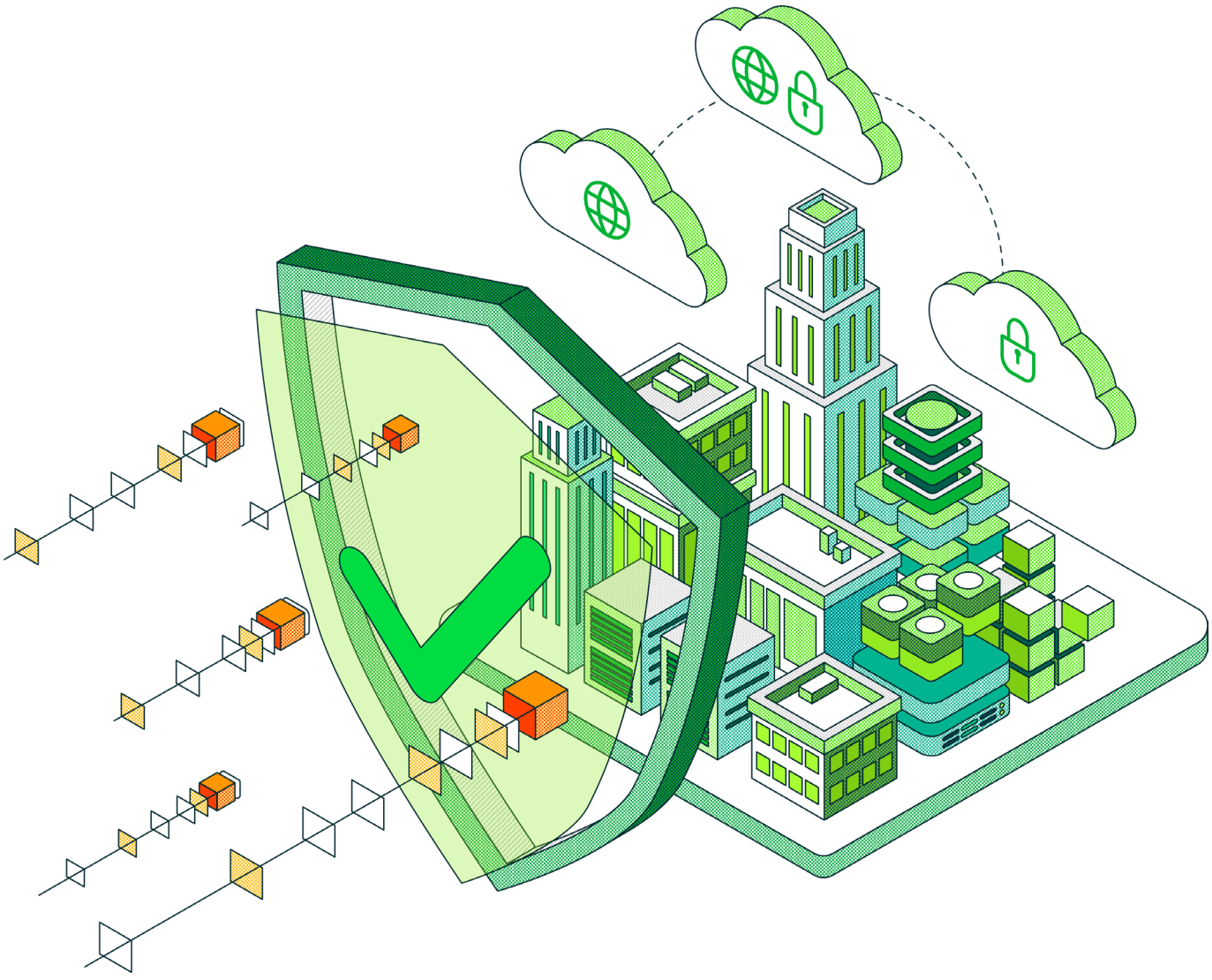
EXECUTIVE BRIEF

# 2023 Data Protection Trends



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 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.

While Gartner predicts a **5.1%** increase in overall IT budgets and the IDC predicted a **5.2%** increase in overall IT spending, this survey revealed that data protection budgets are expected to increase by **6.5%** globally in 2023. You can find the full 2023 Data Protection Trends Report at https://vee.am/DPR23.

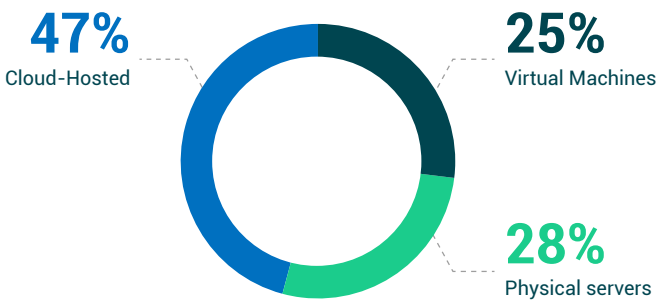
Organizations expect to increase their data protection budget for 2023 by

**6.5%**

# Hybrid Infrastructure 2020 to 2025

Each year the survey asks organizations to estimate the on-premises servers (physical and virtual) as well as those that are cloud-hosted; for the current year, as well what they expect two years later. **Check out the full report** to see a summary of the **12,000** responses across four annual surveys covering 2020 to 2025, but for 2023, the actual distribution of server instances across **4,200** organizations' Hybrid IT is as follows:

**Actual 2023 Hybrid IT Landscape (global)**




Overall, **Physical** servers and **virtual** machines have both stabilized at around **50%** of an organization's overall IT plan, while the rest is **cloud-hosted** — with continued, albeit gradual, shift to cloud-hosted, predominantly due to organizations' cloud-first strategy of new workloads starting up in clouds at faster rates than legacy workloads are being decommissioned in the datacenter, thereby diluting the datacenter within an overall hybrid IT strategy.

| | GLOBAL | North America | Latin America | Europe | MEA | APJ |
|---|---|---|---|---|---|---|
| Physical servers | **28%** | 27% | 26% | 28% | 29% | 29% |
| Virtual machines | **25%** | 25% | 26% | 26% | 25% | 25% |
| Cloud-hosted | **47%** | 48% | 49% | 46% | 46% | 46% |

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.

# What does 'enterprise backup' mean?

For the second year in a row, the most important attribute of an "enterprise backup" solution is the **protection of IaaS and SaaS.** This should not be a surprise when considering how infrastructures are shifting to the cloud.

What might surprise some is that assuring **reliability** is the second most important criteria. But when considering that many organizations 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. Legacy backup mechanisms rarely yield good outcomes when protecting modern workloads.

As such, it makes sense that cloud-hosted protection and reliability would be adjacent and top of mind.

**15%**

of Organizations looking for an enterprise backup solution consider **"Protect IaaS & SaaS workloads, as well as the datacenter"**, as the most important capability

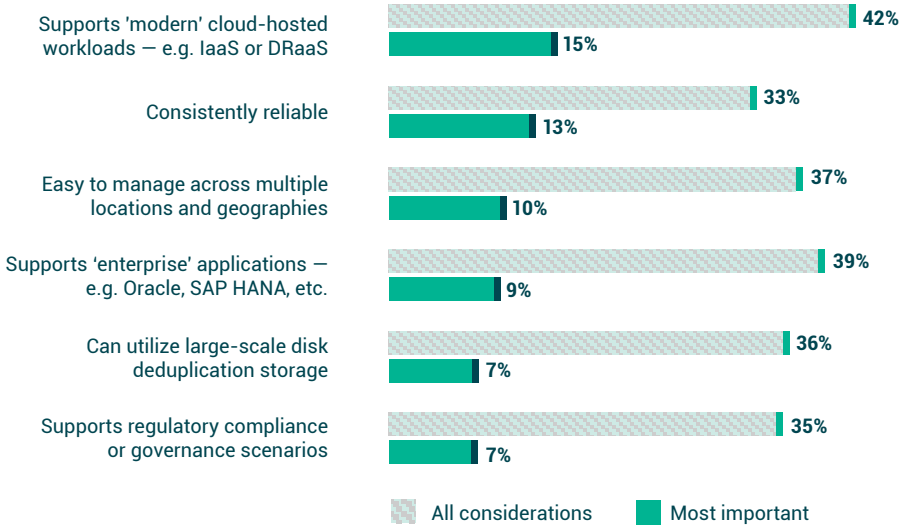



**Figure 1.2**

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?

In fact, 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.

**32%**

of Organizations state that **"Improving Reliability/Success of Backups"** is their motivation for changing backup solutions

# For 2023, 'modern' data protection means 'cyber-resilient'

When considering what modern data protection must address, it is worth noting that the full research report reveals that for the third year in a row, cyber-attacks continue to be the top reason for causing the most impactful outages – with the frequency of ransomware attacks continuing to rise:

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

| | GLOBAL | North America | Latin America | Europe | MEA | APJ |
|---|---|---|---|---|---|---|
| No attacks in 2022 | **15%** | 11% | 11% | 16% | 14% | 18% |
| Only 1 attack | **18%** | 16% | 15% | 19% | 18% | 18% |
| 2 or 3 attacks | **48%** | 53% | 52% | 46% | 48% | 45% |
| 4 or more attacks | **18%** | 19% | 18% | 17% | 21% | 19% |

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

Thus, it is no surprise that the most common, and most important aspect of a "modern data protection solution" is the integration of data protection within a cyber preparedness strategy.

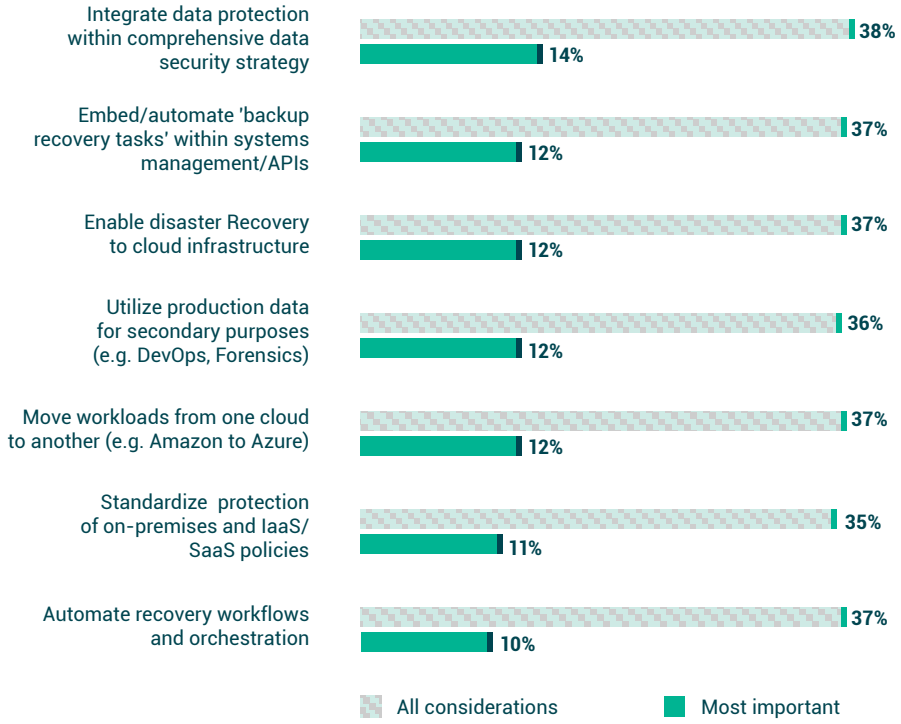



**Figure 1.5**

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

But while cyber resiliency continues to be top of mind for many IT leaders, it would be a significant strategic error to focus all your data protection planning on attacks. Systems outages, caused by networking, application failure, hardware failure, and OS issues are all still commonplace even within modern data centers. Organizations should be prepared for both the breakages that continue to occur as well as human-caused events, such as user errors and cyber criminals.

# BC/DR methods and mechanisms

As cloud services become increasingly more common in data protection strategies, many wonder whether to recover data back to on-premises servers or into cloud-hosted infrastructures. While the research results show relatively balanced interest between on-premises and cloud-hosted recoveries for 2023, most of the recovery data will be coming from cloud-hosted backups. This follows the practice of having less recovery points on premises as well as getting data out of the building to cloud-based storage for data retention and ransomware or BC/DR preparedness.

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%** currently have an orchestrated workflow capability within their current data protection or failover strategy.

**54%**

of organizations expect to use on-prem servers for BC/DR, while **46%** will leverage cloud-hosted infrastructure for BC/DR

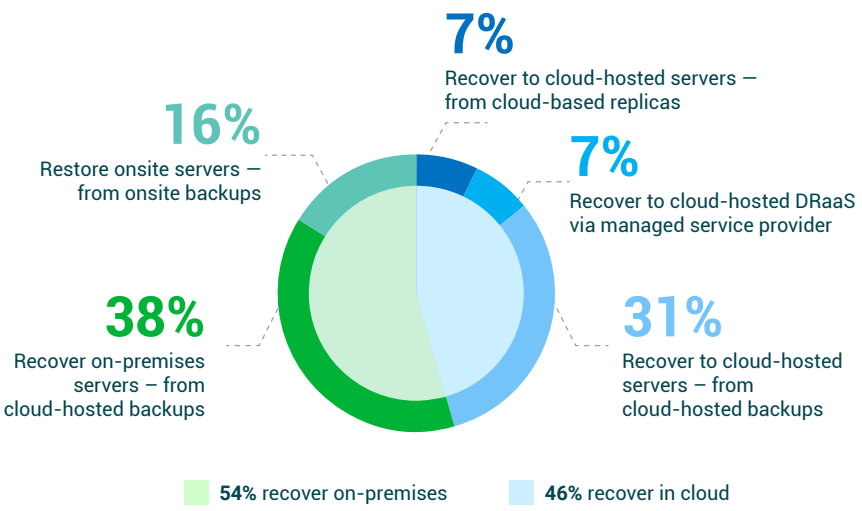



**Figure 2.3**

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

# Cloud-Powered Data Protection continues to gain popularity

Is cloud-based storage a "tape killer?" According to survey results, **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, though this does vary by country or region.

| | GLOBAL | North America | Latin America | Europe | MEA | APJ |
|---|---|---|---|---|---|---|
| % of data to Tape | **50%** | 50% | 48% | 53% | 52% | 45% |
| % of data to Cloud(s) | **63%** | 63% | 60% | 63% | 64% | 63% |

Many organizations have a three-tier operating model for data retention, including:

- On-premises disk for 90-120 days
- Cloud copies, including current copies and previous versions for up to two to five years
- Tape for the minority of data that has mandates to be stored for 10 years or more

As an alternative lens to "% of data using the cloud", it is worth considering "% of organizations using cloud-powered backups" — with **67%** of global respondents using cloud services as part of their data protection strategy today, with the aspiration of **74%** by 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. In 2020, **53%** of organizations had BC/DR capabilities — with **71%** being BC/DR capable in 2023. More importantly is the recognition that while roughly **30%** of organizations continue to leverage multiple datacenters for their BC/DR, the percentage of organizations utilizing cloud-services (IaaS/DR or DRaaS) for BC/DR has more than doubled from 2020 **(23%)** to 2023 **(47%)**, with **55%** expected to be using cloud-powered DR by 2025.

| | GLOBAL | North America | Latin America | Europe | MEA | APJ |
|---|---|---|---|---|---|---|
| % of orgs utilizing cloud-hosted infrastructure for BC/DR | **47%** | 50% | 41% | 43% | 41% | 54% |
| % of orgs with multiple datacenters for BC/DR | **24%** | 22% | 27% | 24% | 25% | 23% |

**74%**

of organizations expect to utilize cloud services as part of their data protection solution by 2025

# Will 2023 be a year of 'change?'

Between the angst of ransomware, the pressures of ensuring IT services, and the challenges of protecting modern IaaS and SaaS workloads, one might presume that many organizations are likely to switch backup solutions 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

**57%**

of organizations expect to change their backup solutions in 2023

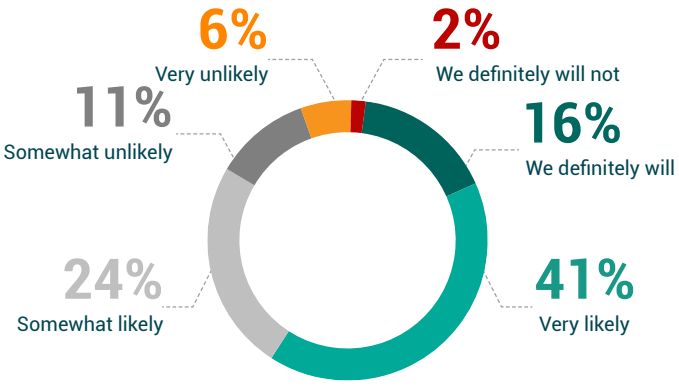



**Figure 3.6**

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

# The Veeam perspective

### The Veeam Data Platform

As organizations continue to transform their infrastructure, ensuring support for cloud aspects such as backup, usage and mobility, 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, 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.

Click here to view the Global complete research report

Questions related to this research data and insights can be directed to **StrategicResearch@veeam.com**