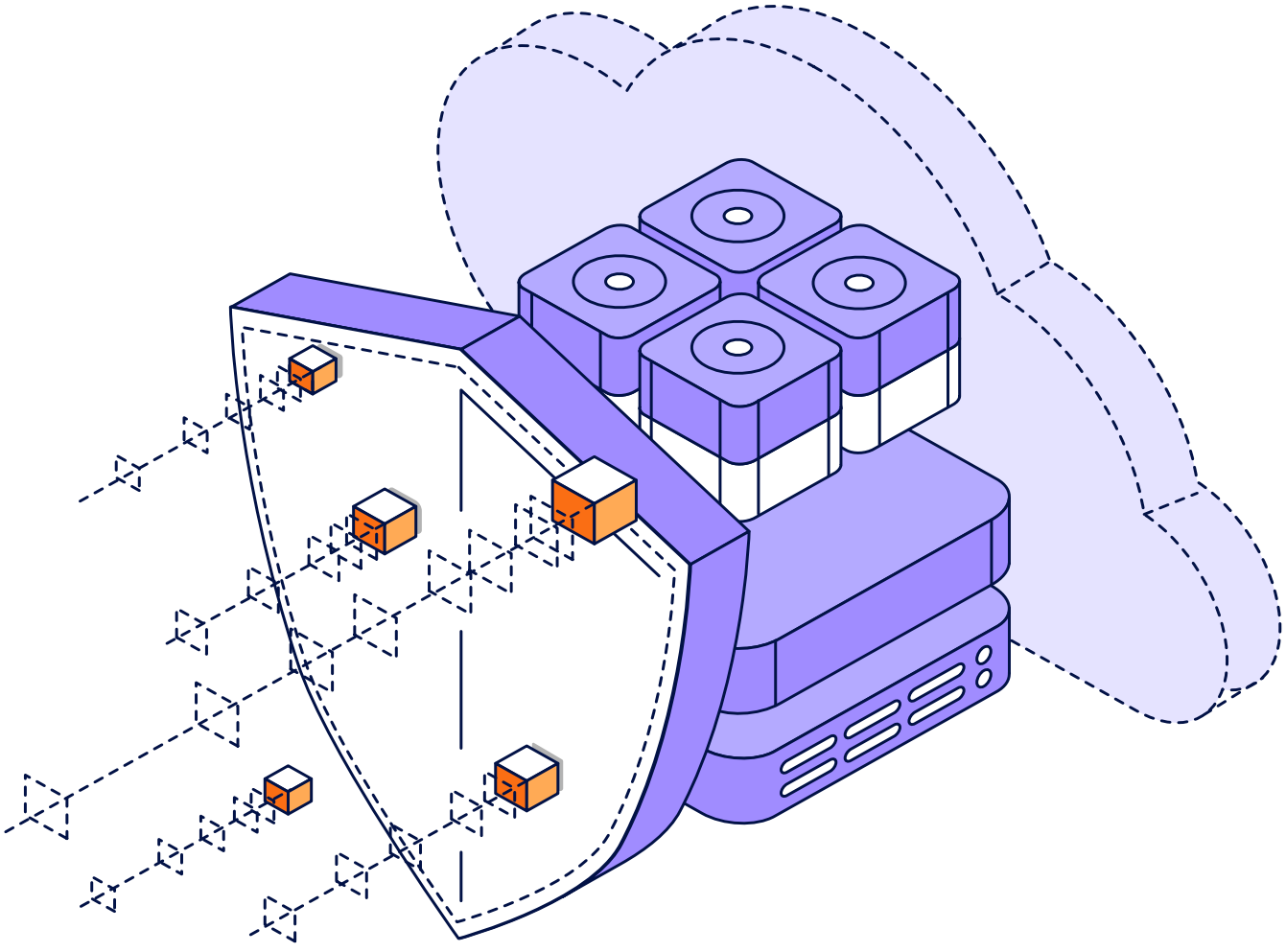
Cyber Resiliency for the Hybrid-Cloud

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

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]

82%

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

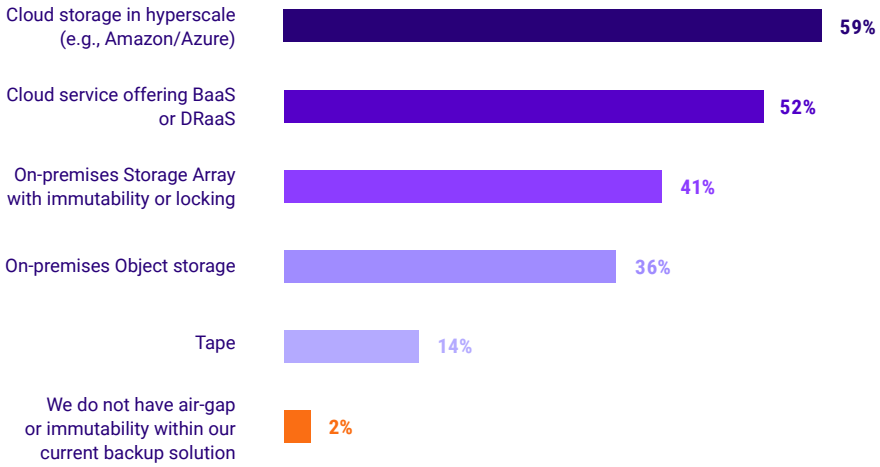


Figure 1.1

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]

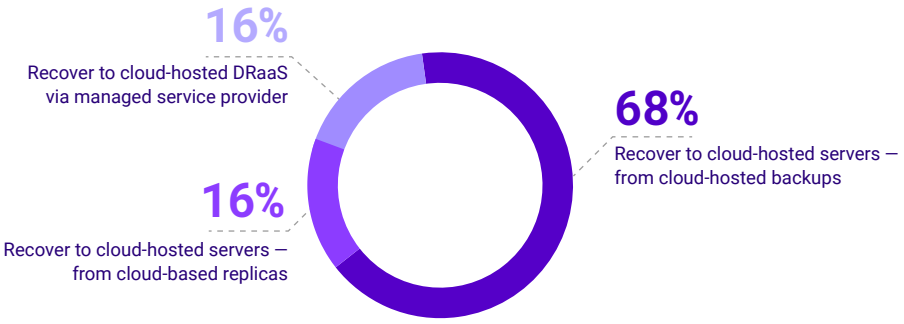


Figure 1.3

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.

Clouds are just as susceptible to ransomware attacks, maybe more

Presumably because cloud-based services are seamlessly accessible within hybrid-IT architectures, the research consistently reveals that **cloud-based workloads are just as likely to become affected during a cyberattack**. *In fact, when considering that many organizations must use different security technologies to prevent access to cloud-services versus their datacenter resources, additional attack opportunities become possible, such as disrupting connectivity between the users and their cloud platforms.*

In much the same way that "the cloud isn't coming, it is here" one must also recognize that IT is not decommissioning on-premises platforms at nearly the same rate as new workloads are starting up within cloud-based services. Organizations continue embracing cloud-hosted infrastructure as part of an increasingly hybrid strategy for delivering IT.

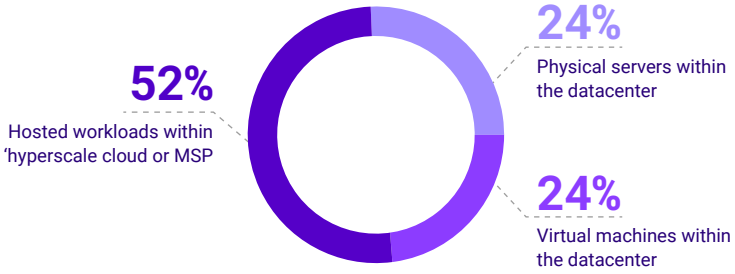


Figure 2.1

Anticipated 'Hybrid' distribution of platforms for production server workloads in 2024.[6]

It should be noted that unlike the evolution of platforms within datacenter-centric IT, there is not just "one cloud" architecture to deploy, utilize and protect: regardless of cloud vendor. Instead, one must consider myriad cloud-architectures, each by a variety of providers whose underlying management frameworks dramatically vary.

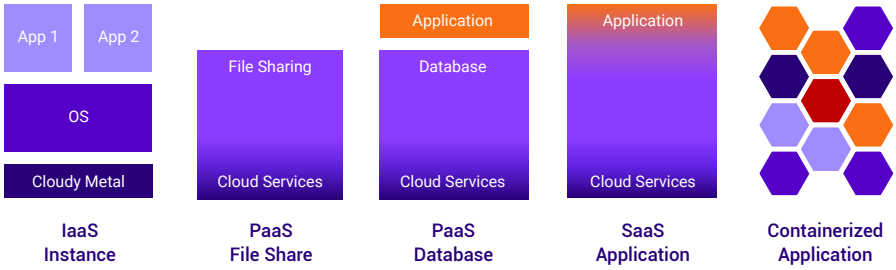


Figure 2.2

Myriad cloud-architectures.

Unfortunately, while cloud-based services are often perceived as resilient, outages still occur — due to issues within the cloud service provider, admin-driven misconfigurations across cloud services and the connectivity between the users and the cloud services themselves. That said, in both the 2021 and 2022 research reports, outages due to cyberattacks increased year-over-year, while remaining the cause of the most impactful outage in both 2021 and 2022 (and no sign of that slowing in 2023).[7]

- **48%** of organizations suffered IT interruptions due to **"Public cloud resources being unavailable".**
- **52%** of organizations suffered IT interruptions due to **"Infrastructure or networking outages".**
- **53%** of orgs suffered IT interruptions due to **"Cybersecurity event".**

In most cyberattacks, while initial entry may be systematically opportunistic (e.g., spamming phishing emails and hoping for one user to click), those same attackers then target systems based on known vulnerabilities or potential failure to adequately secure popular IT platforms. Research from the 2023 Ransomware Trends Report shows that **cyber criminals targeted cloud-hosted workloads in 38% of attacks.**[8]

When 1,200 victims of cyberattacks were asked, a nearly equal amount of cloud-hosted data was encrypted/impacted as the amount of datacenter data.

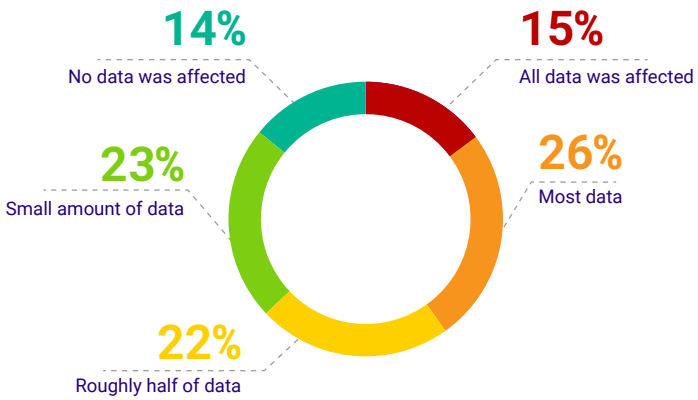


Figure 2.3

% of data hosted on cloud platforms that was affected by the last ransomware attack.[9]

It is important to note that the similarities in infection rates across datacenter data, branch-office/remote data and cloud-hosted data infers two key truths:

- Because hybrid-IT is so seamlessly delivered, once a cyber threat is operating within the victim's environment, the cloud-hosted data is just as vulnerable to attack as the applications and files within the physical data center.
- Because of that seamlessness and equal vulnerability, files, databases and applications that are cloud-hosted must be protected with the same rigor and methodologies as on-premises' workloads.

By 2024, for the first time, it is expected that more workloads will run outside of self-managed physical datacenters than within the raised floors of yesteryear.

Using one cloud to protect another is a good idea; using the same cloud to protect itself is not

2 : 1

majority of data protection being done by the 'traditional' IT backup team compared with the cloud administrators.

When surveyed on 'who' was backing up their clouds' data and 'how' the data is being protected in 2023, all three research projects confirmed that ***the 'core' backup team (or their service provider) that protects the rest of an organization's data on-premises is also most often tasked with protecting cloud-hosted data****. That said, there is still a lot of confusion in the 'how' that is typical when organizations assume that their only option is to use a platform's 'built-in' utility, instea of a heterogenous enterprise backup solution.*

Before considering 'how' organizations are protecting cloud-hosted workload it is notable to consider the various 'who' — with a relatively consistent 2:1 majority of data protection being done by the 'traditional' IT backup team compared with the cloud administrators.

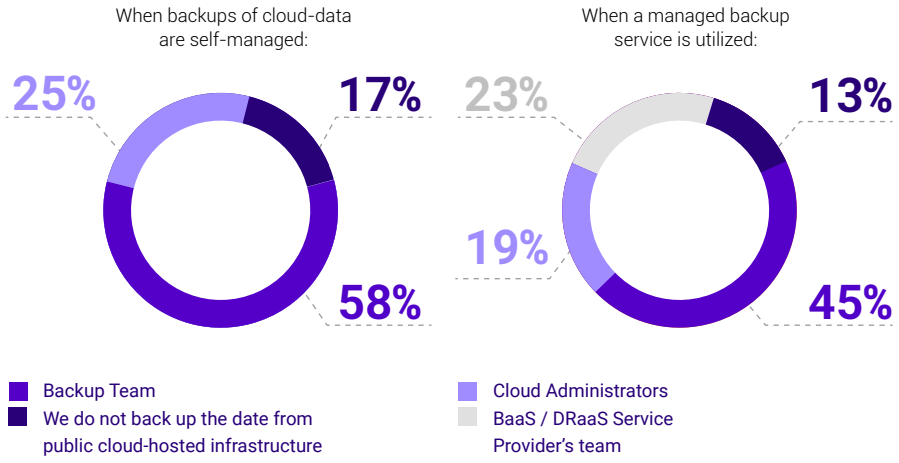


Figure 3.1

Who manages the backups/data protection of cloud-hosted servers in your organization?[10]

Surprisingly, one in eight **(13%)** believe their organizations are not backing up their cloud-hosted infrastructure. After that, the next question for many organizations that are embracing hybrid strategies is the recognition that cloud backups could be within the same cloud, a different region, a different cloud or even back on-premises. This becomes an important consideration when choosing a backup solution for cloud-hosted workloads:

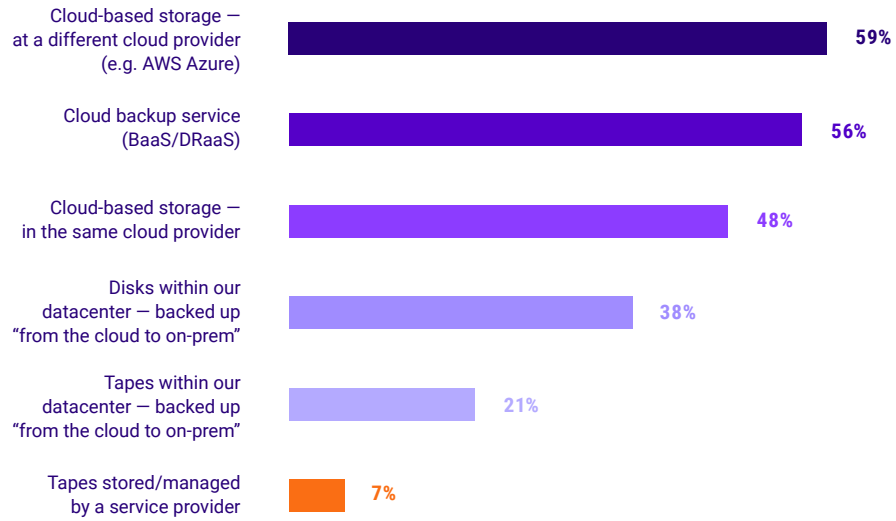


Figure 3.2

For cloud backup data your organization is retaining for one year or longer, where are those backups stored?[11]

- **37%** of IT leaders consider "Ability to move workloads from one cloud to another" as a defining aspect of a 'modern' or 'innovative' data protection solution.[10]
- **88%** of organizations have brought workloads from a cloud back on-premises or moved to another cloud.[11]

Of course, the other option when choosing a backup solution for cloud-hosted workloads is to simply rely on the 'built-in' utility or export function that many cloud companies provide for each particular workload. Often, the limiting factor is simply awareness that third-party tools which comprehensively protect cloud workloads are available.[12]

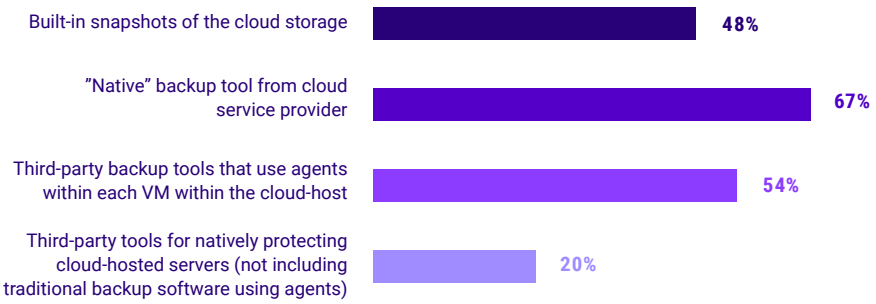


Figure 3.3

Which cloud-hosted data protection mechanisms are you aware of (regardless of whether you use them today)?

If considering snapshots, ask yourself if you would rely strictly on snapshots of your on-premises file servers? Snapshots are powerful recovery tools for near-current recovery points that can be instantaneous. But **snapshots have never been a replacement for backups** because:

- Same silo of exposure (relate standalone NAS to an IaaS storage stack, including common credentials).
- Expensive to retain over time; hence why most organizations retain a few days of snapshots but weeks, months and years of backups.

If considering 'native' workload-centric or built-in utilities, ask yourself if your on-premises platforms are protected by:

- Relying only on ZDLRA (or RMAN) for protecting **Oracle** databases.
- Relying only on NT Backup Utility (or System Tool) for backing up **Windows Servers**.
- Relying only on VDPA for backing up **VMware** hosts.
- Relying only on ASB for backing up **Microsoft 365**.

Now ask yourself, how many tools does your IT team for backup want to manage and how much storage budget do you have (since each of those tools write in differing repositories and formats). Snapshotting and other single-platform utilities (e.g., "built-in") are even more problematic when considering that most are designed with a limited retention range to enable quick rollbacks due to a recent error — such as data overwrite or bad import. When considering how the organization will recover from ransomware that may have been dormant for weeks, these tactical approaches seem insufficient (or cost-prohibitive). These sentiments are quantified in two additional data points:

- **35%** of IT leaders consider **"Standardized protection of on-premises and IaaS/SaaS"** as a defining aspect of a 'modern' or 'innovative' data protection solution.[13]
- **42%** of organizations believe that **"Ability to protect cloud-hosted workloads"** is a must-have attribute for enterprise data protection solutions.[14] That sentiment was both the most common and most important response for 2023.

35%

of IT leaders consider "Standardized protection of on-premises and IaaS/SaaS" as a defining aspect of a 'modern' or 'innovative' data protection solution.

The security, DR, cloud and on-prem teams are not aligned; fix that first!

The three research projects surveyed a variety of personas, including IT leaders responsible for data protection, CISOs and similar executives, security professionals, IaaS/PaaS/SaaS administrators and backup operators. All three research endeavors revealed that no single team owned a core function; there was always overlap in influence and responsibility. And yet, ***rarely did the data show that the respondents believed they were well aligned with each other on either strategy requirements or implementation/usage of technologies.***

While a majority of these research initiatives focus on the technologies used or the reasons/strategies that drive the technology choices, the survey data also reveals a clear and consistent lack of alignment between the personas involved in these endeavors.[15]

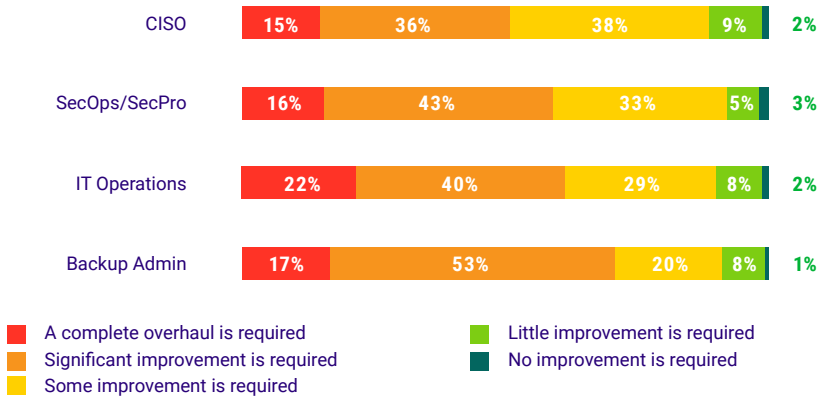


Figure 4.1

How much improvement do you believe is required for your organization's IT Backup team(s) and your Cybersecurity team(s) to be fully aligned?

It is important to note that of the four personas surveyed in the 2023 Ransomware Trends Report, the 'closer' that the professional was to remediating from the event (e.g. Backup Admin vs. CISO), the less satisfied they were with the collaboration and alignment between the teams.

Similar misalignments were seen between SaaS admins & backup admins when considering rationale and tools for Microsoft 365 protection — and again between IaaS/PaaS admins and backup admins when considering the strategies and tools for protecting cloud-hosted servers, file shares and databases.

Questions to consider!

Based on the research encompassing over 7,000 respondents over an eight-month window, a few key questions to consider within your cyber-resiliency strategy include.

- Are our backups both immutable and off-site? Are the backups managed by an experienced provider or are we managing our own?
- Could we use cloud infrastructure as our disaster recovery site? If not, why not?
- Are we backing up all of our cloud-hosted data, including IaaS, PaaS and SaaS workloads? If so, are we using separate tools per cloud or deployed consistently across our clouds (and on-premises workloads)?
- How aligned are our teams related to backing up on-premises, IaaS, PaaS and SaaS?
- How aligned are our teams between cyber-preparedness and data backup?
- When was the last time we tested recovering our cloud-based data?
- When was the last time we tested a datacenter recovery at-scale?
- When was the last time we assessed and updated our cyber and BC/DR playbooks?

If you have questions about the research or its implications, please contact StrategicResearch@veeam.com

To read the complete research reports that were cited here, check out the links below:

- **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.

The Veeam perspective

Veeam's Backup and Data Management Platform

Now more than ever, it's critical for businesses to remain confident their data is protected and always available, whether it's on premises, at the edge or in the cloud. Veeam provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Our customers are confident their apps and data are protected from ransomware, disaster and harmful actors, and are always available with the most simple, flexible, reliable and powerful platform in the industry.

Veeam gives clients the confidence to accelerate Digital Transformation, protect against cybercrime and drive business resiliency, ensuring that your data is always protected and always available. Reduce cost and complexity, and achieve your business objectives with Veeam: the #1 Backup and Recovery.

To learn more, visit **https://www.veeam.com**.

To meet with a Veeam hybrid cloud expert, request a consultation **http://vee.am/hybridcloudinquiry**.

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

1 2023 Ransomware Trends Report, Q29
2 2023 Ransomware Trends Report, Q25
3 2023 Data Protection Trends Report, Q45
4 2023 Data Protection Trends Report, Q46
5 2023 Ransomware Trends Report, Q21
6 2023 Data Protection Trends Report, Q2
7 2023 Data Protection Trends Report, Q13 and Q14
8 2023 Ransomware Trends Report, Q9
9 2023 Ransomware Trends Report, Q6
10 2023 Data Protection Trends, Q17
11 Cloud Protection Trends for 2023, Q4
12 2023 Data Protection Trends, Q35
13 2023 Data Protection Trends, Q17
14 Cloud Protection Trends for 2023, Q4
15 2023 Ransomware Trends Report, Q1