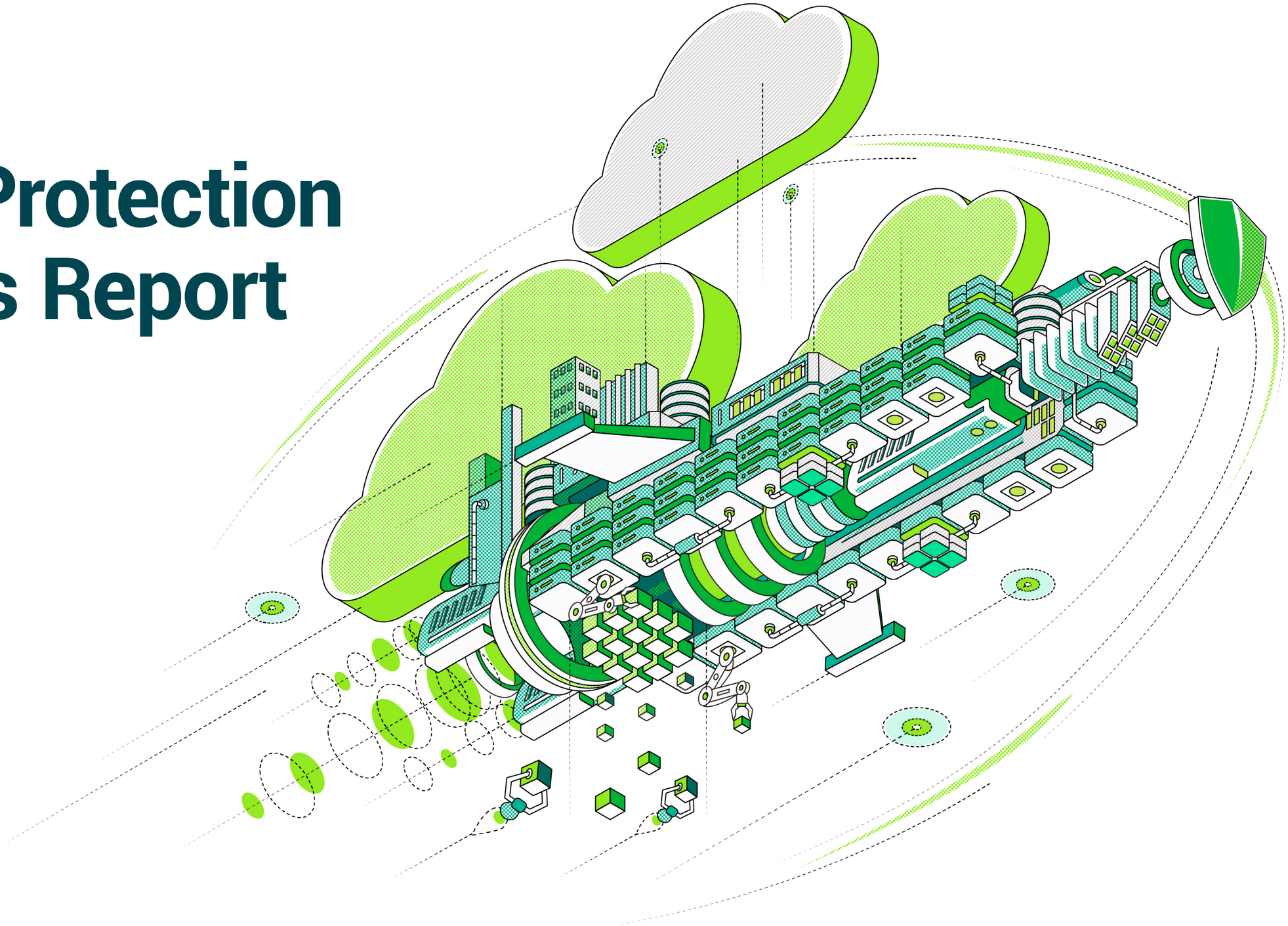
2022

Data Protection Trends Report



VEEAM

Contents

Introduction

Between October and December 2021, an independent research company surveyed over **3,000** IT decision makers and IT professionals about their IT and data protection strategies, challenges and drivers. Almost all the respondents were from organizations with more than **1,000** employees – from **28** different countries.

On average, respondents expected their organization's budget for data protection, including both backup and BC/DR, to increase by **5.9%** in 2022. Recognizing the unique circumstances of IT on-premises stagnation during the pandemic quarantine and resulting supply chain issues, as well as the acceleration of cloud initiatives for the same reasons, it is understandable that 2022 would see a disproportionate investment in data protection to adjust for the diverse production environments now in use today.

As the third annual study of Data Protection Trends, this year's survey was designed to quantify the shifts in overall concerns/goals and strategies for data protection, as well as gain an understanding of the current market landscape on data protection, disaster recovery, cybersecurity/ransomware and containers.

This report is presented in four sections:

1.0 TOP HEADLINES

2.0 REAL-WORLD ISSUES

3.0 IT MODERNIZATION, INCLUDING CLOUD(S) AND CONTAINERS

4.0 CYBERSECURITY AND DISASTER RECOVERY

With most analyst research surveying 200-300, this is the largest known industry research project ever conducted on data protection

About the research

An independent research and analyst firm surveyed 3,393 organizations, covering the following topics:

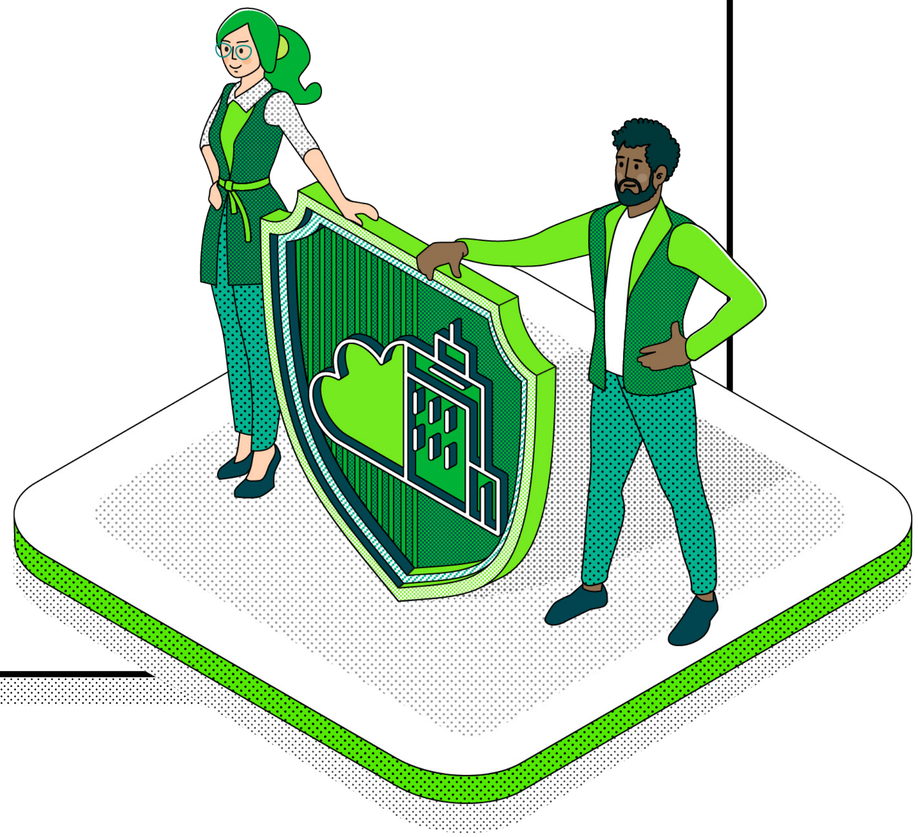
- What is driving change in data protection strategy
- Digital Transformation and IT modernization
- The impacts of new IT delivery models like containers
- How the Reality Gap continues to proliferate
- Cloud-powered data protection
- The evolving threat and mitigation landscapes of ransomware and disaster recovery

Veeam® is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. We provide a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. To learn more, visit www.veeam.com

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

1.0

Top Headlines



1.1

Enterprise ≈ Heterogeneous

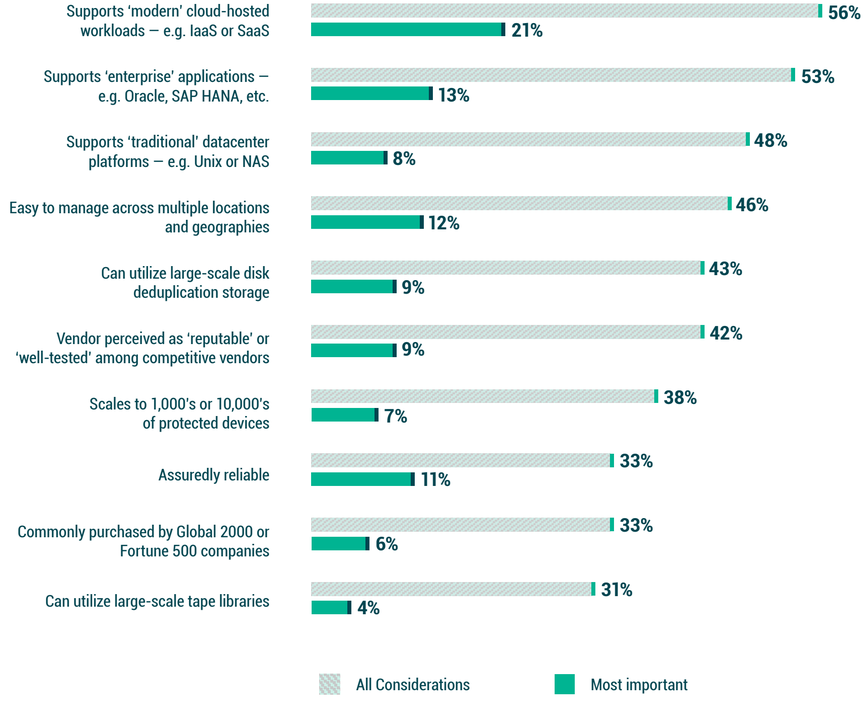
The three most common characteristics of "enterprise" relate to supportability of various categories of workloads: cloud-hosted, business critical applications and legacy platforms.

It is notable that while "reliability" has consistently been a driver for changing data protection solutions (as seen in multiple prior reports, as well as this year in Figure 1.3), reliability was not as paramount to enterprise suitability as modern workloads. Said another way, while there are many important facets, such as scale, reliability, brand reputation, etc., the key takeaway in 2022 is that "heterogeneity" is the synonym for what "enterprise" means today.

Everyone is adding multiple cloud services, but not many are turning off datacenter platforms

Figure 1.1 What does "enterprise backup" mean to you?

If your organization was considering a new "enterprise backup" solution today, which would be most important?



1.2

Hybrid infrastructure 2020-2024

"Hybrid" is normal and here to stay

With over 8,000 data points from three consecutive years, "the new normal" for modern IT is approximately 50/50 between on-premises servers and cloud-hosted servers:

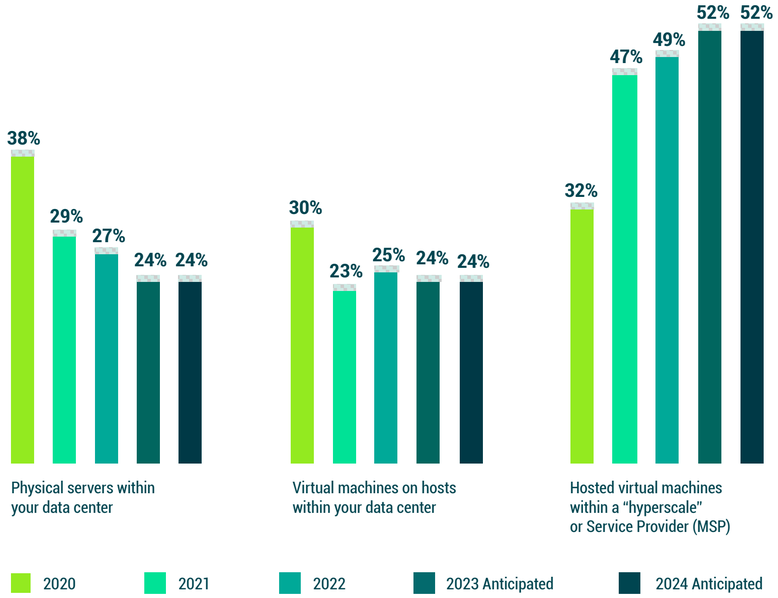
- Within the data center, there is a consistent expectation for both physical and virtual platforms.
- Within cloud, there is a healthy mix of using both hyperscale and MSP-hosted infrastructures.

Two key takeaways from these trends:

1. The data center is not dead nor dying. There are as many good reasons to run a workload on premises as cloud-hosted.
2. Your data protection strategy needs to accommodate physical, virtual and multiple cloud-hosted options.

Figure 1.2 What do you estimate is your organization's percentage of servers in each format currently?

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



1.3

Improved outcomes & economics are driving change

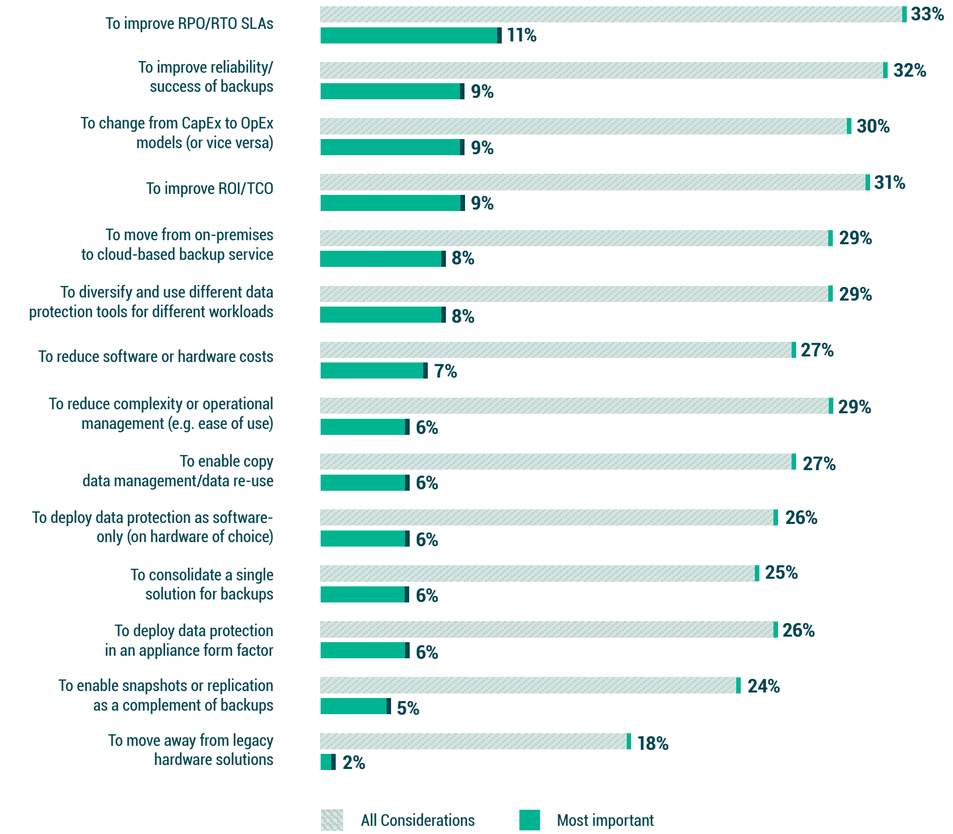
Organizations are looking for "better" data protection

When considering the top six drivers for change, three banded trends occur:

- **Qualitative improvement —** Reducing RPO (data loss), reducing RTO (downtime), and enhancing reliability all equate to data protection that simply "works."
- **Increased value —** Changing CapEx to OpEx reduces initial investment, thereby relieving short-term budgets, while improving ROI/TCO increases the value of what is being spent.
- **Modern capabilities —** Moving from a legacy backup to one that leverages cloud services or is cloud-powered, along with utilizing tools that accommodate an increasingly diverse (and likely cloud-hosted) range of production capabilities.

Figure 1.3 Which of the following would drive your organization to change its primary backup solution to a new solution or service?

Which is most important?



1.4

"Modern" means cloud capable

Modern is cloudy, integrated and automated

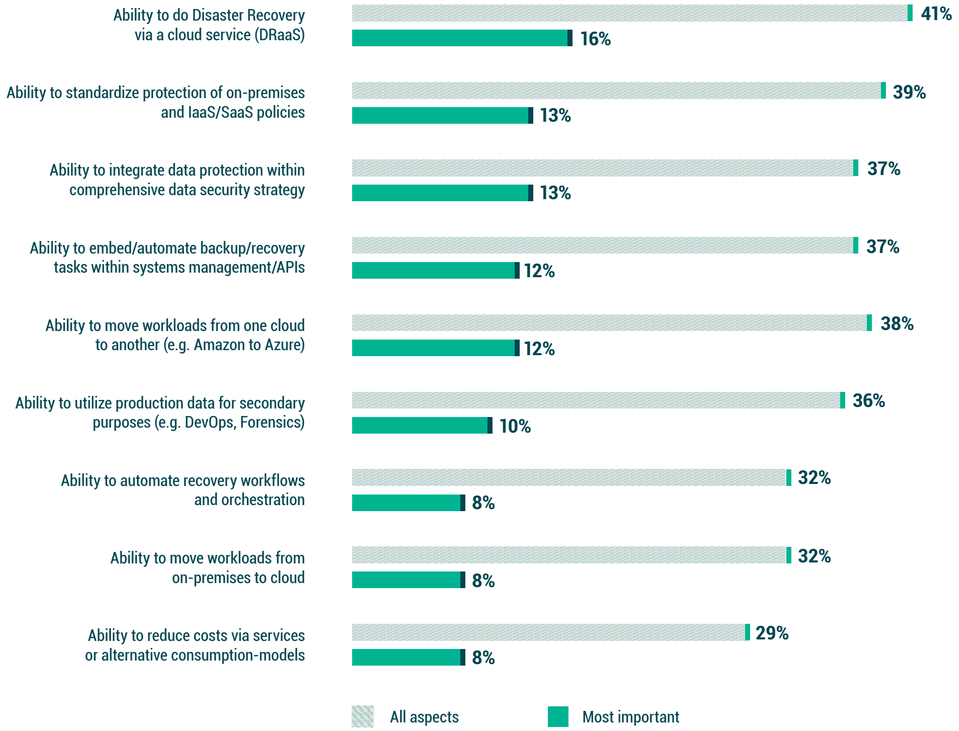
The most common and important aspects of modern/innovative data protection are all "cloudy" — including DRaaS, IaaS/SaaS protection and the ability to move workloads between clouds. **Beyond cloudy-ness,**

- Backup cannot be its own isolated endeavor any more than cyber-preparedness can. Instead, backup should be included as the remediation component within any ransomware strategy.
- Backup should also not be an afterthought to production. When workloads are first provisioned, that is the time to define a workload's data protection requirements. Similarly, as SaaS platforms are brought online (prior to migration or adoption), the backup mechanisms should be enabled.

The lower half of the list are all valuable and might have previously been considered innovative, but today, are simply "expected."

Figure 1.4 Which would you consider to be defining aspects of a "modern" or "innovative" data management or data protection solution for your organization?

Which is most important?



1.5

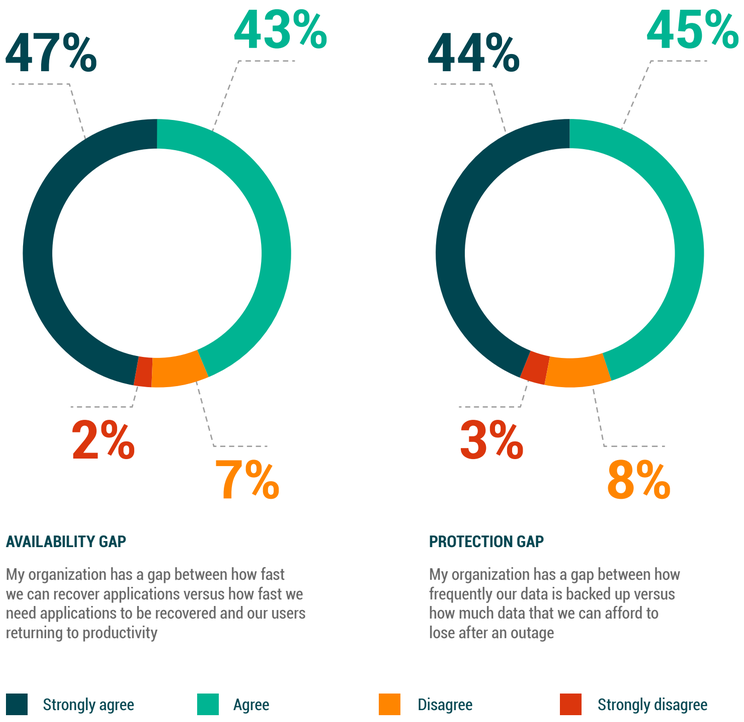
Wider gap continues to proliferate

The gap between what business units expect and what IT can deliver continues to widen, as tracked for the past five years in this project. For 2022:

- **90%** of organizations have an **"availability gap"** between the SLAs expected and how quickly IT can return to productivity.
- **89%** of organizations have a **"protection gap"** between how much data they can afford to lose and how often data is protected.

The rationale is most likely due to the rising criticality of more workloads. But there is an obvious corollary between the top change drivers (Figure 1.3) of improving RTO (availability), RPO (protection) and reliability — versus these perceived "gaps."

Figure 1.5 Does your organization have a "Reality Gap"?



1.6

The Veeam Perspective

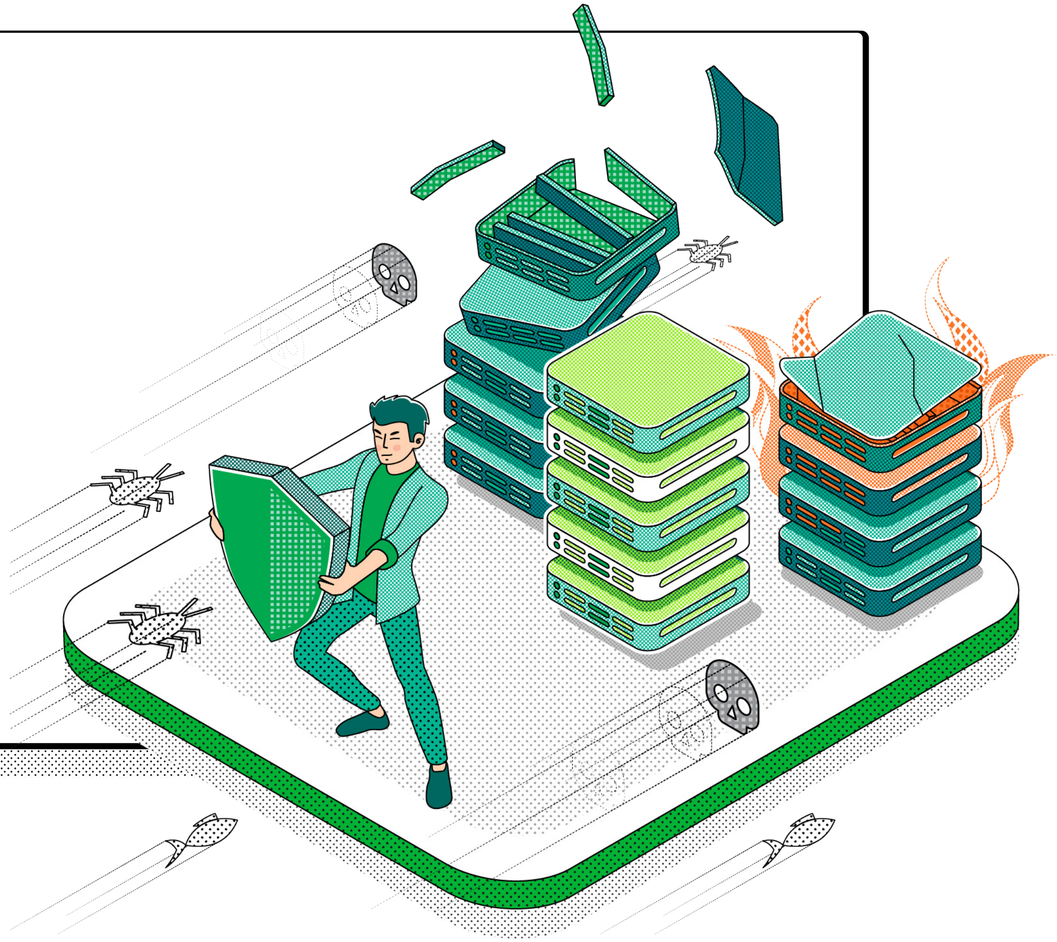
Veeam provides a clear path to Modern Data Protection that is driven by capabilities that focus on achieving any recovery objective, maximizing your investment, and reducing management overhead with products that "just work." Today's modern IT strategy is hybrid- and multi-cloud, so Veeam delivers purpose-built backup and recovery for AWS, Microsoft Azure and Google, with native coverage for IaaS, PaaS and SaaS workloads, available as modular standalone options or unified for centralized management, licensing, and extensive data portability.

Considering all this, it is no wonder that Veeam was named the 2021 Gartner Magic Quadrant leader for the 5th consecutive year. Veeam protects over **400,000** customers worldwide, including **81%** of the Fortune 500 and **70%** of the Global 2,000.

Click here to learn more about the Veeam Platform

2.0

Real-world issues



2.1

Everything is important

There's not much difference between "high priority" and "normal"

While there will always be some workloads or data that is deemed of higher importance, the expectations between those significant workloads and the rest of IT isn't that wide.

Data loss — 55% of "high priority" data and 49% of "normal" data have a data loss tolerance of up to one hour. This means:

- There is not much difference — all data matters
- Backup alone is not enough because it doesn't run hourly. Instead, backups must be combined with snapshots and/or replication.

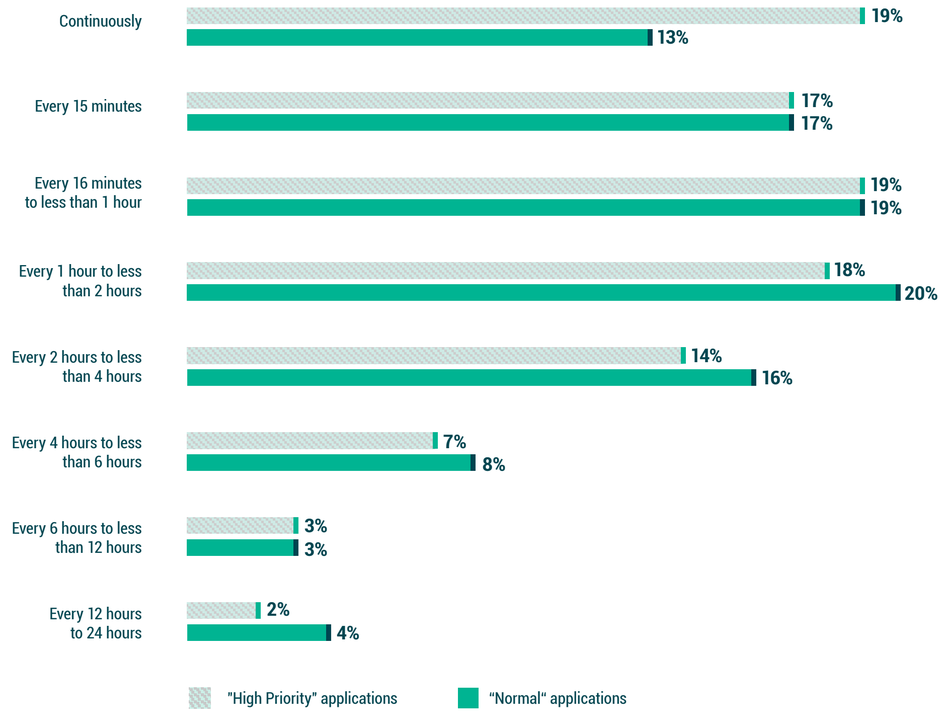
Downtime — similarly, while not shown here, **56%** of "high priority" and **50%** of "normal" applications have a downtime tolerance up to one hour — revealing the same realities that all data matters and the need for better than traditional once-per-day backups.

Other reported statistics not graphed in this report:

- The average outage lasts **78** minutes
- **40%** of servers suffer at least one unexpected outage per year
- IT leaders estimate downtime costs **$1,467** per minute (**$88K** per hour)

Added together, it's no wonder that any amount of downtime or data loss is unacceptable.

Figure 2.1 How often does your organization protect (including backup and replication) its "high priority" & "normal" applications? (data loss)



2.2

Breakages are more common, but cyberattacks are most impactful

Why backup still matters

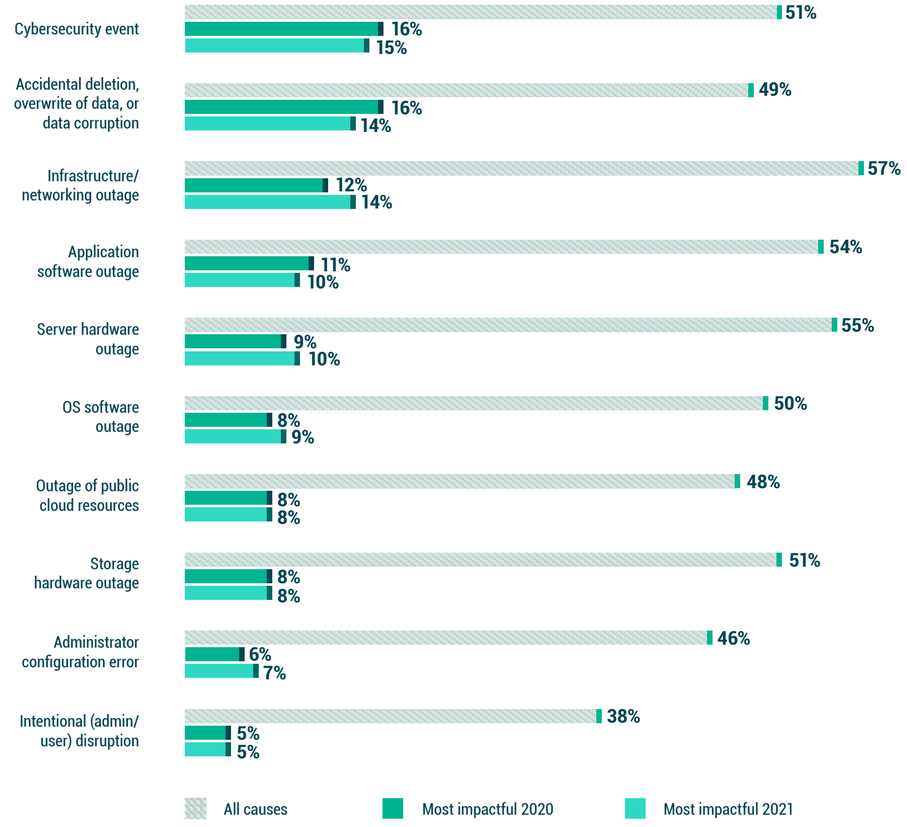
Looking at the broad range of causes of downtime, there are four truths:

1. Cyberattacks are increasingly prevalent
2. Users make mistakes and the "recycle bin" (undo) is not sufficient
3. Stuff breaks – e.g. all of the "outages"
4. Administrators make mistakes too

That said, the most impactful outages for the past two reporting years have been cyberattacks. Refer to section 4.0 Cybersecurity and Disaster Recovery for ransomware frequency, causality and measuring the ability to recover from these attacks.

Figure 2.2 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 and 2021?



2.3

The Veeam Perspective

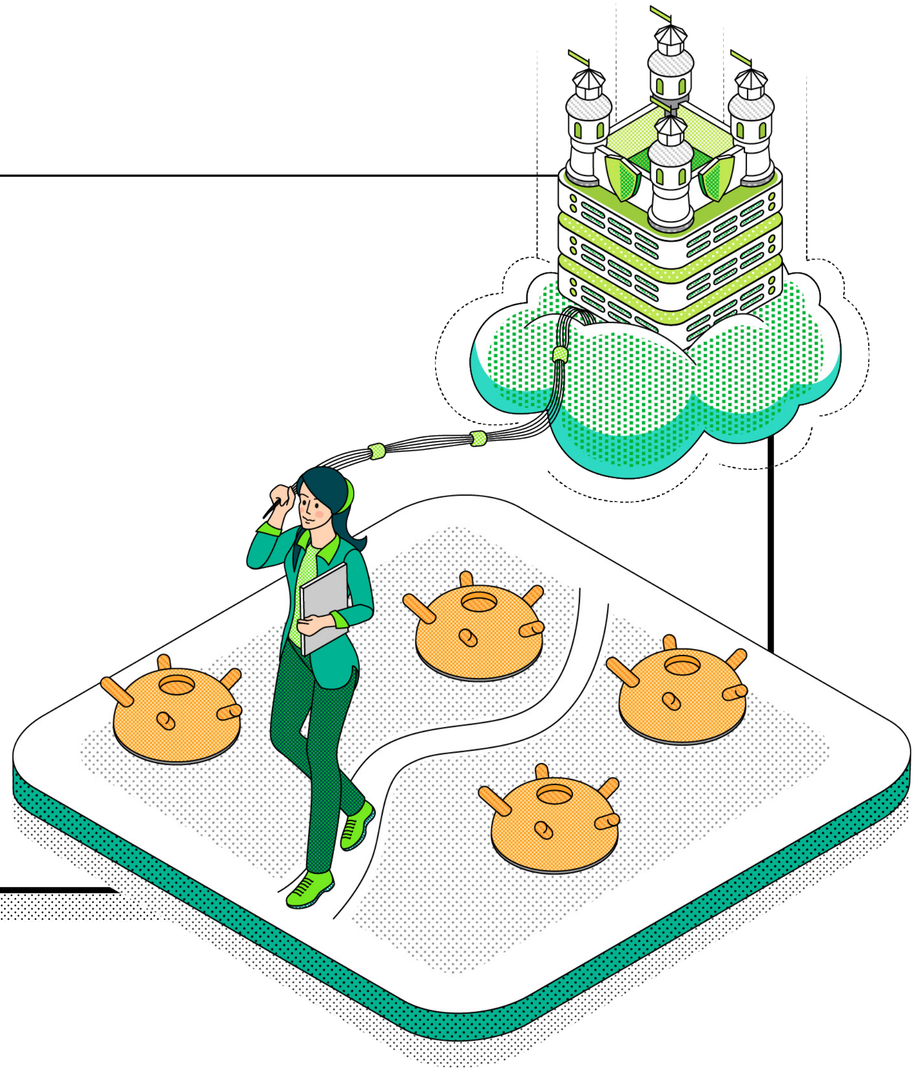
Recognizing that cyberattacks can happen to any workload — and choosing to use SaaS or IaaS doesn't mitigate hardly any of the myriad causes of outages — Veeam enables you to protect everything. Secure Backup is your last line of defense. And as your production platforms change, the Veeam Universal License ensures that you'll be able to flexibly adapt to new workloads and environments while retaining your investments.

- To fill the protection gap, Veeam combines periodic backups with storage snapshots, software-based replication, and continuous data protection
- To fill the availability gap, Veeam pioneered and still uniquely delivers "Instant Recovery" where the business doesn't have to wait for "restore" before they can "resume"

Click here to learn more about the Veeam Platform

3.0

IT Modernization = Clouds & Containers



3.1

Digital Transformation continues

Even as the world continues to emerge from two years of quarantine and supply chain, Digital Transformation (DX) progress continues to move forward, because business still must be done.

It is no accident that the most common inhibitors to DX are inadequate skills and legacy systems. Older systems are expensive to maintain, resulting in less budget and manpower for new initiatives. That said, as most organizations were forced to enable remote workforces in unimaginably fast time periods, many simply accelerated their already-planned IT modernization initiatives, thereby accommodating their users and relieving themselves of the legacy systems and their antiquated means.

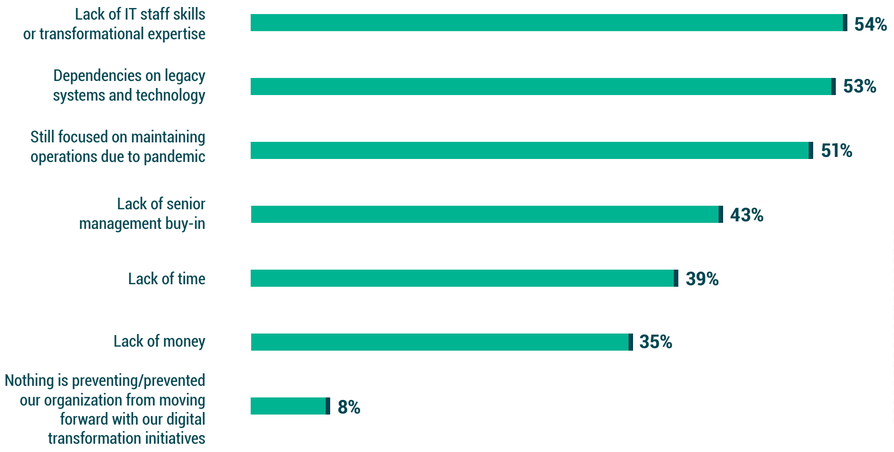
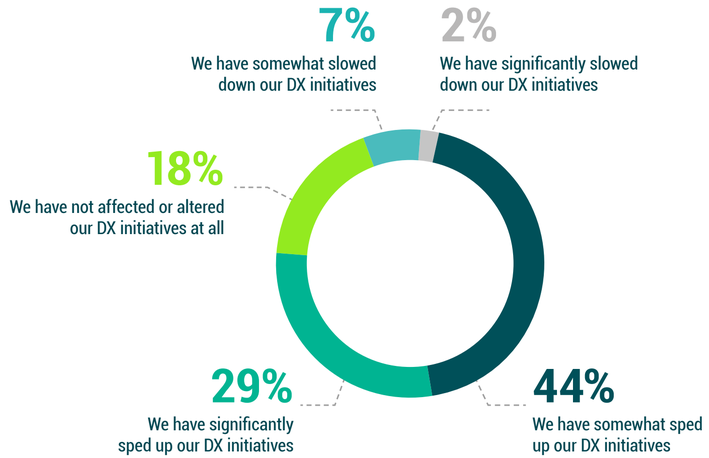


Figure 3.2 What, if anything, is preventing/did prevent your organization's ability to move forward with its Digital Transformation initiatives?

Figure 3.1 Considering the continued pandemic/recovery situation, how would you characterize your DX initiatives or progress since the pandemic?



3.2

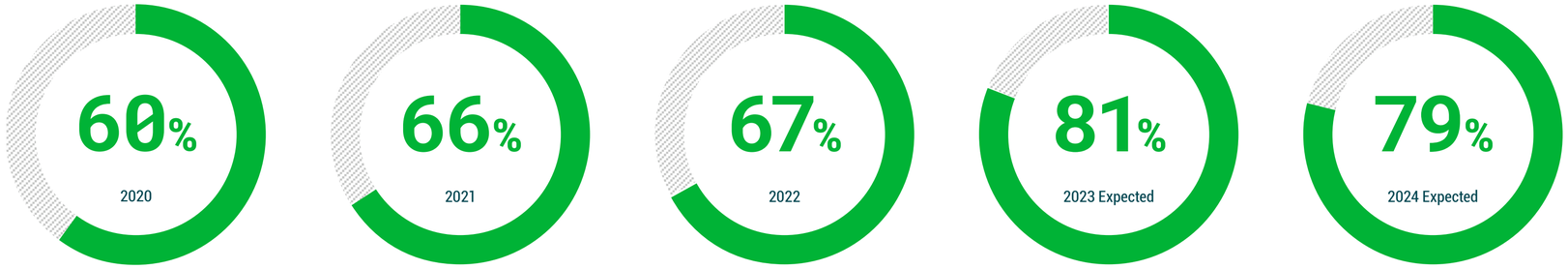
Cloud-powered data protection 2020-2024

Two out of three organizations use cloud services as part of their data protection strategy

In the DPR 2021 report, **78%** of organizations expected to be using the cloud (and **22%** on-premises only), but they didn't make as much progress as they expected. And yet, **4** of **5** organizations do expect to use either cloud-storage or a managed backup service — i.e., Backup as a Service (BaaS) — **within the next two years.**

The difference between trending realities (2020, 2021, 2022) and consistent aspirations (2023 and 2024) will likely continue to be a discussion for organizations trying to be "cloud first" and seeking cloud-powered solutions where appropriate, including data protection.

Figure 3.3 Percentage of organizations that utilize cloud services as part of their data protection strategy.



3.3

Cloudy disaster recovery 2020-2024

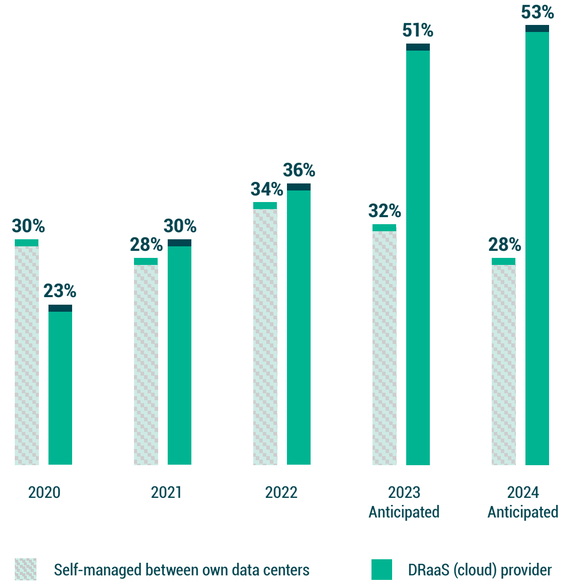
With three years and over **8,000** organizations surveyed on their business continuity and disaster recovery (BC/DR) strategies, it is apparent that roughly **30%** of organizations continue to leverage their multiple data centers for self-managed BC/DR. That can be a great solution, especially if you can leverage orchestration for data movement and skilled IT professionals at both (or all) sites.

Nearly all the "growth" in BC/DR is cloud-powered, likely due to two key merits of cloud-powered disaster recovery:

- **Elastic secondary infrastructure —** Meaning cloud compute/networking when you need it during a crisis (or testing), but not when you don't require it.
- **Outsourced expertise —** Whereby BC/DR experts that would be cost-prohibitive as full-time employees (especially for smaller organizations) that are accessible by Disaster Recovery as a Service (DRaaS) providers and consultants.

There are huge advantages when multiple datacenters can protect each other. But for organizations without secondary sites, the cloud is life-changing

Figure 3.4 Considering your organization's business continuity and disaster recovery (BC/DR) strategy, is your secondary data stored within your own datacenters or at a cloud-provider? What do you anticipate doing in the next two years?



3.4

Who is backing up containers — and how?

New to the survey this year were questions related to containers. Among those respondents who either directly managed/delivered their organization's containers or regularly interacted with those that do:

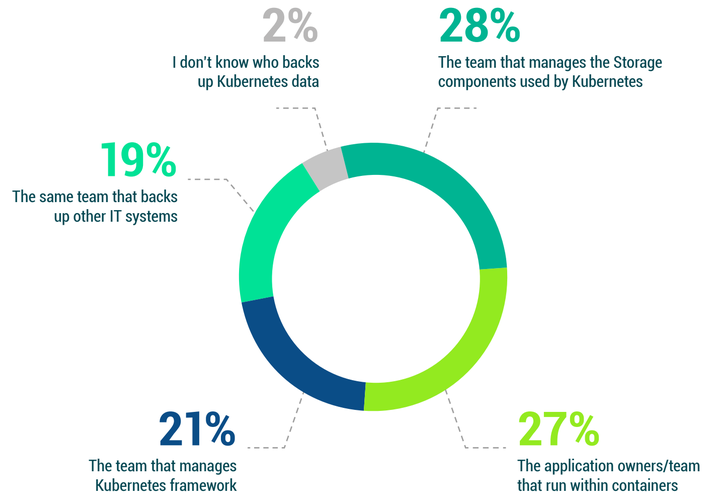
- **56%** of organizations are using containers in production
- **35%** were not yet in production, but planning
- **9%** were not yet planning, but interested in containers

What is more interesting is that the methods used to protect Kubernetes frameworks, or often simply a component of the framework, were relatively split between storage-centric, application-centric, framework-centric functional individuals and those that back up other workloads.

While all of these IT professionals likely have insights, the key concern would be how to recover "the rest" of the Kubernetes Pod or framework, if you were only backing up the underlying storage or using an application-specific approach.

The synergy between Backup (Veeam) and Kubernetes managers (Kasten) shows why Veeam bought and now integrates with Kasten K10

Figure 3.5 Who is responsible for defining the data protection requirements within your organization for containerized applications?



3.5

The Veeam Perspective

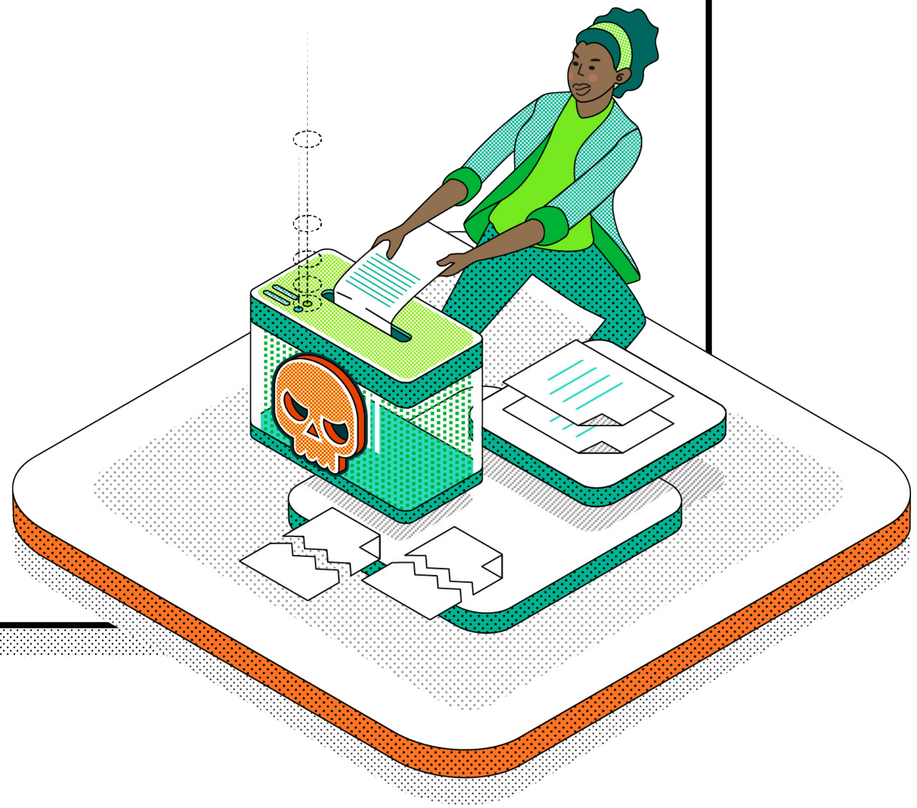
Veeam's ability to move workloads from one platform to another — including physical, virtual, and cloud hosted, and allowing for data leverage and re-use to support DevOps for faster application development — can accelerate your migrations to newer platforms that let you unleash your Digital Transformation (DX) initiatives and retire antiquated systems (and legacy backup tools). Specifically, Veeam enables both cloud-powered data protection, as well as protection of cloud-hosted workloads (IaaS, SaaS, and containers).

- Cloud-powered data protection is an integral facet of the Veeam platform as a software-defined backup solution that can deliver all these data protection strategies:
- Disk and tape solutions on premises, complemented by cloud storage to your favorite hyperscale cloud provider
- Backup as a Service (BaaS) delivered by **10,500+** Veeam Cloud & Service Provider (VCSP) partners
- Disaster Recovery (DRaaS) is often achieved by combining the capabilities of our VCSPs with Veeam Accredited Service Partners (VASP) that specialize in disaster recovery

Kasten K10 by Veeam protects the entire application stack with its Kubernetes-native built data management platform. Insure your containers with full backup and recovery, disaster recovery, application mobility, and ransomware protection.

4.0

Cybersecurity and Disaster Recovery



4.1

Ransomware is a disaster

88% of organizations believe their cybersecurity strategies are completely or mostly integrated with their BC/DR strategy. That reinforces the recognition that ransomware is a disaster, and that most industry organizations understand this point.

While **3** in **4** organizations **(76%)** have suffered at least one attack, **24%** have either not been attacked or they are not aware of it yet. Of those attacked:

- **42%** were user actuated, meaning they clicked on a malicious link, often from a spam email
- **43%** were due to a lack of diligence from an administrator (patches, credentials, etc.)

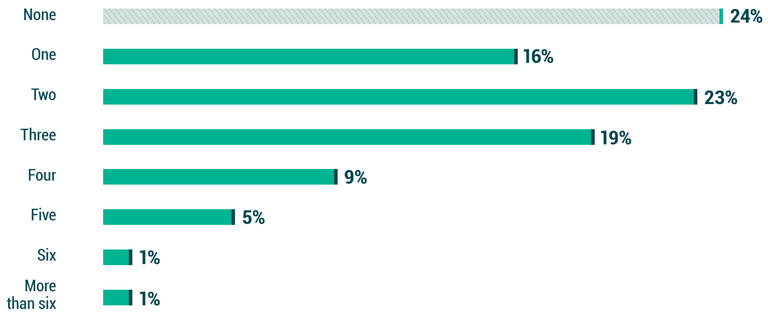


Figure 4.1 Thinking about the most significant ransomware attack your organization suffered in the last 12 months, how did the ransomware enter your organization's environment?

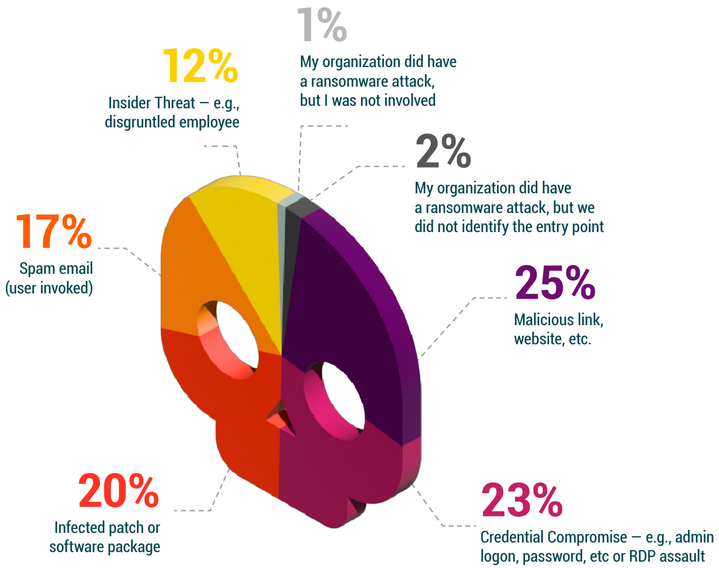


Figure 4.2 How many ransomware attacks has your organization suffered in the last 12 months?

4.2

Recovering from a ransomware attack

On average, organizations were only able to recover **64%** of their data — meaning that over **1/3** of data is typically unrecoverable, according to **1,376** unbiased organizations surveyed.

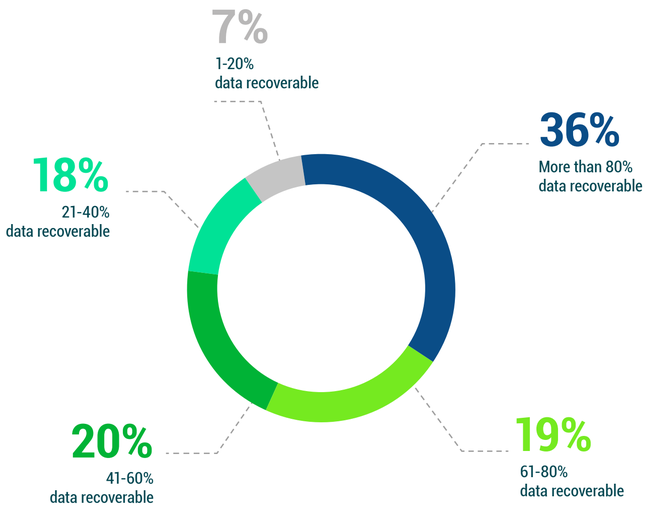


Figure 4.3 Thinking about the most significant attack your organization suffered in the last 12 months, what percentage of data was your organization able to recover from the attack?

4.3

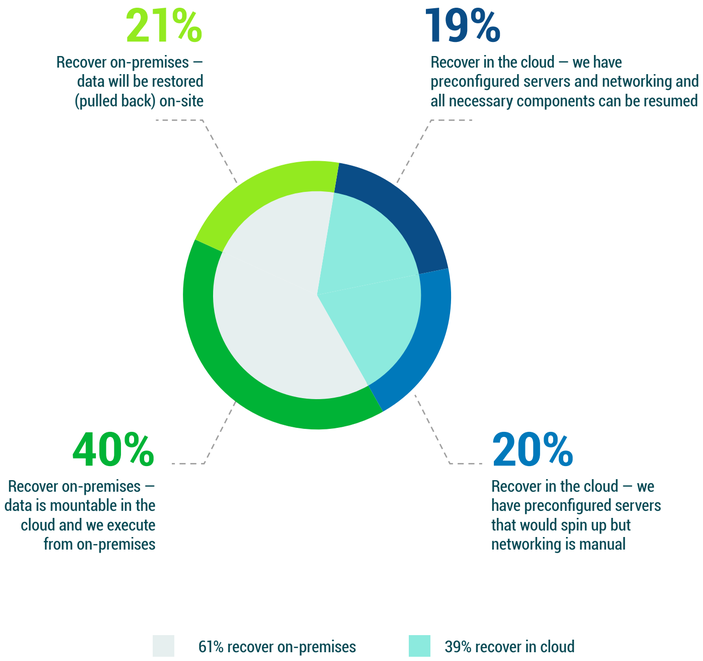
Recovery location and method

There are multiple ways to recover if you're Hybrid

When organizations that store a copy of their data within a cloud were asked where their disaster recovery would fail over to (another data center or cloud) and how the data recovery would be accomplished, there was not a majority opinion:

- One in five organizations will do a traditional **"put the data back where it came from"**
- Two in five would run servers on premises but mount the data from presumably high-performing cloud storage
- One in five would recover with **cloud-hosted servers** but need to manually reconfigure networking and other connectivity for the users to resume production
- One in five have **preconfigured all servers, storage, networking** and the configurations necessary to resume functionality from a cloudy DR infrastructure

Figure 4.4 How are operations resumed for your organization's DR function?



4.4

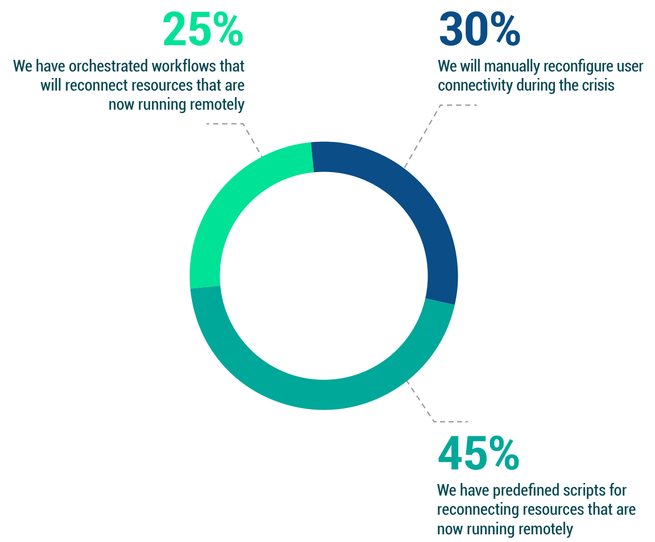
Failover/Failback mechanism for DR

Restarting and reconnecting to servers after a disaster takes multiple complex steps per workload. There are three ways that organizations could accomplish this:

- **29%** will **manually reconfigure** secondary servers during the crisis. Without too much exaggeration, many of those organizations will not be able to get running fast enough to avoid going out of business.
- **45%** will use **preconfigured scripts,** which might be enough or might not be maintained and therefore be error prone during recovery.
- **25%** will use **workflows that are orchestrated,** thereby also having a consistent means of testing prior to an event and executing for real when crises strike.

If you aren't yet using scripted workflows and automated documentation for your DR testing and actual recoveries, check out Veeam Disaster Recovery Orchestrator

Figure 4.5 What kind of failover/failback mechanisms does your organization use for resuming functionality?



4.5

The Veeam Perspective

Ransomware is a Disaster. The ability to quickly restore from a secure backup is your last line of defense when responding to a ransomware attack. To learn more about how Veeam helps test before, alert during and recover after a cyberattack, click here.

Using best practices for off-site or air-gapped backup copies should be part of every DR plan. Veeam recommends that there should be three copies of important data, on two different types of media, with at least one of these copies being off site, air gapped, offline, or immutable. Disaster recovery (DR) testing should also be a priority to ensure data was backed up without errors and was free from malware, ensuring all data can be recovered successfully. To learn more about successful ransomware recovery and the 3-2-1 Rule, click here.

To orchestrate the recovery of cyber and other disasters, Veeam Disaster Recovery Orchestrator is purpose-built as an add-on for environments running Veeam Backup & Replication to orchestrate recovery workflows, automate testing and readiness checks and generate disaster recovery documentation. Veeam customers should check the "DR Pack" for an even more cost-effective way to utilize orchestration to protect their entire environment.

Summary

The last two years have seen significant IT modernization, particularly where cloud-hosted services could be leveraged. This is due to ongoing Digital Transformation initiatives, as well as accelerated cloud adoption during the global pandemic. The rapid modernization of production has forced many organizations to recognize that their protection has not modernized at the same rate, even though their dependency on data and their dissatisfaction with the status quo are both at an all-time high.

Based on these trends, 3,396 IT leaders and implementers agree on the following:

- Data protection will be an area of increased investment to protect their modern workloads that are already in production.
- Drivers for change will be based predominantly around qualitative improvement in reliability, protection frequency and agile recoveries — to improve RPO and RTO. In addition, better economic value and consumption, along with protecting IaaS/SaaS/containers and leveraging cloud for operational backups and disaster recovery, will be key initiatives.
- Improving data protection is in large part being driven by the recognition that cyberattacks, most notably ransomware, is a "when" not an "if" for most organizations — with reliable recovery being the remediation part of one's cyber preparedness strategy. In that way, it is universally understood that "ransomware is a disaster," and that orchestrated recovery from backups is a critical component of every cyber- and BC/DR-plan.

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

About the authors

Jason Buffington
VP, Solutions Strategy

@JBuff

@jasonbuffington

Dave Russell
VP, Enterprise Strategy

@BackupDave

@backupdave

Julie Webb

Director,
Market Research & Analysis

veeam.com