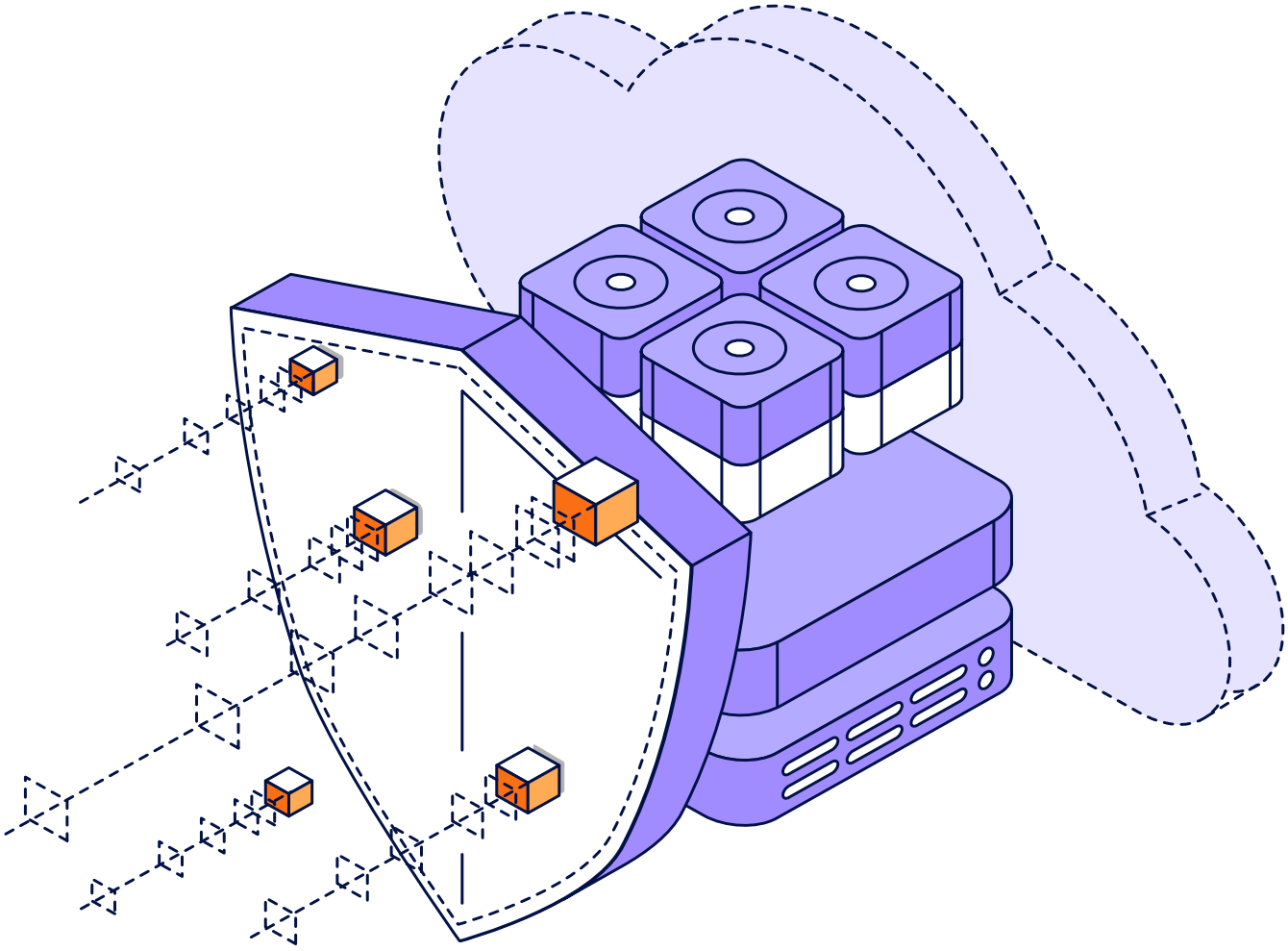
Cyber Resiliency for the Hybrid-Cloud

Lessons learned from 7,000+ IT and security professionals



The last several years have seen the shift from on-premises datacenters to '***cloud, when it makes sense***', to ***cloud-first*** strategies, to ***hybrid everywhere***, to where most organizations are today with '***strategic multi-cloud***' as the normal mode for delivering modern IT. For 2024, the questions are not around whether to utilize cloud-based services, nor which cloud-services to utilize. Instead, organizations are asking themselves how many clouds are necessary — and wondering how their IT teams will manage all their clouds, while ensuring cyber security prevention, data protection and other critical IT controls.

To offer answers to those questions, this research brief curates three independent research sources that were surveyed between Aug 2022 and March 2023, including:

- **Cloud Protection Trends for 2023**
  Surveying 1,700 IaaS, PaaS and SaaS administrators on their data protection strategies.
- **2023 Data Protection Trends Report**
  Surveying 4,200 IT leaders responsible for their organization's data protection strategies.
- **2023 Ransomware Trends Report**
  Surveying 1,200 CISO/SecPro/Backup professionals whose organizations experienced a cyberattack in 2022.

All three research endeavors were conducted by independent research or analyst bureaus from their unbiased panels, with the data then being acquired and published in various forms by Veeam®. In this report, four key areas are consistently revealed:

- Cloud-based services are key to protecting datacenters and cloud-hosted workloads.
- Clouds are just as susceptible to ransomware attacks, maybe more.
- Using one cloud to protect another is a good idea; using the same cloud to protect itself is not.
- The security, DR, cloud and on-prem teams are not aligned; fix that first!

Cloud-based services are key to protecting datacenters and cloud-hosted workloads

82%

organizations now utilizing cloud-based storage that is capable of immutability.

Research consistently shows that cloud-based services are an indispensable aspect of protecting traditional on-premises workloads, as well as cloud-hosted workloads. *Most notably, cloud-based storage enables* ***'survivable' repositories*** *(e.g., immutability) as well as* ***disaster recovery infrastructure*** *when you need it.*

For most organizations, there are nearly universal truths in protecting against ransomware:

- To protect datacenter servers, get your data out of the building (e.g. offsite or in a cloud).
- To recover from ransomware, you'll need backup copies that cyber threats can't affect.

Based on the 2023 Ransomware Trends Research, combining the two axioms is apparent in 2023, as a "lesson learned" — with **82%** organizations now utilizing cloud-based storage that is capable of immutability.[1]

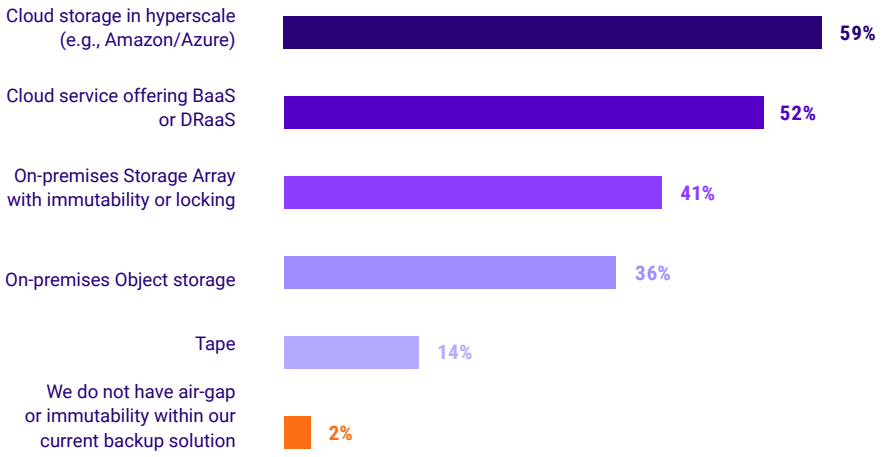


Figure 1.1

Does your organization utilize offline, air-gapped, or immutable backups using the following systems?

After ensuring that the organization has survivable backup copies, then other aspects of a traditional business continuity or disaster recovery (BC/DR) strategy can be considered as well. When considering that cyberattacks are increasingly considered another (albeit special) form of disaster, it is not surprising that many are thinking of cyber resiliency and disaster recovery as highly interrelated. In both cases, the next most pragmatic question is **"Where will you recover or fail over to?"**

As a lessons-learned from cyberattack victims, of orgs' recovery strategies include the capability to recover their datacenter servers to cloud-hosted infrastructure when remediating from ransomware or another crisis.[2]

Figure 1.2

When recovering servers from ransomware, where do you recover your data to?

The data above shows that most organizations have a hybrid strategy that is flexible, based on the scope of crisis. In fact, **71%** of organizations can recover using a cloud, while **81%** can recover using on-premises infrastructure — that's quite a lot of overlap (flexibility). In the broader range of crises that organizations prepare for in their disaster recovery plans, **54%** plan on failing over to an alternate location, while **46% plan on using cloud-hosted infrastructure as their disaster recovery site**. That said, there is more than one way that a cloud-powered disaster recovery site can be accomplished.[3]

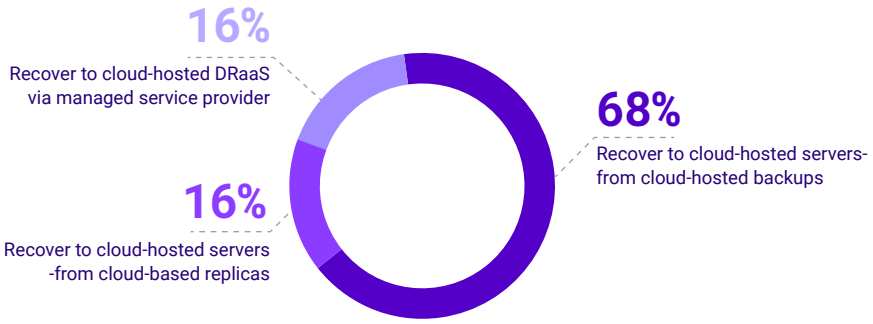


Figure 1.3

When using cloud-services for disaster recovery, how are operations resumed?

Whether your disaster recovery plan utilizes a Disaster Recovery as-a-Service (DRaaS) provider or self-managed cloud-hosted infrastructure, such as Amazon Web Services or Microsoft Azure, there are at last two critical capabilities for success:

- The ability to transform a backup during restoration, such that a production server that was protected while originally physical or virtual — recovered and powered up within a cloud-host.
- The ability to orchestrate the recovery process, including quarantined isolation for malware detection during the restoration workflow.

Unfortunately, only

- **18%** of organizations are able to script orchestrated workflows for failover recovery.[4]
- **44%** utilize an isolated test area or "sandbox" to scan for malware during restoration, as part of ensuring not to re-infect the environment.[5]

These should be hard questions addressable to senior leadership on whether your organization's data protection solution or service can automate recovery at scale and/or ensure safe restoration.