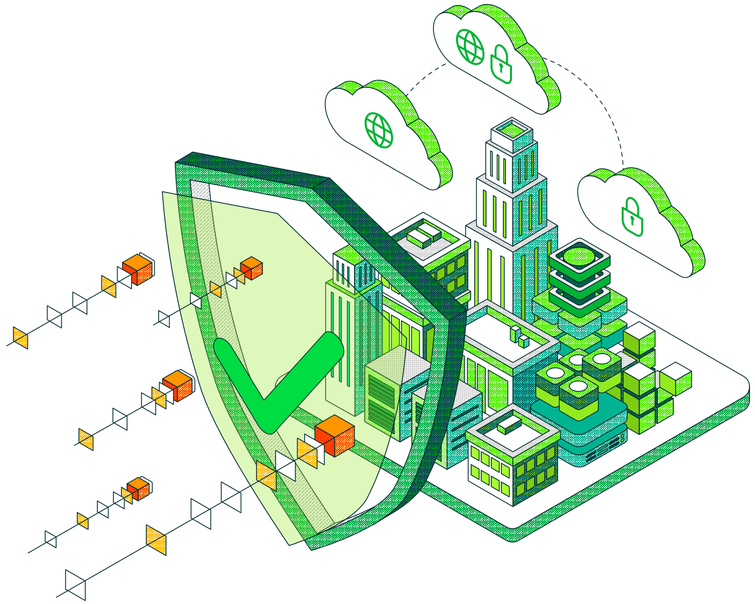
Data Protection Trends Report 2023



Contents

Introduction

In late 2022, an independent research firm completed their survey of **4,200** unbiased IT leaders and implementers on a variety of data protection drivers, challenges and strategies. This broad-based market study on unbiased organizations across **28** countries is conducted annually on Veeam's behalf to understand how the data protection market continues to evolve, so that Veeam can ensure product strategies and market initiatives align with where the market is going.

The global data protection market continues to grow, with respondents revealing that their data protection budgets will increase by **6.5%** for 2023. That is notably larger than expected when compared to how Gartner* predicted a **5.1%** increase in overall IT budgets and the IDC** predicted a **5.2%** increase in overall IT spending.

Of the **2,100** respondents answering budget questions in this survey, **85%** of organizations worldwide expect to increase their data protection budget, while **7%** will remain flat and **9%** will decrease their budgets. Of those increasing their budgets, they will do so by **8.3%** above their 2022 data protection spending.

This report is presented in three sections:

1.0 MACRO TRENDS IN DATA PROTECTION

2.0 CYBERATTACKS AND OTHER OUTAGES

3.0 CLOUD CONSIDERATIONS

* Gartner IT Symposium/Xpo™ 2022, October 2022
** IDC, Global ICT Spending Forecast 2020–2023, October 2022

About the research

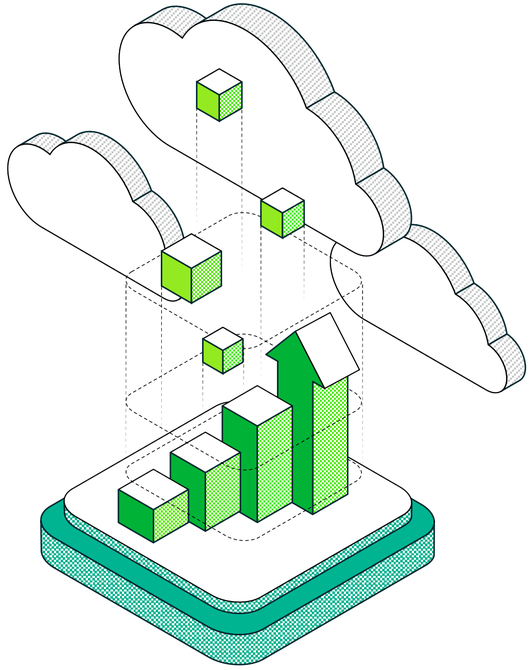
This research report summarizes the responses of 4,200 organizations of all sizes:

- **11%** Small and mid-sized organizations (100 to 499)
- **11%** Commercial organizations (500 to 999)
- **36%** Small enterprises (1,000 to 2,499)
- **24%** Enterprises (2,500 to 4,999)
- **18%** Large enterprises (5,000 or more employees)

Questions about these research findings can be sent to StrategicResearch@veeam.com

1.0

Macro Trends in Data Protection



1.1

Hybrid infrastructure 2020–2025

This chart now encompasses more than **12,000** respondents taken over four years, where each year organizations were asked about the % of on-prem physical versus on-prem virtual versus cloud-hosted servers for today AND what they expected the mix to be two years in the future.

Physical servers and virtual machines have both stabilized at around **50%** of an organization's overall IT plan, with the rest being cloud hosted — and a relatively even balance of physical to virtual within the data center.

And while the 2023 statistics show a very slight resurgence of the data center compared to the cloud, one possible justification is the pent-up demand for updating hardware infrastructure that was already aging during the pandemic, which only now is able to be replaced due to some improvement in IT supply chains.

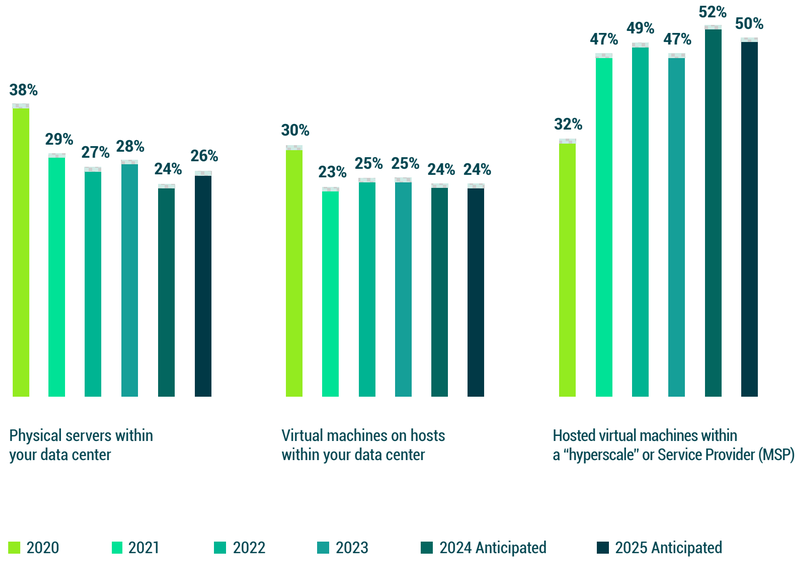
That said, the anticipated shifts between 2022–2024 and 2023–2025 still show an aspiration to gradually dilute data center infrastructure in deference to cloud-hosted services.

The key takeaway is that Modern Data Protection solutions must provide equitable capabilities across all three architectures (physical, virtual and cloud). In addition, one should plan for workloads moving across clouds and even back on premises; and again, the data protection strategy should accommodate that fluidity.

Figure 1.1

What do you estimate is your organization's percentage of servers in each of the following formats currently?

What do you anticipate the percentage will be in two years' time?



1.2

What does 'enterprise backup' mean?

For the second year in a row, the most often sought, and the most important attribute of an "enterprise backup" solution, is the protection of IaaS and SaaS. This should not be a surprise when considering the shifts to cloud seen in **Figure 1.1.**

Again, for the second year, protecting enterprise applications such as Oracle or SAP HANA is the second most common requirement for "enterprise backup" solutions.

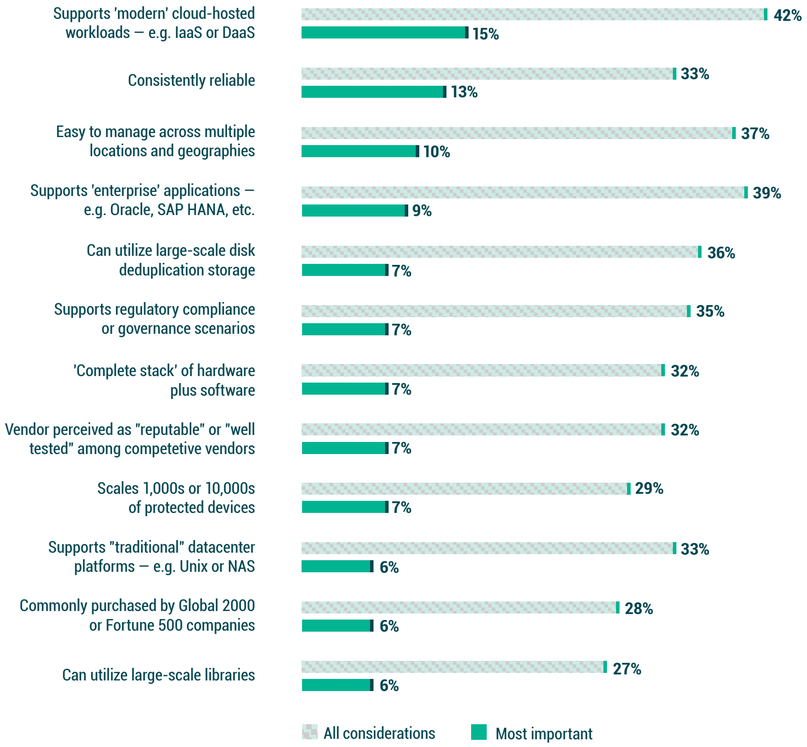
What might surprise some is that assuring reliability is the second most important criteria. But when considering that many legacy IT environments may be running legacy backup solutions that were designed for the physical data center era, those solutions likely run agent-based approaches for protecting cloud workloads, much like they attempted to run agents within VMs during the virtualization era of the past 15 years.

Legacy backup mechanisms rarely yield good outcomes when protecting modern workloads; so, one would presume that reliability when protecting modern workloads has suffered. As such, it should come as no surprise that cloud-hosted protection and reliability would be adjacent and top of mind.

Figure 1.2

What does 'enterprise backup' mean to you?

If your organization was considering a new 'enterprise backup' solution today, which attribute would be most important to them?



1.3

Does your organization have a reality gap?

There are two kinds of gaps:

- The **availability gap** asks whether IT systems are durable enough to ensure business productivity
- The **protection gap** ensures that data isn't lost

In both cases, four out of five organizations have the perception or belief that they have a gap – i.e., a sense of dissatisfaction or anxiety between what business units expect and what IT services can deliver.

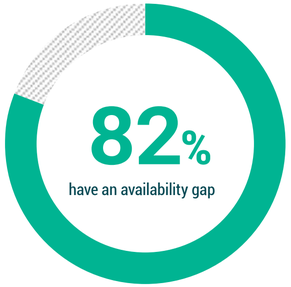
In an era of hybrid cloud, it is important to recognize that some cloud-hosted offerings are natively durable; implying that in certain circumstances, the **availability gap** might be closing. Meanwhile, the **protection gap** still exists as much, if not more in cloud services as it does within the data center because most cloud providers do not back up their 'subscribers' data.

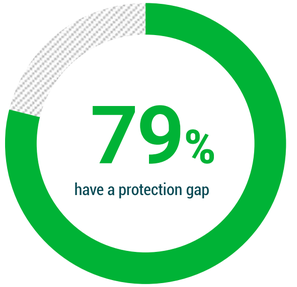
For example, Microsoft 365 provides infrastructure that is natively durable, meaning that users can transparently receive e-mails from one of multiple data centers with no difference in the user experience. However, user deletions and overwrites are also replicated to all copies within milliseconds. More importantly, regulatory mandates for seven-year retention or destruction apply just as much to durable cloud services as they do to data center servers, hence the protection gap still matters just as much as it ever has.

Figure 1.3

My organization has an "Availability Gap" between how fast we can recover versus how fast we need applications to be recovered and our users returning to full productivity.

My organization has a "Protection Gap" between how frequently our data is backed up versus how much data that we can afford to lose after an outage.





1.4

Why change backup solutions?

When organizations were asked what would drive them to change their primary backup solution, the most common, as well as the most important, reason was **improving reliability**, which is consistent with what organizations are looking for in an enterprise backup solution **(Figure 1.2)**.

The next several criteria relate to flexibility and choice of methodology; with opposite points of view nearly adjacent to each other:

- Diversity of tools <> Consolidate to a single solution;
- From BaaS to OnPrem <> From OnPrem to BaaS;
- Deploy software-only <> Deploy as an appliance;

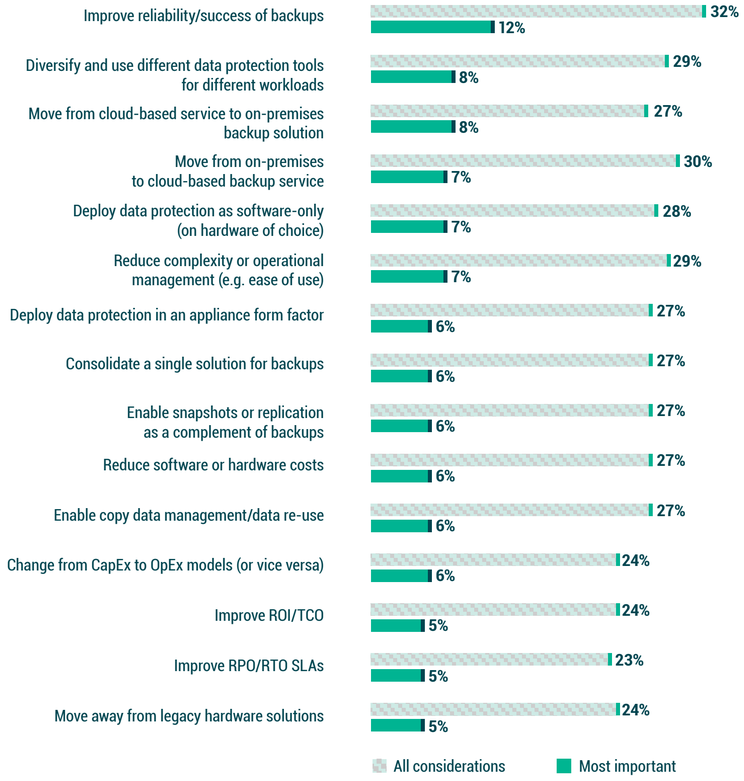
Two other notes:

- All three economic considerations are near the bottom third of the list, implying that if functionality doesn't improve, then simply saving money won't drive change.
- Improving RPO/RTO SLAs (qualitative improvement) is near the bottom of the list, whereas simply foundational reliability and success is at the top.

Given concerns of ransomware and the native durability of some cloud services, the key requirements for 2023 are **assured reliability** and **flexibility of choice**.

Figure 1.4

Which of the following would drive your organization to change its primary backup solution to a new solution or service?



1.5

What to look for in 'modern' data protection?

It should not come as a surprise, during ransomware and various other cyberattacks, that the most common and most important aspect of a "modern data protection solution" would be the integration of data protection within a cyber preparedness strategy.

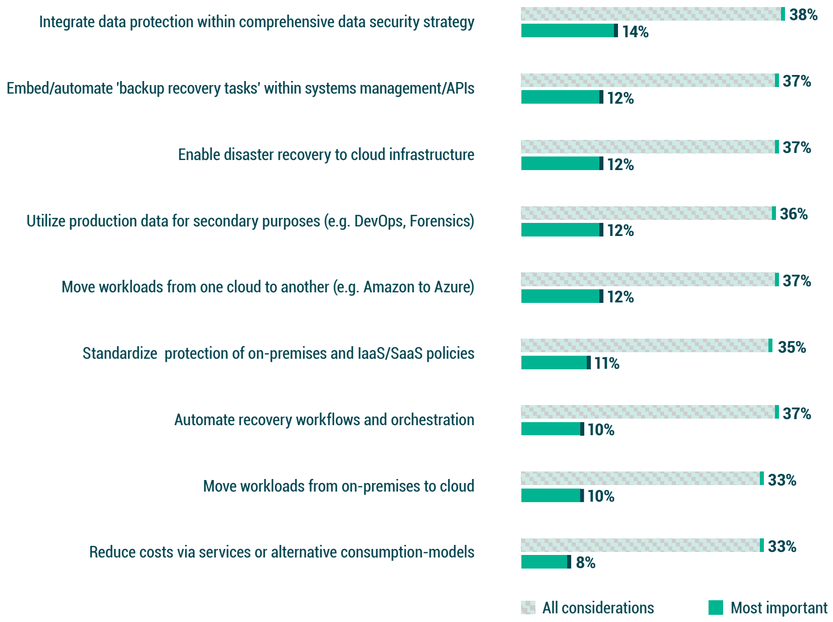
Adjacent to that, backup should be more integrated within a broader systems management framework (or managed via APIs). These two imply that backup, like cybersecurity, should be holistic parts of a single IT strategy.

Many of the other most common merits deal with **cloud-based services as part of either production or protection strategies**, with perhaps the most compelling being the ability to move workloads from one cloud to another. While there are many ways to move production workloads from on premises to a cloud, hyperscaler tools do not enable an organization to move workloads from a cloud back to on premises or to another cloud. This is admittedly only achievable through some third-party backup technologies.

Figure 1.5

Which would you consider to be defining aspects of a "modern" or "innovative" data protection solution for your organization?

Most important?



1.6

The Veeam Perspective

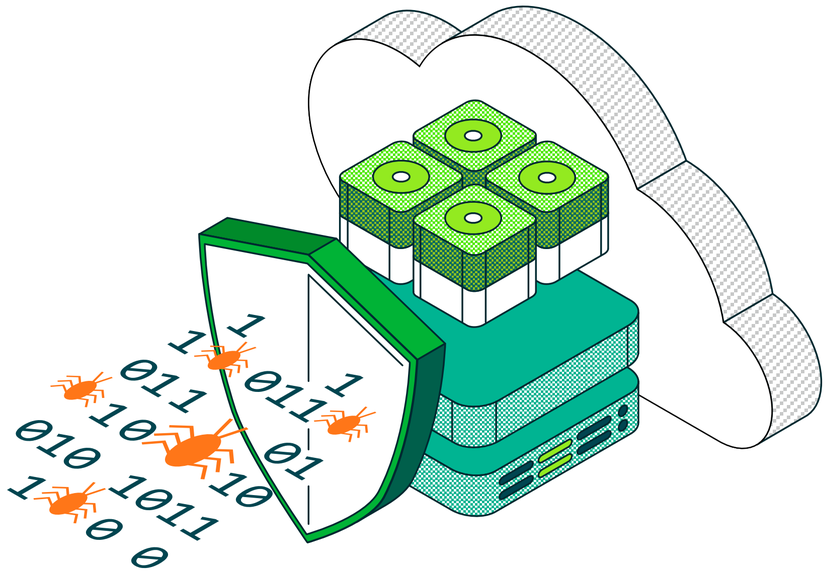
The Veeam Data Platform provides secure solutions at scale that enable Modern Data Protection that is driven by capabilities focused on achieving any recovery objective, getting the most out of your infrastructure and improving confidence with reliable products that “just work." Today's modern IT strategy is hybrid- and multi-cloud, so Veeam delivers purpose-built backup and recovery for the entire enterprise data center, including AWS, Microsoft Azure and Google, with native coverage for IaaS, PaaS and SaaS workloads unified for centralized management, licensing and extensive data portability.

Considering all this, it is no wonder that Veeam was named the 2022 Gartner Magic Quadrant leader for the 6th consecutive year. Veeam protects over 450,000 customers worldwide, including 81% of the Fortune 500 and 70% of the Global 2,000.

Click here to learn more about the Veeam Data Platform.

2.0

Cyberattacks & Other Outages



2.1

What causes outages?

Consistent with the other data points related to the imperatives around ransomware prevention and remediation, when organizations were asked about the most common cause of outages over the last three years, as well as the cause of the most impactful outage for each of those three years, ransomware was number one.

Said another way, cyberattacks caused the most impactful outages for organizations in each of 2020, 2021 and 2022.

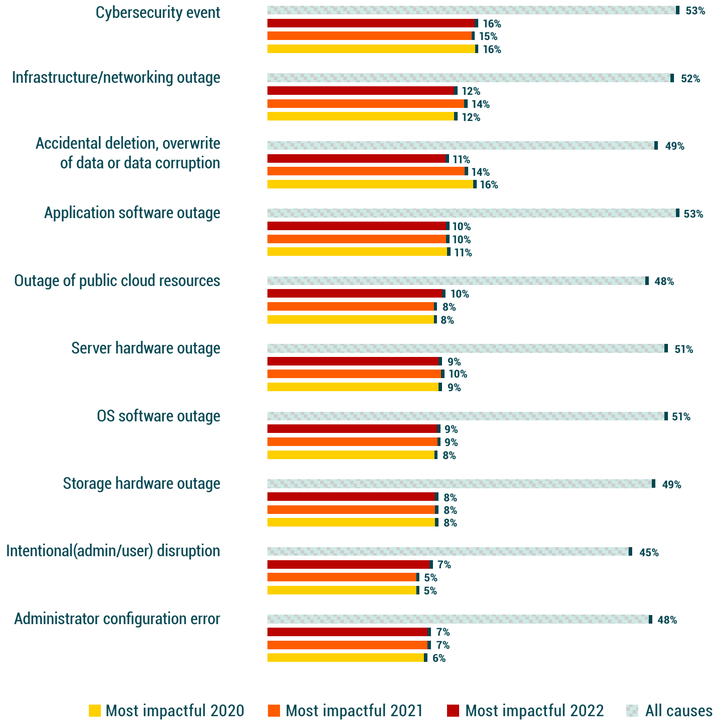
That said, it would be a significant strategic error to presume that the only design criteria for backup is in preparation for ransomware remediation. Systems outages, caused by networking (which can be exacerbated by cloud services) as well as application failure, hardware failure, and OS issues are all still commonplace even within modern data centers.

So, organizations' data protection strategies should encompass both the breakages that continue to occur as well as human-caused events, including both user error and cyber criminals.

Figure 2.1

Over the past two years, what were the most common causes of the outages that your organization experienced?

Which was the most impactful in 2020, 2021, and 2022?



2.2

Unexpected outages happen more often than you think

In 2022, just over one in four servers had at least one unexpected outage in the last year. Admittedly, this statistic is down from the **40%** of servers that experienced at least one unexpected outage in 2021 (as reported in the DPR2022 report).

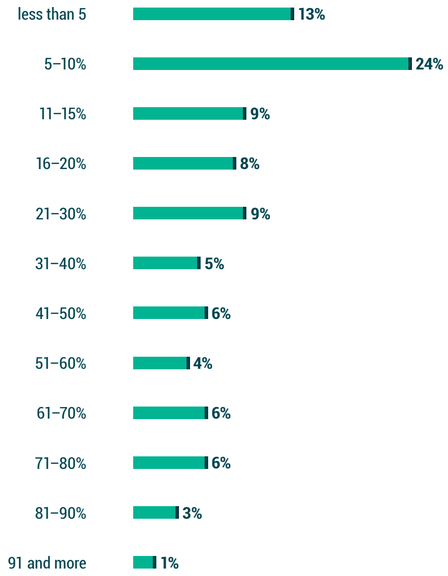
One would presume that as organizations continue to embrace cloud-hosted services with more native resiliency or durability that is built in, outages and therefore availability issues might recede.

Notwithstanding "availability," organizations have a wide range of concerns related to data protection (long-term retention, previous versions, etc.) that will continue to need addressing even as IT availability gains some level of improved resiliency through cloud solutions.

28% of servers have at least one unexpected outage

Figure 2.2

What percentage of your servers had at least one unexpected outage (even an unplanned reboot) within the last 12 months?



2.3

BC/DR site recovery methods

As cloud services become increasingly more common in data protection strategies, a frequent question is whether to recover data back to on-premises servers or into cloud-hosted infrastructures instead.

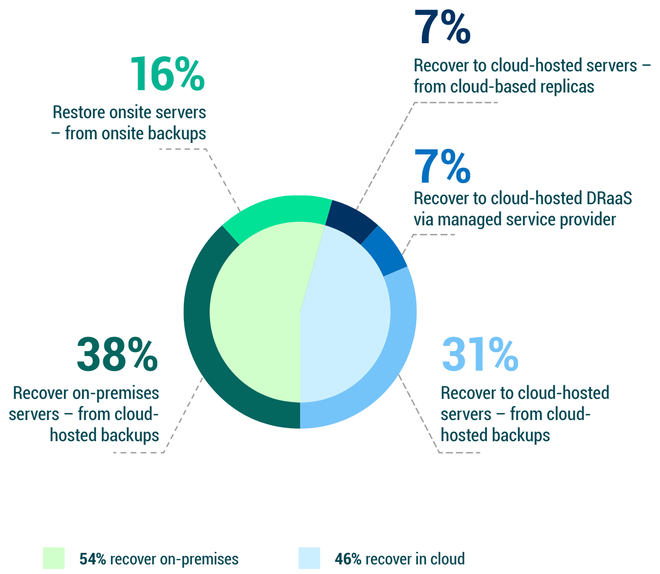
There is nearly an even interest between on-premises and cloud-hosted recoveries for 2023, which marks a **7%** shift toward cloud-hosted recoveries since last year:

- In 2022, **61%** planned on recovering on premises versus **39%** in the cloud.
- For 2023, **54%** expect to recover on premises versus **46%** in the cloud.

But even for those organizations that are recovering on premises, the majority of the source data will come from cloud-hosted backups. This is consistent with the sentiment regarding less recovery points on premises and more urgency to get data out of the building to cloud-based storage as part of data retention and ransomware or BC/DR preparedness.

Figure 2.3

How are operations resumed for your organization's DR function?



2.4

BC/DR failover mechanisms

When considering both operational recoveries and disaster recoveries, one of the key considerations beyond simply having recoverable data is how quickly the restored and recovered servers can be brought online to resume business operations. When organizations are looking at failover mechanisms:

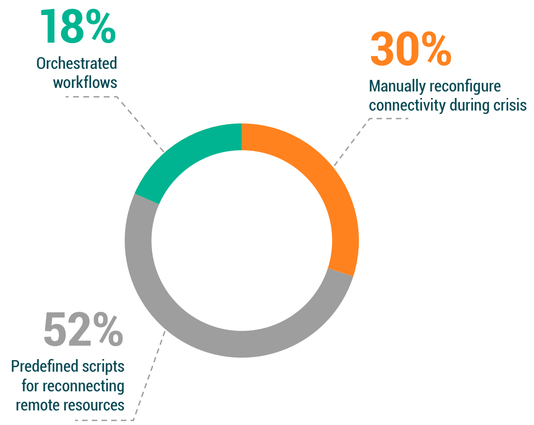
- One in three **(30%)** surprisingly expect to manually reconfigure resources during the crisis.
- Half **(52%)** are planning on using scripts.

When considering the best practice of assuming that the primary experts are no longer available during a crisis, a strong recommendation from most BC/DR planners is to utilize orchestrated workflows, whereby the expertise can be encapsulated in processes. It's also recommended to test workflows the same way that it will be executed during an actual crisis.

Unfortunately, this year's survey results revealed only **18%** (less than one in five organizations) currently have an orchestrated workflow capability within their current data protection or failover strategy.

Figure 2.4

What kind of failover/failback mechanisms does your organization use for resuming functionality?



RANSOMWARE TRENDS REPORT 2022

2.5

Ransomware is a disaster

One of the most heartening discoveries of last year's Data Protection Report 2022 was the acknowledgement that a growing number of organizations handle their cybersecurity or ransomware remediation strategy as part of their more holistic BC/DR planning process. That sentiment is shared by **82%** of organizations in 2023.

This is understandable considering the increasing frequency of ransomware attacks:

- In 2021, **76%** of organizations were successfully attacked by ransomware at least once.
- In 2022, **85%** of organizations made that same declaration.

In both cases, the inverse is overly optimistic; of the **24%** (2021) or **15%** (2022) of organizations that believe that they were not hit, many have simply not discovered the intrusion yet. As startling as those statistics are, the results of those attacks are even worse. When organizations were asked about their most significant attacks suffered in 2022:

- **39%** of their entire production data set was successfully encrypted or destroyed.
- Only **55%** of the encrypted/destroyed data was recoverable.

Be sure to also check out the Ransomware Trends Report for 2022.

Figure 2.5

How aligned are your organization's strategy(s) for cybersecurity vs. Business Continuity/Disaster Recovery (BC/DR) strategy?

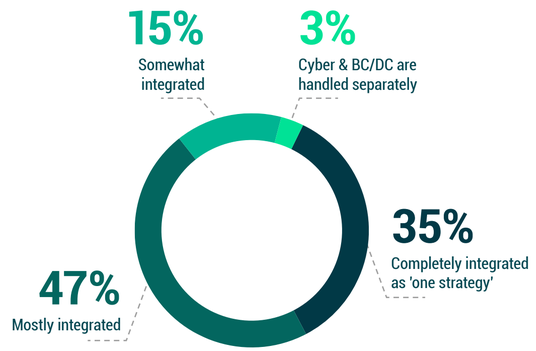
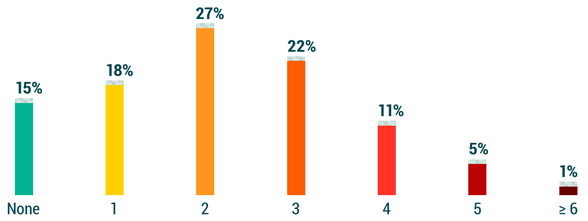


Figure 2.6

How many ransomware attacks has your organization suffered in the last 12 months?



2.6

Challenges to achieving Digital Transformation

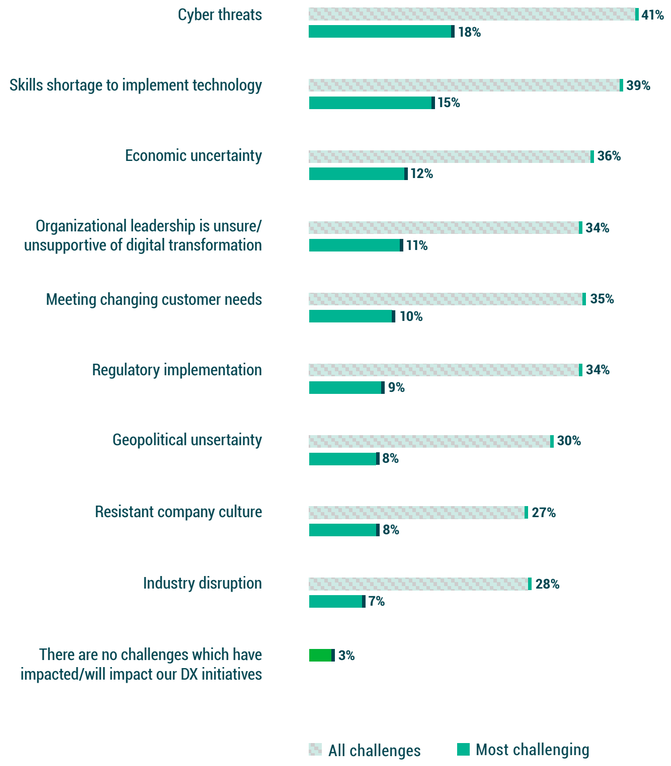
Ransomware is not just an operational or tactical concern. When organizations were asked about the various hindrances to Digital Transformation and IT modernization initiatives for 2023, cyberthreats were considered the most common challenge as well as the most concerning. This is likely due to two reasons:

- As the most common cause of outages and impactful outages **(Figure 2.1)**, it is a direct hindrance to DX or ITM because organizations are forced to divert all available manpower and resources to recovery.
- Financial resources and expertise that might have been applied to agility-creating Digital Transformation initiatives must instead be applied to simple cyber prevention.

Figure 2.7

When it comes to your organization's ability to achieve your Digital Transformation initiatives, which do you believe will be a challenge over the next 12 months?

What will be most challenging in 2023?



2.7

The Veeam Perspective

Cyberattacks have become the number one threat to organizations and has forced companies to re-think their data protection strategies. Veeam's focus has been to ensure data is securely backed up and tested so you can reliably restore in a crisis and eliminate the threat of data loss. We do this by providing multiple layers of immutable storage both in the cloud or on premises based on your network design. This flexibility also lowers operational costs and increases security by using the existing storage platforms.

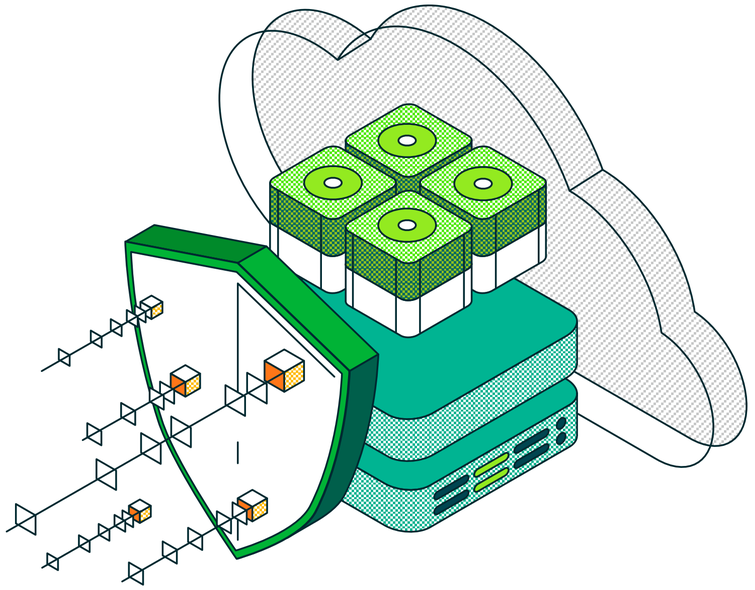
As attacks have become more sophisticated, we see an increasing need to add automation and orchestration to disaster recover processes. Veeam provides the ability to automatically create, test and maintain disaster recovery plans to provide consistency in the BC/DR process. Our alerting and reporting capabilities provide instant notification of changes to the environment that may indicate an attacker is accessing backup repositories. Together, these capabilities remove manual tasks from the DR process and increase efficiency in recovery.

The year-over-year increase in ransomware attacks makes the verification of backup data critical to a successful recovery. Without secure, trusted backups, you risk data loss and increase the possibility of a ransom payment. To avoid these worst-case scenarios, the speed of data recovery is critical, which is why Veeam provides the fastest recovery options in the industry, allowing you to get back to normal business operations without reintroducing threats into the environment. Veeam also has the people to help you every step of the way, including onboarding services, account management, and a specialized ransomware SWAT team to assist in the event of a ransomware attack.

To learn more, click here.

3.0

Cloud Considerations



CLOUD PROTECTION TRENDS FOR 2023

3.1

Long-term retention media

While many aspects of data protection strategies have evolved over the last 30 years, one consistent requirement remains: long-term data retention. Only **2%** of respondents do not have long-term regulatory mandates, implying that **98%** are susceptible to some industry, national, or other regulatory mandate to retain data for previous versions – for an average of 5.4 years.

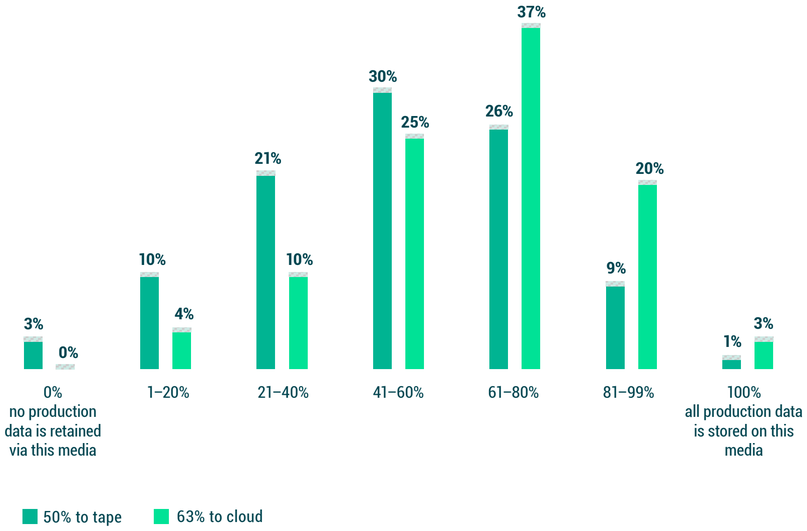
Other research reveals that organizations leveraging cloud services are retaining their previous versions for far less time than what is mandated. This implies a lack of understanding of compliance requirements in that data still retains the same long-term regulatory requirements, regardless of whether that data resides within on-premises servers or cloud services.

Is cloud-based storage a "tape killer"? According to **Figure 3.1**, **50%** of data is still written to tape at some point during its data lifecycle, whereas **63%** of data is now stored in the cloud at some point. Many organizations have a three-tier operating model for data retention, including:

- On-premises disk for 90–120 days
- Cloud copies, including a near current copy for BC/DR as well as previous versions of data that does not have long-term regulatory mandates for up to two to five years
- Tape for a minority of data (perhaps **20%** to **50%**) that has regulatory mandates to be stored for 10, 20, 50 years or more.

Figure 3.1

In addition to whatever disk-based backup solution you may be running, approximately what percentage of your production data is also backed up to tape and cloud?



3.2

Cloud-powered backup 2020–2025

Like the interleaving of DPR 2020, 2021, 2022, and 2023 results in **Figure 1.1**, **Figures 3.2** and **3.3** look at the annual changes and anticipated intentions around cloud-based data protection strategies.

When asked how the cloud services fit within their data protection strategy, organizations show a continued progression towards leveraging cloud services. It is notable that while organizations have not made much progress from 2021 to 2023, their aspirations remain consistent:

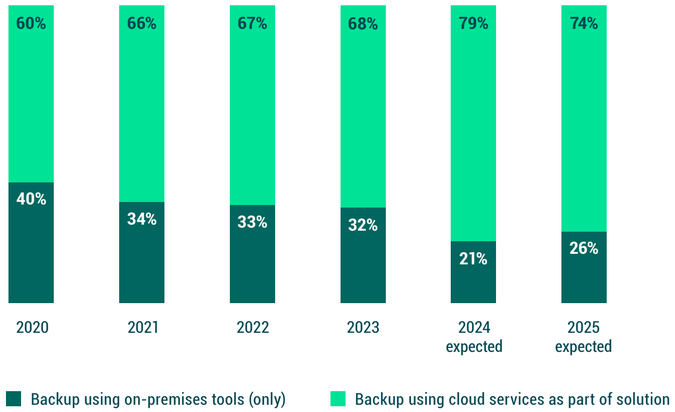
- 2022 respondents stated that **67%** of their backups used cloud services, with the intent to move towards **79%** within two years.
- 2023 respondents stated the same **67%** usage of cloud services today, with the aspiration of **74%** within two years.

Even with the tempering between 2024 and 2025 intentions, there is still a consistent desire to increase the use of cloud services as part of their data protection strategy even more so than today.

Figure 3.2

Which is your primary method of backing up today?

Which do you anticipate as your primary backup method in two years?



3.3

Cloud-powered disaster recovery 2020-2025

Easily one of the most powerful synergies between cloud-powered services and data protection is the advent of cloud-powered disaster recovery, whereby cloud infrastructures are leveraged instead of, or in compliment to, a secondary data center. It is exciting to see that over five years, the number of organizations that will have BC/DR capabilities has increased from **53%** to **74%**

Even in 2023 and beyond, there are still many reasons why organizations can achieve great agility and flexibility in their BC/DR strategies by leveraging multiple self-managed data centers. That said, the percentage of organizations using this approach may be declining as cloud-hosted secondary infrastructures become more commonplace, including both self-managed cloud hosting.(e.g., Amazon, Azure, GCP) as well as Disaster Recovery as a Service (DRaaS) which continues to grow from **23%** up to **55%**:

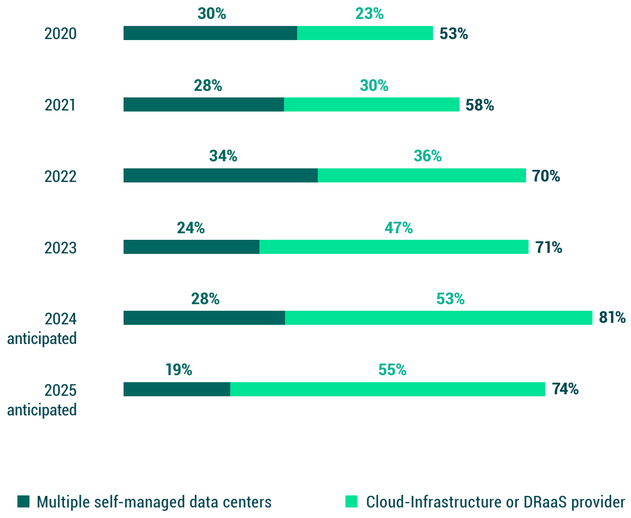
- 2022 revealed nearly even usage between data centers **(34%)** and cloud **(36%)**, with the aspiration of still using data centers at **28%** while cloud-based DR radically grew to **53%.**
- By similar margins, 2023 revealed **24%** using multiple data centers and **47%** using a secondary cloud infrastructure, with aspirations of **19%** using data centers and **55%** using cloud infrastructures by 2025.

There was a **10%** shift from 2022 to 2023, and in the aspirations of both samples, the percentage of organizations leveraging multiple data centers will decrease by roughly **5%** over 2 years, while the number of organizations leveraging cloud-powered DR will grow by **10%** or more.

Figure 3.3

Does your organization's BC/DR strategy primarily rely on your own datacenters or cloud-hosted infrastructure today?

What do you anticipate in two years?



3.4

How is Kubernetes backed up?

Containers, and more specifically Kubernetes, shows all the hallmarks of a burgeoning mainstream production platform, with the same kinds of data protection strategy disparities as one saw earlier in early adopters of SaaS five years ago or virtualization 15 years ago.

- As a positive, the strategy for defining data protection is being influenced by at least four major stakeholder groups, listed in **Figure 3.4**, with surprisingly equal representation.
- As a negative, the most cited method for protecting containers **(Figure 3.5)** is to simply protect the underlying storage. It is, however, reassuring that only **5%** of organizations that leverage Kubernetes believe that they have no data to back up.

One in four organizations use a third-party backup tool for protecting the containers framework in its entirety. If containers follow the same adoption curve to mainstream that SaaS and virtualization did in the past, a significantly growing portion of the market will discover that simply protecting the storage (or other underlying components) will be unsatisfactory when trying to restore, due to either data corruption or a cyber event. At which point, like every burgeoning platform before it, third-party backups will become the norm.

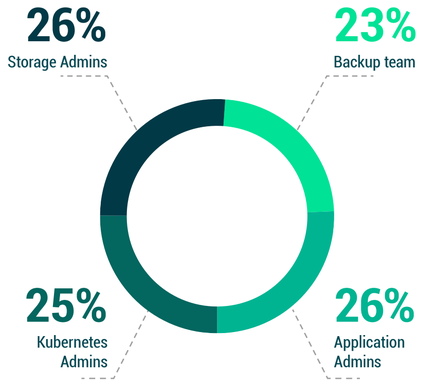


Figure 3.4

Who is responsible for defining the data protection requirements within your organization for containerized applications?

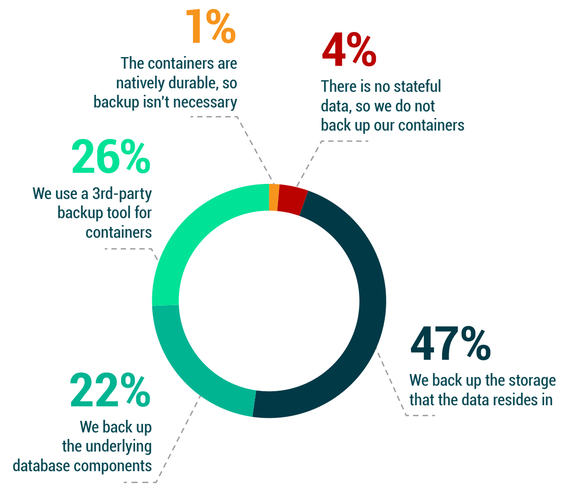


Figure 3.5

How does your organization primarily back up data within its containers?

3.5

Will 2023 be the year of 'change?'

Between the angst of ransomware, the pressures of ensuring IT services across a rapidly evolving and often remote/hybrid user community, and the challenges of protecting modern IaaS and SaaS workloads, one might presume that many organizations are likely to switch backup solutions in an effort to adapt to these changing pressures and conditions.

You'd be right! Ignoring the **35%** of near-neutral responses:

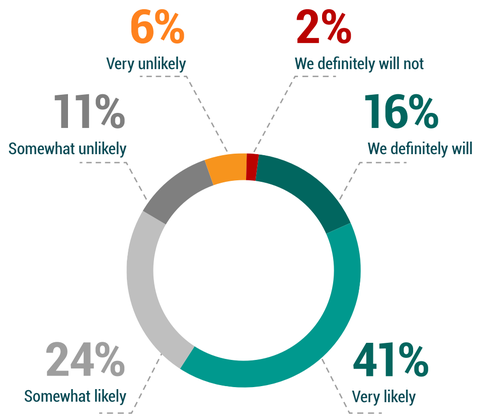
- Only **8%** of organizations are unlikely to switch their primary backup solution in 2023
- Meanwhile, **57%** of respondents expressed that they are likely or definitely will switch backup solutions

For those reading this research, ask yourself:

- What is driving your interest in switching solutions? **(see Figure 1.4)**
- What should you be looking for in a more modern approach to enterprise backup? (**Figures 1.2 and 1.5)**

Figure 3.6

What is the likelihood that your organization will switch its primary backup solutions/services within the next twelve months?



3.5

The Veeam Perspective

As organizations continue to transform their infrastructure, ensuring support for backup of cloud-based workloads, effective usage of backup to the cloud, and ultimately the assurance that backup can support mobility across clouds, there's a need for a solution that makes the complex comprehensive. The Veeam Data Platform offers:

- Storage cost control with an intelligent cloud storage tiering architecture;
- Purpose-built, Kubernetes-native backup and restore, disaster recovery and mobility for containerized applications;
- Broad workload support across IaaS/PaaS/SaaS services;
- Centralized monitoring and management, coupled with extensive API coverage;

New or current Veeam users should check out Veeam Backup for AWS, Azure, Google Cloud Platform, Microsoft 365, Salesforce and Kasten for Kubernetes to see industry-leading capabilities built for the unique needs of the hybrid cloud.

For Veeam users who are looking for "as a Service," or to fill a resource gap, Veeam partners with an extensive network of BaaS and DRaaS providers, and professional services specialists, to ensure users maximize their Veeam + cloud investments.

For questions on this research or its usage: StrategicResearch@veeam.com

Summary

This analysis covers the opinions of **4,200** unbiased organizations on a variety of data protection trends, with the most notable insights being:

- **Reliability** and **consistency** (of protecting IaaS and SaaS alongside datacenter servers) are the key drivers for improving data protection in 2023. For organizations that are struggling to protect cloud-hosted data with legacy backup solutions, it is likely they will supplement their data center backup solution with IaaS/PaaS and/or SaaS capabilities.
- **Ransomware** is both the most common and most impactful cause of outages, but it would be irresponsible to over rotate your data protection solution to be singularly focused on cyber preparedness, because other disasters (fire, flood, etc.) and user errors (overwrites, deletion, etc.) still occur. That said, ensuring your data recovery tools can integrate with other cyber detection and remediation technologies is paramount for comprehensive cyber resilience.
- **Cloud-based services** seem nearly inevitable for organizations of all sizes. But similar to how there isn't just one type of production cloud, there isn't just one protection cloud scenario. Organizations should consider cloud tiers for retention, Backup as a Service **(BaaS)**, and ultimately Disaster Recovery as a Service **(DRaaS)**.

About Veeam Software

Veeam® is the leader in Modern Data Protection. The company provides backup, recovery and data management solutions through a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Veeam customers are confident their apps and data are protected from ransomware, disaster and harmful actors and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects **450,000** customers worldwide, including **81%** of the Fortune 500 and **70%** of the Global 2,000. Headquartered in Columbus, Ohio, with offices in more than 30 countries, Veeam's global ecosystem includes **35,000+** technology partners, resellers and service providers and alliance partners. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @Veeam-Software and Twitter @Veeam.

About the authors

Jason Buffington
VP, Market Strategy

@JBuff
@jasonbuffington

Dave Russell
VP, Enterprise Strategy

@BackupDave
@backupdave

Julie Webb

Director,
Market Research & Analysis

veeam.com