veeam Insights

The State of Hybrid and Multi Cloud 2024

A research brief from the
2024 Data Protection Trends Report

Table of contents

Introduction

Each year, independent research firms are commissioned to survey IT leaders and implementers responsible for their organizations' data protection strategies. One of the most important aspects of this annual research is to understand organizations' strategies towards hybrid- and multi-cloud architectures as their IT teams endeavor to facilitate their business processes. While the first several months after COVID caused a significant acceleration of cloud adoption, the succeeding four years have shown a relatively consistent distribution of workloads across data centers, private clouds, and multiple public clouds.

For 2024, organizations stated that nearly half of their production workloads run within a public cloud with the rest remaining equally divided between physical servers and virtual machines within their data centers.

What has not been seen in past decades' IT landscapes is the diversity of "gold standard" production platforms of choice. In times past, a best of breed data center might rely almost solely on Novell NetWare or Windows Server infrastructure — which was later surpassed by virtualized infrastructure from VMware, Hyper-V, and other hypervisors. In those past generations, it was not uncommon to see a true migration from yesteryears' platform of choice to the new platform with a single best of breed data protection solution being chosen that matches the new platform (e.g., Veeam for VMware) with the myriad clouds.

What do you estimate is your organization's percentage of servers in each of the folowing formats in 2024?

27% Virtual machines within data center

28% Physical servers within data center

45% Cloud-hosted server instances within "hyper scale" or Service Provider (MSP)

In 2024, while data centers continue to deliver critical IT services for organizations of all sizes, it is not uncommon to also be:

- Leveraging Azure, AWS, Google, and other infrastructure clouds
- Embracing purpose-built infrastructure services for file shares or databases
- As well as utilizing mainstream SaaS platforms such as Microsoft 365 or Salesforce

With such excitement around cloud services, it would be easy but incorrect to assume that the importance of the modern data center is diminishing. Instead, data suggests that most organizations have a "cloud smart" strategy of considering cloud hosted workloads by default for new workloads by default which in turn dilutes the percentage of IT services still provided by the data center without those workloads actually being migrated from those physical facilities.

Moreover, it is becoming increasingly common for business processes and economic considerations to affect which workloads will be hosted on- or off-premises. In fact, even within each cloud, one cannot assume that the "journey to the cloud" is a one-way journey nor to one service provider. Instead, there is both opportunity and challenge created by the business requirement of being able to fluidly move workloads between data centers and clouds, between clouds, and back again.

This research brief will provide data and insights for three key stakeholders who are faced with the imperative of leading a "cloud smart" strategy for their organizations:

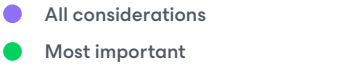
- **Executive leaders** responsible for IT delivery to their organizations
- **Implementers of IT architectures** that utilize cloud services
- **Backup professionals** responsible for the data protection of corporate resources on- and off-premises

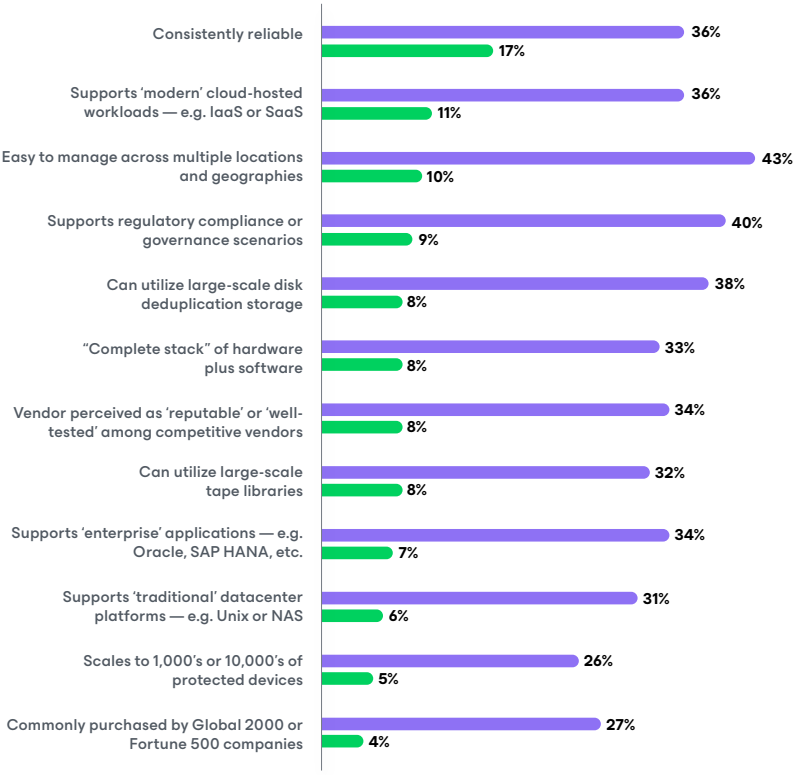
'Enterprise' Backup Must Protect IaaS/SaaS

According to 1,200 enterprise organizations, the two most important capabilities for their next data protection solution are "improved reliability" and "improved protection of cloud-hosted workloads."

'Enterprise Backup' must protect IaaS/SaaS

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? (n=1.200)





While protection of "enterprise" applications (e.g., Oracle) and "traditional" data center platforms (e.g., NAS) still appear in the broader list, both are far lower priorities presumably due to organizations already having legacy backup solutions for those legacy platforms. In contrast, when legacy backup methods are attempted to protect modern workloads (e.g., clouds), then the reliability of protection and recovery logically and significantly reduces. As such, it is not a surprise to see "reliability" and "protection of clouds" being adjacent as the most important drivers for change.

For the IT leader, the opportunity to utilize cloud hosted infrastructure in compliments to data center components should enable operational agility and economic efficiency as they deliver IT services on whichever platform(s) are most ideal per workload.

For the hybrid architect, the impetus is to be vigilant as their teams modernize production strategies that they be mindful to also modernize protection strategies so that business critical workloads do not go from *"well-protected"* within the data center to *"under protected or non-protected"* within the cloud.

For the data protection expert, the challenge is either complimenting the data center centric standard backup solution with various cloud provided utilities (e.g. each production cloud offering a copy job, recycle bin, or built-in snapshot), or chose a modern backup platform capable of protecting not just legacy workloads but also mainstream clouds. The latter has the added consideration of providing consistency as workloads fluidly migrate between clouds based on changing business imperatives.

Modern Protection Must Be Broader Than Just Cyber Resiliency

While it is reasonable that the most visible impetus for modernizing data protection should be in alignment with cyber resiliency against the ever-present and almost inevitable threat of ransomware, it would be a huge error to base one's data protection strategy solely on that looming threat. According to the latest research, while cyberattacks were the most common and most impactful causes of IT outages — with 40% of organizations experiencing an attack — most of the other crises that have always impacted IT and business processes persist including:

37%
suffered outages due to **infrastructure** issues

34%
suffered outages due to **application software** issues

33%
suffered outages due to **human error** (e.g., deletion, overwriting, etc.)

32%
suffered outages due to **operating system** issues

31%
suffered outages due to **public cloud unavailability**

29%
suffered outages due to **natural occurrences** (e.g. fire, flood, weather, etc.)

It is worth noting that almost none of these outage causes are mitigated due to leveraging cloud-based resources versus one's own data centers. As such, cloud-hosted workloads have the same requirements for not only backups but also disaster recovery. While cloud services might reduce errors caused by physical storage or server componentry, every other rationale for a modern data protection approach to data centers should also apply across hybrid and public clouds.

For the IT leader, including both the Chief Information Officer and the Chief Information Security Officer, organizations' disaster recovery strategies that already encompass significant IT outages must now broaden to include cyberattacks and access issues to public clouds as part of *"what to prepare for."*

For the hybrid architect, including IT architects as well as security-minded engineers, the blurring of specialties necessary for providing cloud-hosted services differs from the specialized roles of access control and prevention/detection security specialists versus IT operations and/or specialists in infrastructure, virtualization, servers, etc. While this blurring may make consumption of IT services more seamless for users, the burden of securing those resources against the myriad outage causes above is more daunting.

For the data protection expert, recognizing that data is data, regardless of whether it is served from servers or services, means that data protection must be approached universally. In this case, the *"what to protect"* must now include cloud-hosted infrastructure (IaaS), as well as platforms such as cloud-hosted files and databases, along with mainstream SaaS applications.

Organizations are Looking for Modern Data Protection That is "Cloudy"

When organizations were asked what the most defining aspect of "modern" data protection would be, many cited at least one cloud-centric capability:

39%
want the ability to move from one major cloud to another (e.g. Amazon to Azure)

38%
want consistent protection of on-premises and IaaS/SaaS workloads

37%
want their data protection solution to migrate their on-premises workloads to a cloud

27%
want to use cloud-infrastructure as their disaster recovery site

Some of these capabilities specifically align with broader IT imperatives:

For the IT leader, all four capabilities align with wanting flexibility for the organization in whether and which cloud(s) to leverage in delivering IT to their business constituents. The top entry is arguably the most important as organizations struggle with which hypervisor(s) to utilize within their data centers as well as which clouds to complement with. While almost every major platform provides a utility to move workloads to their technology, rarely — if ever — do any provide a utility to move it elsewhere. Thus, unsurprisingly, IT leaders scored this capability highest as an attribute of modern data protection.

For the hybrid architect, whose teams have given up countless weekends migrating workloads from servers, to hypervisors, to alternative hypervisors, and now to cloud(s) — the first step is always a good backup and then a successful test restore. Instead, it is reasonable that IT implementers in this year's survey would recognize the potential to simply 'restore' the backup into the new cloud — a.k.a. migration. Not only is the backup "tested" but the original environment remains unaffected in case the migration is aborted.

For the data protection expert, building on the recognized benefits described for the hybrid architect, the reality for those responsible for managing data protection and utilizing the capabilities outlined above does require that the organization's data protection solution be equally capable of protecting the diverse data center and mainstream cloud services, as well as 'transforming' server instances that were protected on one hypervisor or cloud into the constructs needed when restoring that server instance into a different hypervisor or cloud host — e.g. Amazon to Azure, VMware to Hyper-V, VMware to Azure, etc...

How These Considerations are Forcing Change

With such potential agility and effectiveness coming from adopting a "cloud smart" strategy, enthusiasm for leveraging a hybrid- and multi-cloud strategy is justifiably high. But without a set of modern data protection capabilities that are purpose built for the myriad clouds in the modern enterprise, many digital transformation and IT modernization efforts will fall short. Thus, it is not surprising that 92% of organizations have increased their data protection budgets for 2024 with an average increase of 6.6% — which is notable compared with IDC's overall IT budget increase forecast of only 3.5%. Said another way, while IT overall may be getting a slightly higher budget, the disproportionate increased investment in data protection will likely be at the expense of other lesser priority IT initiatives.

For the IT leader, who likely drove the budget planning, this shows a commitment to ensuring that all the organization's data is protected both within the data centers and across the clouds.

For the hybrid architect, there is an assurance and recognition for the need of holistic data protection as part of a "When you modernize production, you must modernize protection."

For the data protection expert, responsible for achieving these outcomes, it should not be a surprise that 54% of organizations intend to change their primary backup solution over the course of 2024. While some might supplement their legacy data center backup solution with another mainstream backup that can protect myriad clouds, this may be the catalyst where the "burden to change" of their legacy backup solution is easily outweighed by the "burden of running multiple point products for each unique cloud service."

This research brief is based on 1,200 survey responses from the unbiased IT leaders and implementers responsible for their organization's data protection strategies, which was conducted in late 2023 and published in January of 2024. The data was curated, and the sentiments were authored by former analysts from ESG and Gartner with a combined 70 years in the data protection industry.

To download the full Data Protection Trends Report for 2024, click here

Jason Buffington
@JBuff
VP, Market Strategy
Veeam Software

Dave Russell
@BackupDave
VP, Enterprise Strategy
Veeam Software

About Veeam Software

Veeam, the #1 global market leader in data protection and ransomware recovery, is on a mission to empower every organization to achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud. The Veeam Data Platform gives IT and security leaders peace of mind that their apps and data are protected and always available. Headquartered in Seattle, with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, 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.