities.

Widespread dissatisfaction with existing backup solutions, driving demand for more effective alternatives.

A concerning gap between expected versus actual recovery times, highlighting opportunities to enhance disaster recovery strategies.

A lack of confidence among organizations in their backup and recovery preparedness, reinforcing the need for expert guidance and proactive solutions.

IT teams are spending over 10 hours per week managing backups, emphasizing the need for automation and efficiency-driven solutions.

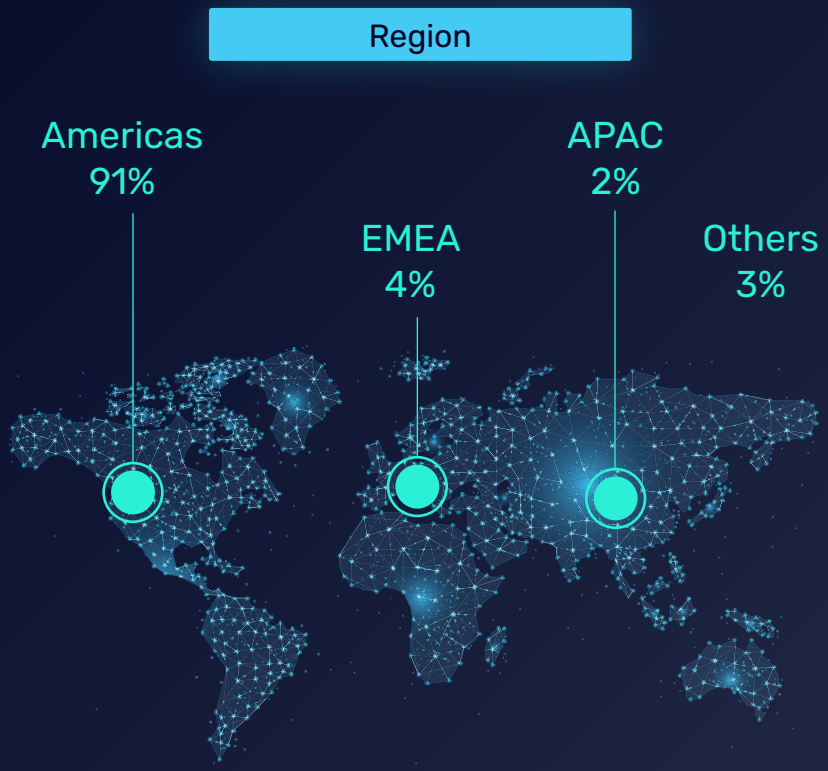
For MSPs, these insights provide a roadmap to closing clients' data protection gaps, refining service offerings and unlocking new revenue opportunities. For internal IT teams, they offer a benchmark for evaluating and improving backup and disaster recovery strategies. Whether you're positioning yourself as a strategic partner in BCDR or fortifying your own organization's resilience, this report offers actionable takeaways to help you stay ahead in 2025 and beyond.

Demographics

The State of BCDR 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

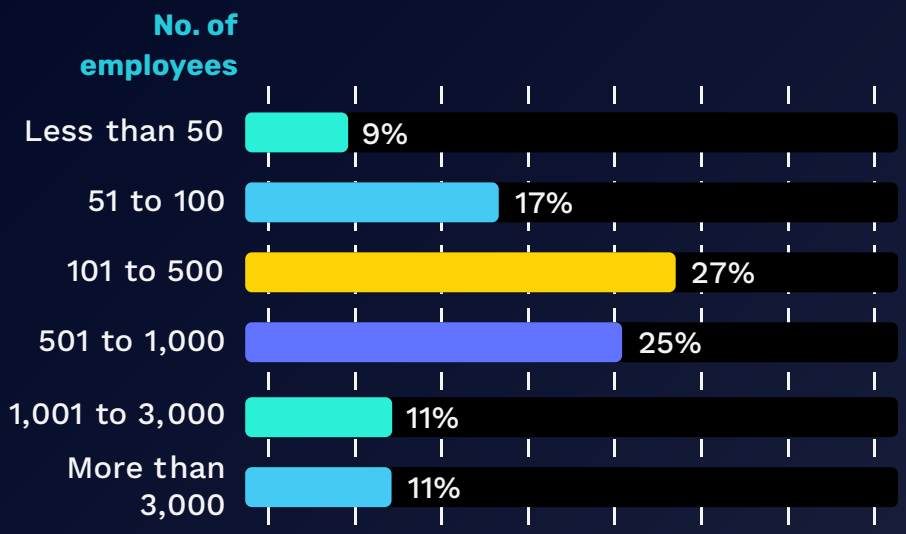
The majority of respondents are from the Americas (91%), reflecting strong engagement from North and South America. Contributions from EMEA (4%), APAC (2%) and other regions (3%) add valuable perspectives from businesses operating in varied economic and regulatory environments.



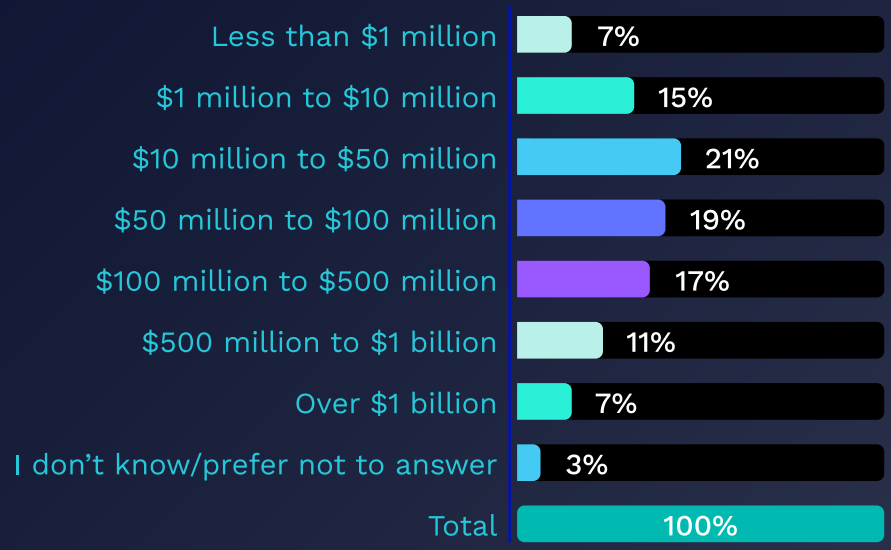
Company size and revenue

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.

Company size



Annual revenue - 2024



Industry trends shaping data protection strategies

As businesses evolve, so do 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.**

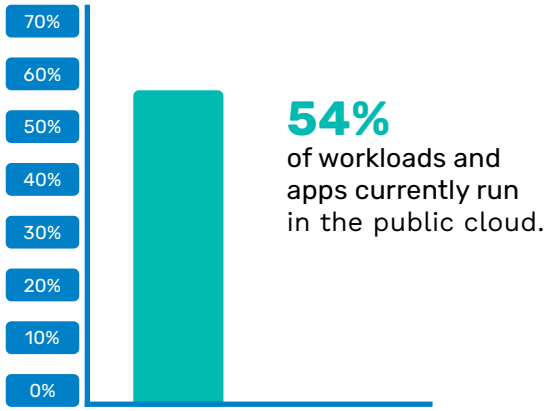
Nearly half of the organizations surveyed back up copies to the public cloud using platforms like Azure Blob, further highlighting the critical role of the cloud in modern data protection strategies.

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.

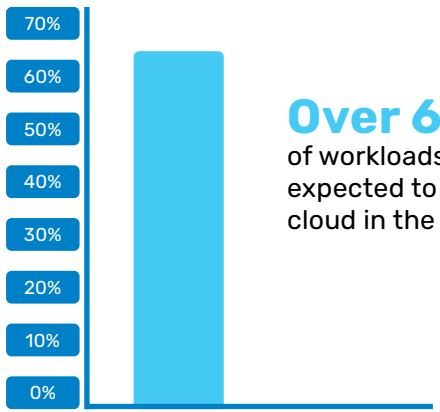
While nearly 90% of respondents said they use native data protection tools for Azure, many are unprepared for major disasters, **with 60% of these setups lacking true disaster recovery capabilities for their Azure virtual machines (VMs).**

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



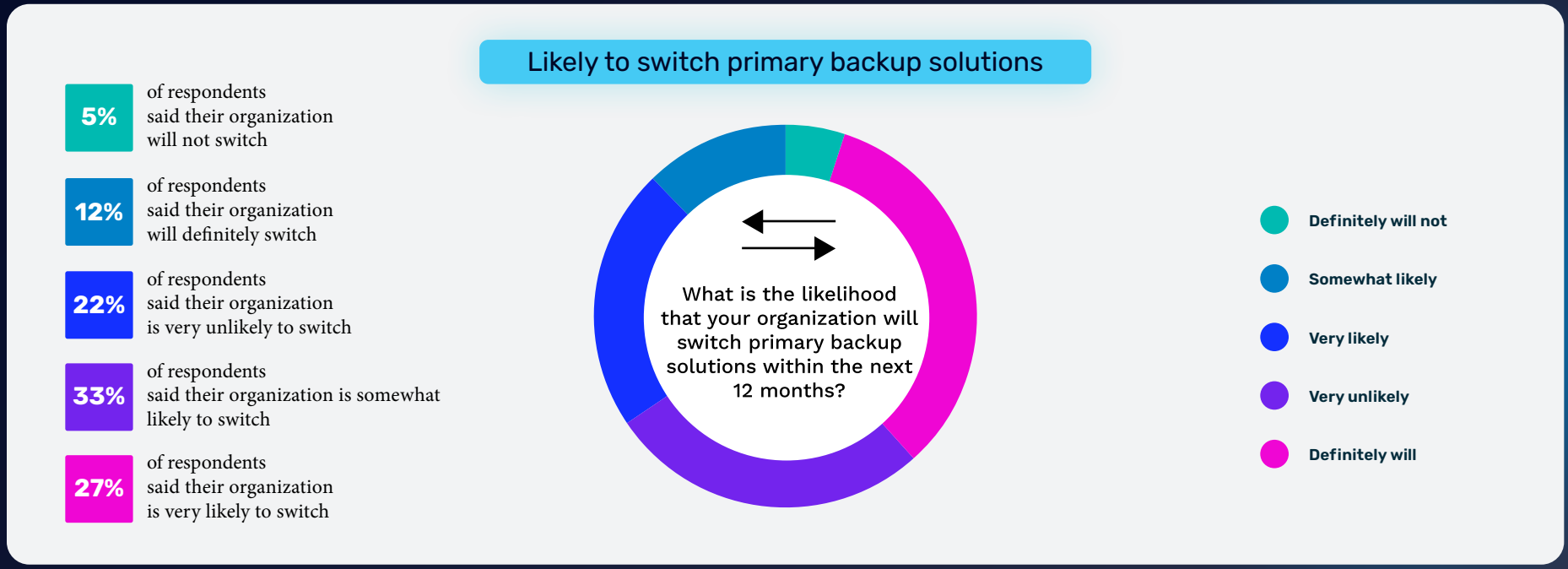
Over 60%
of workloads and apps are expected to run in the public cloud in the next 24 months.

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

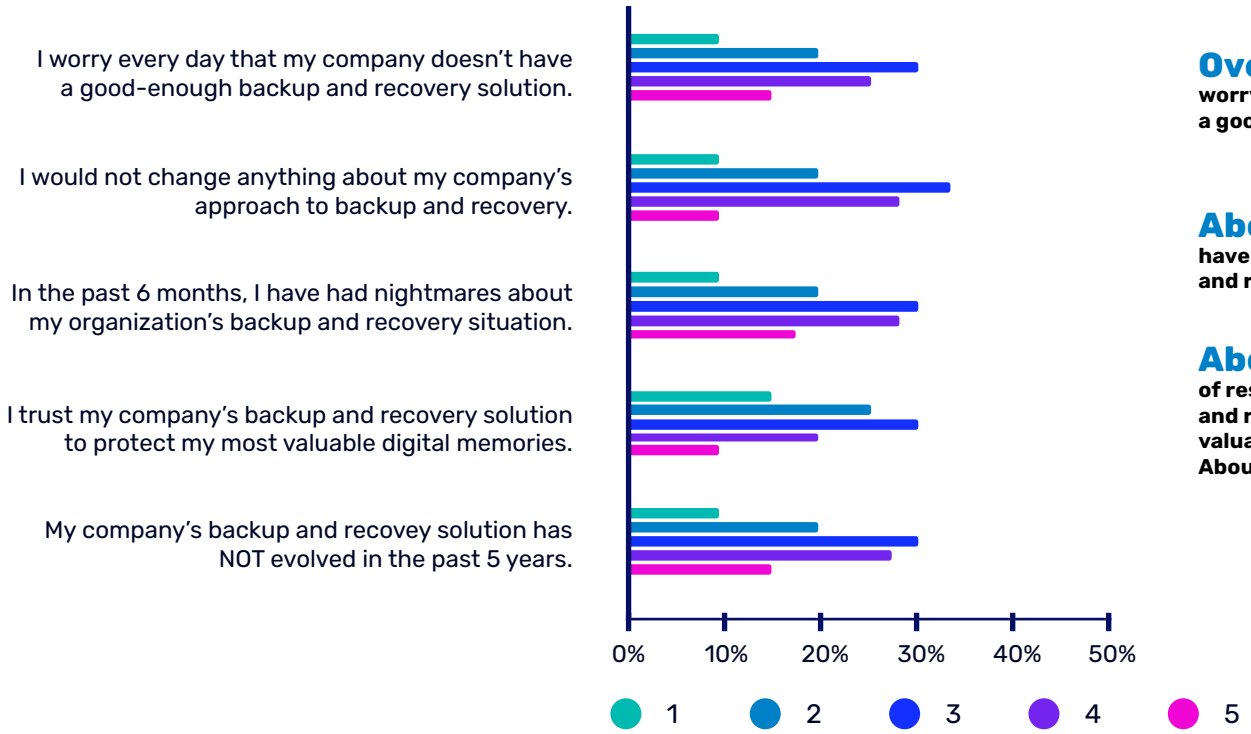
This trend emphasizes the need for vendors to address pain points, such as cost, ease of use and disaster recovery capabilities.



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.

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.

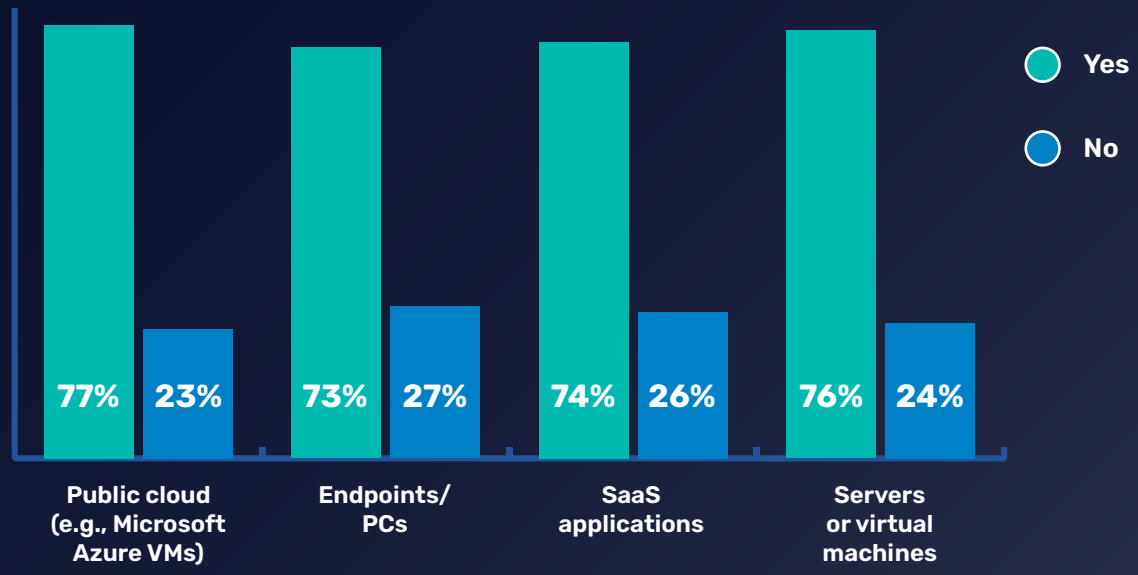
Security of backup systems

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?



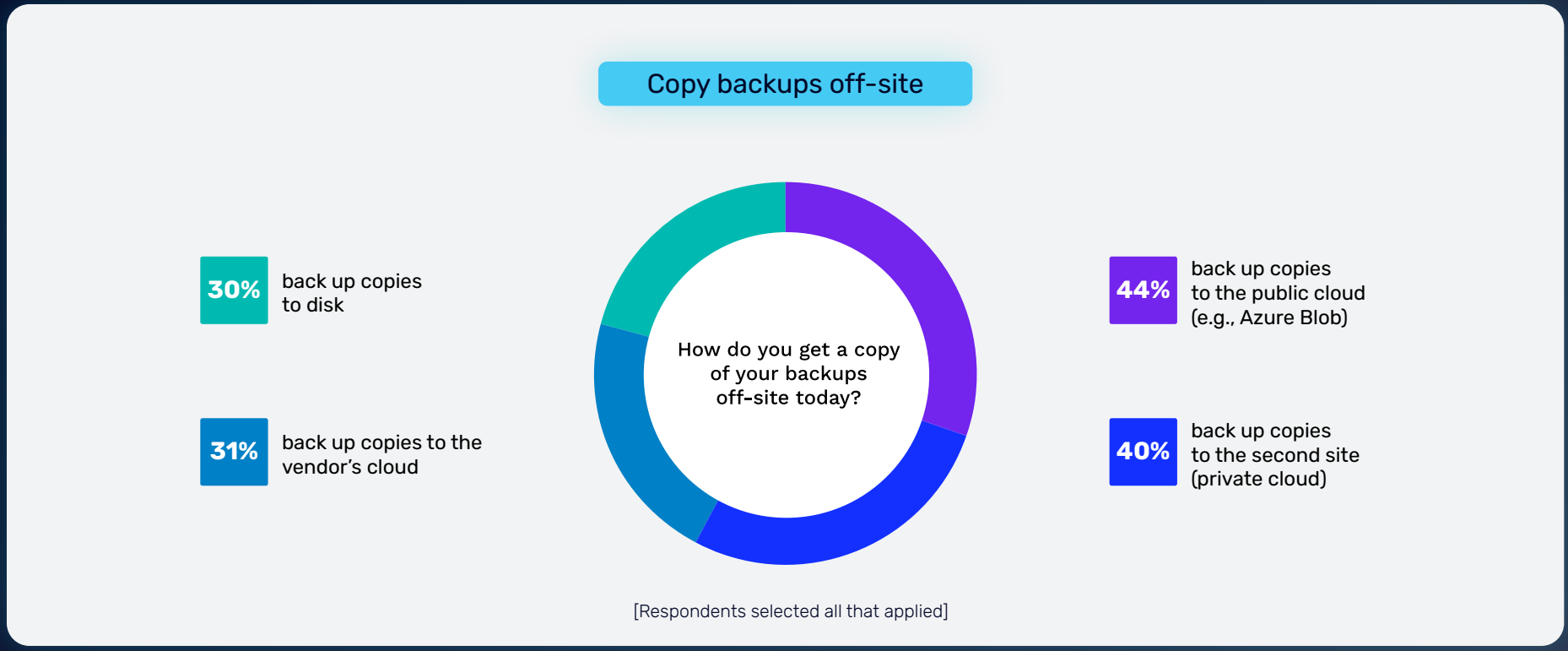
How businesses store sensitive credentials

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.

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.

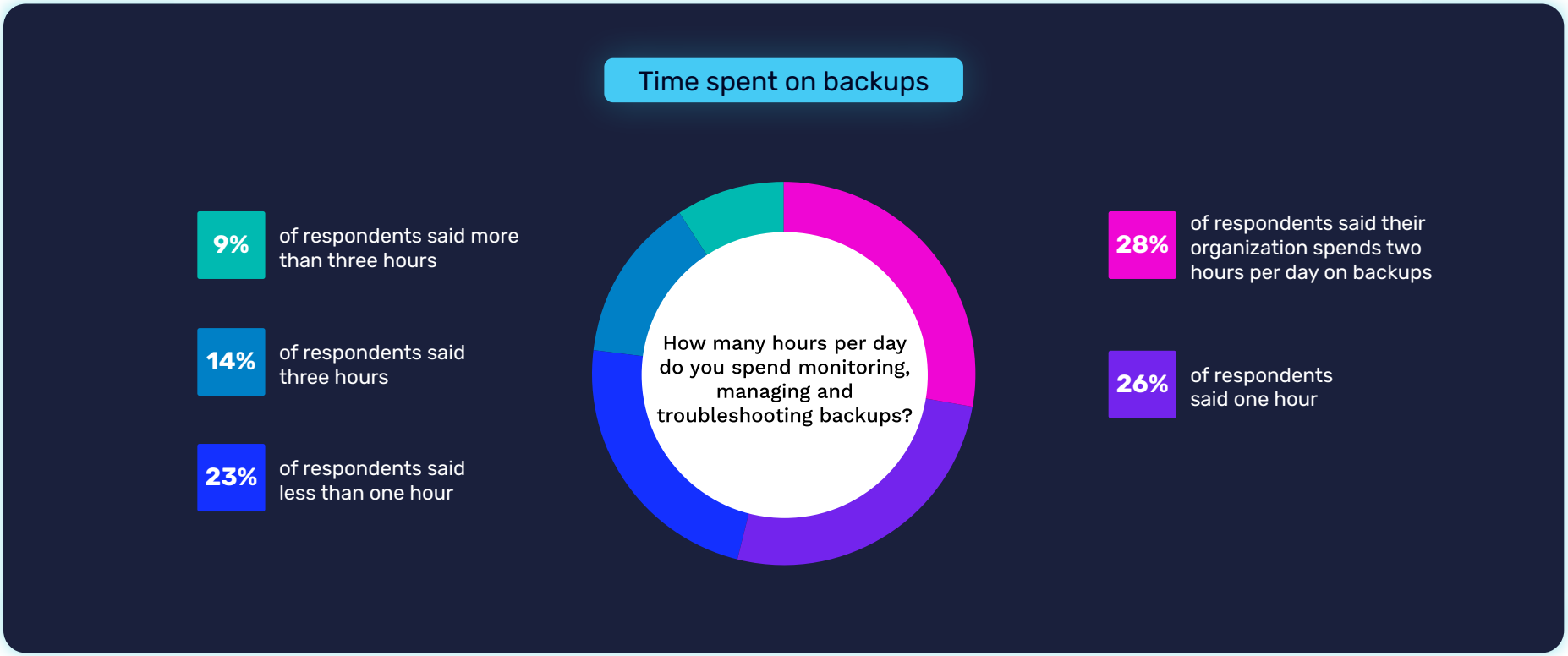


Challenges in backup and recovery

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 report revealed several obstacles hindering effective backup and recovery strategies — from time-intensive management tasks to infrequent testing practices and response inefficiencies.

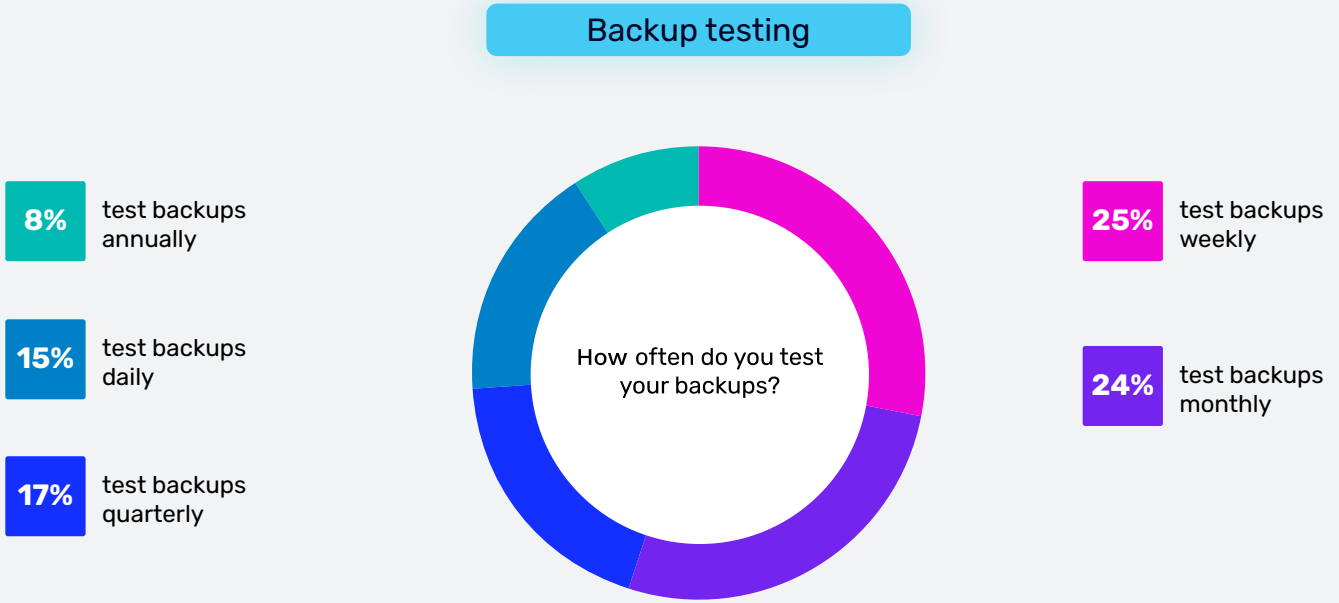
Time-intensive processes

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. In the years since our 2022 survey, the time spent managing backups has steadily increased. The cohort spending less than one hour per day dropped from 39% in 2022 to 23% in 2024, while the cohort spending three hours or more daily skyrocketed from 5% in 2022 to 23% in 2024.



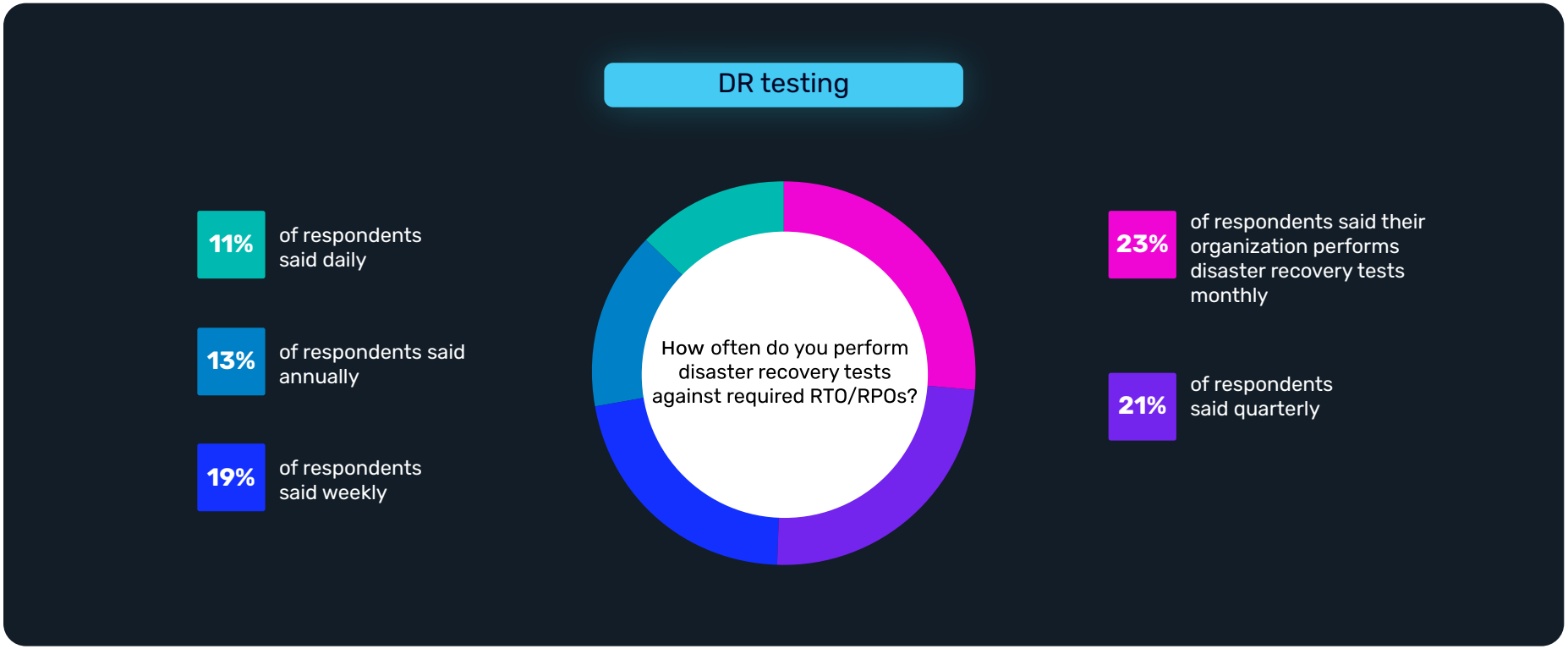
Backup testing practices

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.

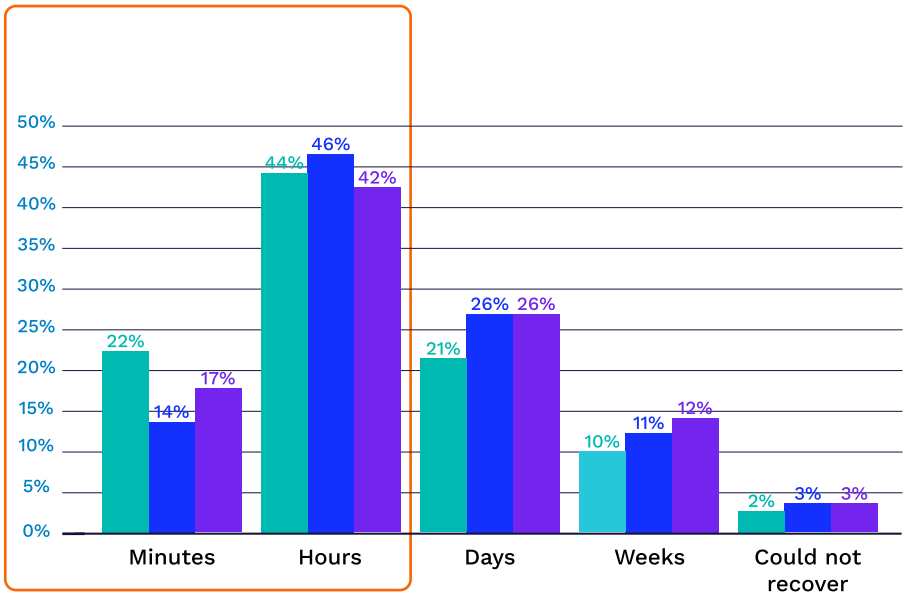


Perception vs. reality

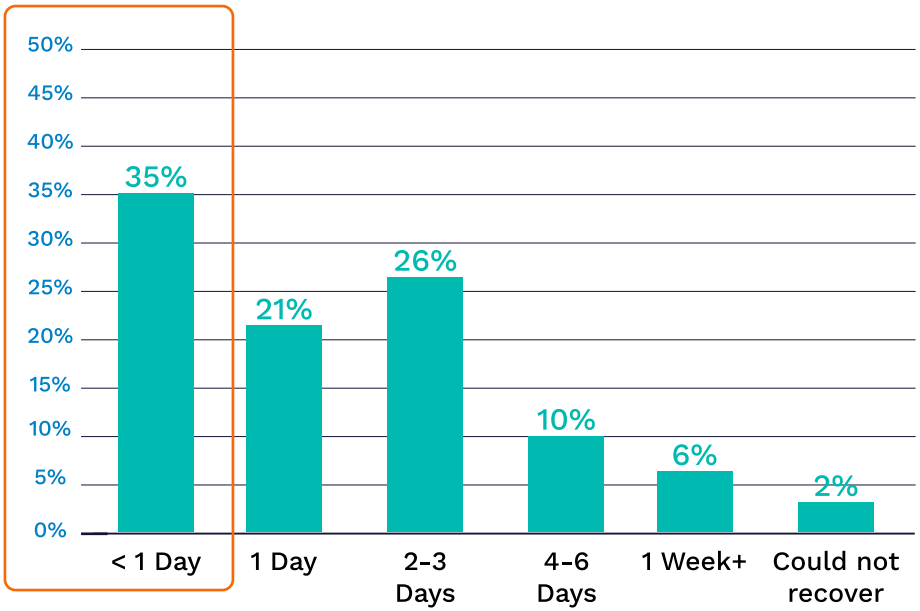
The reality of recovery falls short of respondents' perceived capabilities, revealing a striking gap between expectations and actual outcomes during downtime events. In the survey, **more than 60% of respondents believed they could recover in under a day; however, in reality, only 35% could.**

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?



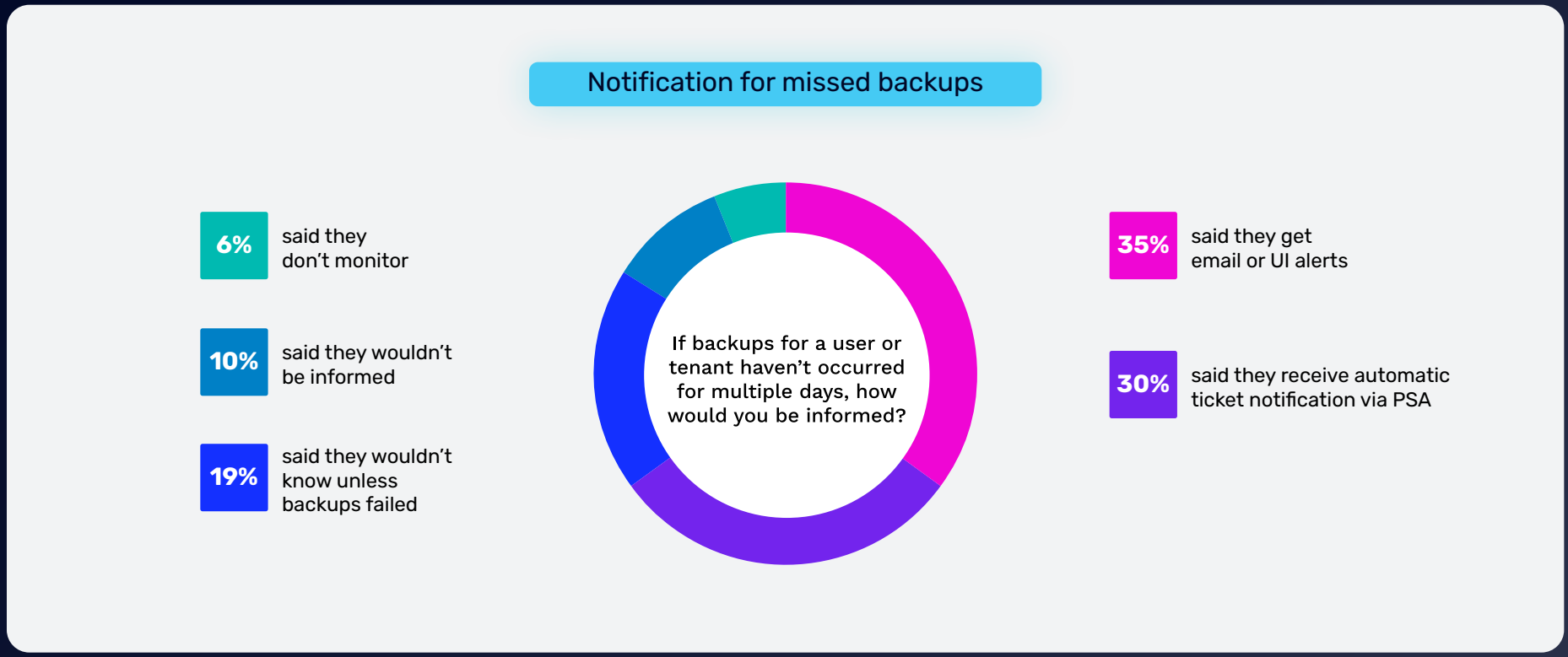
Files **Server/VMs** **Application Data**

Insurance companies often demand proof that businesses conduct regular incident response testing and can meet RTO goals. If an organization lacks a strong plan or misrepresents its cybersecurity capabilities, it risks denied claims or reduced payouts after an incident.

Qualifying for cyber insurance requires having a well-documented and tested incident response plan. This demonstrates an organization's readiness to detect, respond to and recover from cybersecurity incidents — a key requirement for insurers. Your ability to help implement and test these plans strengthens your organization's (or your clients') security posture and compliance with cyber insurance standards.

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.

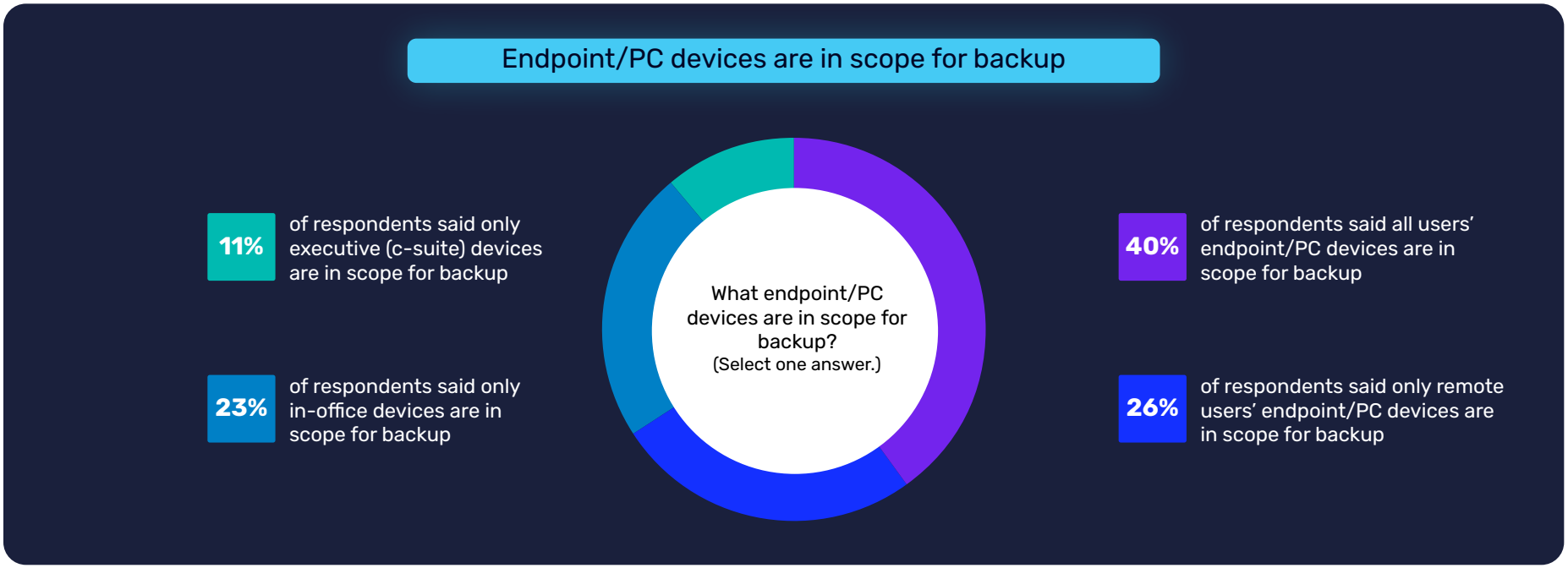
On-premises backup and recovery

While cloud adoption grows, on-premises systems continue to play a vital role. Protecting these systems, from endpoint devices to servers, 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

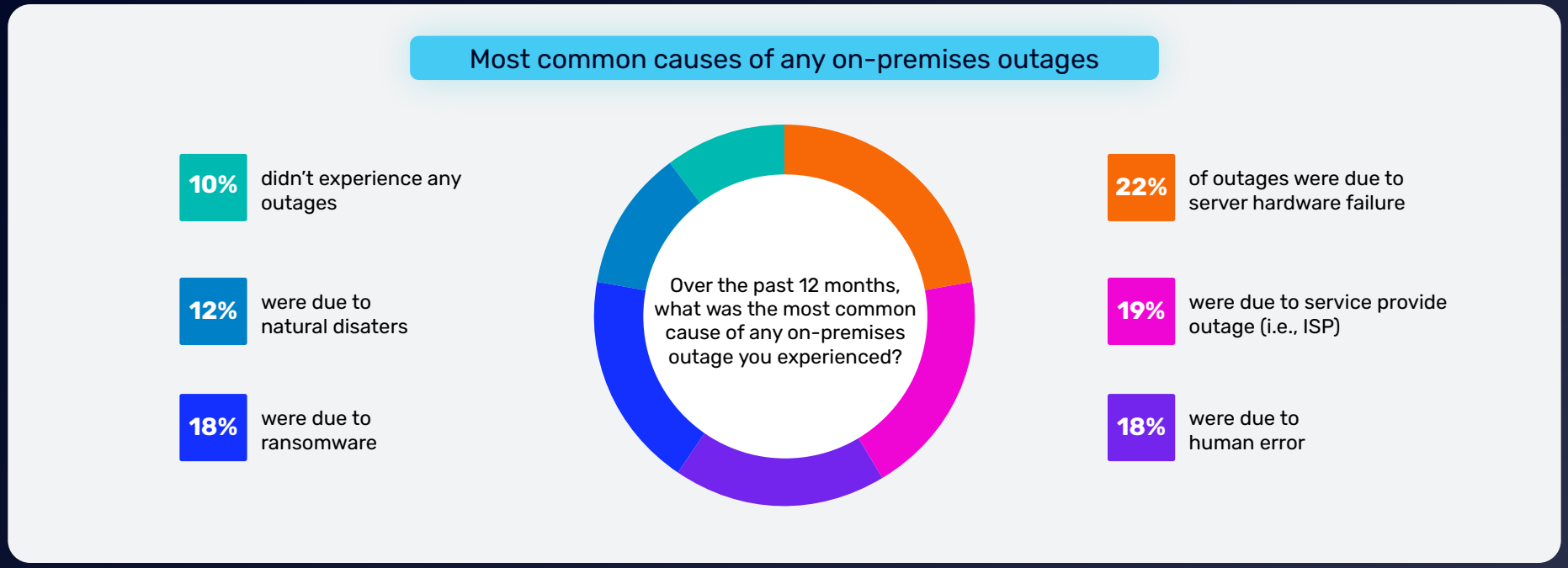
Endpoint devices play a critical role in business operations, particularly with the rise of remote work and hybrid environments. The good news is many organizations are taking endpoint protection seriously. Around 40% of respondents said their organizations plan to back up all endpoint/PC devices, including 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.



Main causes of on-premises outages

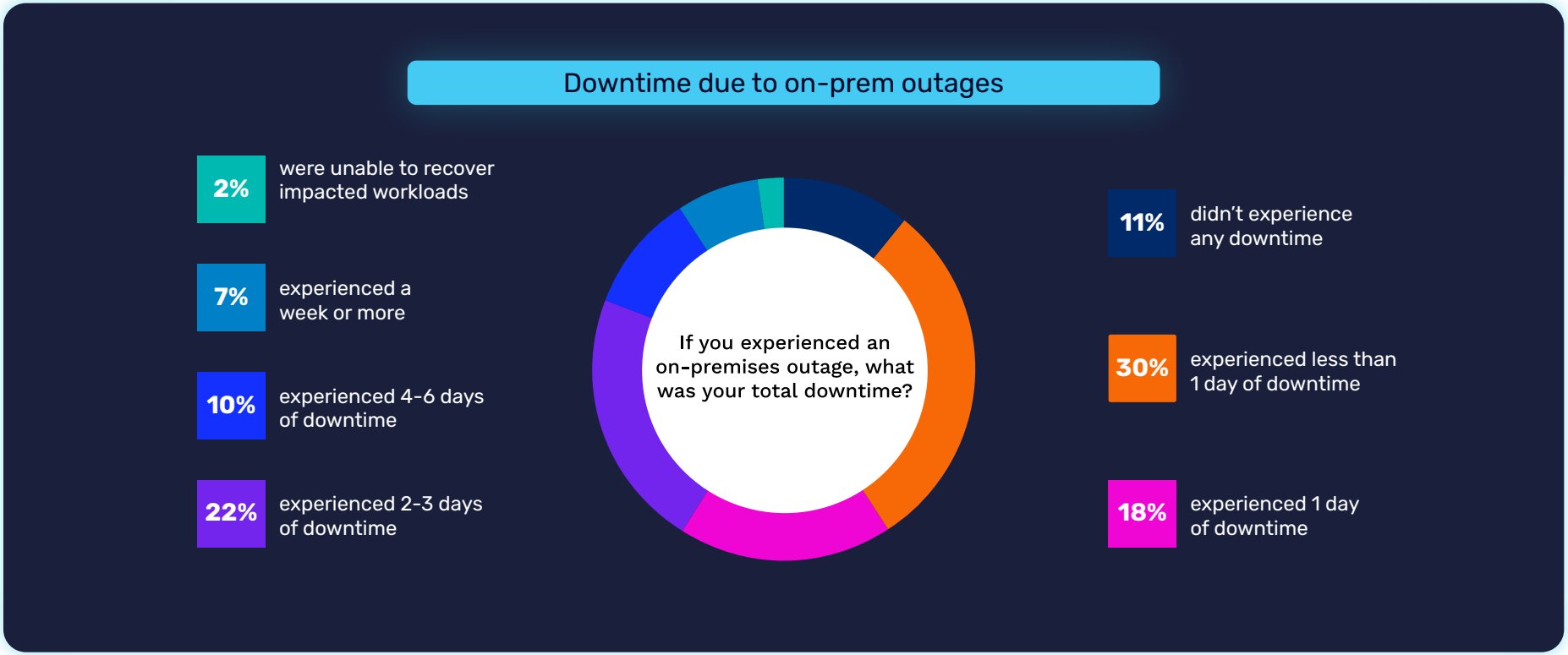
Outages in on-premises environments remain a significant challenge for businesses large and small. For more than 20% of organizations, server hardware failure was the leading cause of on-premises outages over the past year. Service provider outages (e.g., ISP disruptions) accounted for 19% of disruptions. 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.



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.

Don't let data loss or downtime steal your thunder. Download the Data Resilience Checklist for IT Teams now to master the three-pronged strategy — Prepare, Protect and Recover — to achieve true data resilience.



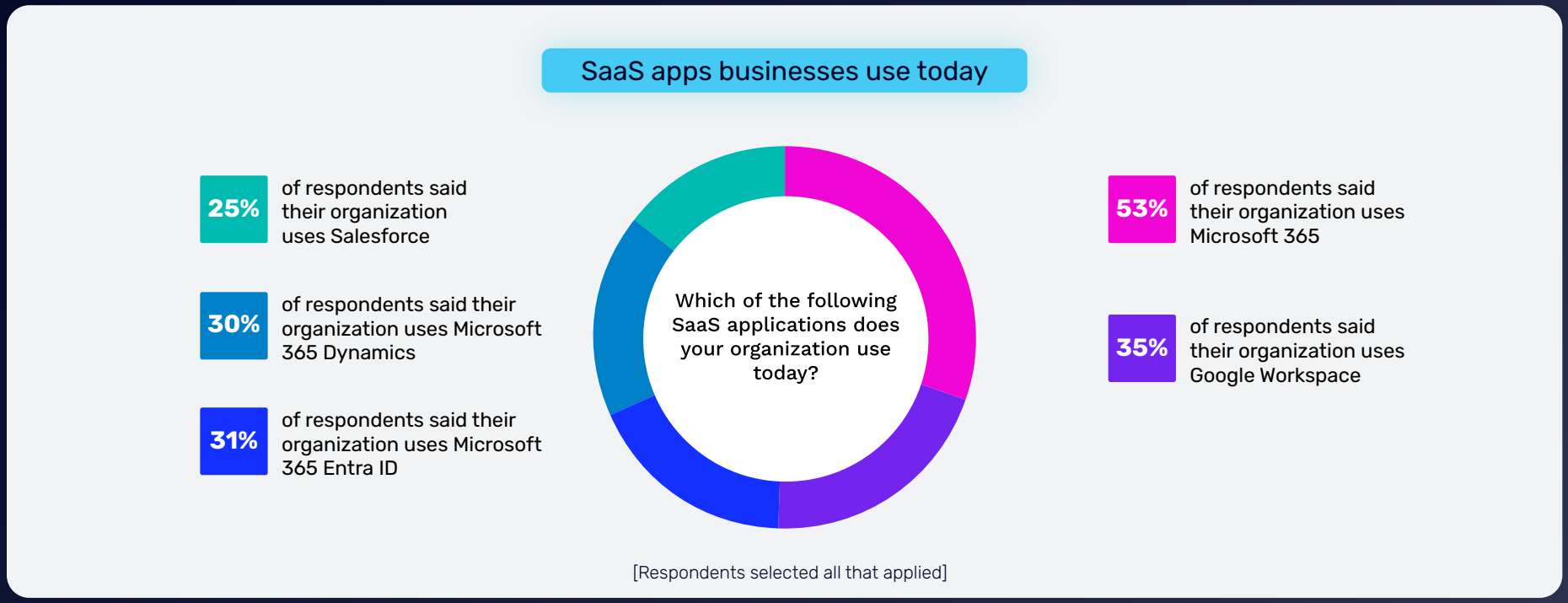
SaaS backup and recovery

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 BCDR Report 2025 reveals key trends, tools, challenges and gaps in how businesses approach SaaS backup and recovery.

Key SaaS applications businesses use today

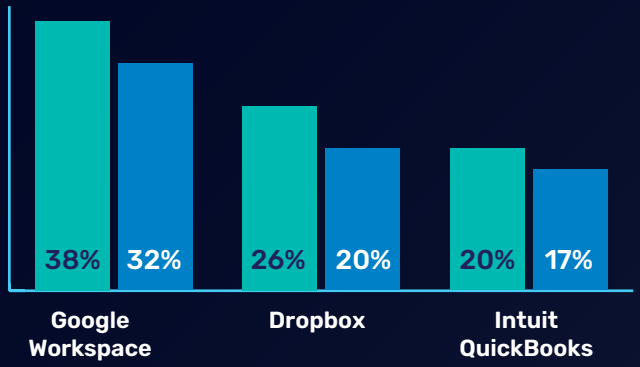
With regard to collaboration solutions (commonly delivered via the SaaS model), Microsoft 365 remains the leader, with a 53% adoption rate among respondents. However, it has seen a decline in market share compared to 2022 adoption rates, which saw a 71% adoption of Microsoft 365 among our respondents.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

The adoption of Google Workspace (35%) has risen steadily in the last 2 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%).

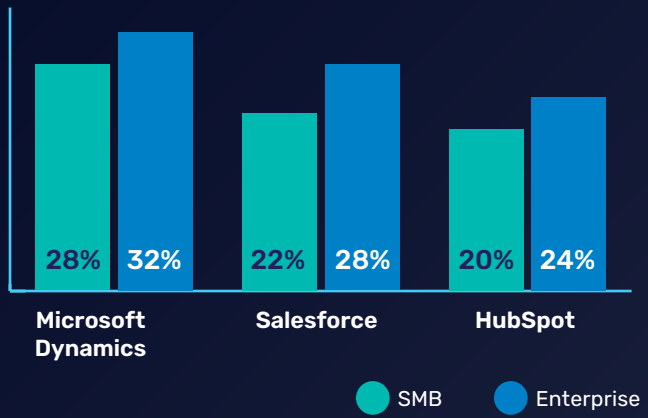


SaaS adoption rates per cohort

SMBs are more likely to adopt:



Enterprise organizations are more likely to adopt:



Tools businesses use to back up SaaS data

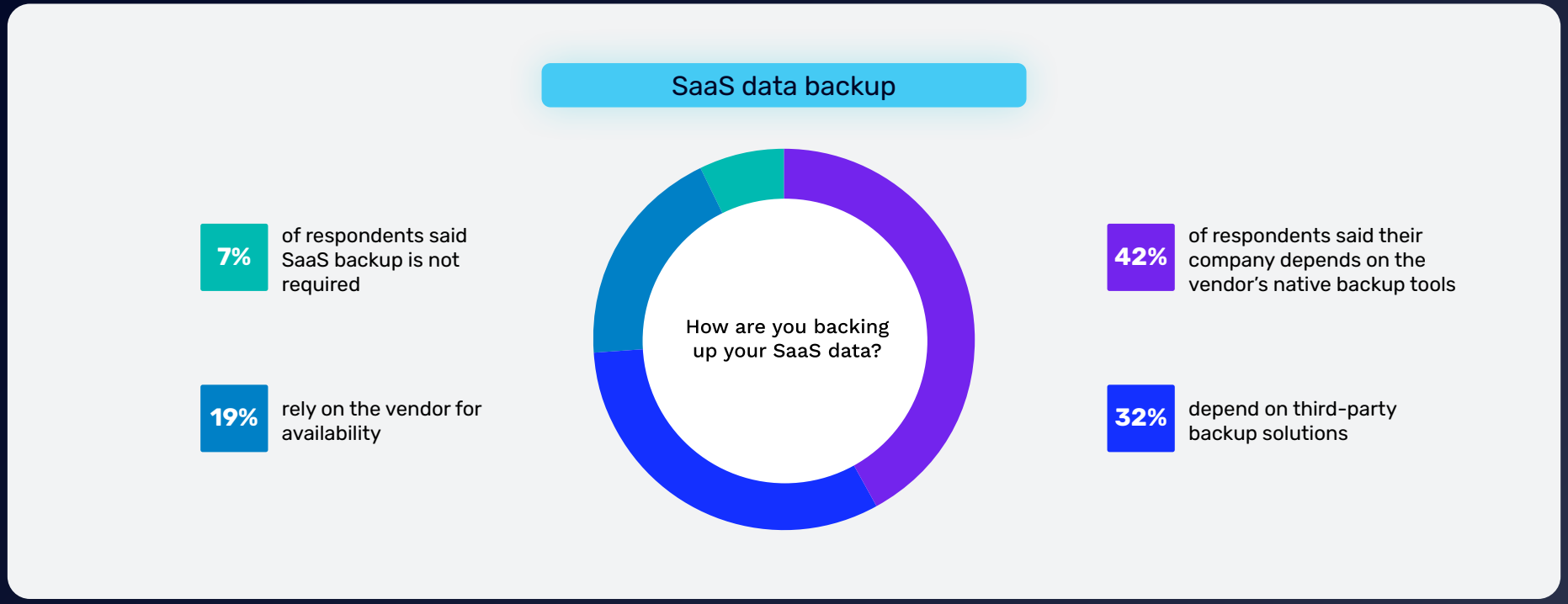
As organizations increasingly rely on SaaS applications to drive productivity and collaboration, the importance of data protection has never been greater. While awareness of the Shared Responsibility Model (SRM) – which clarifies that businesses, not SaaS providers, are responsible for protecting their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

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

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

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.

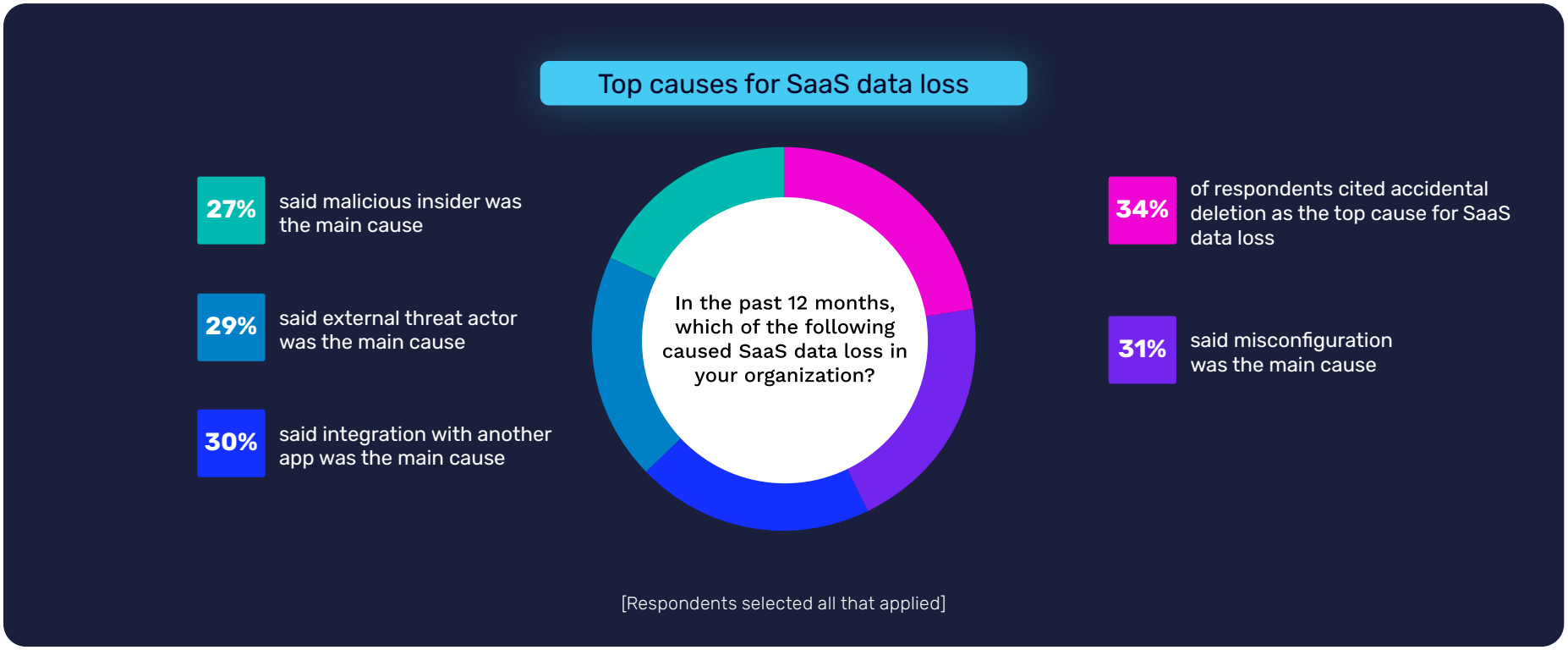


SaaS data lifecycle management

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 3rd 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 risks of loss of institutional knowledge and critical records, and non-compliance.

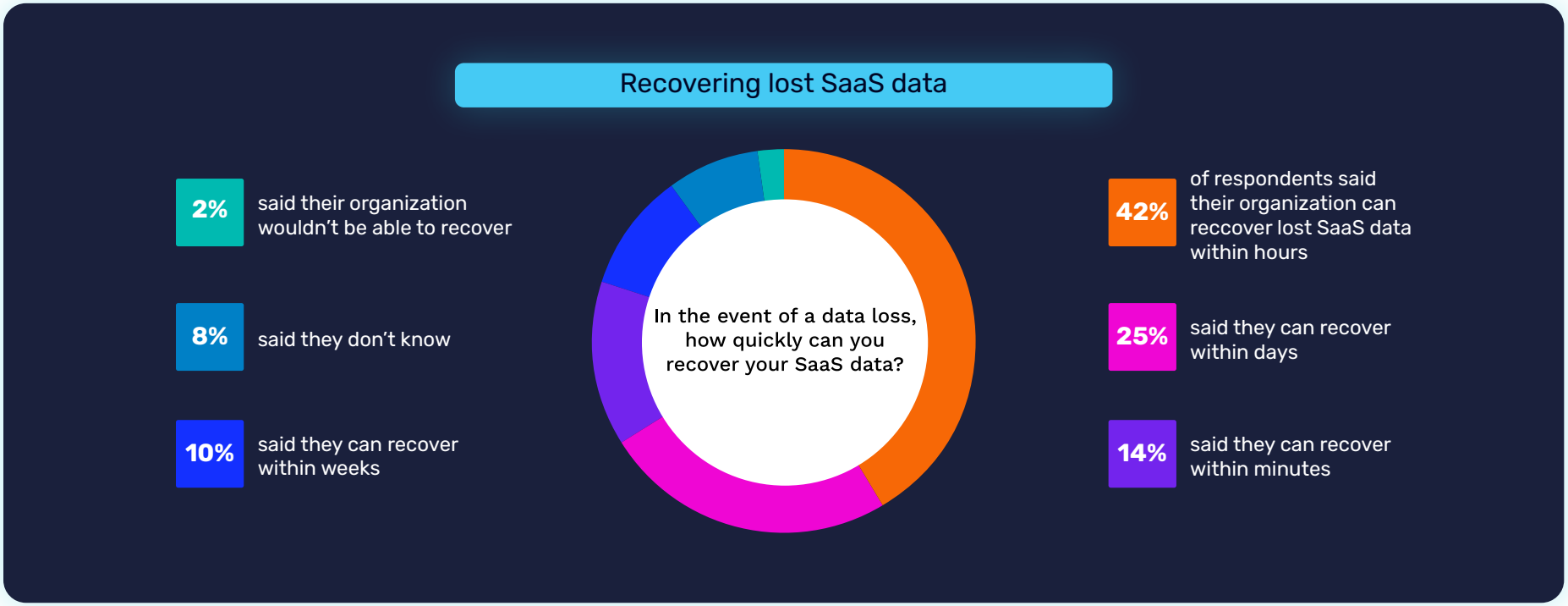
Top causes of SaaS data loss

Data loss in SaaS applications occurs from 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 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.



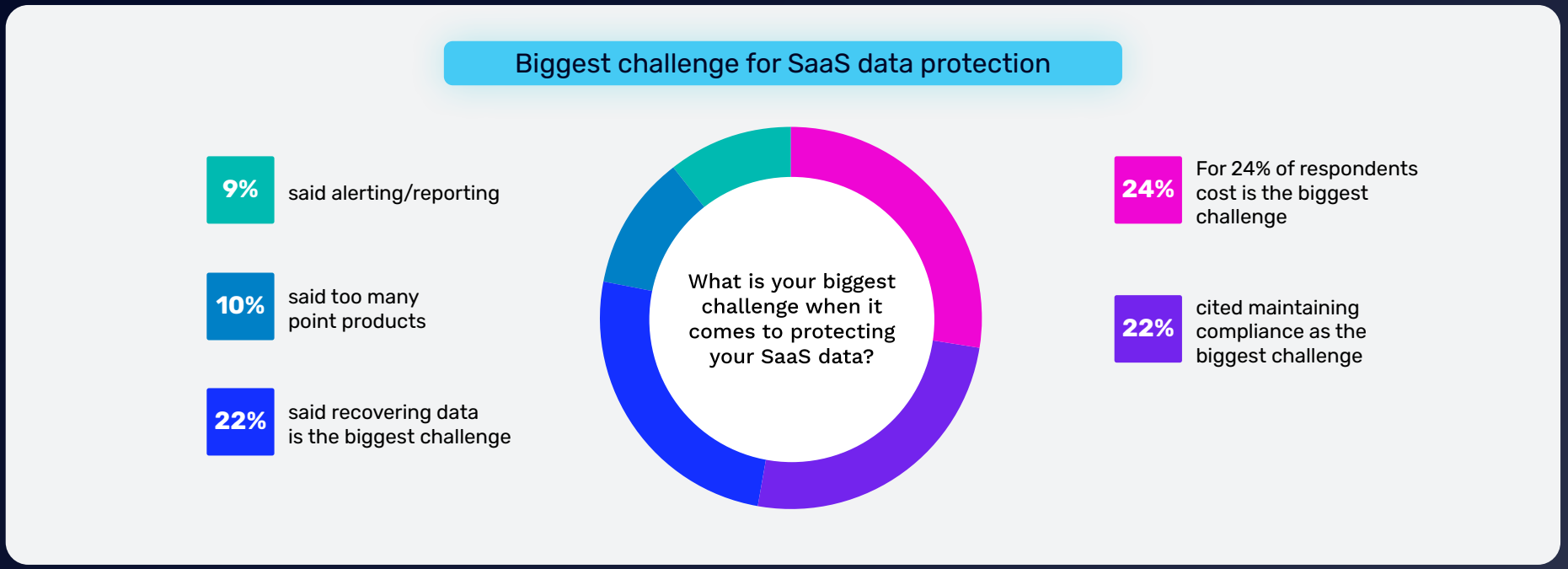
How quickly can businesses recover lost SaaS data

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.



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.



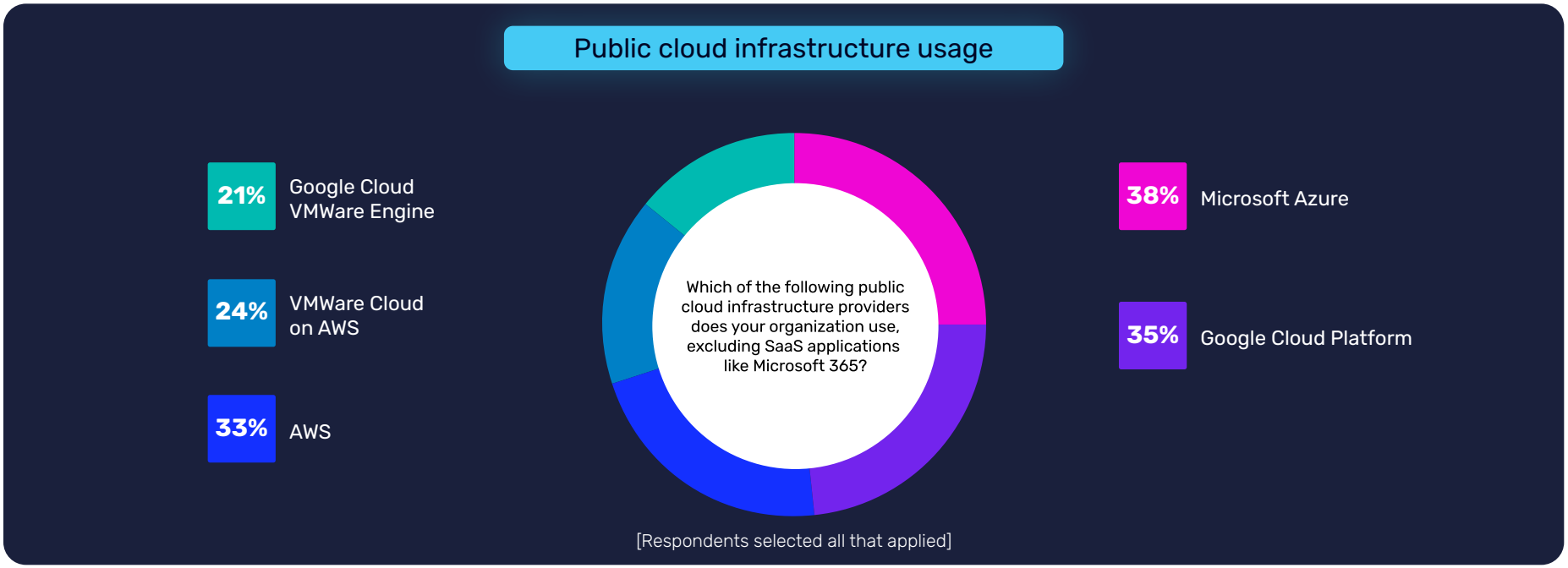
Current state of cloud adoption

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.

Explore the "State of the MSP Industry 2025 Look Ahead" report to see how high-performing MSPs are leveraging cloud adoption to drive growth and stay ahead.

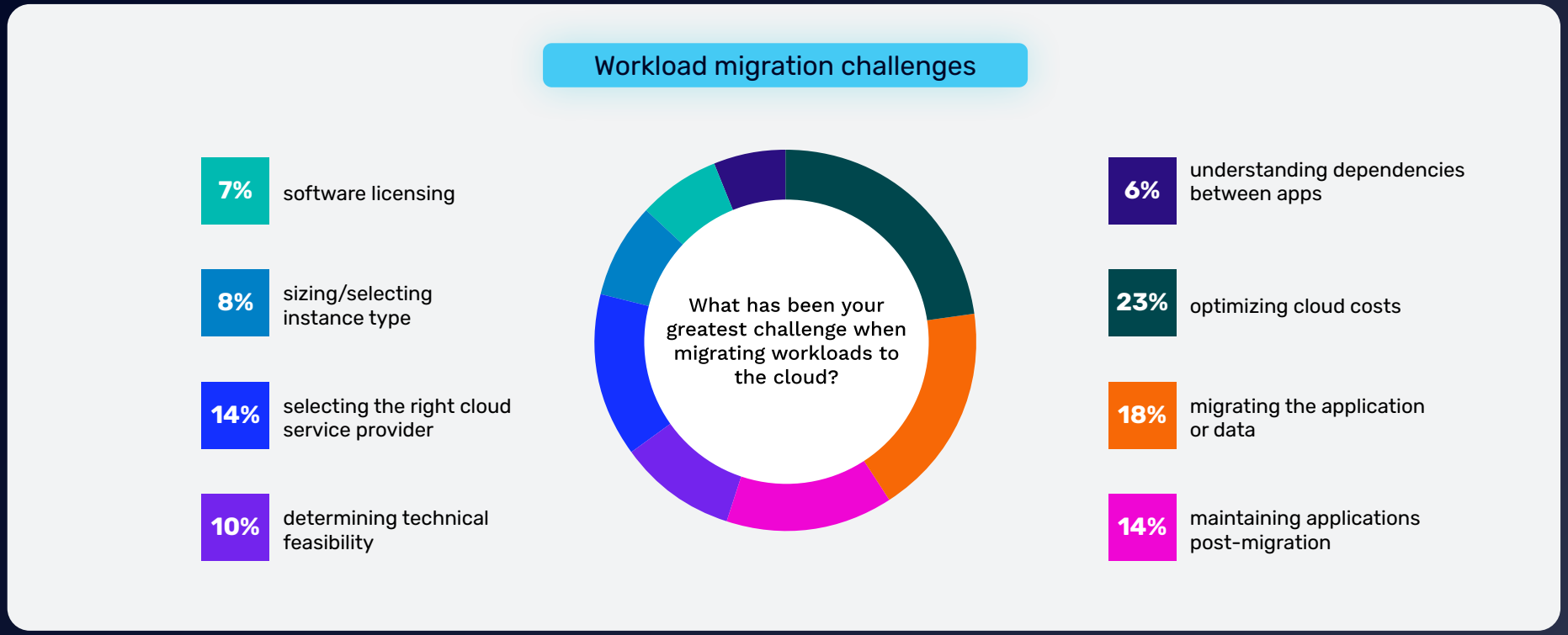
Top public cloud infrastructure businesses use today

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.



Greatest challenges when migrating workloads to the cloud

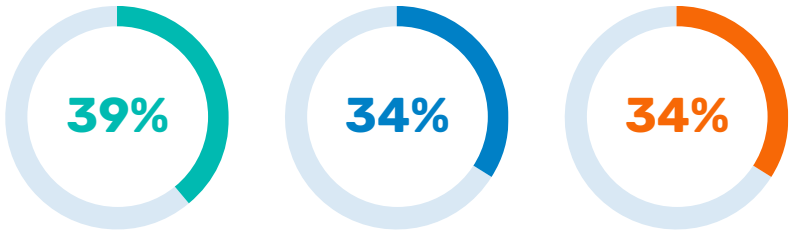
Migrating workloads to the cloud involves numerous challenges, including technical, financial and operational complexities. Optimizing cloud costs, cited by 23% of respondents, emerged as the greatest challenge when moving workloads to the cloud. For nearly 20% of organizations, workload migration remains 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 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

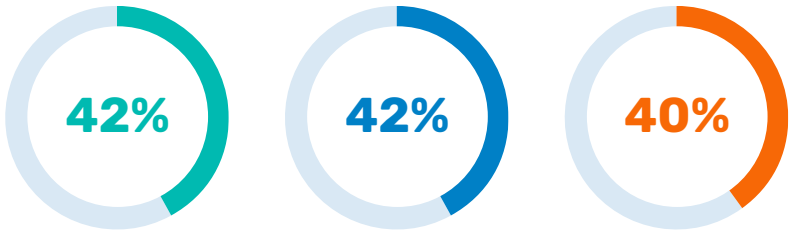


Non-sensitive analytics

IoT & Edge

Sales & orders

Top data types unlikely to migrate



Personal identifiable information (PII) or protected health information (PHI)

Corporate financial data

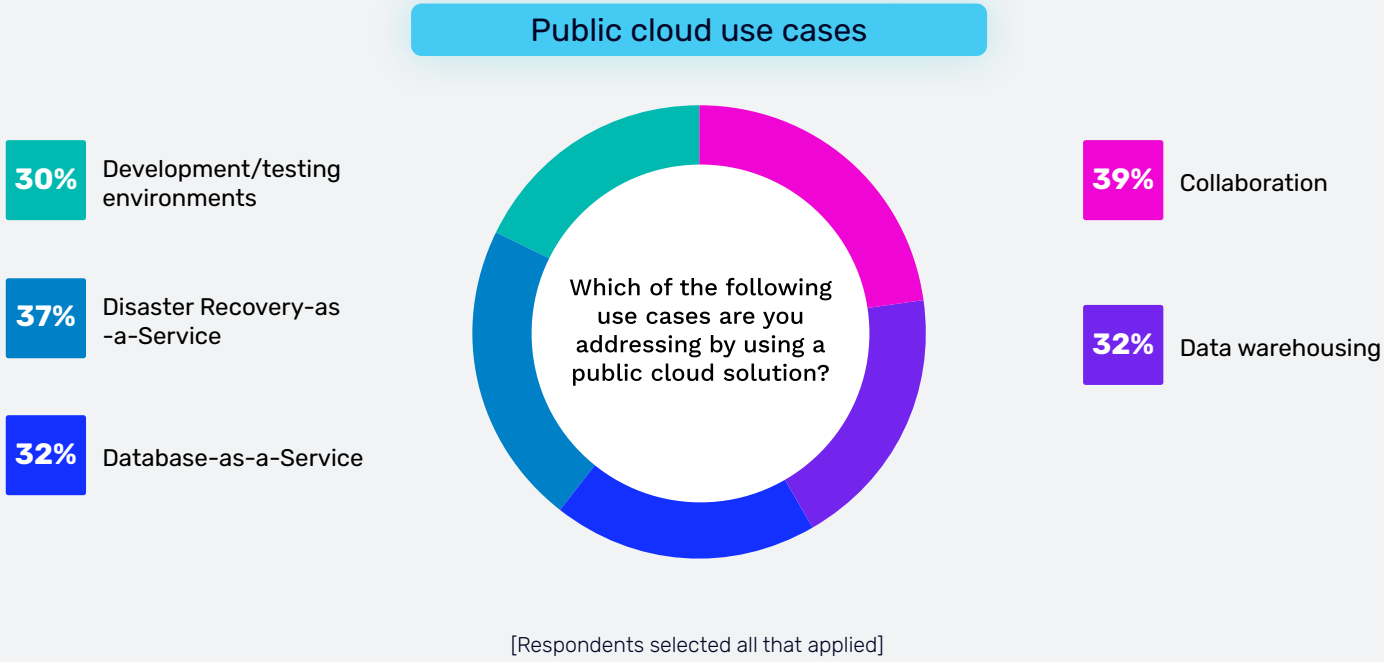
Sensitive intellectual property (IP)

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

The reluctance to migrate more sensitive data underscores the 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 are heavily regulated by law. Organizations leery of migrating this data suggests doubt remains with regard 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.

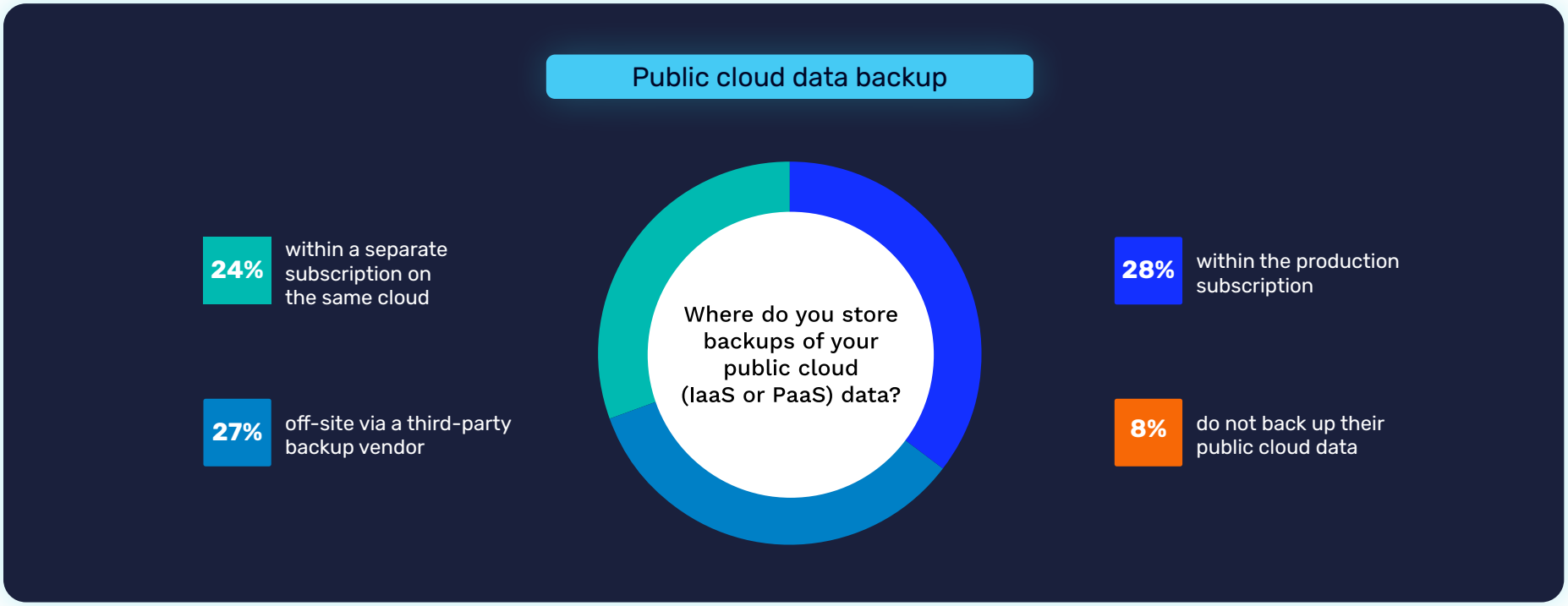
Public cloud solutions use cases

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.



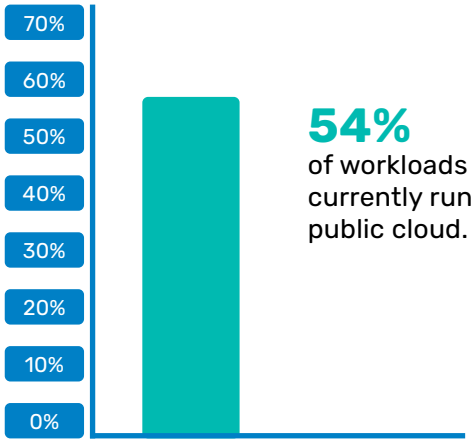
How businesses store backups of public cloud data

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.

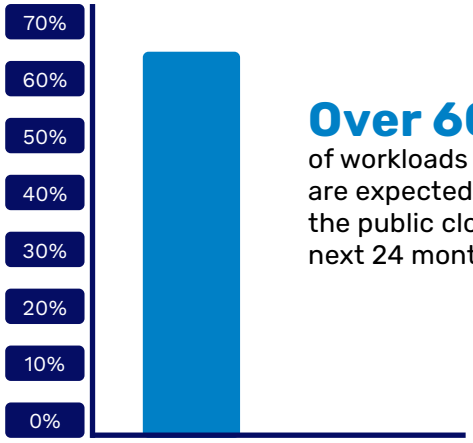


Workloads and applications in the public cloud

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.



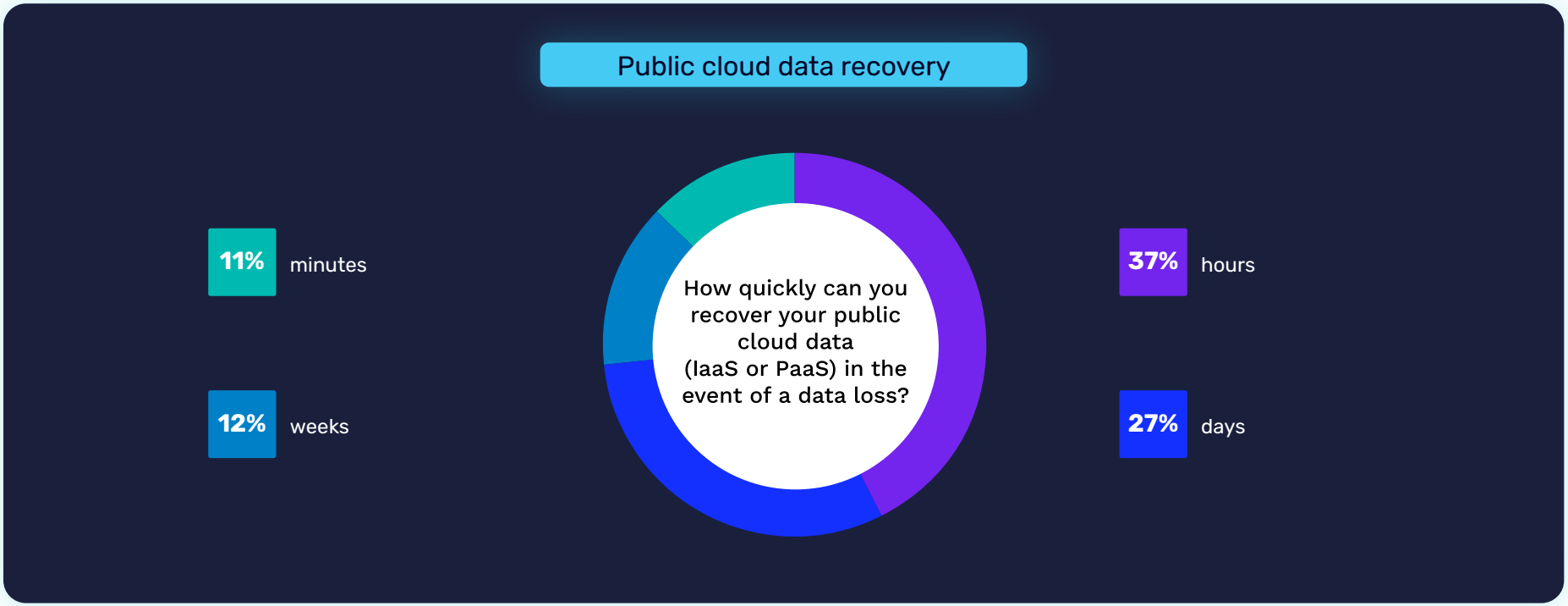
54%
of workloads and apps currently run in the public cloud.



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

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, both MSPs and internal IT teams must adopt robust strategies and tools to safeguard critical 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. To strengthen resilience:

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

Set clear RTOs and RPOs: Ensure RTO and RPO goals align with business objectives and 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: Regularly assess and update backup and recovery policies to reflect technological advancements, regulatory changes and organizational priorities.

Enhance the security of backup systems

With cybercriminals increasingly targeting backup systems to disrupt recovery efforts and maximize ransomware effectiveness, organizations must strengthen their defenses. Follow these steps to fortify backup systems:

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

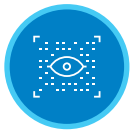
Protect against ransomware: Use immutable backups and air-gapped storage to ensure data integrity in the event of an attack. Differentiate the backup infrastructure from production (i.e., a hardened Linux backup appliance protecting a Windows environment) where possible.

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

Train staff: Educate employees and stakeholders on threat detection, risk mitigation and security best practices to reduce human error and insider threats.

Leverage advanced technologies

Modernizing backup and recovery processes with advanced technologies and scalable solutions can improve efficiency and reliability. Organizations 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 BCDR solutions that provide real-time visibility into backup performance and alert to potential issues before they escalate.

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

Vendor partnerships

Selecting the right BCDR vendor is critical, as it directly impacts the effectiveness of an organization's data protection strategy. Key considerations include:

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 offer 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 evolving data protection 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 business continuity and disaster 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.

These findings send a clear message: organizations must continuously invest in, adapt and innovate their data protection strategies. As data volumes surge and cyberthreats become more sophisticated, both MSPs and internal IT teams must ensure critical assets are safeguarded, compliance requirements are met and business disruptions are prevented.

What's next? Use this report as a blueprint to assess and enhance your BCDR strategy. Identify gaps, strengthen your approach to data protection and ensure your organization — or your clients — remain resilient against evolving threats.

Visit our website to discover industry-leading solutions that help you deliver comprehensive data protection and drive new growth opportunities.

Explore Datto's industry-leading solutions

Enhance your backup and disaster recovery capabilities with solutions designed to minimize data loss, reduce downtime and improve operational efficiency.

Book a demo today!

About Datto

Datto is a leading global provider of security and cloud-based software solutions purpose-built for managed service providers (MSPs) and IT professionals. Our proven Unified Continuity solutions enhance cyber resilience and efficiency and drive growth.

Delivered through an integrated platform, our solutions enable MSP partners and IT pros to protect over one million businesses worldwide. From proactive threat detection and prevention to fast, flexible recovery, we help businesses minimize downtime and data loss — whether in servers, virtual machines, cloud applications or anywhere the data resides.

datto
A Kaseya COMPANY