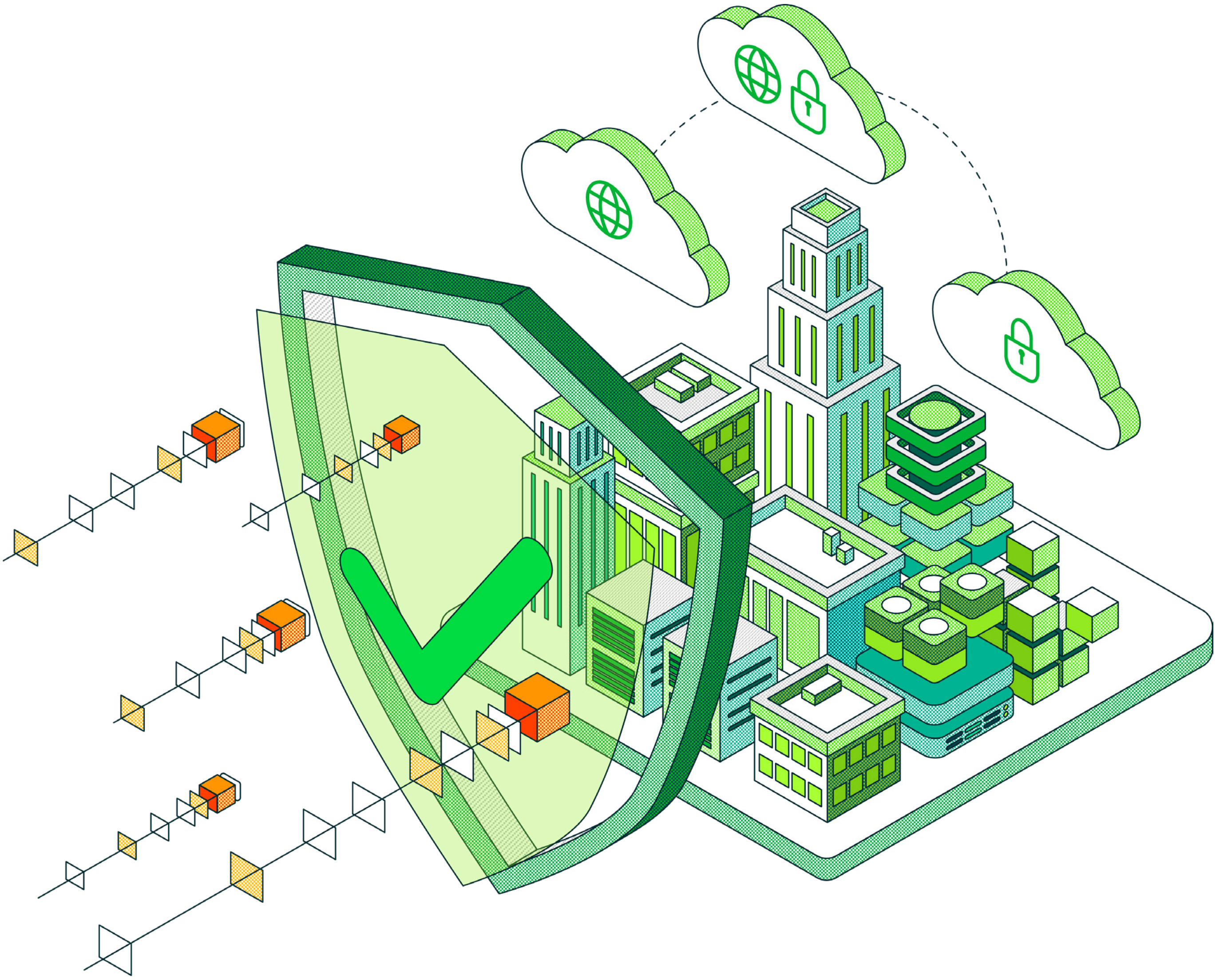
EXECUTIVE BRIEF

2023 Data Protection Trends

Financial Services Edition



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 — including 348 financial services organizations. 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 predicts a 5.2% increase in overall IT spending, this survey revealed that data protection budgets are expected to increase by 5.9% financial services in 2023. You can find the full 2023 Data Protection Trends Report at https://vee.am/DPR23.

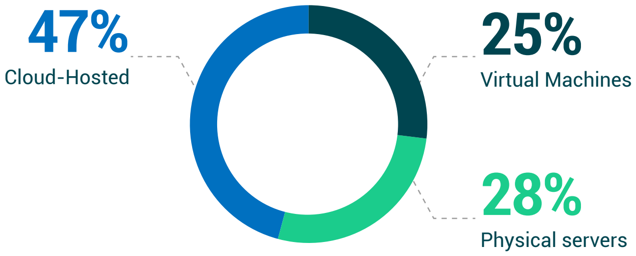
Organizations in financial services expect to **increase their data protection budget** for 2023 by

5.9%

Hybrid Infrastructure 2020 to 2025

Each year, the survey asks organizations to estimate how many on-premises (physical and virtual) and cloud-hosted servers they currently have as well as 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. For 2023, however, the actual distribution of server instances across **4,200** organizations' Hybrid IT is as follows:

Actual 2023 Hybrid IT Landscape (global)



Globally, physical servers and virtual machines have both stabilized at around **50%** of an organization's overall IT plan, while the rest is cloud hosted. There is also a continued, albeit gradual, shift to cloud-hosted servers, predominantly due to organizations' cloud-first strategy. New workloads are starting up in clouds at faster rates than legacy workloads are being decommissioned in the data center, thereby diluting the data center within an overall hybrid IT strategy.

Financial services data is nearly an exact mirror of the global finding. Hybrid IT continues to be the norm, with a relatively even balance between servers within the data center and those that are cloud hosted. Within the data center, there is a good mix of both physical and virtual servers.

And while these statistics are inclusive of financial services sector, server-centric workloads, it is notable that serverless or container-centric workloads continue to grow in popularity, with **53%** of respondents running containers in production in 2022.

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 across all industries, assuring reliability is the second most important criteria. This is pretty shocking when considering that many organizations may be running legacy backup solutions that rarely yield good outcomes when protecting modern workloads.

38%

of financial services organizations are looking for their next ‘Enterprise backup solution’ to **protect IaaS & SaaS workloads, as well as the datacenter**

Modern or innovative data protection (global)

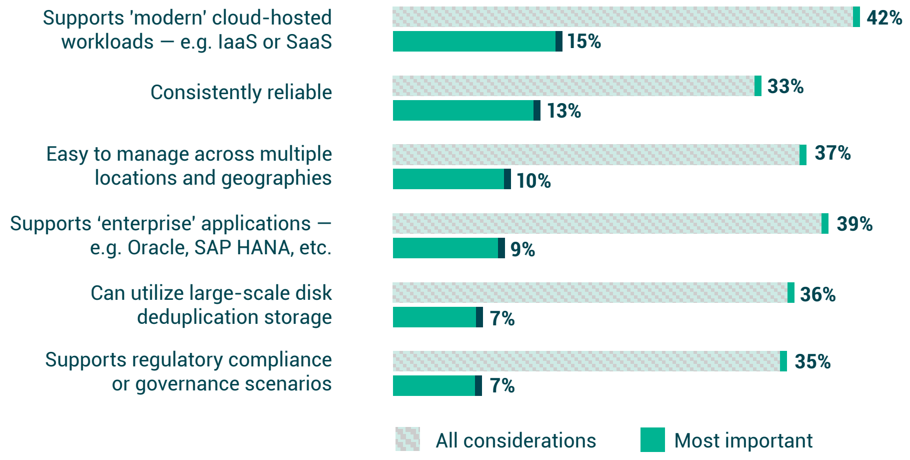


Figure 1.2

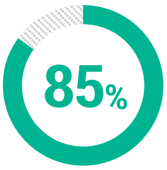
What does “enterprise backup” mean to you?

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

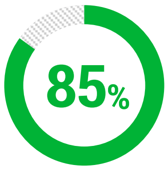
Following the adage of, “When you modernize production, you must modernize protection,” data protection strategies must be equally inclusive of physical, virtual and cloud-hosted workloads. Modern strategies should also enable workload movement from one platform type to another without sacrificing protectability. Following the global trend, **38%** of organizations in financial services stated that being able to standardize their protection capabilities across their data center, IaaS and SaaS workloads is a key driver in their 2023 strategy.

As such, it makes sense that cloud-hosted protection and reliability would be adjacent and top of mind. In fact, when organizations were asked what would drive them to change their primary backup solution, the most common reason, as well as the most important, was improving reliability, which is consistent with what organizations are looking for in an enterprise backup solution. Among financial services organizations, “Improving Reliability/Success of Backups” was a top priority for **35%** of them.

There is also an overarching sentiment from IT leaders that they aren’t protected well enough, for a variety of reasons, including dissatisfaction with the status quo and the ever-present gloom of imminent ransomware risks. Among organizations in financial services:



have an **“Availability Gap”** between how quickly they need systems to be recoverable and how quickly IT can bring them back



have a **“Protection Gap”** between how much data they can lose and how frequently IT protects their data

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, cyberattacks 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.

Within financial services organizations, ransomware attacks occurred with similar frequency. For organizations in financial services:

- Only **16%** experienced no ransomware attacks in 2022
- **15%** experienced only one attack
- **49%** experienced two or three attacks
- And **20%** experienced four or more attacks in 2022

In fact, **48%** of financial services organizations stated that ransomware (including both prevention and remediation) was their biggest hindrance to Digital Transformation or IT modernization initiatives, due to its burden on budgets and manpower. As startling as those statistics are, the global results of those attacks are even worse. When financial services firms 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 recoverabl

Thus, it is no surprise that when asked what financial services firms were looking for in a “modern” data protection solution, the most common, and most important aspect is the integration of data protection within a cyber preparedness strategy.

Modern or innovative data protection (global)

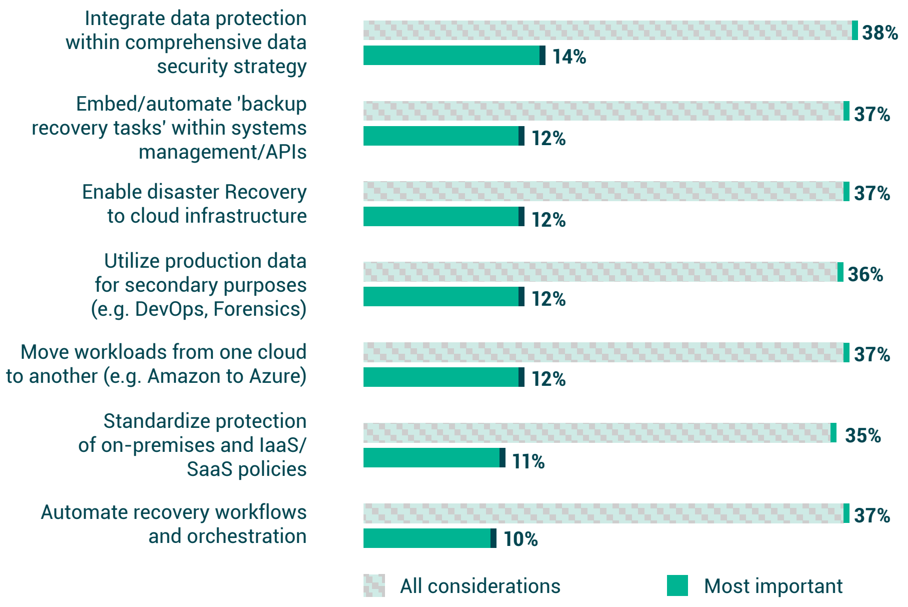


Figure 1.5

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 globally 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. The research results show relatively balanced interest between on-premises and cloud-hosted recoveries for 2023, but most of the recovery data will be coming from cloud-hosted backups.

27%

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

While cyber events continue to be highly visible in financial services organizations, natural disasters and IT systems' failures continue to drive broader business continuity and disaster recovery (BC/DR) initiatives. In fact, **75%** of organizations consider their cyber and (traditional) BC/DR initiatives to be either mostly or completely integrated.

To achieve that among organizations in financial services:

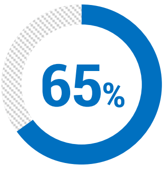
- **37%** want to orchestrate recovery workflows, instead of relying on manual processes
- **27%** will leverage on-premises infrastructures for their BC/DR
- **46%** will leverage cloud infrastructures for their BC/DR, using IaaS or DRaaS

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

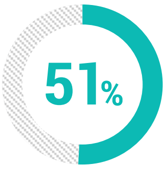
Cloud-Powered Data Protection continues to gain popularity

Is cloud-based storage a "tape killer?" According to global 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.

That said, cloud-powered data protection is not the misunderstood "tape killer" that early pundits predicted. When discussing the media used within their backup systems, financial services organizations reported that in addition to disk-based protection:



of production data is stored in a **cloud** at some point in its lifecycle



of production data is stored on a **tape** at some point in its lifecycle

Looking across all industries, 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

Within financial services, every facet of IT continues to be candidates for cloudification, with data protection being a common scenario. **77%** of financial services organizations anticipate using Backup as a Service (BaaS) or Disaster Recovery as a Service (DRaaS) to protect at least some of their servers over the next two years.

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!

When asked, **55%** of financial services respondents expressed that they are likely, or definitely will switch backup solutions. This is consistent with the global response rate below.

55%

of financial organizations expect to change their backup solutions in 2023

Change solutions (global)

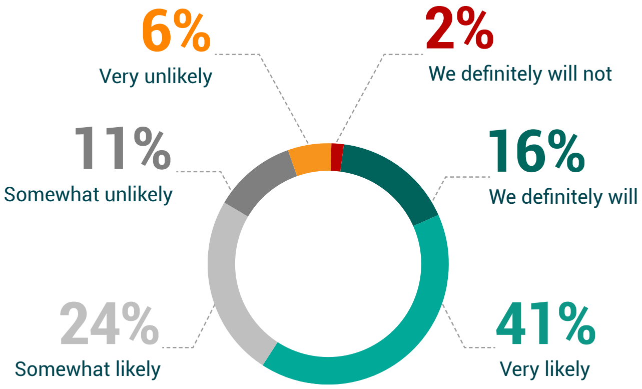


Figure 3.6

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 and 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**