veeam Insights

covenco
DATA MANAGEMENT & INFRASTRUCTURE 365

Cloud Protection Trends Report 2024

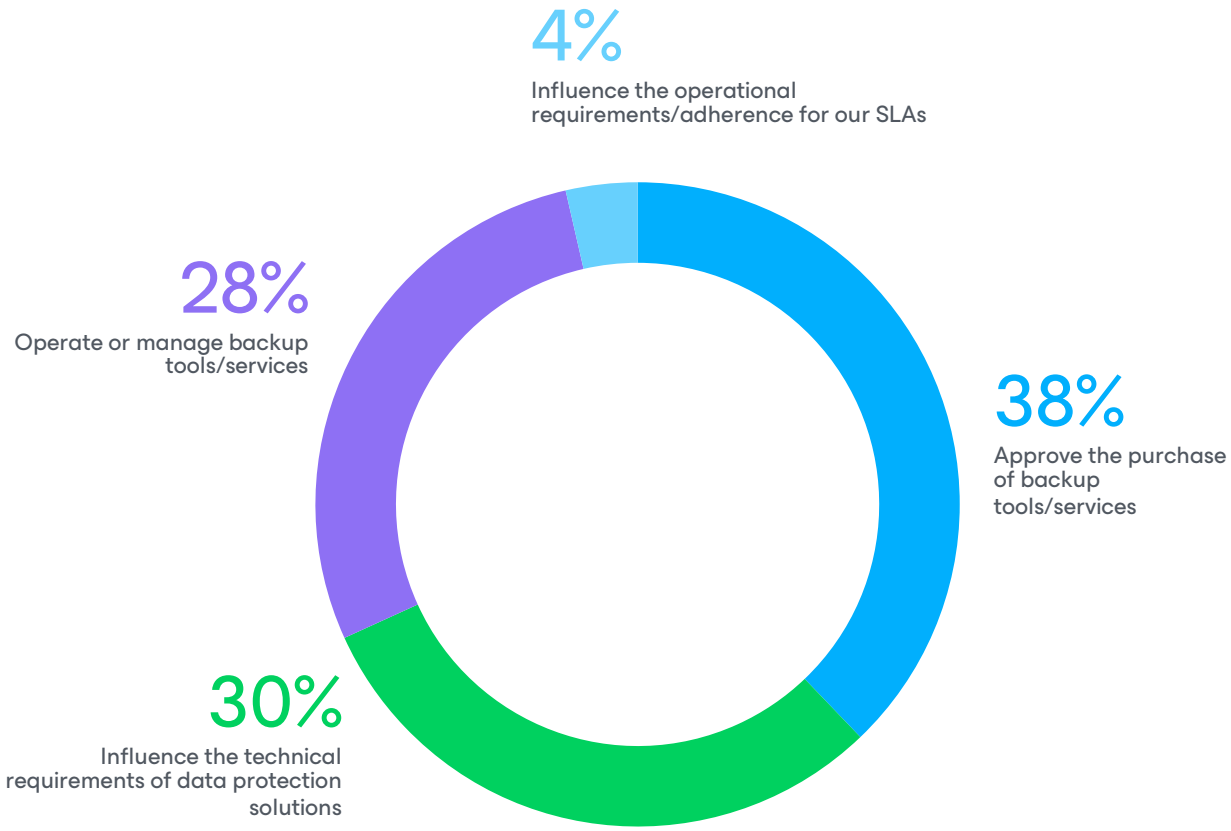
Introduction

The 2024 Cloud Protection Trends Report is the latest unbiased cloud-centric industry research studies looking at cloud-powered protection mechanisms of production data located both on- and off-site, including:

- **Cloud storage** or **vault**, cloud-hosted object, blob, or purpose-built cloud storage utilized by data protection solutions.
- **Backup as a Service (BaaS),** where the backup software is predominantly operated from, and its primary repositories reside within, cloud storage.
- **Managed BaaS**, where third-party service providers offer BaaS that includes not only the software and repositories, but also monitoring, troubleshooting, and/or expertise.
- **Disaster Recovery as a Service (DRaaS),** enabling IT teams to resume functionality of their production servers within a cloud-host, instead of an on-premises datacenter.

Over the last five years, Veeam has sponsored nine different research projects with independent analysts or survey providers to continually monitor market shifts and assess strategies related to leveraging cloud services in production. This year's report summarizes the most recent 1,600 unbiased responses from IT decision makers who are responsible for data protection of their on-premises servers or workloads and use cloud services as part of their data protection strategy.

Which best describes your role(s) in regard to your organization's data protection strategies and tools?



What do Organizations Want from Cloud-based Backup?

According to the 2024 Data Protection Trends Report, the two top drivers affecting changes in data protection strategy are:

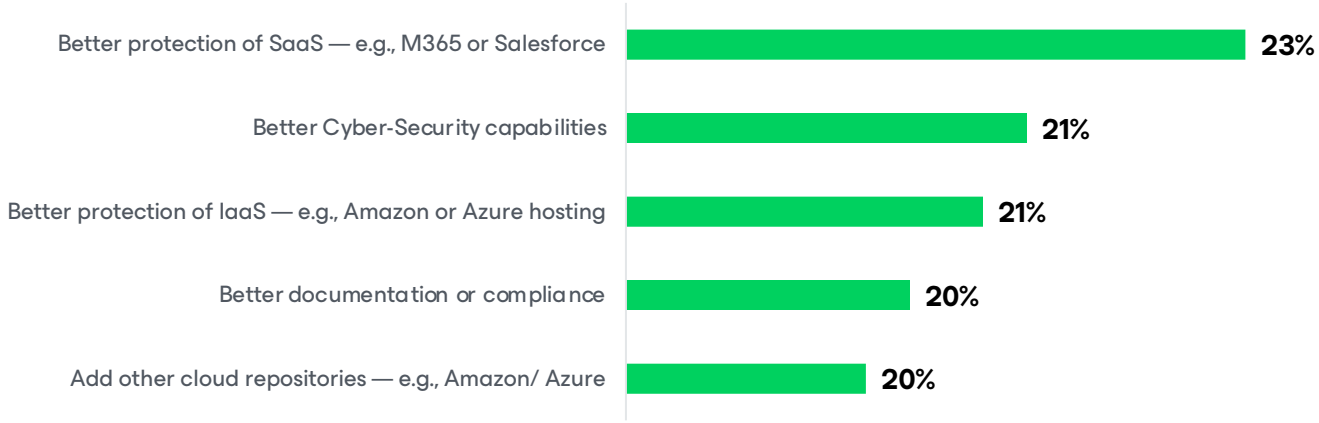
- The desire to integrate cyber technologies with data protection/backup
- Improved/consistent protection of cloud-hosted workloads

Respondents to the Cloud Protection Trends Report survey reveal similar reasons behind what is driving their consideration of cloud-powered protection as seen in **Figure 1**:

These top concerns included not only cyber capabilities and improved protection for Software as a Service (SaaS) and Platform as a Service (PaaS), but also a particular interest in leveraging cloud storage as part of a comprehensive data protection strategy. One of the more interesting aspects of this chart is the relatively "flat" distribution of desired capabilities, indicating that there is not a single key scenario that differentiates one cloud-powered solution from another. Instead, there are myriad capabilities that organizations are looking for across their cloud-based backup services that are not being entirely met today.

Figure 1

If there was anything you could change about your organization's existing cloud-based backup services, which would it be?



In 2024, BaaS Means Cloud-powered, Managed, and Trusted

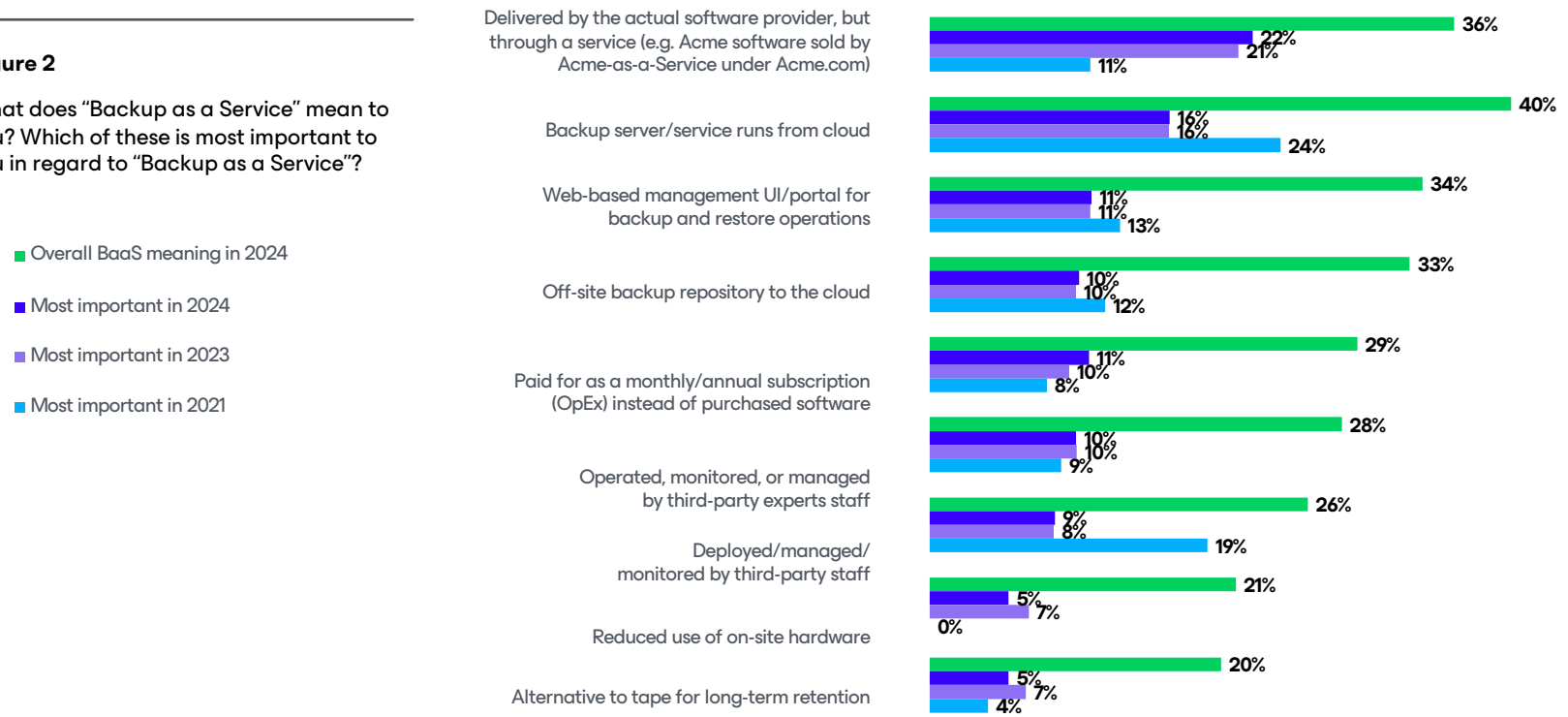
One of the most intriguing questions asked of IT leaders over these industry reports has been regarding their expectations around "What does Backup as a Service (BaaS) mean to you?"

When looking at the most common and most important responses of what customers are seeking in BaaS solutions, the top three 'foundational' considerations continue to be:

- The backup engine runs as a cloud service instead of as an on-premises executable
- The solution is managed via a web-based UI
- The data resides in a cloud repository outside of the production environment

Figure 2

What does "Backup as a Service" mean to you? Which of these is most important to you in regard to "Backup as a Service"?

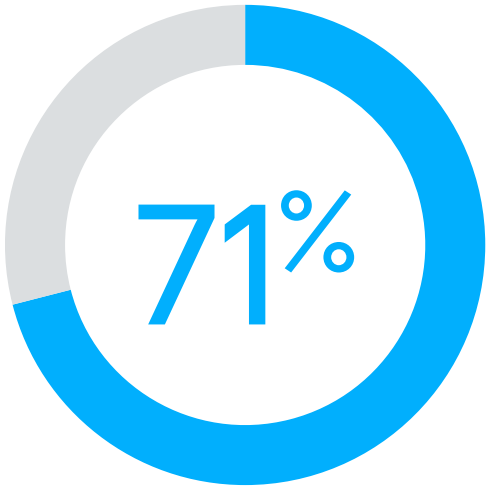


It is notable that, like many other early cloud-based services, the initial justifications and presumptions have all waned as adoption into mainstream has continued, e.g., reducing on-site hardware or subscription pricing. That said, the most significant market change over the last four years has been the customer expectation that backup services should be provided by the same vendor who produces the actual backup software itself.

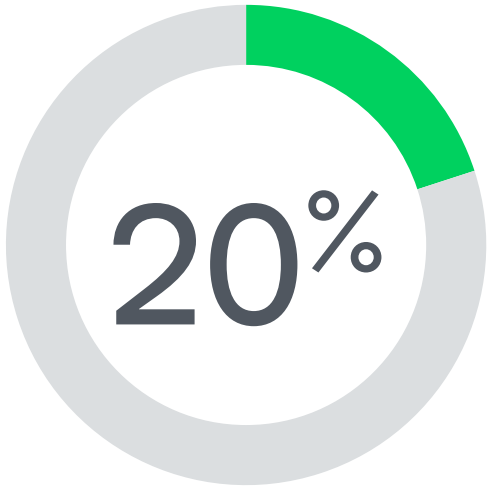
When asked what the single most important aspect of BaaS was, respondents said that it should be "delivered by the first-party software vendor."

Significantly, respondents from **Figure 2** (above) who selected 'off-site repository in the cloud' as a key merit for BaaS were then asked if they could "only choose one place where that off-site data should reside," where would they prefer — as shown in **Figure 3**.

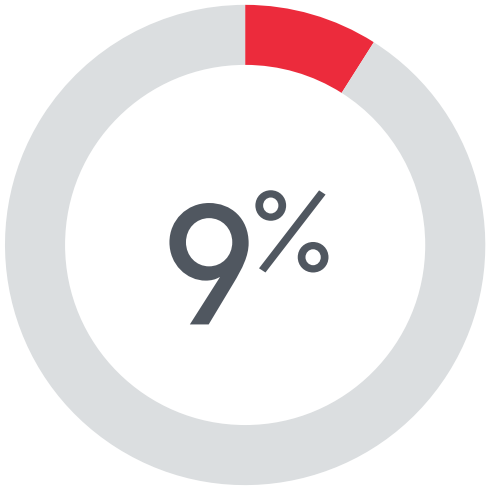
Figure 3



of organizations would prefer to store within a **hyperscale cloud**



would prefer to store within a **managed service provider**



would prefer to store within one of their **own data centers**

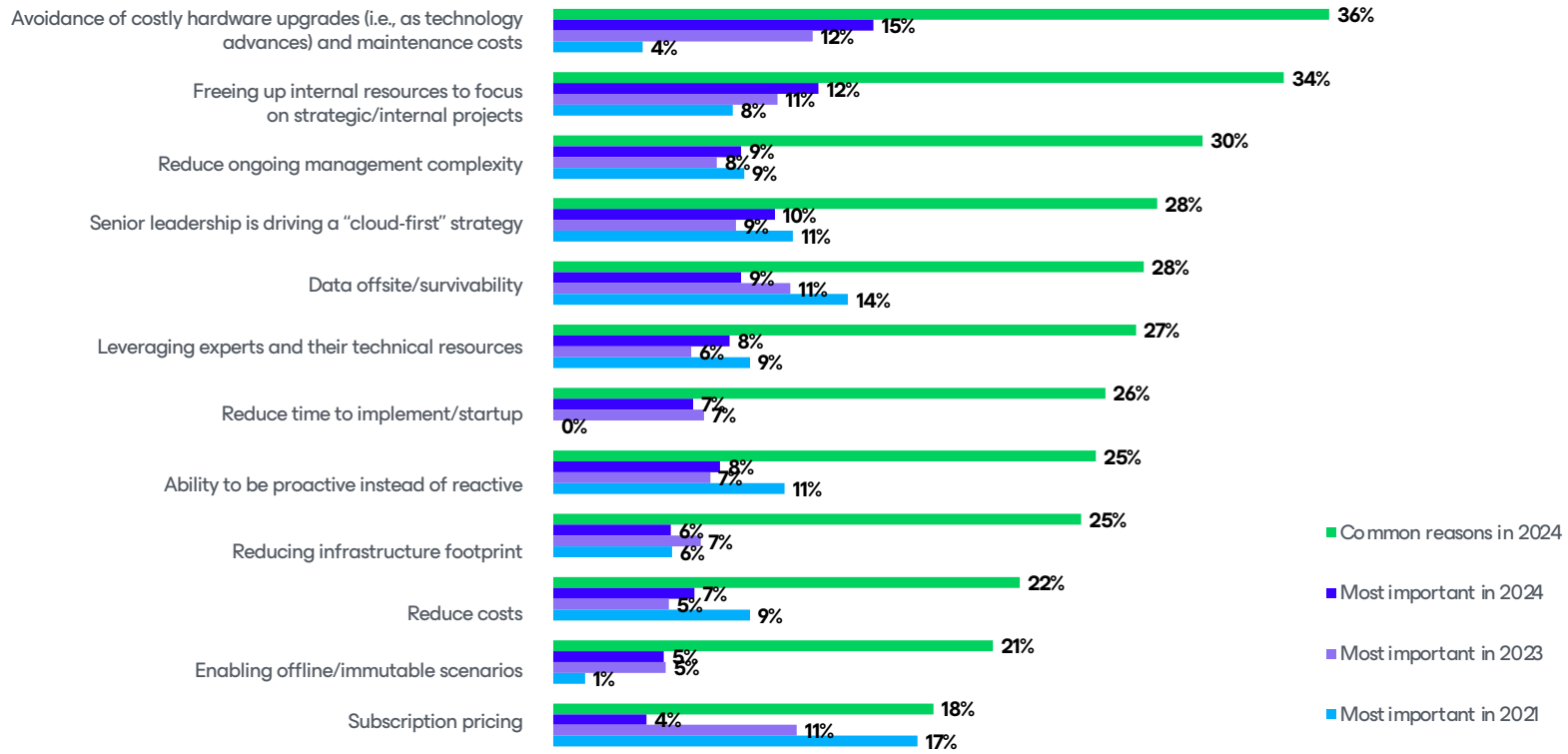
Why BaaS?

Whenever organizations choose to leverage cloud-powered services instead of utilizing infrastructure within their datacenter(s), the question of "why?" is usually based on business goals and/or functional enablement.

When organizations were asked **why they use BaaS,** instead of traditional on-premises hardware/software, their primary reasons all point to operational efficiency, such as reducing hardware upgrades, internal resources, and/or manageability.

Figure 4

Which of the following best describes why your organization uses or would use Backup-as-a-Service (BaaS), instead of traditional backup software/hardware? What is the main reason your organization uses or would use a backup service (BaaS), instead of traditional backup software/hardware?

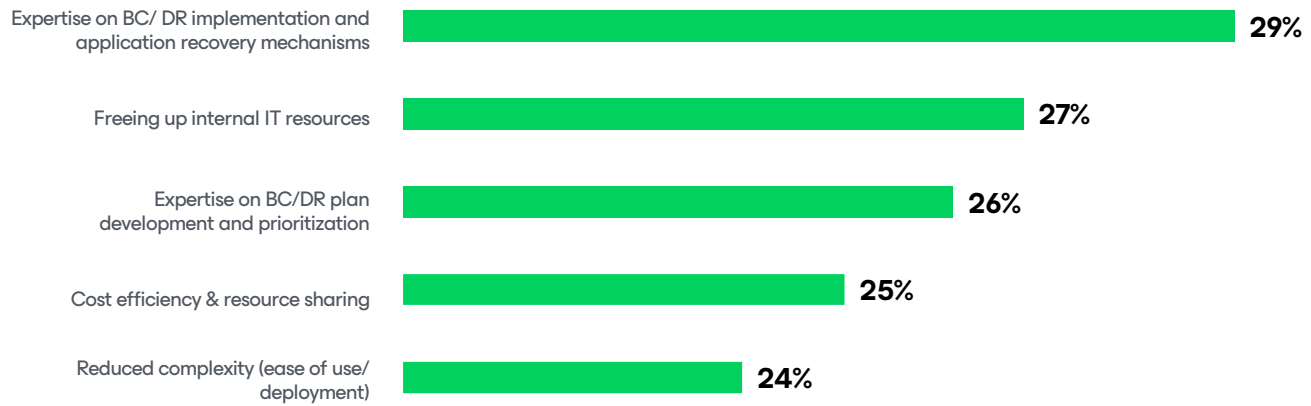


Why DRaaS?

When organizations were asked **why they use DRaaS** instead of secondary data centers, their primary reasons were around expertise, including utilizing the expertise of third-party subject matter experts for implementation. Other reasons included planning and reducing the demands of their internal experts to leverage their IT employees for more strategic purposes.

Figure 5

Which of the following best describes why your organization uses or would use Disaster Recovery as-a-Service (DRaaS), instead of managing your own secondary datacenter?



The Journey to Cloud-Powered Protection has Many Paths

For most organizations, when first adding cloud services to their data protection strategy, the first step is simply to augment existing on-premises data protection tools with a cloud storage retention layer. However, most organizations eventually realize that the power of cloud-powered protection is not simply in where the repository resides, but rather in leveraging expertise in the ongoing management of the overall solution.

With that in mind, two key questions in this near-annual report are:

- How did your organization first utilize the cloud as part of data protection?
- What type of cloud-powered data protection do you currently use? Self-managed cloud storage or a managed BaaS offering?

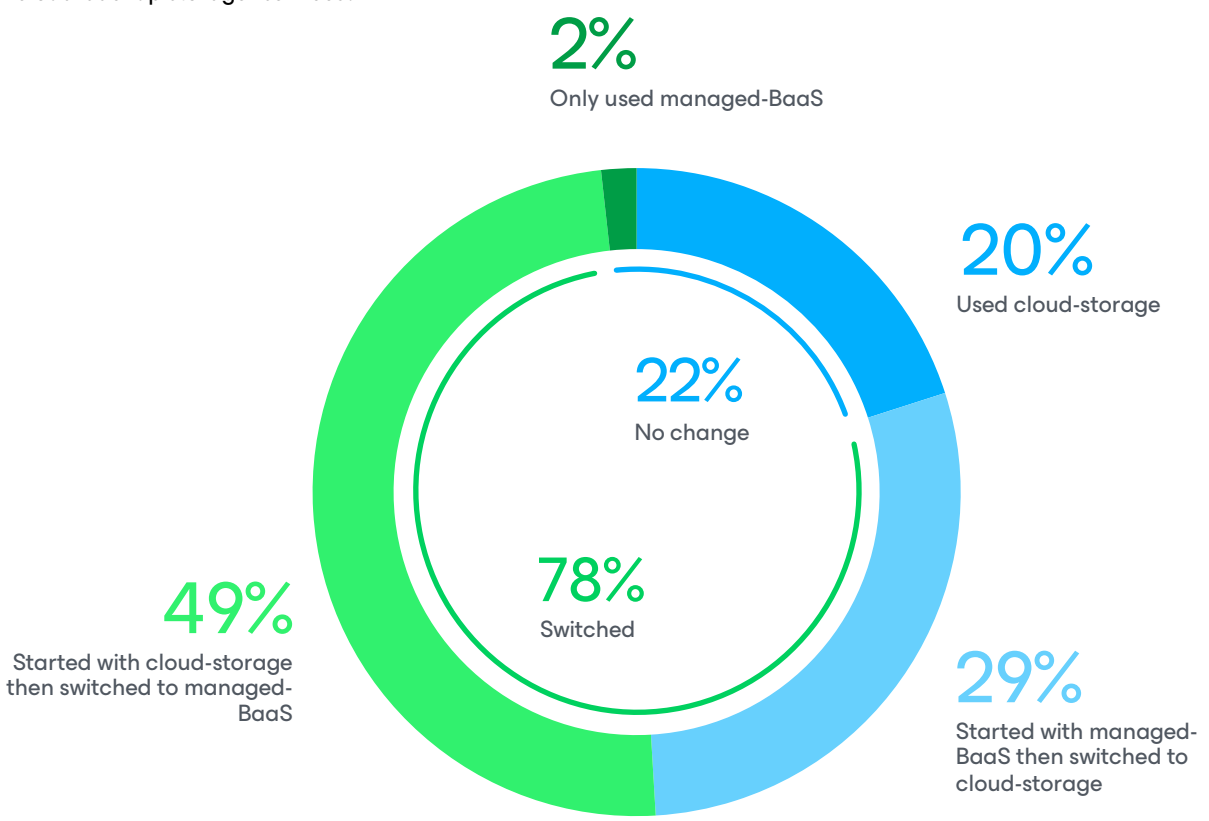
In 2024, nearly an even number of organizations simply leverage cloud storage (49%), while the rest (51%) subscribe to a managed backup service.

Perhaps more interesting is that only 22% of respondents are still using the same mode that they originally began using for their cloud-powered data protection, while 78% switched from one mode to the other. If fact, of those that switched, nearly 2 to 1 switched to a managed BaaS service compared to those that switched to a self-managed solution.

The high propensity to switch — and most respondents switching to a managed service — implies that **to fully leverage the benefits of cloud-powered protection, most organizations will eventually choose for their cloud services to be managed or curated by experts or operators outside of their own IT teams.**

Figure 6

How would you describe your organization's use of and journey with cloud-backup storage/ services?



On Average, Orgs Have More Roles Responsible for Protection Than Recovery

Within traditional data centers, most organizations used to rely solely on specialized backup administrators partnering with 'application owners' within the data center. This ensured a blending of expertise between those that know **how** to protect and those who know **what** to protect and how to recover.

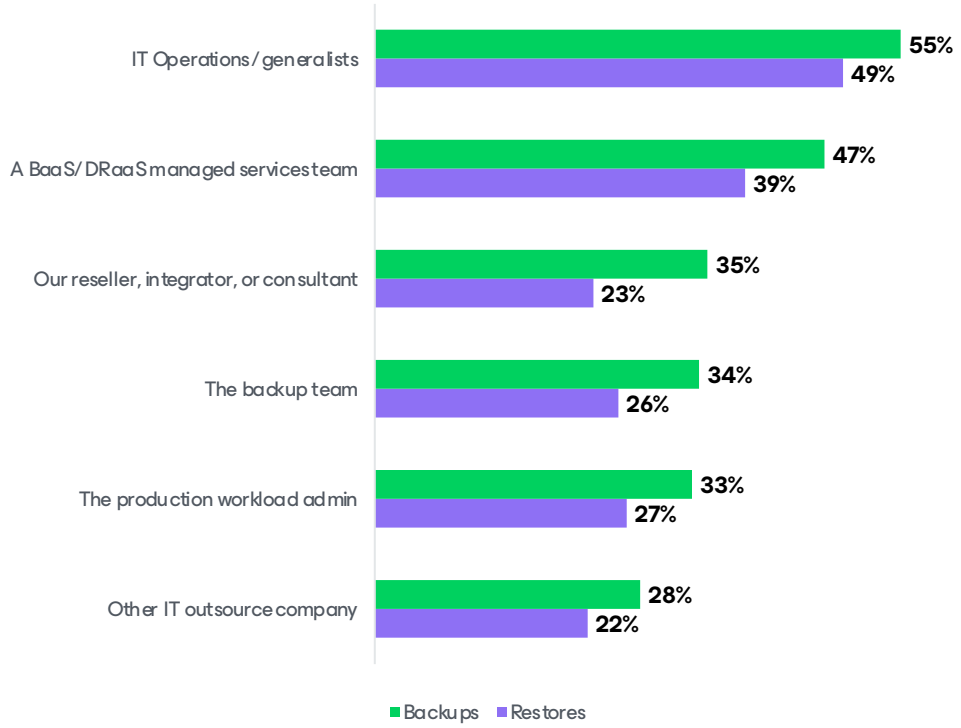
Within modern organizations that leverage cloud-powered protection services, the breadth of roles and their proportion of contribution has significantly changed:

- The most common group responsible for ensuring protection (and the most likely to be called in first in the event of a disaster) are "IT operations" generalists.
- When organizations utilize managed BaaS or DRaaS, those service providers' teams are the second most likely to be tasked with ongoing protection, as well as ad-hoc restore activities.
- In a nearly equal tie for third is not only the backup team and the workload administrators, but also the trusted reseller/integrator who otherwise augments the overall IT staff.

As a side note, the average organization has 2.3 different roles tasked with ensuring backups and only 1.8 roles responsible for restoration. This implies that, while more stakeholders are accountable for ensuring data protection, a higher level of expertise and judgment is required to decide how and when to restore data into the production environment.

Figure 7

Who primarily would manage the backups from this new backup service? Who primarily needs to perform restores?



IT Still Wants to Run Their BaaS, More Than Outsource

IT Teams want a mix of service levels when dealing with outsourced BaaS and DRaaS

Earlier data — as seen in **Figures 3, 4, and 5** — suggests that expertise is more expected for disaster recovery (DR) scenarios as opposed to "just" in backup situations. It is important to recognize that many organizations have different expectations for the level of "concierge, turnkey, or white glove" services provided by their managed service provider. One question that has been asked in each survey since 2021 was, "whom would IT leaders prefer to manage the daily operations of their backup services?"

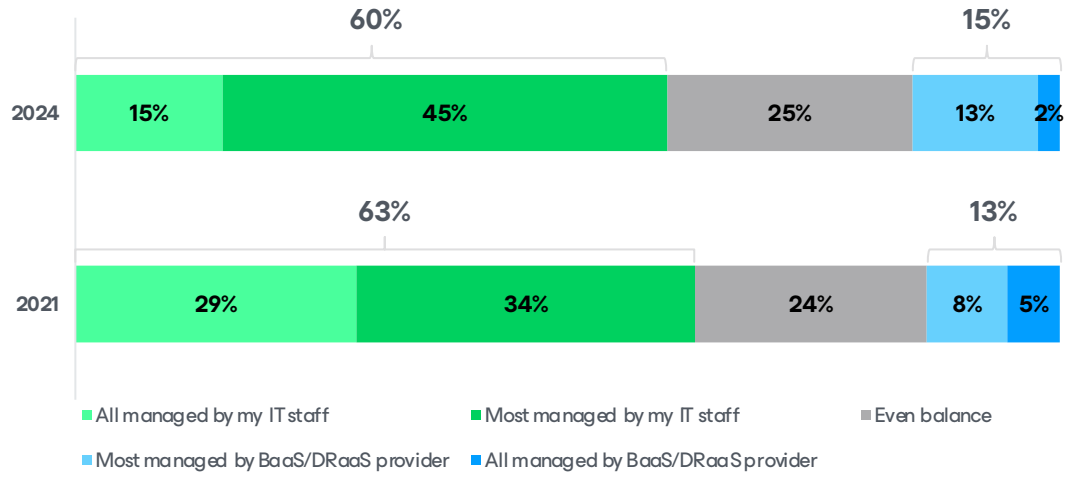
Interestingly, different respondents — even three years apart — show very consistent sentiments; IT teams have a wide range of expectations for the level of hands-off services provided by their MSP partners.

- Roughly one in four organizations expect an "even balance" in the distribution of responsibilities between their IT staff and the teams from their BaaS/DRaaS provider.
- Nearly 4:1 respondents presume that most or all daily tasks will still be managed by their own IT staff rather than delegated to the BaaS/DRaaS provider teams.

It is worth noting, that while "fully outsourced" use of a BaaS or DRaaS provider may have the smallest percentage of subscribers, the data suggests that providing this white glove, full-service experience is the desired outcome for at least one in seven subscribers and likely the single strongest differentiator between "utility/commodity" BaaS providers and "strategic" DRaaS providers.

Figure 8

In your opinion which of the following describes how you'd ideally like to utilize a BaaS or DRaaS service?



How to Choose a Provider

Organizations are Looking for Outcomes

The journey to successful cloud-powered protection requires organizations to answer three questions for themselves:

1. Whether to use cloud-powered services vs. self-managed on-premises technologies?
2. Which software, vendor, or technology is most capable of protecting the organization's production platform(s), potentially including datacenter and cloud-hosted workloads?

Once one has decided to leverage cloud services and which underlying technologies that they trust most, the reality that not all service providers offer the same level of capabilities or competencies becomes very clear. Thus, a final — but equally important — question comes up:

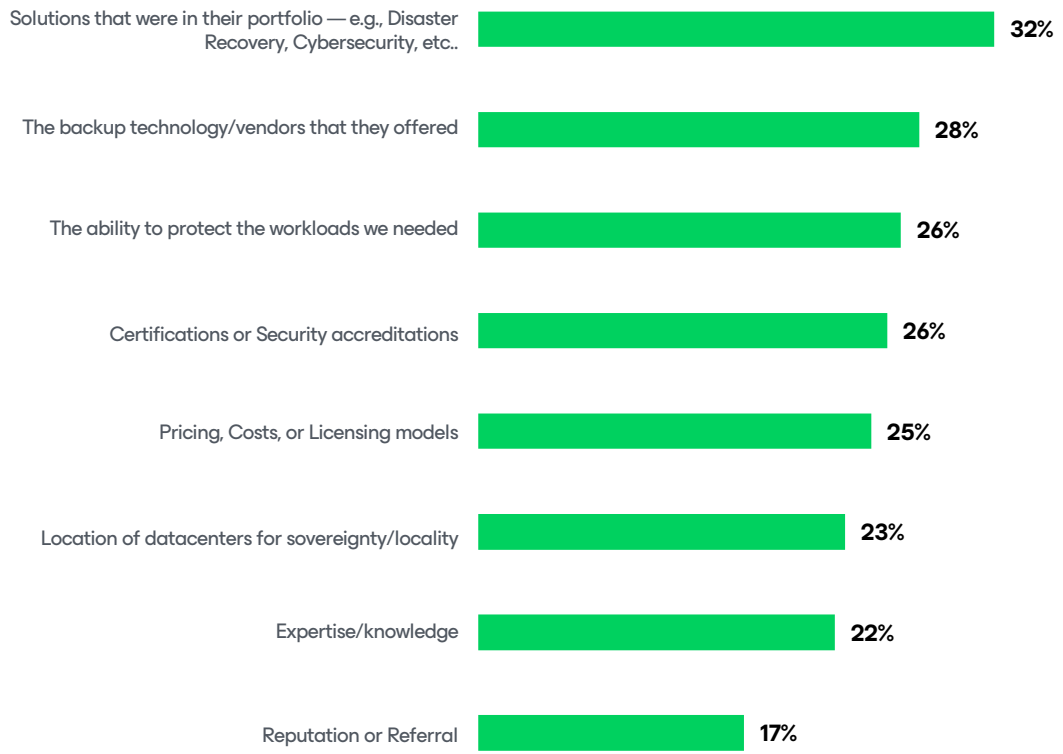
3. Which managed service provider do I want to partner with?

Organizations were asked why they chose their current cloud backup service provider, the top three reasons all related back to the "outcomes" (e.g., the capabilities provided by the technology and MSP teams).

Of particular interest, when organizations chose their MSP, 51% of respondents chose either "solution outcomes" or "expertise" as a primary determinant when choosing their managed provider. Of those solutions or areas of expertise, DR was the number one desired scenario, followed by hybrid cloud operations and cyber resiliency.

Figure 9

What were the top factors on how your organization chose its current cloud-backup service provider?



Organizations Satisfaction with Cloud Services

Having gone through the journey of choosing to leverage cloud services and selecting a managed service provider to fulfill those capabilities, it is worth noting that 90% of subscribers are either very satisfied, or completely satisfied with their current managed service provider.

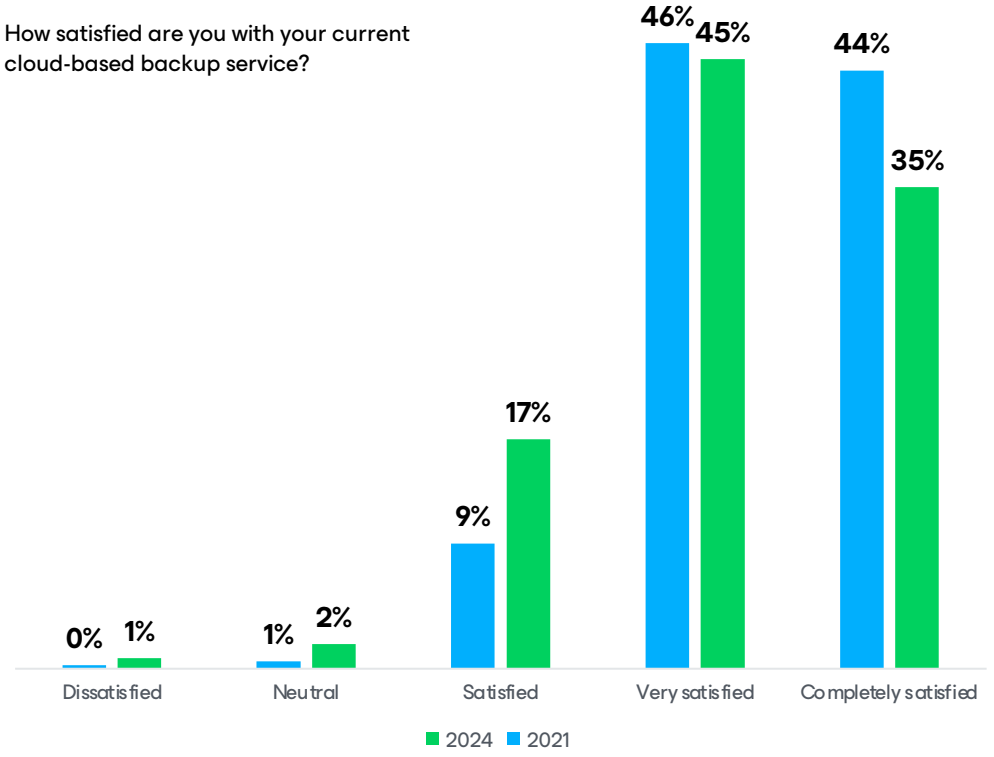
That said, subscribers of cloud-powered protection solutions were asked what would cause their organization to switch to a different service provider. The top three considerations — or drivers of change — relate to what and how their production platforms are being protected. This includes assured capabilities for cloud-hosted infrastructure (IaaS/Platform as a Service [PaaS]) and SaaS, which in most cases directly correspond to the underlying backup software technologies being used.

Years ago, economics was historically a top driver for cloud-powered services when organizations were first trying to move from large CapEx (capital expenditure) strategies to monthly OpEx (operational expenditure) consumption models. Today, the consideration of economics more likely implies that organizations are starting to see BaaS in a more commoditized "utility" — i.e., where simply providing copies to an off-site location without delivering either expertise or additional capabilities is so mainstream that price becomes the determinant of choice.

Today, more strategic offerings such as improved disaster recovery or regulatory compliance serve as differentiators, likely causing many organizations to move from commodity BaaS capabilities to more strategic DRaaS solutions moving forward.

Figure 10

How satisfied are you with your current cloud-based backup service?



Summary

Veeam has contracted with independent research firms to survey **18,793** IT leaders over the past five years to remain cognizant of where and how organizations want to consume cloud-powered data protection capabilities, as well as what service providers want to offer to their subscribers. This year's **1,600** unbiased IT decision makers essentially answered three questions:

1. Whether to use cloud-powered data protection services with cyber resiliency and cloud production (IaaS/SaaS) capabilities being top of mind?
2. How will those cloud services be used and by whom? With the expectation that the organizations' IT teams may still conduct the majority of daily tasks while embracing the trusted expertise offered by third-party providers — especially for DRaaS vs. BaaS scenarios?
3. Which provider to partner with? Where solution outcomes and expertise competencies were the primary determinants?

This research report is based on 1,600 survey responses from the unbiased IT decision makers responsible for data protection of on-premises servers or workloads and using cloud services as part of their data protection strategy, which was conducted in late 2023 and published in May 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.

Veeam recognizes that organizations need the ability to choose the right providers and capabilities for their unique data protection needs:

- To learn more about Veeam Data Cloud, Veeam's own backup services offerings for Microsoft 365 and Microsoft Azure, click here.
- To learn more about the **13,000** Veeam Cloud Service Providers (VCSPs) that provide a range of managed and turnkey services for protecting data centers, remote offices, and many mainstream cloud platforms (e .g., Microsoft 365, Salesforce, Amazon, Azure, or Google) click here.

About Authors

The industry analyses of this data were authored by the following contributors:

Jason Buffington

VP, Market Strategy
@JBuff

Dave Russell

SVP, Strategy
@BackupDave

Julie Webb

Director, Market
Research & Analysis

About Veeam

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 Seattle, Washington, 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.

For questions on this research: StrategicResearch@veeam.com

veeam Insights