
veeam
Insights
Data Protection
Trends Report
2024

Introduction

In late 2023, an independent research firm surveyed 1,200 IT leaders and implementers on a wide range of their data protection challenges and strategies. This is the fifth annual release of the Data Protection Trends report in its current methodology* to quantify the challenges and drivers of the data protection industry, always using analyst and research firms to garner an impartial understanding of how data protection must continue to evolve.

2024 is starting off with IT teams having an interest in changing solutions and their own roles, which will either radically improve their cyber preparedness and compliance postures or further widen the expectations between what business units are expecting and what IT is able to deliver.

Aside from organizational and methods changes, the primary drivers of change and what organizations are looking for remains consistent in 2024, with the reactive pressures against ransomware and the proactive initiatives of embracing and protecting cloud-hosted workloads.

Unsurprisingly, 2024 will be another year where most data protection strategies will be fundamentally designed around preparing organizations against ransomware and other large IT interruption at scale.

2024 is Another Year for Changing Solutions

For the second year in a row, over half of organizations anticipate changing their primary backup solution. It is notable that while the intent to change remains high and consistent (54% for 2024 vs 57% for 2023), there is a growing percentage of those remaining with the status quo (8% not intending to change in 2023 vs. 27% in 2024). It is worth noting that one could consider changing from a self-managed solution to managed service (offering the same backup software), as well as changing technologies or vendors. In any case, it will be another year of change. Perhaps this is not surprising considering:

85% of organizations recognize an 'Availability Gap' between how fast they could recover versus what the business processes require. 76% of organizations recognize a 'Protection Gap' between how much data they could afford to lose and how often their data is protected.

Also consistent is the expectation to grow data protection budgets, with 2024 spending expected to be 6.6% higher than the previous fiscal year. This is especially impressive since Gartner revised its overall 2023 spending down from 5.5% to 4.3% growth while IDC is expecting 5.4% growth in data replication and protection software. Meaning that this survey reveals that backup spending is exceeding the expectations of the major industry analyst firms. In fact, 92% of organizations intend to increase their data protection budgets for 2024, which is up from the 85% who planned to increase in 2023.

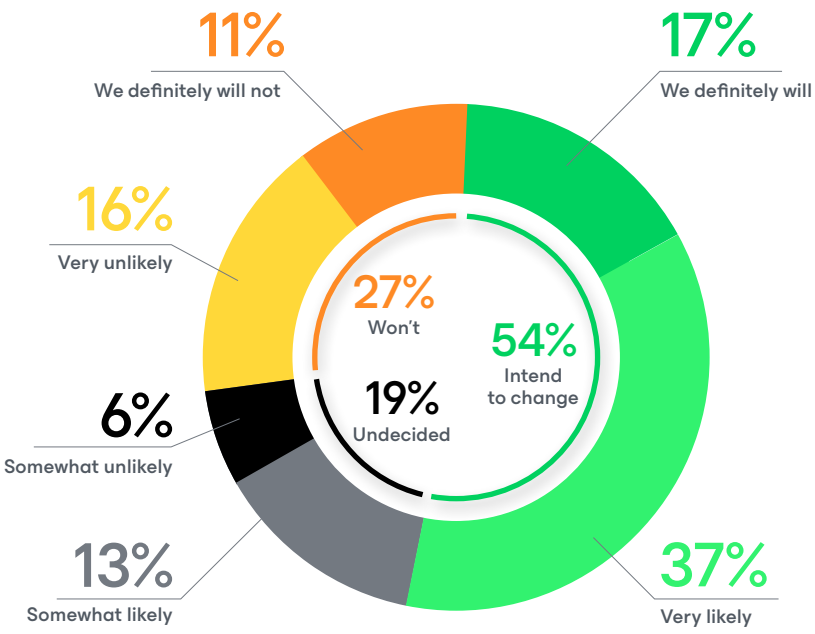


Figure 1

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

https://www.gartner.com/document/4714599
https://www.idc.com/getdoc.jsp?containerId=US51037523

2024 Could Also be a Year for Changing Roles

New to the survey for 2024 was the discovery that nearly half (47%) of IT leaders and implementers for data protection intend to seek a new job outside of their current organization. In contrast, only 1 in 3 intend to remain in role/org and another 1 in 5 are undecided. Perhaps this is less surprising when considering that the top five concerns (in order) that respondents had were:

- Lack of new skills or learning opportunities
- Inability to influence strategic direction
- Ramifications of a cyberattack or other disaster
- Lack of career development/progression
- Lack of management support

Other than cyberattacks/disasters, the four other concerns are 'solvable' by simply enhanced leadership support.

This market shift is both a challenge and an opportunity:

- It is incumbent on senior leadership to retain their existing data protection talent, to ensure their preparedness for cyber resiliency and other disaster preparation. Losing those experts puts the organization at a significant disadvantage when crises inevitably strike
- There is a strong opportunity to recruit data protection talent that may bring new skills in ensuring the hardening of data protection against cyber criminals, as well as new knowledge to protect modern production workloads that reside in clouds, such as Microsoft 365, Kubernetes containers, or other IaaS/PaaS architectures

One established way that organizations are choosing to de-risk their exposure against labor or skill shortages is by engaging managed BaaS or DRaaS providers that ensure deep solution knowledge, operational monitoring, and primary technical support.

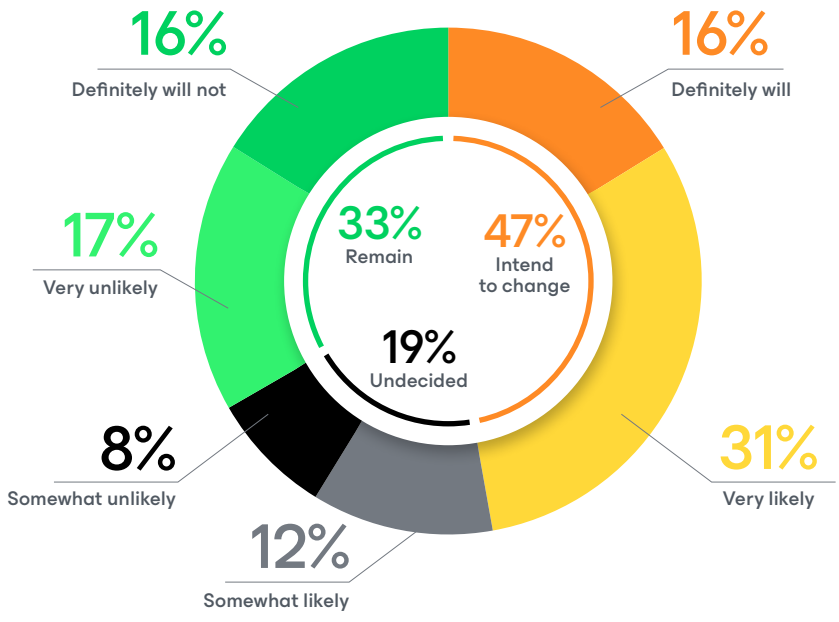


Figure 2

How likely is it that you will seek a new job outside of your current organization within the next twelve months?

Reliable Protection of IaaS & SaaS are Enterprises' Priorities

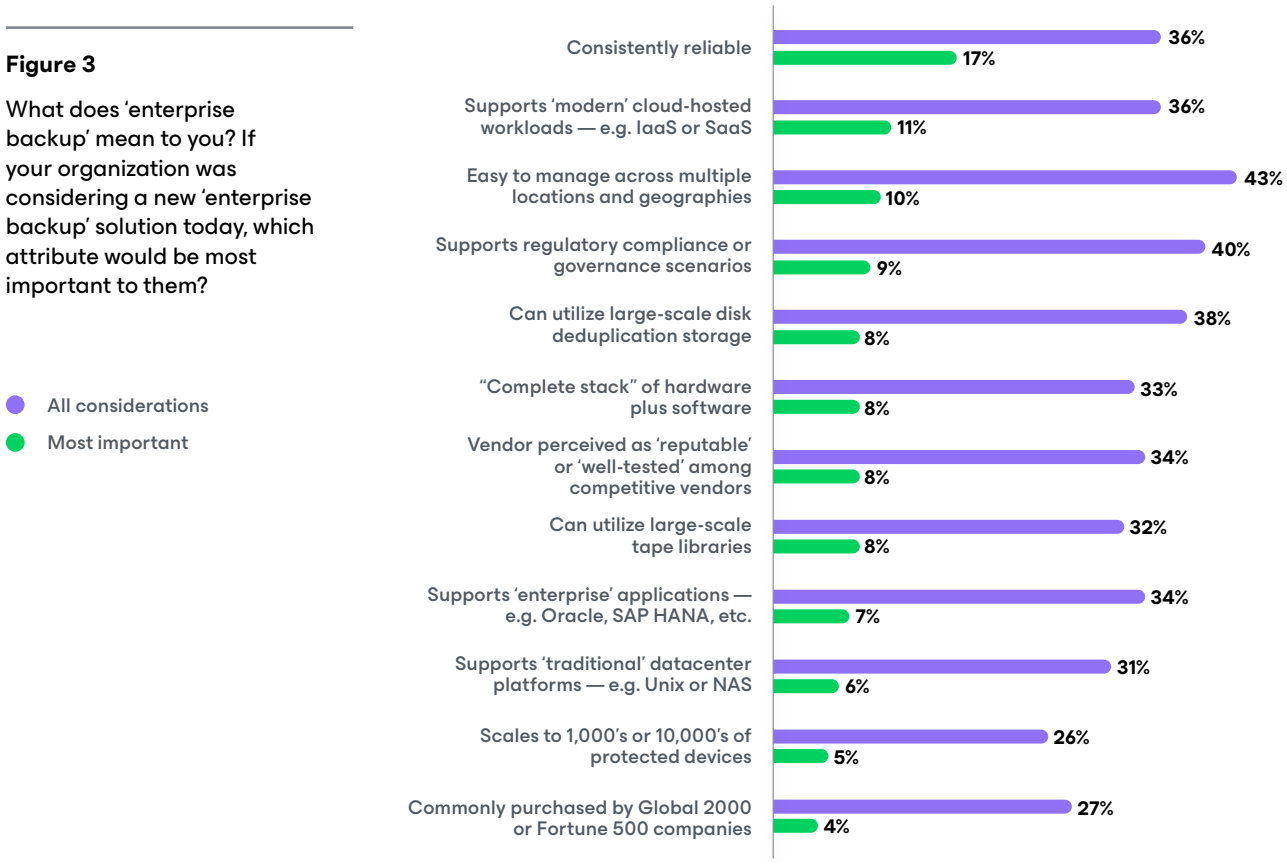
For the second year in a row, the two most important attributes sought in an 'enterprise backup' solution are **reliability** and the **protection of cloud-hosted workloads** (IaaS & SaaS). That said, the most common attributes being sought are the typical synonyms of 'enterprise' in **manageability** across locations and **compliance/governance**.

It is not a surprise that (improving) reliability and (better) protection of IaaS/SaaS are not only top of mind but adjacent in the list, since it is well understood that using legacy backup methods to protect modern workloads often results in unreliable or incomplete backups, thereby being unable to restore. It is notable that enterprise application (e.g. Oracle/SAP) and datacenter platform (e.g. UNIX or NAS) scored low in the list due to having been addressed as 'table stakes' by any backup solution, even those legacy offerings that have been datacenter-centric for decades. That said, datacenter workloads are not diminishing at the same rate that cloud-hosted workloads are spinning up. In 2024:

- 28% run on **physical servers** within datacenters
- 27% run within **virtual machines** within datacenters
- 45% run as **server instances** within cloud-hosts

Figure 3

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?



Data Protection Trends 2024 Report — published by Veeam in January 2024
N=1,200 unbiased IT Leaders and Implementers responsible for their organizations' data protection strategies.

Reliability and Ransomware Continue to be the Drivers of Change

For the past five years, **improving reliability/success of backups** has been one of the top two drivers for changing backup solutions, usually in the undeniable top spot like this year.

That said, the other top driver has changed over the years from qualitative improvement (RPO/RTO) to economic improvement (TCO/ROI), but more recently as well as this year — in preparation against ransomware. While one could argue that ensuring the ability to restore (by improving the reliability backups) is also inherently in response to cyber resiliency initiatives, respondents are also explicitly changing their primary backup solution in order to gain better **integration with detection/remediation capabilities,** as well as more **hardened or secure repositories** — e.g. immutability.

It is also notable that while economics is always part of any IT modernization conversation, sentiment around ROI/TCO as well as reducing actual costs were both among the least deterministic drivers of change; implying that saving money without improving capabilities is moot in the current threat landscape.

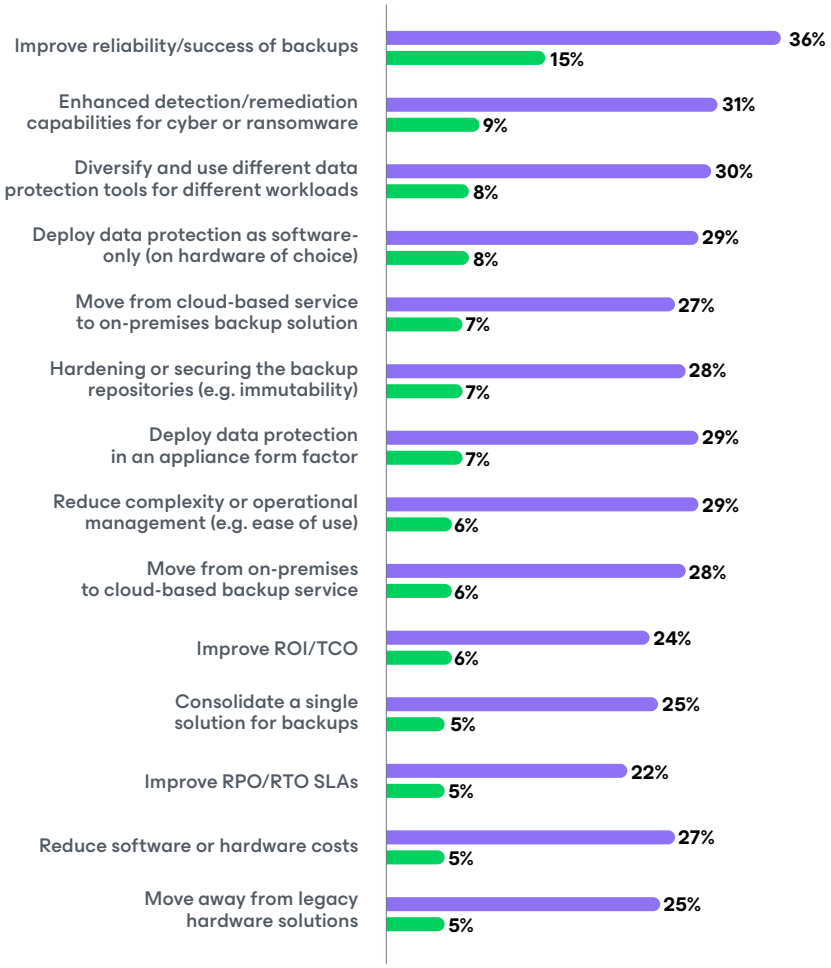


Figure 4

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

All considerations
Most important

Data Protection Trends 2024 Report — published by Veeam in January 2024
N=1,200 unbiased IT Leaders and Implementers responsible for their organizations' data protection strategies.

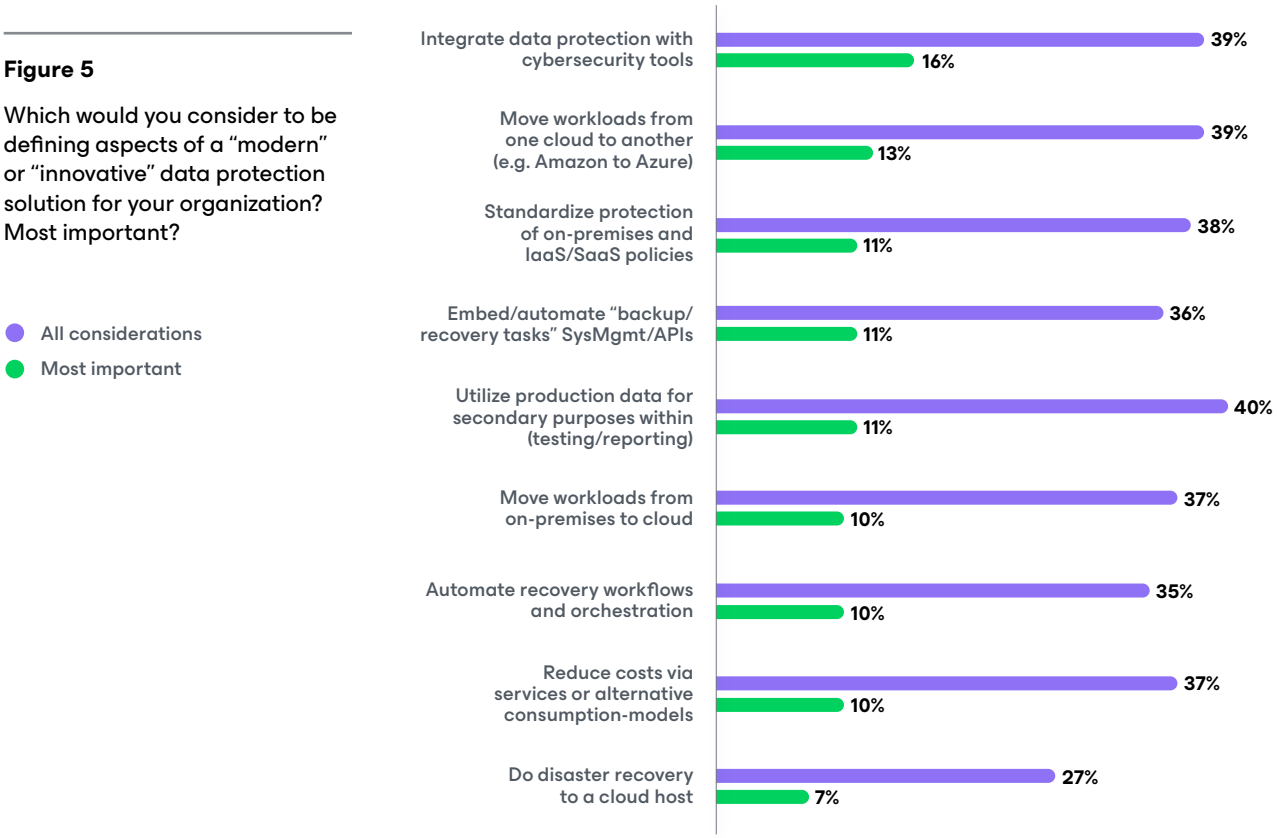
‘Modern’ in 2024 Must be Cyber-integrated and Hybrid-flexible

For the past few years, two macro themes of what does ‘modern’ or ‘innovative’ data protection mean, including integration between data protection and cybersecurity tools, as well being able to provide protection across myriad cloud scenarios. For the second year in a row, the most common and most important aspect of a modern data protection solution is one that integrates with cybersecurity tools, presumably across a range of capabilities from detection through remediation. It is notable that 2 out of 5 (41%) consider some aspect of mobility in cloud scenarios as most important characteristic of a modern solution, including:

- The ability to move a workload from one cloud to another, e.g. developed in Amazon, moved to Azure to utilize usage credits
- Standardization of protection between on-prem workloads and IaaS/SaaS, presumably again due to datasets needing to move based on business mandates (as well as technical considerations) but not wanting protection policies or assured recovery to suffer as a result
- It is notable that migrating a workload from on-premises to a cloud and the ability to disaster recovery to a cloud host are also both in the top ten since the mechanics of transforming an on-prem server (physical or virtual) into a cloud-hosted instance is nearly identical between the two initiatives. Said another way, a migration is simply a disaster that you can schedule

Figure 5

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



Data Protection Trends 2024 Report — published by Veeam in January 2024
N=1,200 unbiased IT Leaders and Implementers responsible for their organizations’ data protection strategies.

74% of Organizations Protect Their Microsoft 365 Data

As with most mainstream production platforms in their early years, workload owners often underestimate the need for purpose-built backup solutions, especially in regard to cloud-hosted platforms.

- In 2020[1], 69% relied solely on the built-in recycle bin or utility, while only **27%** backed up their Microsoft 365 data
- In 2022[2], 47% relied solely on the recycle bin or built-in functionality, while **45%** backed up their Microsoft 365 data
- In 2024, only 3% rely on the recycle bin, while 41% utilize 'legal hold' within enhanced M365 tiers and **74%** back up their Microsoft 365 data

Thankfully, only 4% still incorrectly assume that because Microsoft 365 is natively resilient, it does not require backups. That is contrary to Microsoft's published guidance on their Shared Responsibility Model and in fact, Microsoft announced it is developing a backup utility to do backups of M365 for organizations whose primary back up solution may be insufficient.

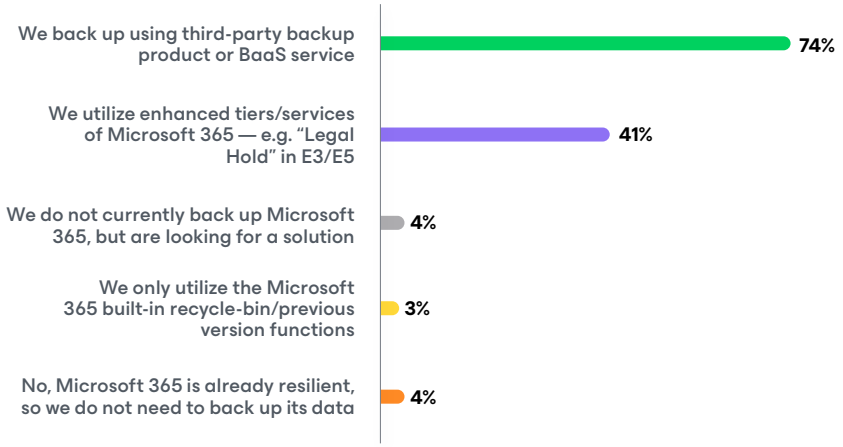


Figure 6

Does your organization back up the data from within Microsoft Office 365?

[1] 2020 Data Protection Trends Report (n=1,550), June 2020

[2] 2022 Data Protection Trends Report (n=3,400), February 2022

Containers are Everywhere, but Their Backups are Scattered

For the third year in a row, 52%+ of organizations stated that they are running containers in production with another 35%+ in planning/deployment phases, equating to 90%+ each of the three years surveyed. But only 25% protect their containers deployments with a tool that is purpose-built solution.

The unfortunate and dangerous reality is that most administrators only back up the underlying storage or the database components, with the presumption that they'll be able to reconstruct the rest of the platform on their own.

- Imagine if you only backed up the storage under your hypervisor host?
- Imagine if you only backed up the database from your web application?

This is less surprising when you learn that the role responsible for backing up containers varies widely across organizations, with nearly even distribution between database admins (27%), storage admins (24%), backup admins (21%), and Kubernetes admins (29%). Even over the three years surveyed, there has been only minor variation between these roles, with slightly fewer storage admins being involved and slightly more Kubernetes admins taking lead.

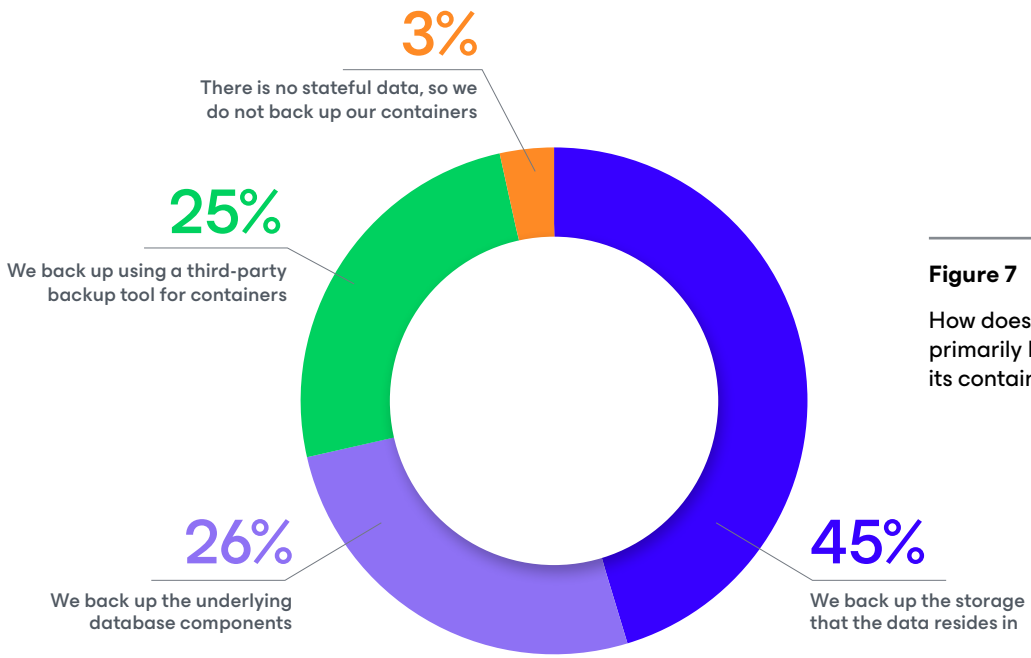


Figure 7

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

Data Protection Trends 2024 Report — published by Veeam in January 2024
N=1,200 unbiased IT Leaders and Implementers responsible for their organizations' data protection strategies.

Get Your Data Out of the Building

While disk-based backups within the same locale as the production data remains the most agile way to restore, there continues to be massive interest in complementing those disk repositories with tapes and/or cloud repositories in 2024:

- 52% of production data is also backed up to tapes
- 61% of production data is also backed up to clouds

Of the 1,200 organizations, only 4 respondents did not use tape somewhere in their data protection strategy and not one claimed to not use cloud repositories. Elsewhere in the survey, 88% were either very likely or almost certain to use a Backup as-a-Service (BaaS) or Disaster Recovery as-a-Service (DRaaS) for at least some of their production servers. One of the most impressive trends over the past five years has been the increase in BC/DR readiness, in large part due to leveraging cloud-based infrastructure in lieu of a secondary physical data center or traditional hotsite:

- From 2020 through 2026, roughly 28% (+/- 2%) maintain secondary datacenters with disaster recovery capabilities
- In 2020, 23% utilized cloud-hosted infrastructure as their DR site, with that expected to double to 47% by 2026

It is exciting to see that while only half (52%) of organizations had a BC/DR capability in 2020, three-fourths (74%) will by 2026. It is notable that for many organizations, their ability to be DR or cyber prepared are not just because of an agile or more affordable cloud site, but also the expertise that comes from managed service providers.

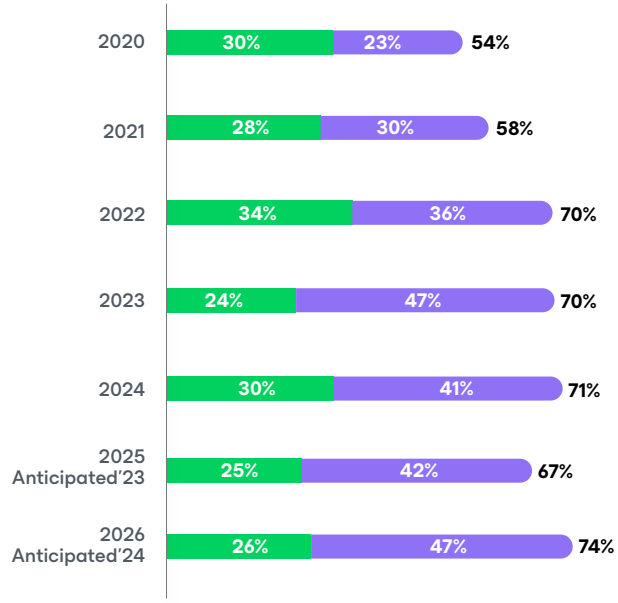


Figure 8

Which of the following is your organization's primary method of business continuity and disaster recovery (BC/DR) today? In two years time?

- Multiple self-managed data centers
- Cloud-infrastructure or DRaaS provider

Organizations are Balancing Cyber Against Compliance and Modernization

In a world of "need to's" (compliance) and "want to's" (modernization), some interesting trends are occurring:

When asked about hindrances to Digital Transformation (DX), near the top of the list were:

- Environmental sustainability, social, and governance (ESG)
- Skills shortage to implement technology
- Economic uncertainty

When asked about compliance and governance initiatives, near the top of the list were:

- Long-term data retention
- Regulatory mandates related to data
- Data geographic sovereignty

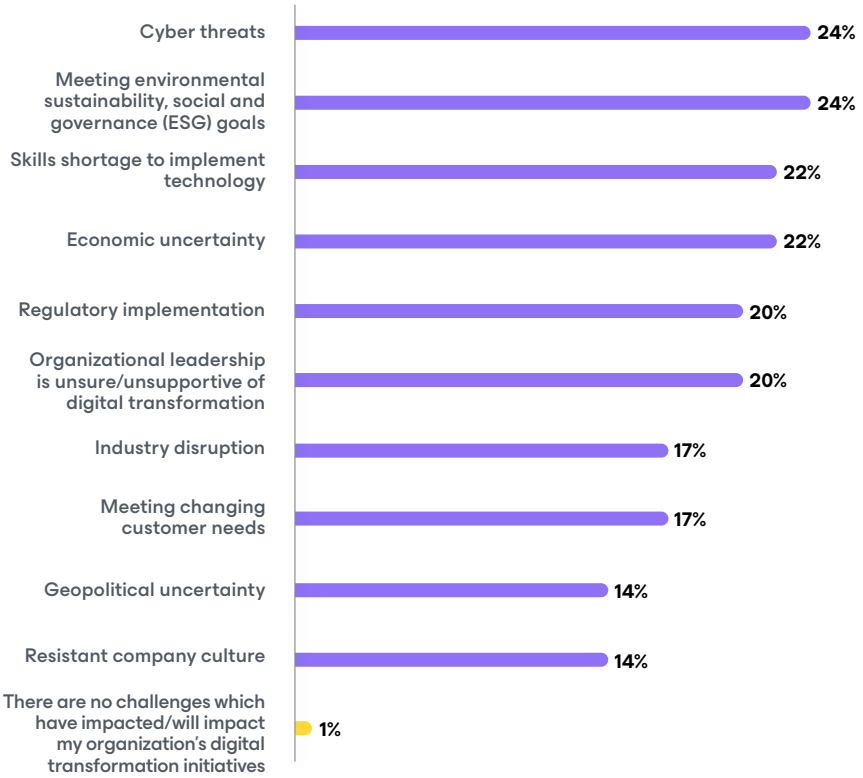
Unfortunately, those were #2, #3, and #4:

- The top corporate initiative for 2024 is **cyber education related** to phishing
- The top hinderance to IT modernization in 2024 is **cyber threats**

Quite literally, organizations cannot invest where they want or need to, because of their efforts to protect themselves via cyber villains.

Figure 9

Of the below business/IT challenges, when it comes to your organization's ability to achieve your digital transformation initiatives which do you believe will be the biggest challenges over the next 12 months?



Cyberattacks Were Most Common and Most Impactful Causes of Outages (Again)

37% of servers had at least one unexpected outage in 2023 — but why?

For the fourth year in a row, a cyberattack was the cause of the most impactful outage. That said, with many of the historical causes continue to plague IT — which is why backup is as relevant as ever:

- **Infrastructure outages,** which has the added risk of being affected by bad actors to prevent you from reaching your distributed or cloud-hosted workloads. They don't have to take down those platforms, just deny your ability to reach them
- **Storage hardware** failures and **application software** issues have been around as long as computing, due to having the lowest time to failure and most frequently/precariously maintained layer, respectively
- It is worth nothing that rounding out the top five is outages in **public cloud resources**; thereby validating that cloud services do go down and that running your application in a cloud host does not guarantee uptime — i.e. backup and Cyber/BC/DR still matter for clouds

New to the survey question this year was **natural disasters** (fire/flood/hurricane/etc). Though it was thankfully among the least frequent of occurrences, still 1 in 4 organizations experienced a natural event. So, while they may not occur as often, it would be prudent to not dismiss what we as an industry have always considered a doomsday scenario.

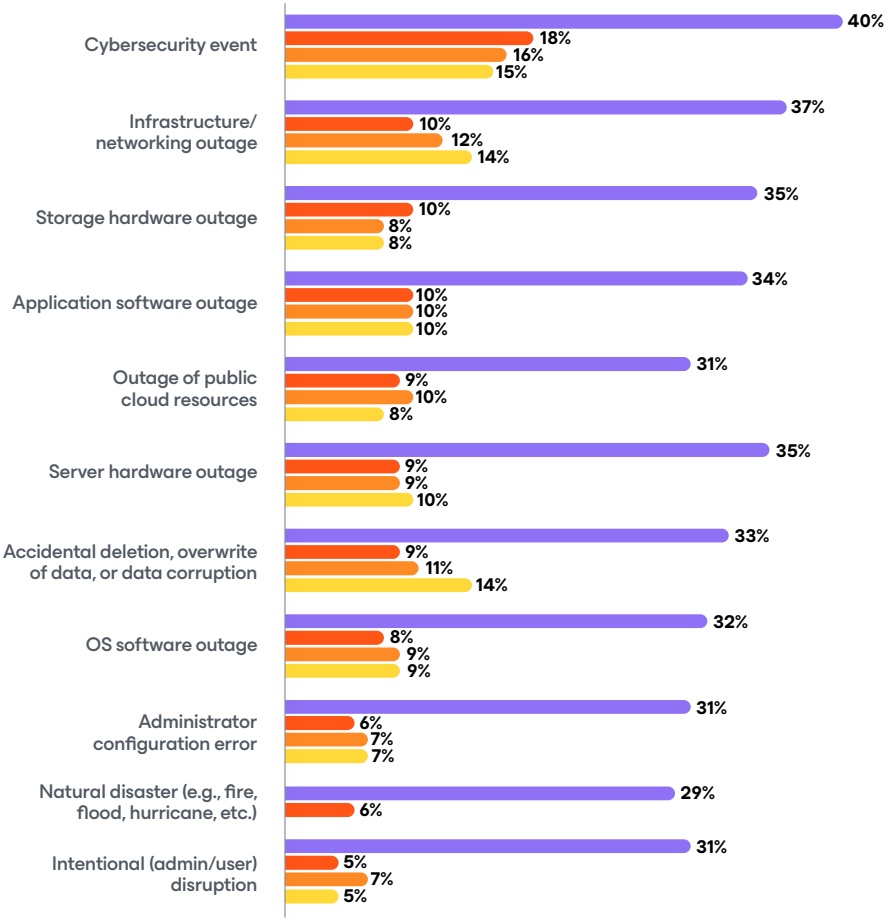


Figure 10

Over the past two years, what were the most common causes of the outages that your organization experienced? Which was the most impactful in 2021, 2022, and 2023?

- All causes 2023
- Most impactful 2023
- Most impactful 2022
- Most impactful 2021

Ransomware is Still a 'When' More Than an 'If'

In validation to the concerns and high mindfulness of cyber preparedness seen earlier in this research, it is unfortunate that 3 out of 4 organizations suffered at least one ransomware attack in the preceding twelve months. When looking at the boundaries of this question:

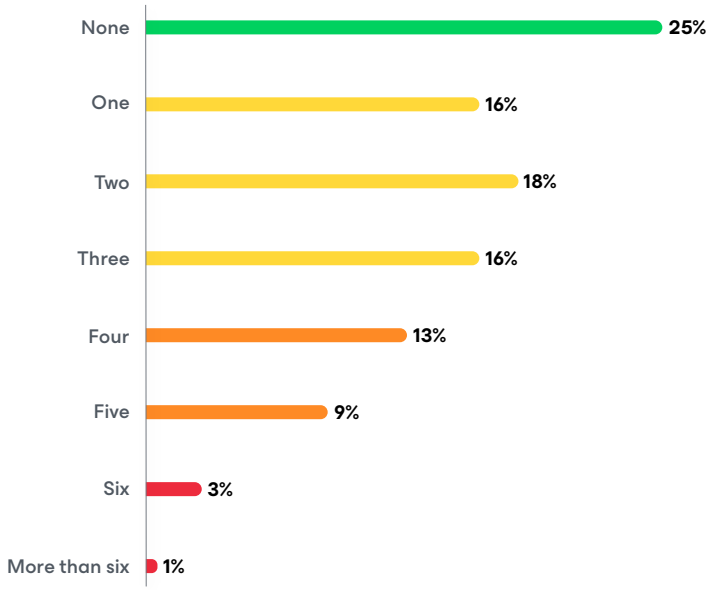
- 25% stated that they were not attacked, which should be noted with caution since many security firms warn that the attacker can be lurking in your environment for 60 to 200 days prior to incurring damage or asking for the ransom. If true, then a high percentage of those respondents may simply have not discovered the breach yet
- 26% stated that they were attacked four or more times in the past year

Yes, more organizations were hit quarterly than believe not at all.

For more information on what happens during and after a cyberattack, please check out the 2023 Ransomware Trends Report, which summarizes 1,200 organizations that were breached in the preceding twelve months and the lessons learned from the nearly 3,000 attacks that they experienced.

Figure 11

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



If You Needed to Recover From a Cyberattack or Other Disaster, Could you?

Imagine a relatively small disaster of part of a datacenter (a few racks) or a ransomware breach that was caught relatively early — with 50 servers being affected. Unfortunately, only 32% believe they could recover that relatively small server stack in a business week. Now imagine how your business processes would be affected without being able to access your data for that week or more.

Several supporting statistics from the research paint a grim picture:

- When asked about their last large-scale server recovery test, only 58% met their recovery SLA's. As a DR planner, that's good news in that you now know what to look for to fix the other 42%. For anyone else in the company, it should set your expectations that 2 out of 5 servers won't be there when you need them
- When asked about testing and documentation update frequency, organizations only test or update every 7.3 months, which is notably worse than the 4.4 month averages just two years ago
- Why do organizations test less and fail their SLAs? Because without orchestrated recovery processes, manual resumption is difficult, time-consuming, and prone to errors. Unfortunately, only 13% have orchestrated workflows as part of their failover/failback processes

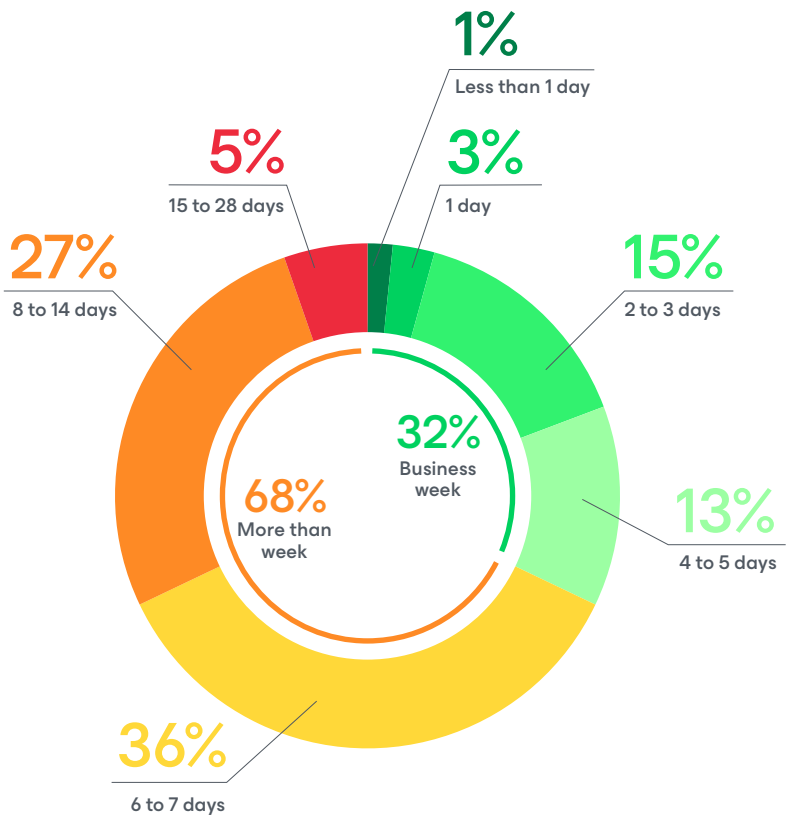


Figure 12

If your organization had to fail over 50 servers due to a disaster or cyber event, how long do you estimate it would take from starting the recovering of the first server until the last server was online?

Summary

This analysis covers the opinions of 1,200 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 2024. 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 the research

Veeam has commissioned analysts or research firms 8 times over 10 years to produce an industry report on the evolving data protection landscape; for the purposes of affecting its product strategy as well as helping the market be better informed.

Since 2019, consistent sources of panels and the data analysis by analysts formerly at Gartner and ESG were added to enable year-over-year comparisons and statistically defensible regional, vertical, and segment analyses. These research endeavors were conducted using 'double-blind' surveys, whereby the research firms' respondents were unaware who was seeking the data and Veeam had no visibility or affect on who responded to the survey beyond defining the persona of 'IT Leader or Implementer responsible for data protection strategies within their organization.'

To download additional materials from this research, click here

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

About Veeam Software

Veeam®, the #1 global market leader in data protection and ransomware recovery, is on a mission to empower every organization to not just bounce back from a data outage or loss but bounce forward. With Veeam, organizations achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud. The Veeam Data Platform delivers a single solution for cloud, virtual, physical, SaaS, and Kubernetes environments that gives IT and security leaders peace of mind that their apps and data are protected and always available. Headquartered in Columbus, Ohio, with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, including 73% of the Global 2000, who trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @Veeam-Software and X @Veeam.

About the authors

Jason Buffington
VP, Market Strategy
@JBuff

Dave Russell
VP, Enterprise Strategy
@BackupDave

Julie Webb
Director, Market
Research & Analysis