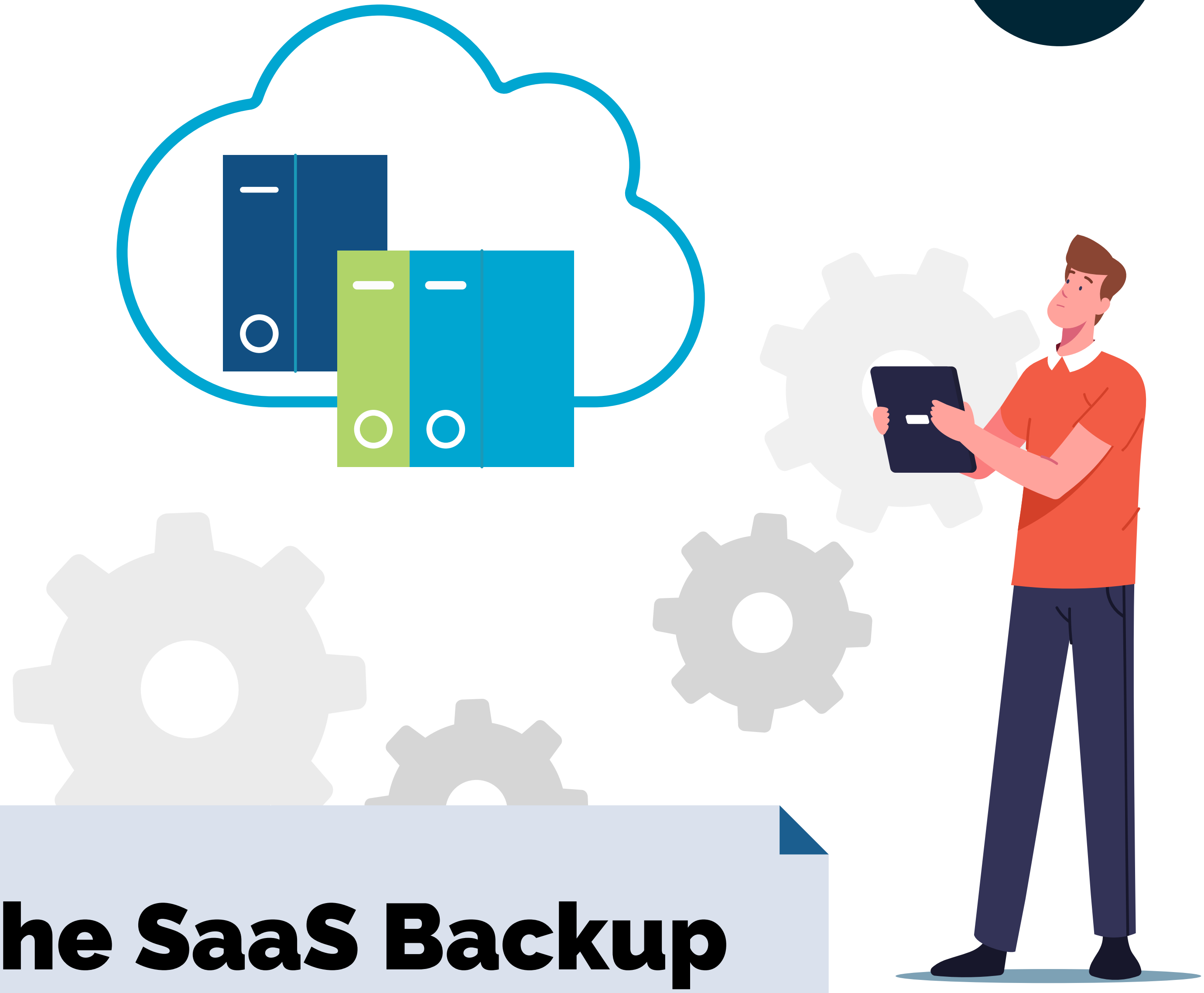
SPANNING
A Kaseya COMPANY

2022



The SaaS Backup & Recovery

Report 2022

The SaaS Backup and Recovery Report 2022 from Spanning provides new insights into the SaaS universe, the current state of SaaS data protection and what you should know to enhance your data protection strategy.

Introduction

Software-as-a-Service (SaaS) has become a core component of today's IT infrastructures. SaaS is quickly gaining popularity among businesses looking for easily accessible, flexible, hassle-free and cost-effective business solutions. SaaS adoption has increased at an unprecedented rate, especially in the wake of the disruption caused by the COVID-19 pandemic. The global SaaS market size was $130.69 billion in 2021 and is expected to grow to $716.52 billion by 2028, at a CAGR of 27.5% during the forecast period.

On the flipside, the prying eyes of cybercriminals are noticing the rapid move to SaaS environments. It's no surprise that 2021 has been a record-breaking year for cyberattacks. With threat actors more active than ever and looking to compromise sensitive data for quick, easy payouts, businesses must rethink their IT security posture across all fronts, including SaaS data protection.

The SaaS Backup and Recovery Report 2022 from Spanning provides new insights into the SaaS universe, the current state of SaaS data protection and what you should know to enhance your data protection strategy. This report also explores the top IT priorities for businesses in 2022, what organizations look for in an IT vendor, the biggest risk facing businesses today and why SaaS data backup is crucial for mid-market enterprises (MMEs).

Key findings

Three key takeaways gleaned from the 2022 SaaS Backup and Recovery Survey:

1

Backup and disaster recovery emerged as the top IT priority for businesses in 2022

Rampant cyberattacks and remote work environments have increased the need for backup and disaster recovery. **Approximately 80%** of respondents cited backup and disaster recovery as the top IT priority in their organization.

2

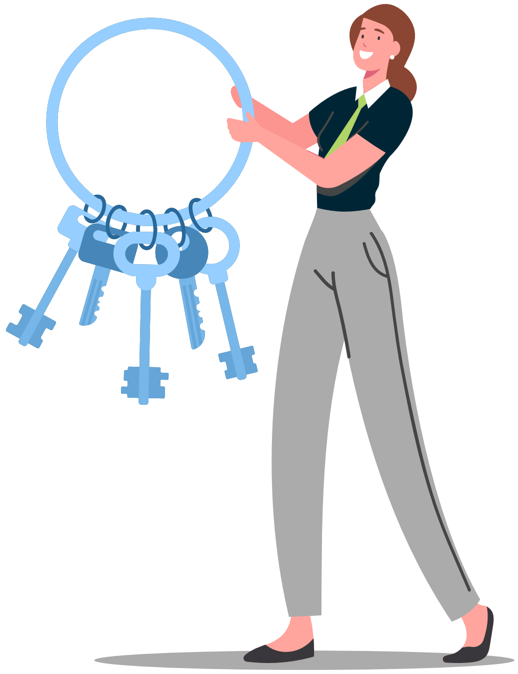
Cybersecurity is the greatest IT risk for organizations today

Businesses worldwide experienced 50% more attacks per week in 2021 compared to 2020. Small and midmarket businesses are quickly realizing that they are attractive targets for cybercriminals. **Nearly 55%** of respondents consider cybersecurity the greatest risk to their organizations today.

3

Risk mitigation is the top driver for MMEs maintaining SaaS backup

SaaS data loss due to human error, malicious insider action or cyberattacks could cause irreparable damage to businesses, regardless of their size. **More than 54%** of IT leaders surveyed said SaaS backup is crucial to reduce risks associated with unforeseen disruptive incidents.



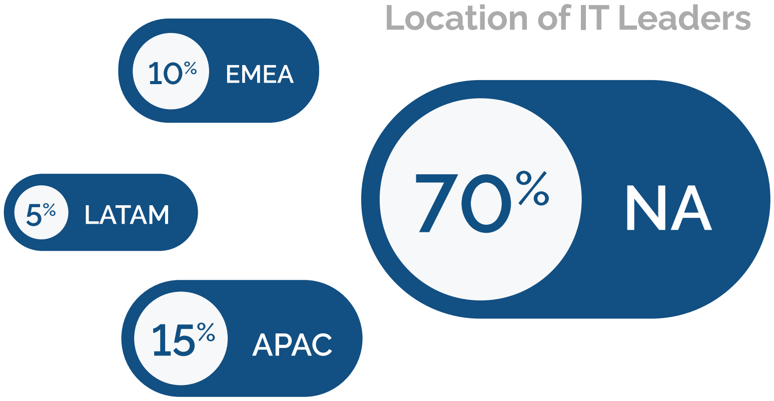
Our respondents - —

For the purpose of this report, we surveyed thousands of IT leaders across four continents.

Geographic Locations

The vast majority of respondents for the 2022 SaaS Backup and Recovery Survey were from North America (70%), followed by APAC (15%), EMEA (10%) and 5% from Latin America.

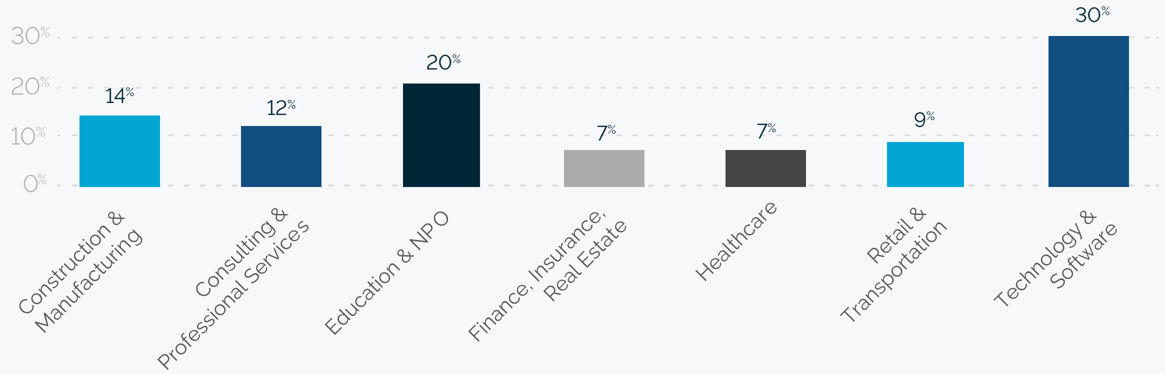
Location of IT Leaders



Industries

We received responses from several industry verticals. The greatest representation was from Technology and Software (30%), followed by Education and Not-For-Profit (20%), Construction and Manufacturing (14%), Consulting and Professional Services (12%), Retail and Transportation (8%), Healthcare (7%), Finance, and finally Insurance and Real Estate together comprising 7%.

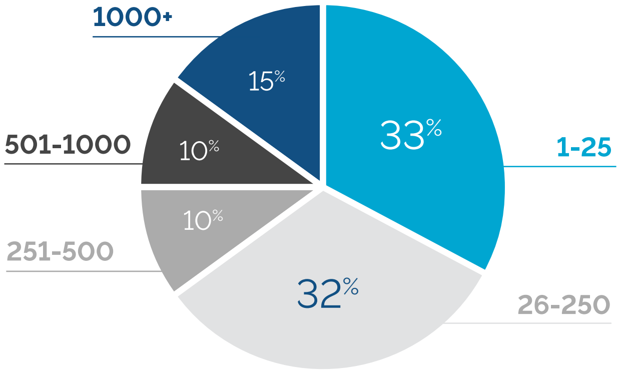
Respondents by Industry



Employee size

The company size of the respondents varied from “less than 50” employees to “more than 1,000.” More than 30% of our respondents were from companies with fewer than 26 employees, another 32% were from organizations with 26 to 250 employees; 15% of respondents were from companies with over 1,000 employees and 20% were from organizations with 251 to 1,000 employees.

Employee Size



Detailed findings - —

Let's take a look at the key findings of the report in detail.

Top three IT priorities for businesses in 2022

As businesses look to regain their footing, IT pros have an enormous task of keeping SaaS-based solutions secure while ensuring data and systems are available 24/7/365 even in the face of a disaster. According to our respondents, the top three IT priorities for businesses in 2022 are backup and disaster recovery, improving cybersecurity mesh and enhancing data fabric.

Backup and disaster recovery

Almost 80% of respondents listed "backup and disaster recovery" as the top priority for IT departments. It's no secret that unplanned downtime can bring a business to a grinding halt. According to Gartner, the average cost of IT downtime is $5,600 per minute. With enterprise downtime now more expensive than ever, the ability to recover quickly and be up and running again is an important determinant factor for business success.

Improve cybersecurity mesh across business

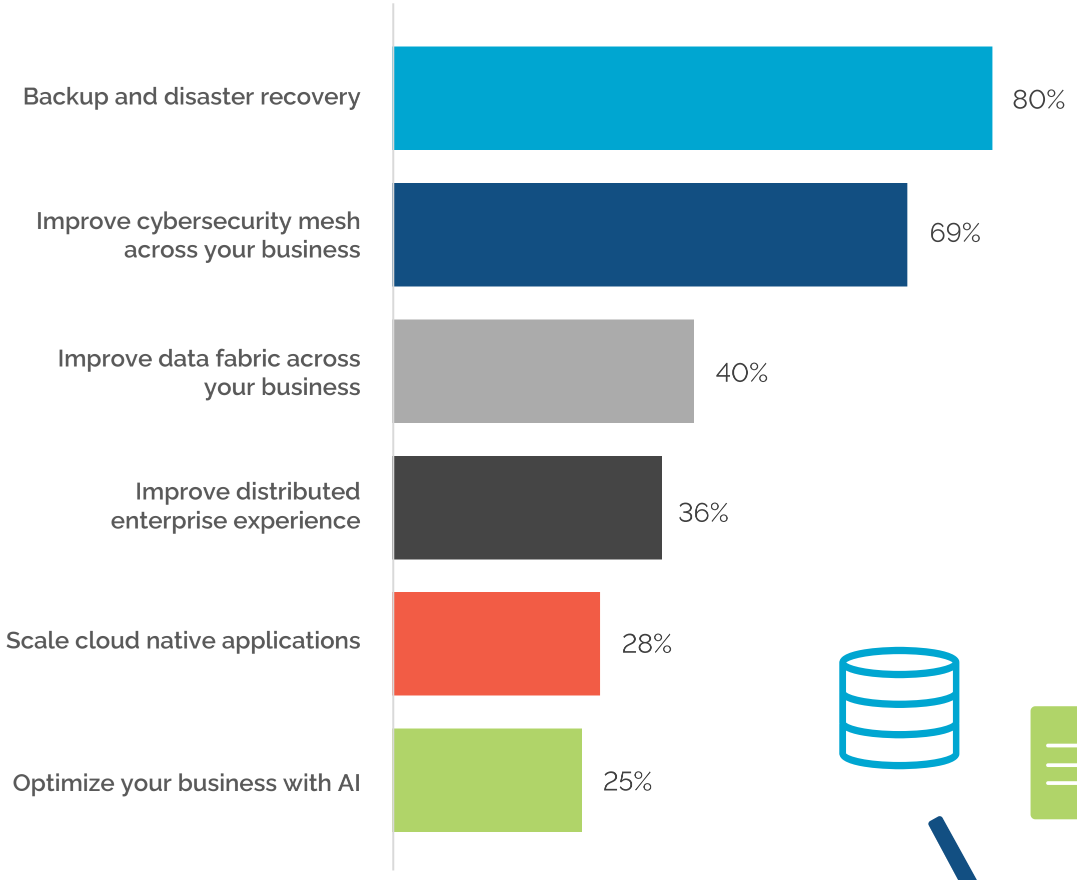
The second-highest priority among businesses is "improving cybersecurity mesh across business," which aligns with the pandemic-driven, highly accelerated digital transformation. The sudden shift to remote work turned businesses upside down, leading to rapid adoption of cutting-edge technologies and migration to the cloud to support remote workforces. According to Gartner "The cybersecurity mesh is a modern conceptual approach to security architecture that enables the distributed enterprise to deploy and extend security where it's most needed." The cybersecurity mesh will enable businesses to secure any digital asset(s) — data, devices or applications — regardless of where they are.

Gartner Analyst Felix Gaehtgens said, **"Organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a coherent ecosystem will reduce the financial impact of individual security incidents by an average of 90%."**

Improve data fabric across business

"Improving data fabric across business" emerged as another top mission-critical priority for mid-market enterprises. Today's highly distributed, ever-changing data landscape and increasing volumes of unstructured data call for a robust data management and integration solution that goes beyond conventional data management practices. Data fabric is a powerful architecture that combines traditional practices with new technologies to provide a holistic view of data across environments, including hybrid and multicloud environments. The unified architecture enables businesses to monitor and manage data regardless of where it is stored, automates repetitive tasks, provides seamless access and greater control over data, and helps improve data security. With data fabric, modern businesses can harness the power of big data to meet burgeoning demands while staying competitive in this new economic environment.

Top Priorities in IT Departments



Key IT vendor criteria that matter to MMEs - —

The COVID-19 pandemic accelerated digital transformation and changed the way businesses operate. During these uncertain times, IT vendors played an important role in supporting remote work environments, enabling organizations to maintain business continuity. While businesses globally continue to recuperate from the devastating impacts of the global pandemic, many of the changes that transpired will remain for the foreseeable future. Therefore, reliance on IT partners will continue, and they will be critical to the success of an organization.

In this regard, we asked our respondents what key criteria they look for in an IT vendor. Here are the top three:

Easy access to support

More than 30% of respondents cited "easy access to support" as the top IT vendor attribute that makes doing business with them easy. Finding the right IT partner can help businesses save time, money and effort. Since vendors are at the core of an organization's mission-critical processes and functions, easy access to support is crucial to meet business demands and take action on new initiatives. Besides, there's nothing more comforting than knowing that support teams are always available, and ready to listen to you and solve your problems.

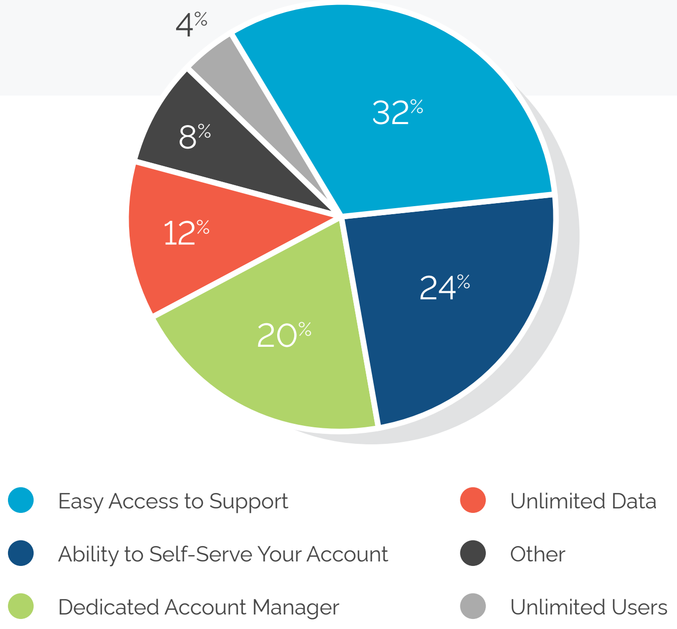
Ability to self-serve

Nearly one-quarter of the respondents (24%) listed "ability to self-serve" as another important IT vendor criteria. IT self-service capabilities offer multiple benefits to businesses of all sizes, right from reducing costs and empowering employees to minimizing downtime and maximizing productivity.

Dedicated account manager

About 20% of respondents said having a "dedicated account manager" makes doing business with an IT vendor easy. Account managers are advocates for your business goals and needs. A dedicated account manager will take the effort of knowing a company's needs. Having a dedicated account manager serves as a single point of contact, which streamlines processes, saves time and ensures your requests are fulfilled. Since account managers are aware of your company's goals and objectives, they can advise you on what product/services will or will not work for your business. IT vendors that provide a dedicated account manager will be the preferred choice for MMEs in 2022 and beyond.

What makes doing business with an IT vendor easy?



Greatest risks organizations face today - —

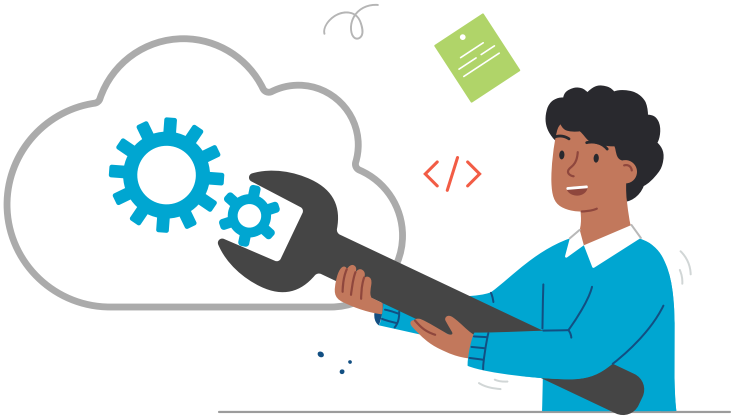
Risks in business are common. From a new competitor entering the market to business interruption and security breach, business risks can appear in all forms and sizes. More than half of the respondents (54%) to our 2022 SaaS Backup and Recovery Survey highlighted cybersecurity as their biggest concern, followed by backup and recovery (13%) and compliance (10%).

Cybersecurity

More than 50% of the respondents revealed that their organization's biggest risk in 2022 is cybersecurity. In 2021, businesses worldwide were overwhelmed by the frequency and sophistication of cyberattacks. According to the FBI, there has been a 400% increase year-over-year in phishing attacks. It is estimated that on average 30,000 websites are hacked every day. With about 300,000 new pieces of malware being created daily to target individuals and organizations, it's no surprise that cybersecurity is the greatest risk organizations face today.

Backup and recovery

More than 13% of respondents cited backup and recovery as a major cause for concern associated with IT. Businesses lose 4 million files daily, which is equivalent to 44 files every second. With the average total cost of a data breach increasing from $3.86 million to $4.24 million in 2021, the stakes are sky-high. Having a backup and recovery solution in place is one of the safest ways to ensure your data is protected and business remains unhindered when disaster strikes.

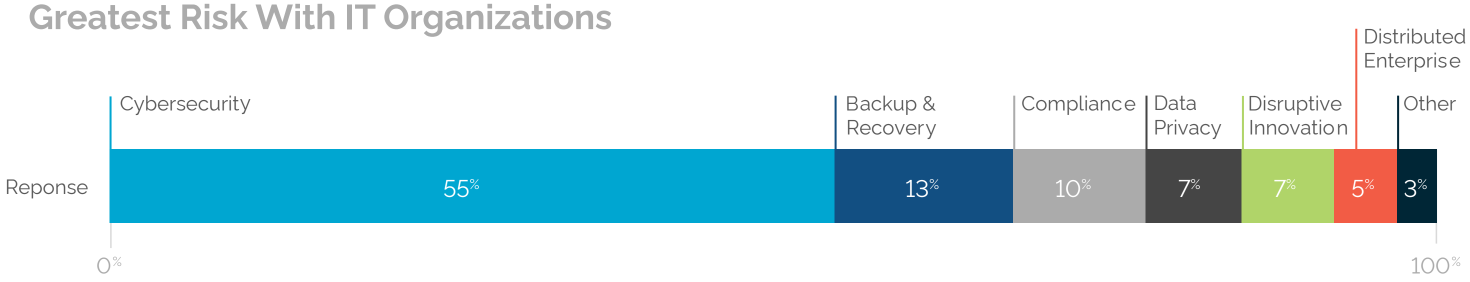


Compliance

For 10% of respondents, compliance is the greatest risk for their organization. Today, there are several regulations that focus on data protection, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA).

Every organization, regardless of its size or vertical deals with compliance risk. Hackers, viruses and malware are some common cyber-risks that could lead to privacy breaches. Organizations that handle sensitive information, such as social security number, health records and credit card details, should take suitable measures and build a robust compliance program to ensure their systems and data are secure.

Greatest Risk With IT Organizations



Top drivers for backing up SaaS data - —

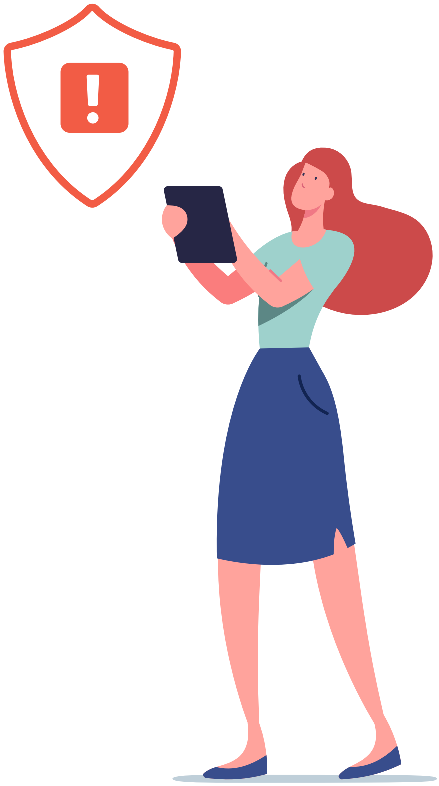
We asked our respondents why SaaS backup is important for their company. The majority of respondents (54%) revealed SaaS backup is critical to reduce risk, while about 17% of companies said they use SaaS backup to protect against user error, and 15.2% of the respondents use SaaS backup to mitigate the impacts of ransomware attacks.

Reduce risk

Data is the lifeblood of business and is constantly at risk. Businesses with inadequate data protection can suffer in numerous ways, including loss of business opportunities, diminished reputation and angry/frustrated customers. More than 50% of respondents in our survey highlighted backing up SaaS data as a necessary step to minimize the risk of data loss and downtime.

Protect against user error

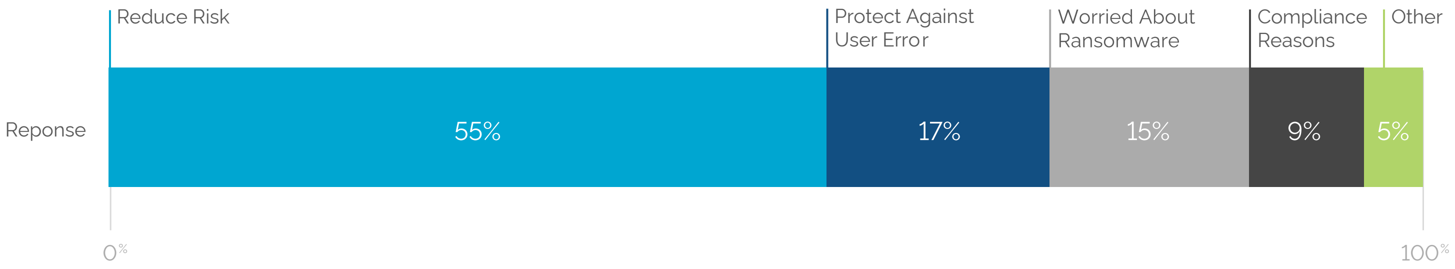
About 95% of cybersecurity breaches occur due to human error. Businesses understand that user error is inevitable and are relying on SaaS backup to protect their business and data against human mistakes.



Ransomware

Ransomware has become a lucrative business for cybercriminals, and they have been very successful at it. More than 80% of U.S. organizations experienced security incidents related to ransomware and phishing in 2020. With the total average cost of a ransomware attack reaching a staggering $4.62 million in 2021, SaaS backup is now a must-have for businesses. Our survey found that more than 15% of MMEs utilize SaaS backup to mitigate the risks associated with ransomware attacks.

Why SaaS Backup Is Important



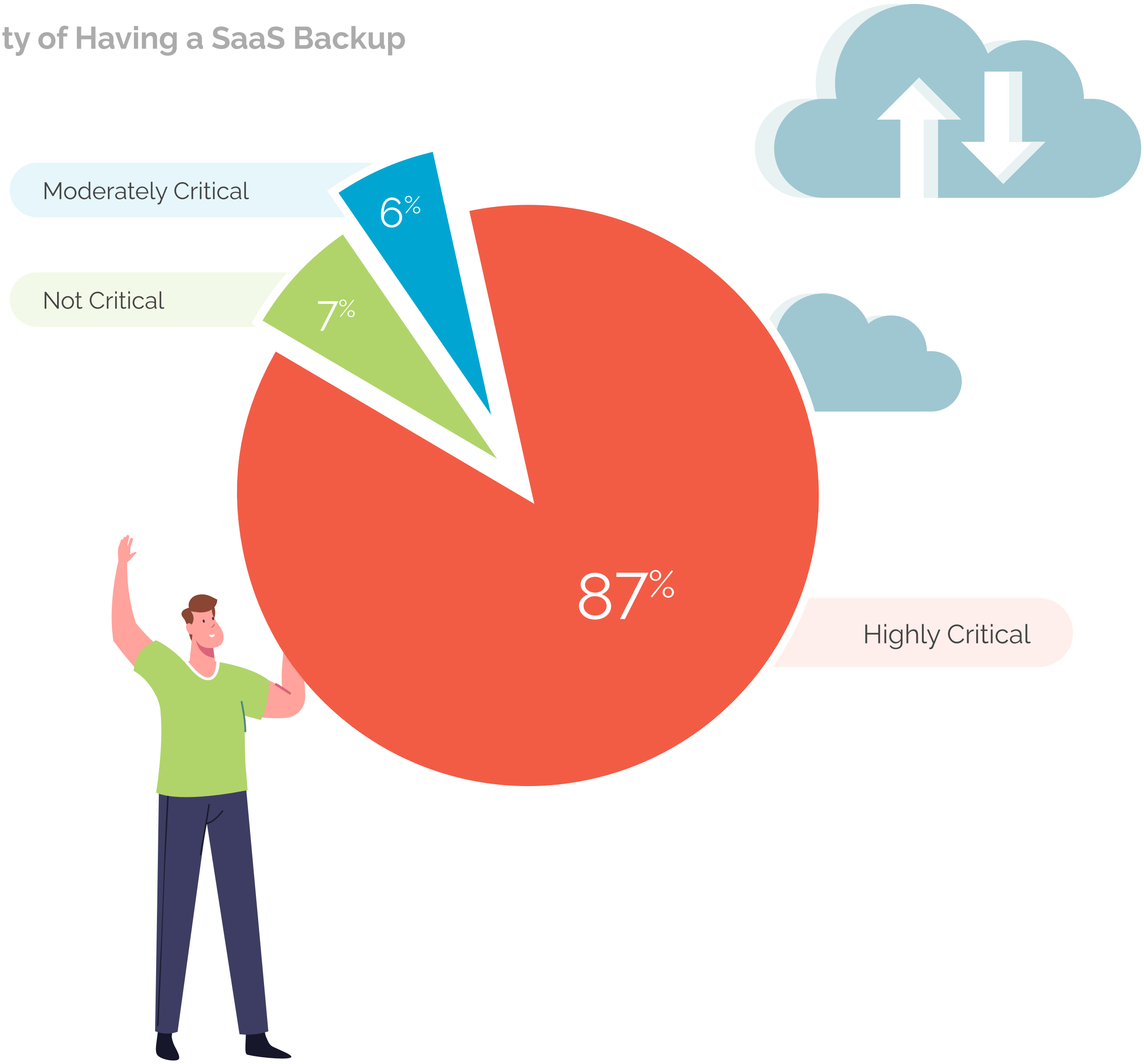
SaaS backup and recovery is critical for MMEs - —

We asked our respondents about the criticality of having a SaaS backup for their business. A staggering 87% of MMEs said SaaS backup is highly critical for their business. About 7% of the respondents don't consider SaaS backup as critical.

A cyberattack occurs every 39 seconds, which is a massive problem for data-driven business environments since they can't afford data loss and downtime.

Check Point Research revealed that businesses witnessed 50% more attacks per week in 2021 compared to 2020. To stay competitive, businesses must ensure their data is securely backed up and protected, and easily recoverable in case of emergencies.

Criticality of Having a SaaS Backup



Top three SaaS solutions for MMEs - —

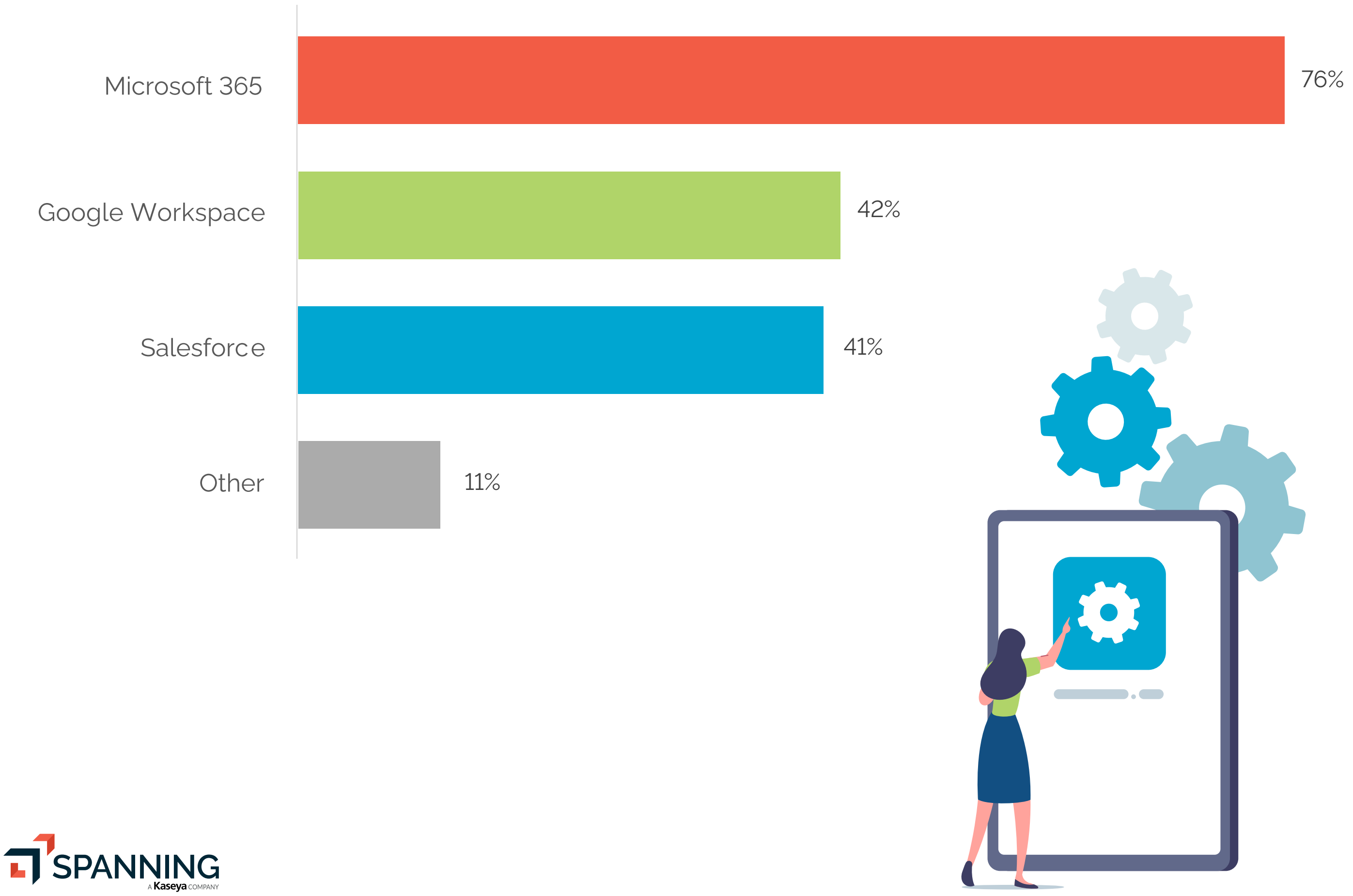
SaaS solutions grew in popularity and their adoption drastically increased as social distancing became a mandate in the wake of the global pandemic. Cloud computing has enabled companies to change the way they operate and is now an integral part of modern business.

When asked what other SaaS applications they would like to have backup and recovery for, more than 75% of respondents said Microsoft 365, followed by Google Workspace (42%) and Salesforce (40%).

As of 2021, around 50% of all corporate data is stored in the cloud. The data suggests that businesses globally trust their cloud service providers with their sensitive data. However, the harsh reality is businesses using SaaS solutions, such as Microsoft 365, Google Workspace and Salesforce, lose data every day. In fact, 77% of companies that use SaaS applications suffered a data loss incident over a 12-month period.

SaaS providers such as Microsoft, Google and Salesforce operate under the shared responsibility model. Under this model, SaaS vendors are responsible for application uptime and availability, whereas customers are responsible for protecting their data against the most common causes of data loss, such as phishing, ransomware and malware attacks, human error, malicious behavior, and configuration and sync errors. Therefore, having a backup of your critical SaaS data can be the difference between recovering quickly from a catastrophic incident or grappling with expensive downtime and data loss.

Essential SaaS Solutions You Use in Your Business



Conclusion - —

About 80% of respondents cited backup and disaster recovery as the top IT priority in their organizations. More than half of the respondents (54%) consider cybersecurity as the greatest risk to their organizations today. More than 50% of respondents reported that SaaS backup is crucial to mitigate risks associated with disruptive incidents. More than 30% of respondents cited easy access to support as the top IT vendor quality that makes doing business with them easy. A staggering 87% of MMEs said SaaS backup is highly critical for their business. Microsoft 365, Google Workspace and Salesforce emerged as the top three SaaS solutions that MMEs would like to have backup and recovery for.

Spanning Backup for Microsoft 365, Google Workspace and Salesforce fills the gaps in native functionality to protect critical data against the most common causes of data loss like phishing, ransomware and malware attacks, human error and more. Spanning is unique in its ability to enable both administrators as well as end users to quickly find and restore data to its original state in just a few clicks. This helps users restore lost or corrupted files quickly and meet even the most ambitious recovery time objectives (RTOs).

Some regulations require companies to keep data within their company's geographic borders. At Spanning, we support the idea of holding your valuable data in your preferred location to manage its sovereignty and enhance security. Our data centers are well distributed in the U.S., EU, Asia-Pacific, Canada and in the UK, to meet the unique needs of our customers.

We focus on making sure that our products are easy to use. But we know that sometimes our customers have questions, or just simply need a little help. That's why we provide 24/7/365 support via email to all our customers.

To learn more about SaaS data backup and recovery, and how Spanning Backup can help protect your Microsoft 365, Google Workspace and Salesforce data effectively, visit us today.