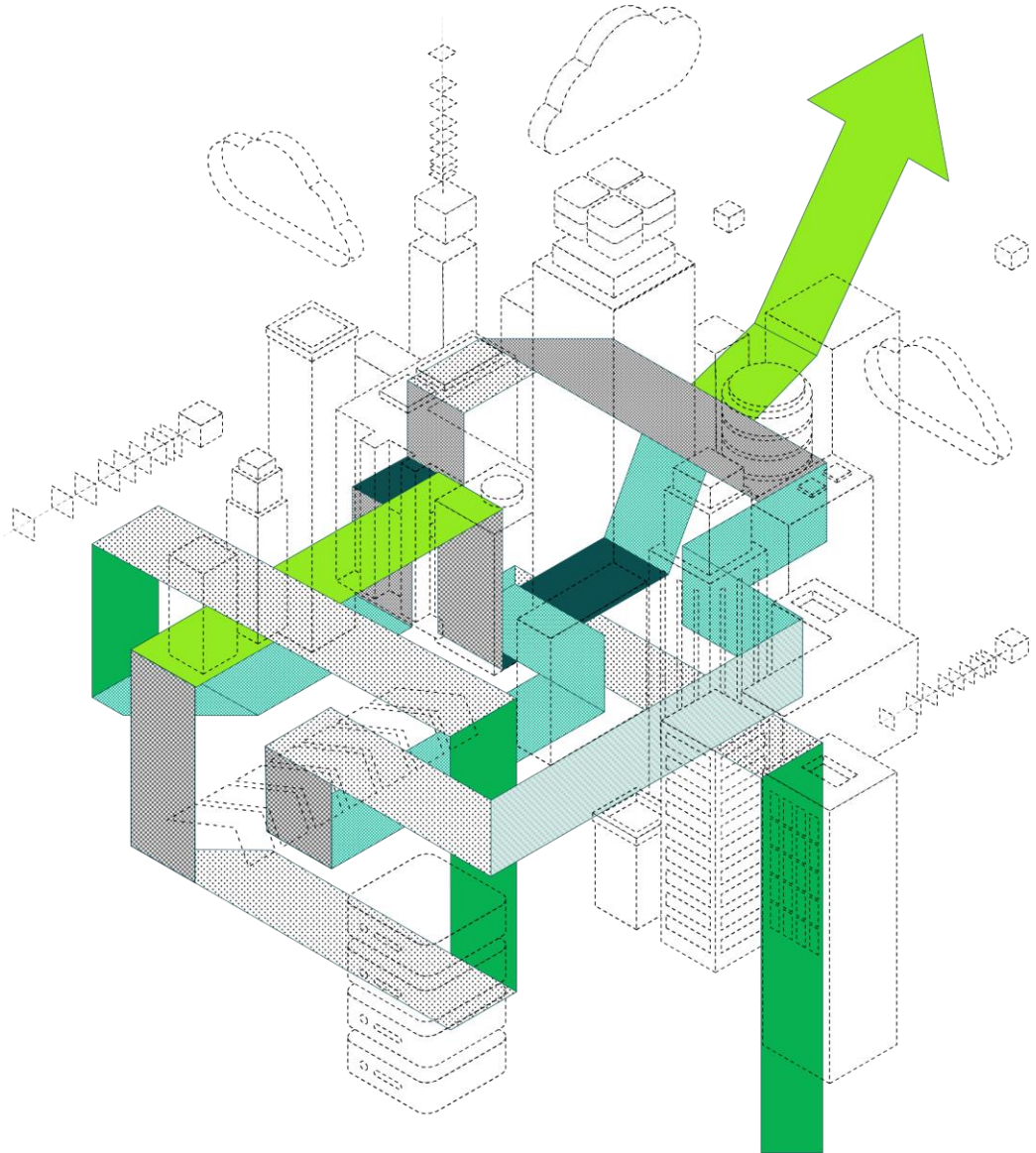
VEEAM

2021 Cloud Protection Trends Report



Introduction

"WHEN YOU MODERNIZE PRODUCTION, YOU MUST MODERNIZE PROTECTION"

@JBuff

One of the most transformational modernizations of "production" IT is the utilization of cloud-based services in lieu of, or in supplement to, traditional servers within data centers.

This research report summarizes a recent global survey of 1,550 unbiased organizations across 14 countries to understand their approaches toward cloud-based production IT today – and the ramifications for their data protection strategies moving forward. This includes how they expect to be prepared for the myriad of IT challenges they face, including hybrid cloud solutions, disaster recovery initiatives, as well as SaaS and container usage.

This report is presented in four sections:

1 | The realities of hybrid cloud

2 | Disaster recovery to cloud-hosted infrastructure

3 | SaaS-based applications such as Microsoft (Office) 365

4 | Containers

About the research

An independent research firm was commissioned by Veeam to survey 1,550 unbiased IT decision makers respondents responsible for IaaS, SaaS, PaaS, and backup in the AsiaPac, Europe, North America and South America regions, to assess the challenges, drivers and backup considerations among IaaS, PaaS and SaaS personas

This was conducted to better understand the market landscape of adoption trends, drivers, challenges, and protection strategies for cloud-powered production IT in 2021.

The Veeam perspective

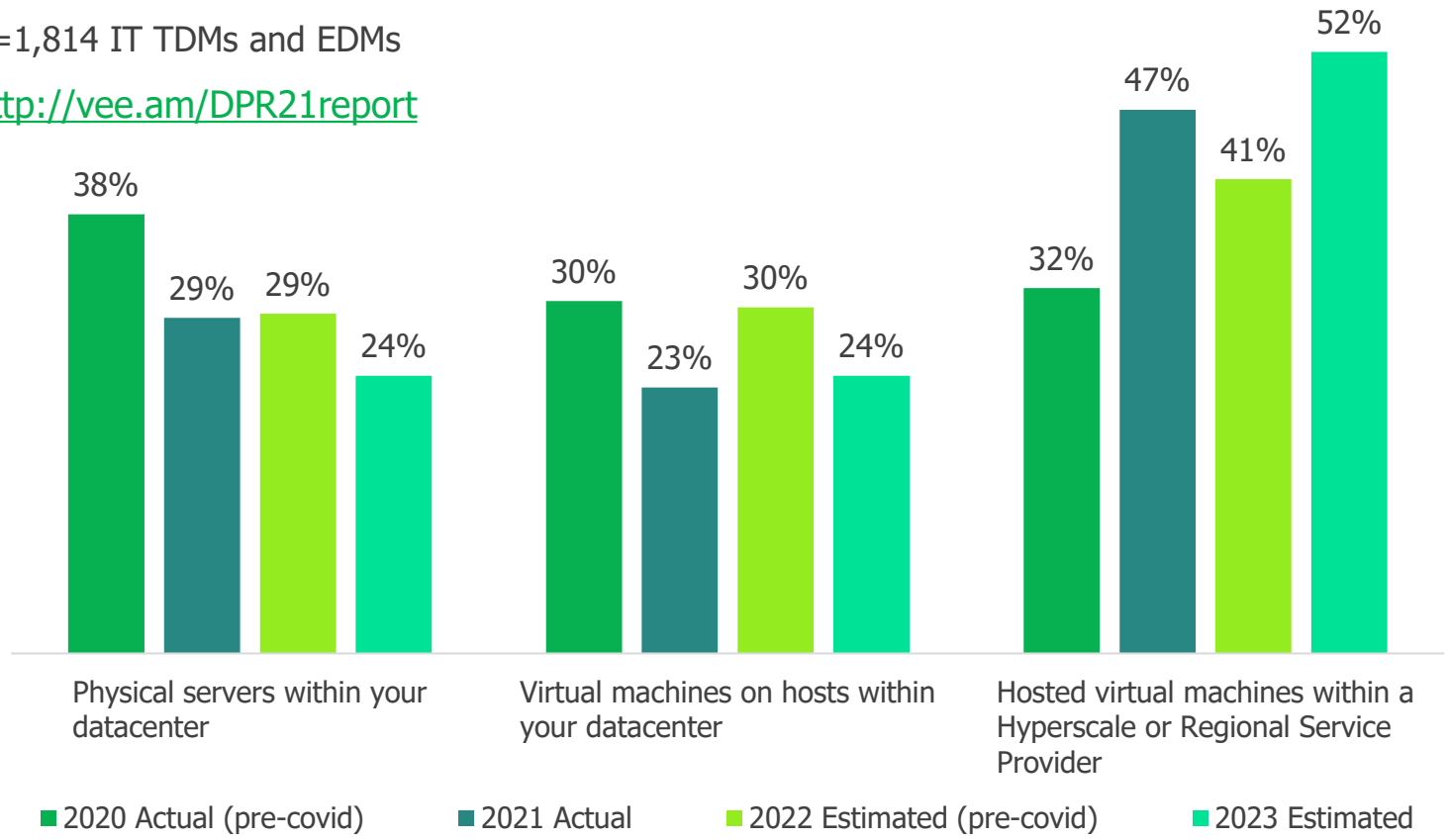
While the majority of this report is based on unbiased research from an independent firm, this section is included as Veeam's commentary, mention of applicable capabilities or offerings, etc.

Hybrid is here

Approximately what percentage of your organization's production data is protected by each of the following mechanisms? Thinking ahead two years, which of the following do you anticipate being your organization's primary method of backing up data?

n=1,814 IT TDMs and EDMs

http://vee.am/DPR21report



For the past few years, Veeam has sponsored an independent research firm to conduct what is believed to be the largest data protection report in our industry. Looking at the year-over-year trajectory of hybrid IT:

- **Physical servers** (left) are expected to gradually decline within one's overall IT infrastructure
- **Virtual servers** (middle) are anticipated to remain "flat" – 30% from 2020 to 2022… or 23/24% from 2021 to 2023
- **Cloud-hosted servers** (right) are expected to grow to nearly half of all servers by 2023

As COVID accelerated IT modernization, organizations accelerated their usage of multiple cloud-hosted IT delivery models, including:

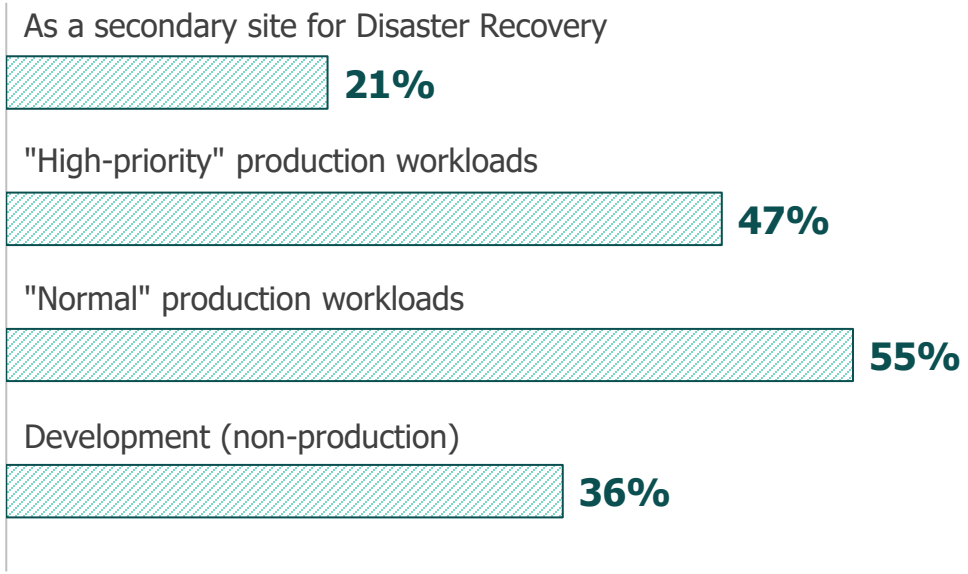
- **IaaS for Production** – running servers within managed service providers or hyperscale clouds.
- **IaaS for Disaster Recovery** – leveraging that cloud infrastructure as a secondary "site" for BC/DR
- **Software-as-a-Service** – running applications directly as a cloud service, e.g. Office 365
- **Containers** – running "native" serverless applications and frameworks, e.g. Kubernetes

One key point = Regardless of how your data is hosted in a cloud, it is still your data.

Realities of hybrid cloud

FIG 1.1
For which use cases does your organization use a cloud-hosted infrastructure?

n=1,553

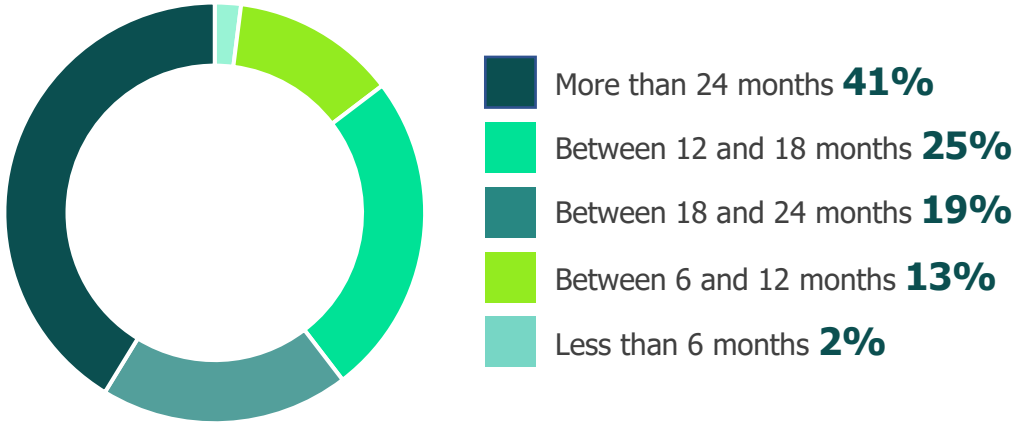


Reality # 1: The IT world is undeniably hybrid and not in "transition" before the data center goes away. There will be a mix of physical, virtual, and hosted for the foreseeable extended future – so organizations will need to continue managing this hybrid state for their data protection.

Reality # 2: The cloud is not "new" for most organizations; over 40% of all respondents have been using production services in the cloud for more than 24 months.

FIG 1.2
How long have you been using the public cloud in production?

n=846



The Veeam perspective

Data is moving and IT platforms are changing. Physical to virtual to cloud to containers, this evolution shows that data lives in multiple places, so organizations need the flexibility to protect their data regardless of physical location, hypervisor or application. Protecting, recovering and managing that data is where Veeam can help.

FIG 1.3
Of the production workloads brought online within a cloud in the last year, where did they originate?

n=850

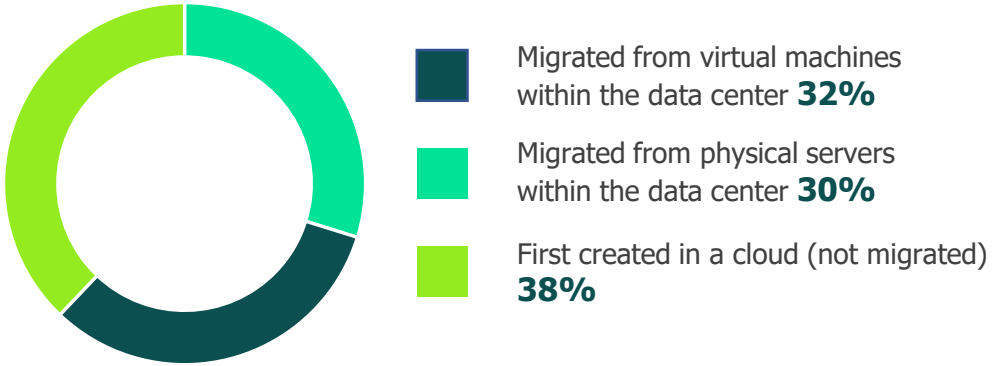
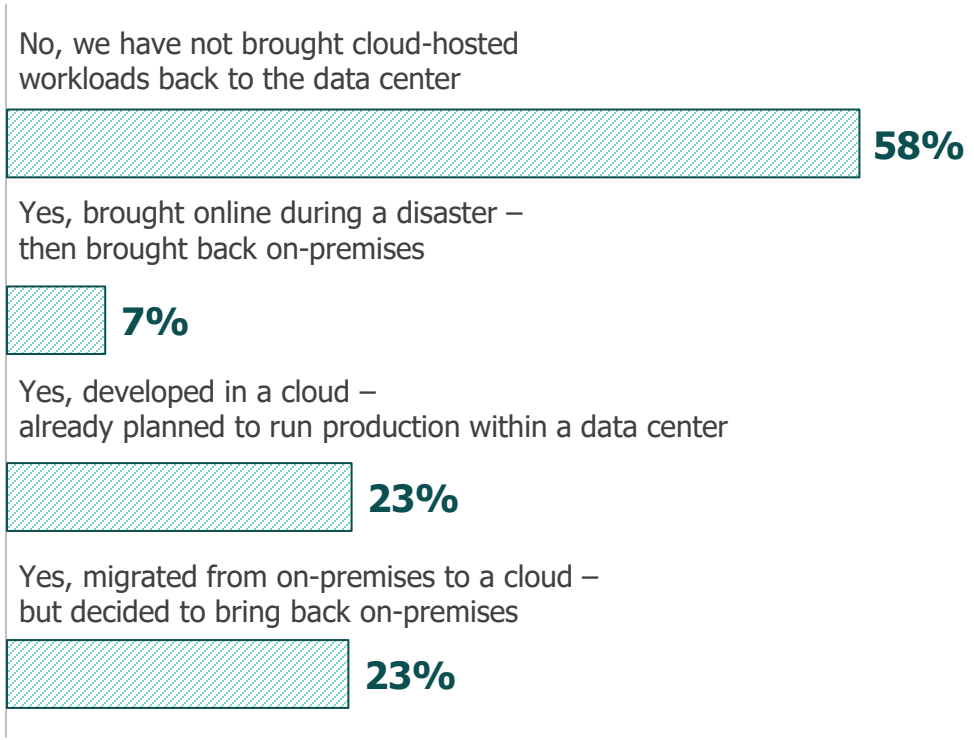


FIG 1.4
Have you brought any workloads BACK from a public cloud host to on-premises?

n=945



To the cloud & back again

Increased use of cloud does not necessarily mean the decline of the data center; it means the *dilution* of physical/virtual servers as organizations *add* cloud-hosted servers to their environment.

Only 3 of 5 cloud-hosted servers were migrated *from* the data center – the other 38% were first created in the cloud; validating the "cloud first" strategy that many orgs are running under. It is also notable that "On-prem to cloud" is not always a one-way path. While 58% of organizations have not brought any workloads back on premises, 2 in 5 orgs have for one or more purposes.

So, while hybrid cloud is growing, it is not accelerating at the expense of the modern data center – it is in addition to.

The Veeam perspective

Irrespective of where a workload might live today (or in the future), it always needs protection – even when in the public cloud.

Veeam Platform is the most complete data protection solution for all data — on-premises and cloud-hosted. Veeam is designed to accelerate business agility by providing a single platform for cloud, virtual, physical, SaaS and Kubernetes data management and protection that extends beyond "just" backup.

FIG 1.5
Which team(s) within your organization are involved in determining your data protection strategy and requirements for public cloud resources?

n=945 IaaS Admins
n=332 Backup Admins

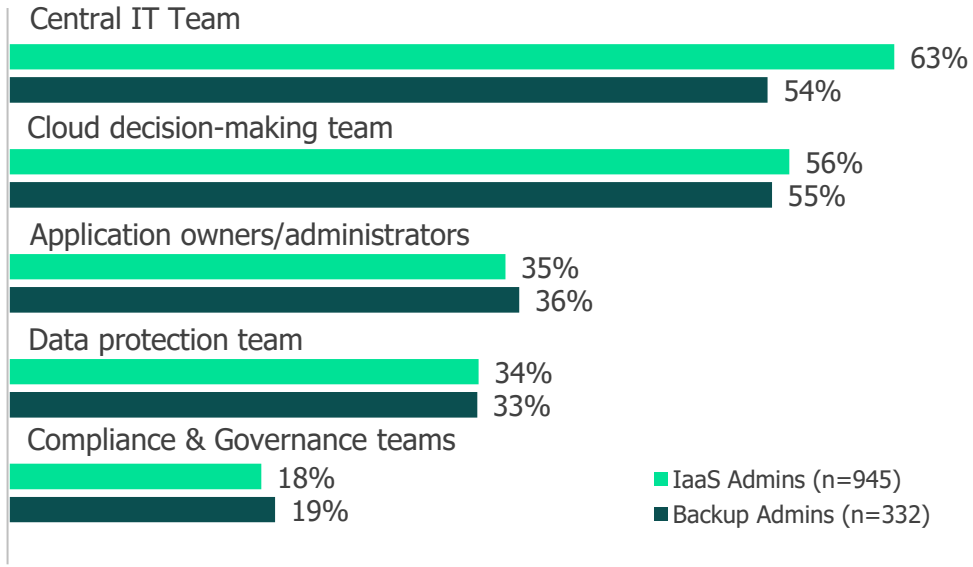
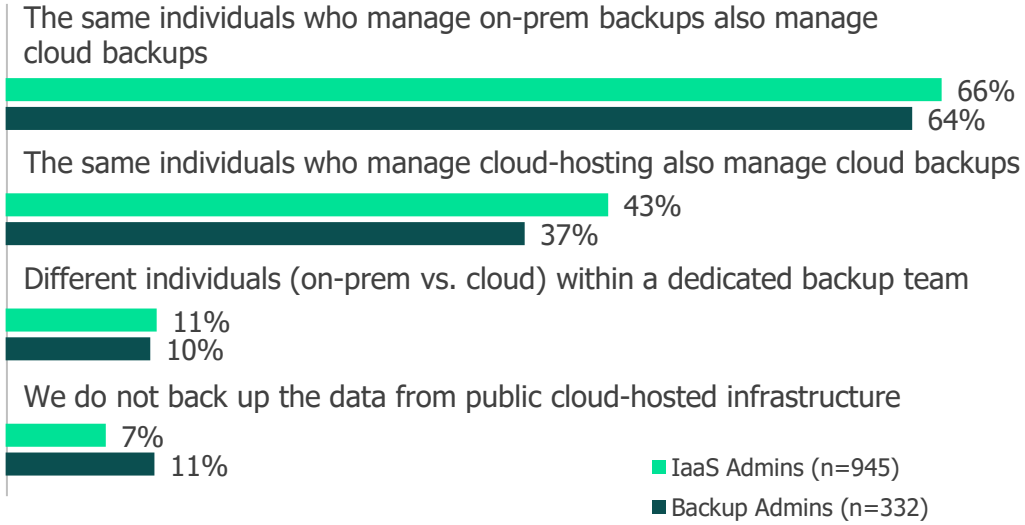


FIG 1.6
In general, who manages the backups/data protection of public cloud-hosted resources?

n=945 IaaS Admins
n=332 Backup Admins



Who is backing up the cloud?

Traditionally, the responsibility for backup has fallen to the data protection team under central IT; however, the cloud approach is changing this.

New stakeholders (LOB owners, DevOps, and Compliance) are now leaning in on core data protection decisions. This makes complete sense as traditional IT solution stacks evolve toward PaaS (microservices and containers) and SaaS; the owners of the investments into those services are now taking a vested interest in backup and recovery capability.

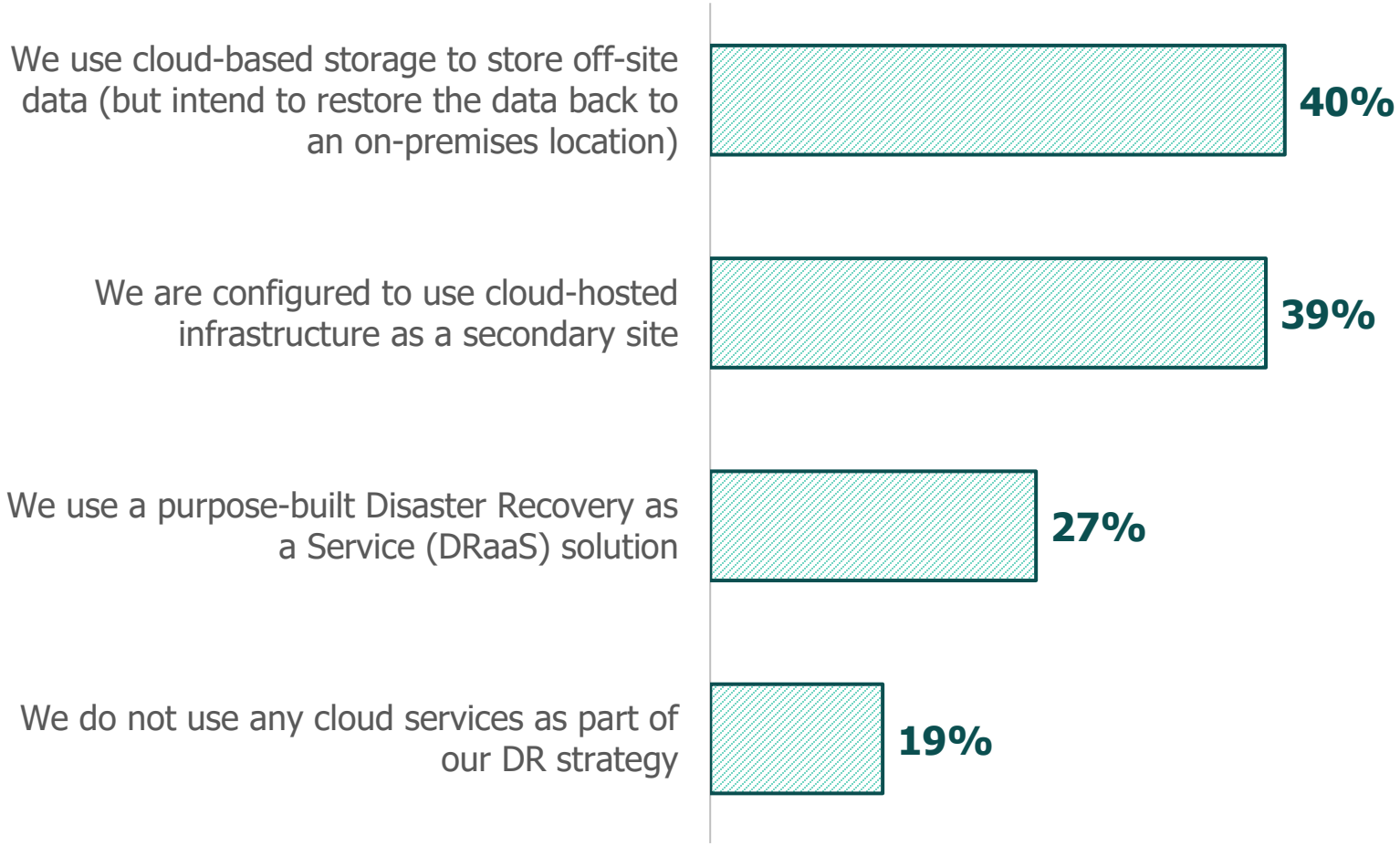
The Veeam perspective

Veeam's modular approach to cloud-native backup and recovery provides purpose-built backup and recovery available as:

- A single platform for centralized multi-cloud data protection, management and cloud mobility and cloud-hosted workloads
- A standalone solution for AWS, Azure and Google Cloud for cost-effective backup and recovery within each cloud

FIG 2.1
How do cloud services contribute to your disaster recovery (DR) strategy?

n=1,277



Cloud-based DR

For many organizations, backup storage and/or secondary infrastructure for disaster recovery (DR) are their first endeavors in cloud services, often in evolutionary phases:

- Start with survivable data (via backup or replication) to an off-site location
- Then, typically a self-managed cloud infrastructure in lieu of secondary data centers to be reconstituted during crises
- Finally, leveraging purpose-built DR capabilities (e.g. DRaaS) not only for secondary infrastructures, but also orchestrated workflows, BC/DR expertise, best practices, and testing/documentation

FIG 2.2
How are operations resumed for your DR function?

n=1,007

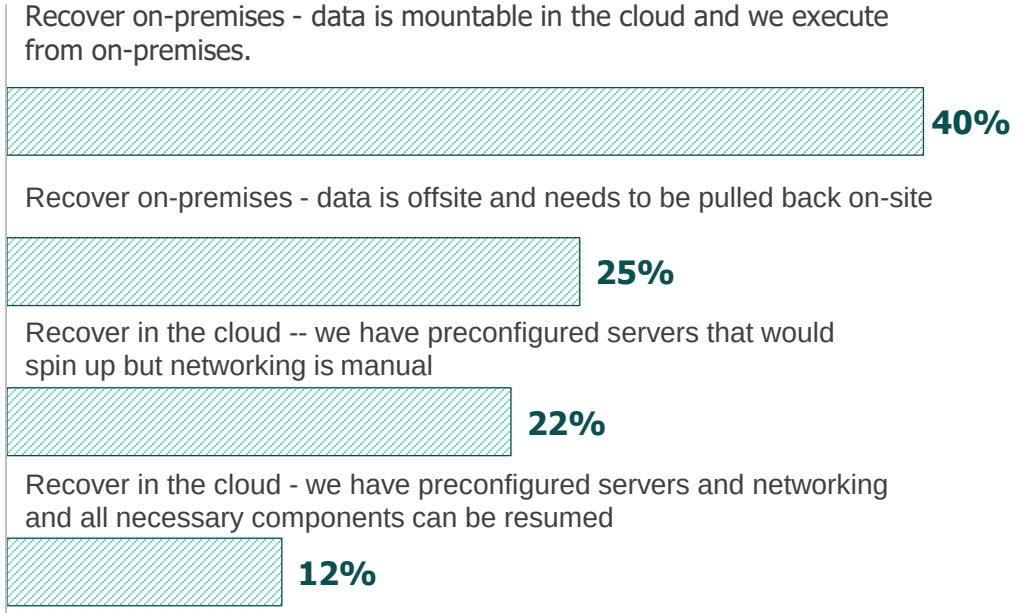
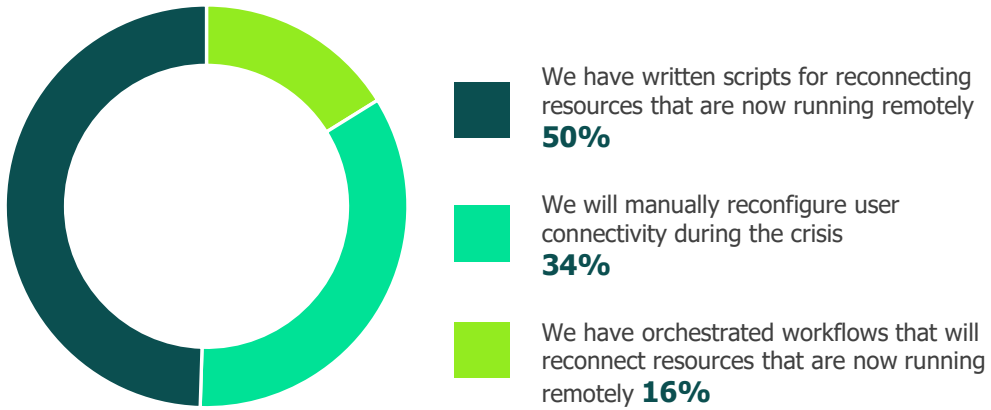


FIG 2.3
What kind of failover/failback mechanisms do you use for resuming functionality?

n=1,007



Cloud-based DR

Even before cloud-based DR, the capabilities to recover after crises of all sizes varies predominantly due to the agile-ness of the secondary data:

Are you "restoring data" or "recovering servers"?
There are reasons for each, but this choice will define your strategy based on your protection capabilities.

Where will the recovery occur?
At the original location, alternate location, or cloud-host; based on how the business process resumption will occur.

How much can you orchestrate?
What capabilities can you pre-script the recovery actions, ideally for consistent testing and for predictable actual recovery.

The Veeam perspective

From an operational standpoint, restoring to the cloud is similar to restoring to a data center hypervisor using Veeam, making it simple for Veeam customers to test and execute cloud-based DR plans.

Veeam partners are service providers are excellent resources to help ensure your cloud infrastructure is ready to receive the workloads ahead of time. Having the proper cloud architecture and ability to readiness verification is crucial to success.

FIG 2.4
What challenges have you experienced in using/testing the public cloud for DR?

n=1,007
Current cloud DR users

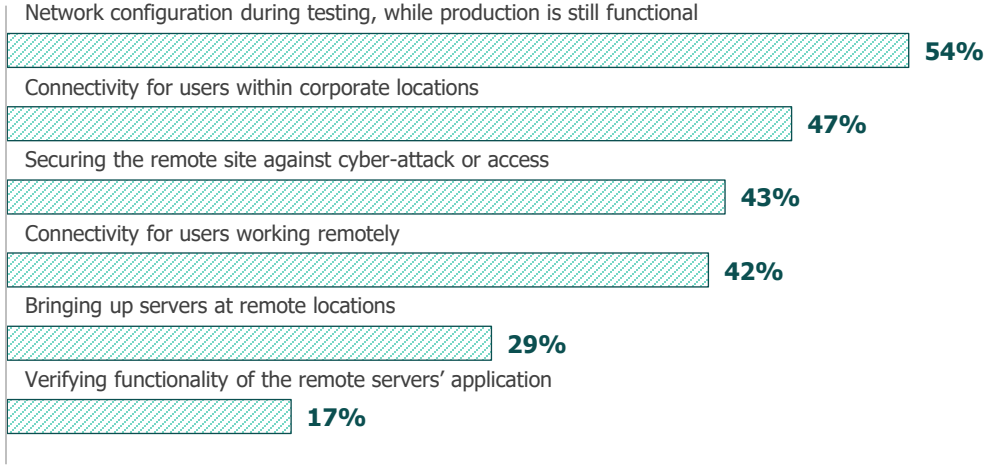
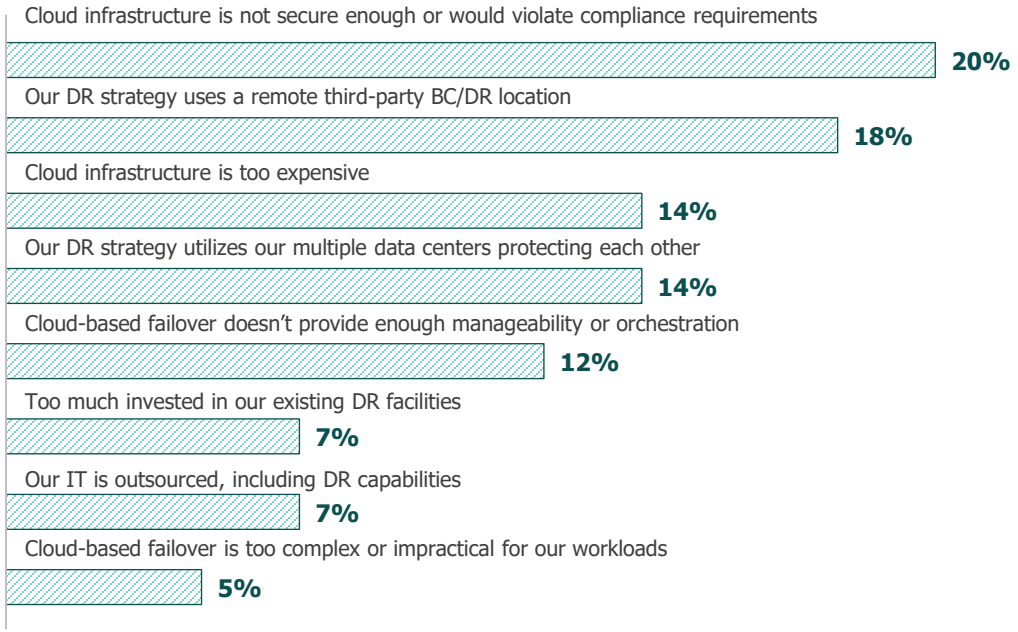


FIG 2.5
You stated that you do not use cloud-hosted infrastructure as part of your DR strategy. Why not?

n=241
IT professionals
NOT using cloud DR



Cloudy DR isn't Easy (yet)

Re-hosting servers that went down in one location and came back online elsewhere is already hard. It can be even more difficult if those servers went down as datacenter servers and came back within a cloud host.

How to reconnect the networks to ensure productive access without exposing a security risk is a key consideration among both current DR users and those not yet leveraging cloud DR, which is even more complicated when the recovery is from less than a whole-site failure, so current users must now access some old and some rehosted servers simultaneously.

This is certainly achievable, but not (yet) easy.

The Veeam perspective

Veeam's portable data format allows for easy, bi-directional data movement from on-prem to cloud 1, cloud 1 to cloud 2, cloud 1 to on-prem, and all combinations.

Data portability and cloud mobility are differentiating concepts and capabilities for the Veeam Platform.

FIG 3.1
Which team(s) within your organization are involved in determining your data protection strategy and requirements for SaaS-based applications?

n=276 SaaS admins
n=332 Backup admins

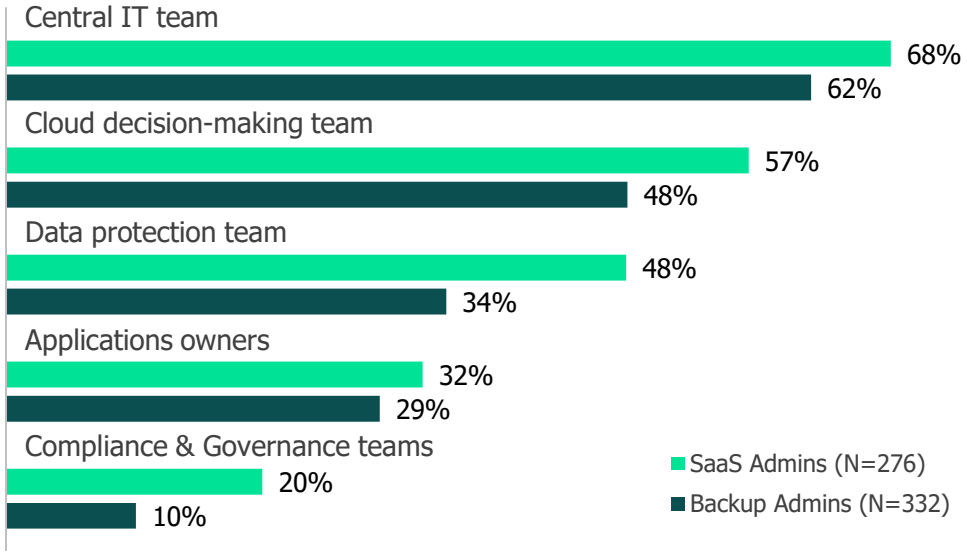
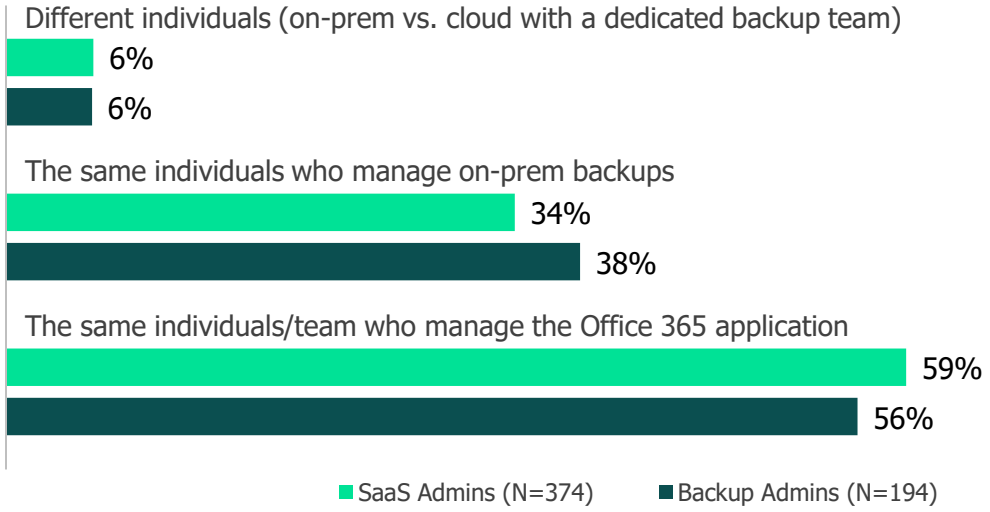


FIG 3.2
Who manages the backups/data protection for Office 365?

n=374 SaaS admins
n=194 Backup admins



Why Back Up Office 365?

Office 365's backup strategy has very similar behavior to what we also saw earlier in cloud backup. As in the previous case, the core IT operations team is defining strategy far more often than the back of admins. That said, who's responsible for backups differs – it is not typically central IT doing backups; it's the SaaS admin.

This makes a lot of sense because the SaaS application requires a different kind of expertise that IT is probably not going to have. Not only backup, but more importantly, restore.

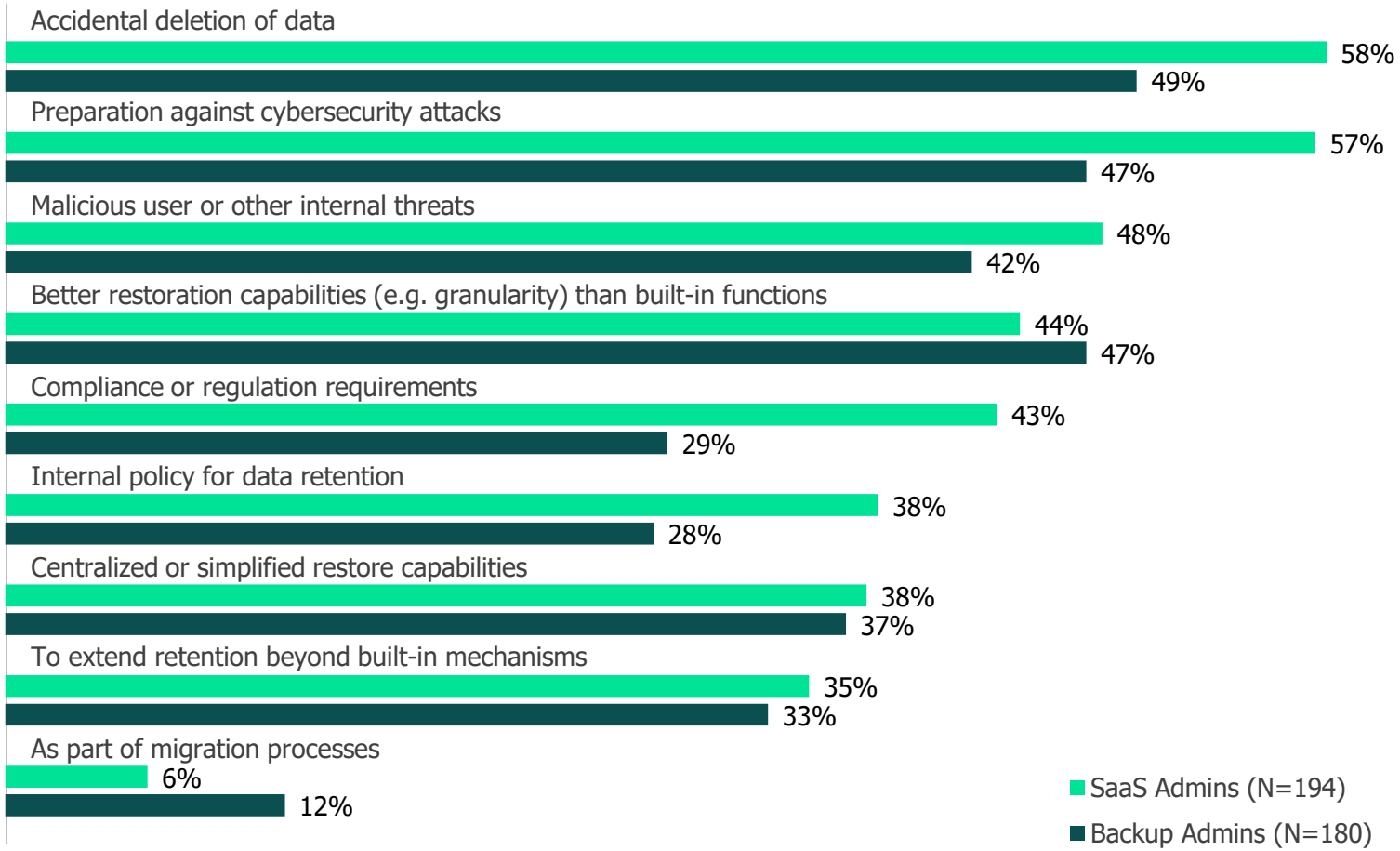
The Veeam perspective

Regardless of the team in charge of the backup, the most important step for these organizations was in first determining that Office 365 data was their responsibility and needed to be protected.

Veeam Backup *for Microsoft Office 365* is a comprehensive solution that is easy to learn and manage. So that even the least experienced IT admin can get up and running, estalishing Office 365 backup jobs and performing restores very quickly.

FIG 3.3
What are your primary reasons for protecting the data from Office 365?

n=194 SaaS admins
n=180 Backup admins



Why Back Up Office 365?

It is an urban myth that SaaS, particularly Office 365 admins, don't believe that their data should be backed up, and that perhaps the recycling bin is "good enough".

The reality is that both SaaS admins and Backup admins agree on the reasons Office 365 still requires traditional backups above and beyond the built-in availability mechanisms. Most notably the actual deletion of data, resiliency versus cyberattacks and malicious threats, and long-term retention and regulatory requirements.

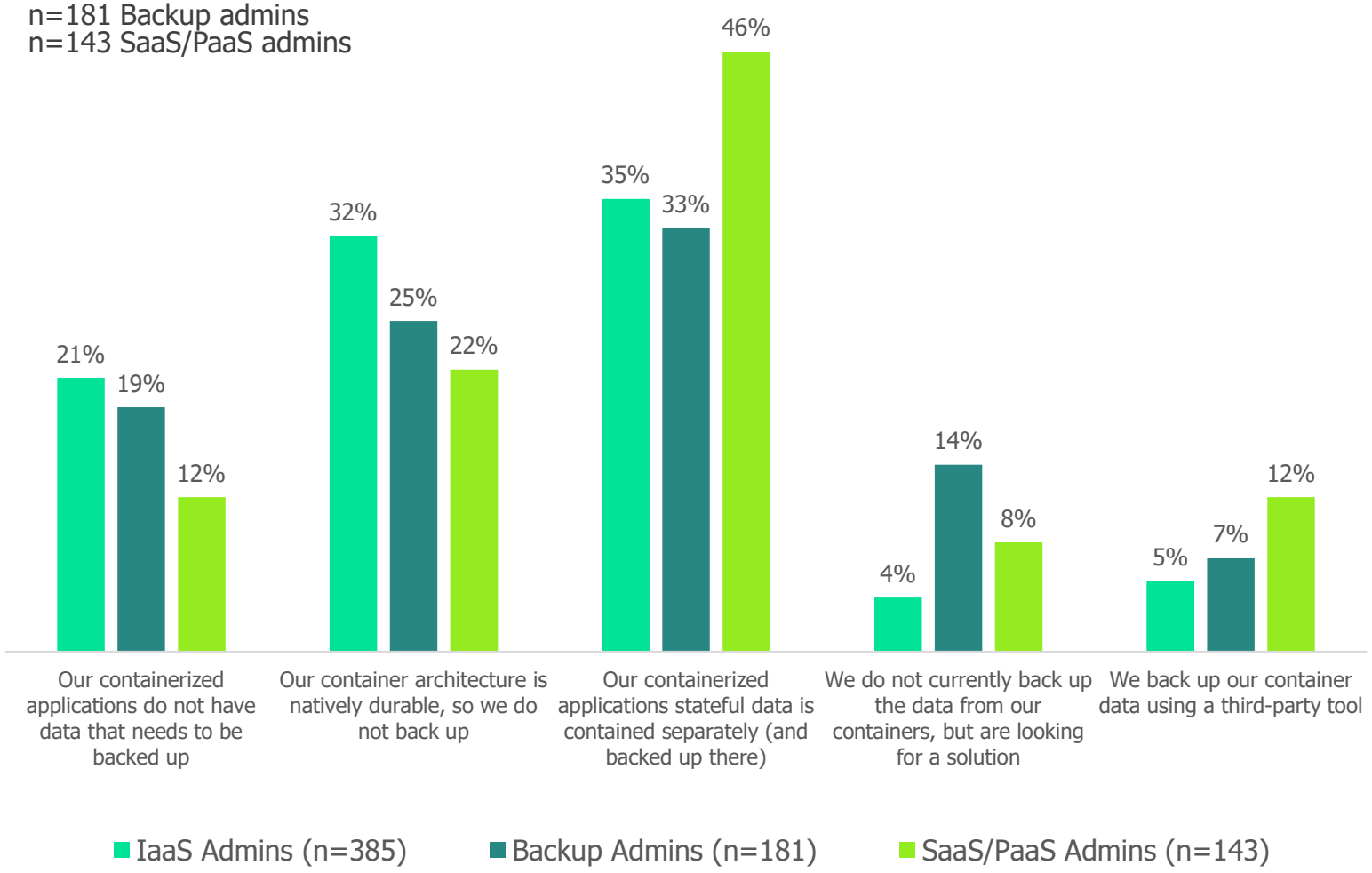
The Veeam perspective

Too many IT professionals still assume that because Office 365 is natively resilient, it doesn't need to be backed up. Others still don't know what to look for in a backup vendor or make the mistake of choosing a vendor that insufficiently protects the myriad applications within Office 365 or doesn't accommodate their recovery needs.

Veeam Backup *for Microsoft Office 365* allows the flexibility to deploy and store data in nearly any cloud or hardware platform, enables customizable protection per application, and helps recover data in whatever way makes the most sense for each organization.

FIG 4.1
How are you backing up data within your containers?

n=385 IaaS admins
n=181 Backup admins
n=143 SaaS/PaaS admins



Containers

Even though the IT roles in charge of deploying, managing and protecting containers (and its data) varies greatly, there is relative consistency between personas as to whether container-based data needed to be backed up, and if so, by what kinds of mechanisms.

As more "stateful" container applications are brought into production, the need to protect the data holistically (meaning native within the container, instead of "just" the storage repository) is likely to grow – and presumably the requirement for third-party native backups.

The Veeam perspective

Kubernetes environments requires an application centric approach vs. infrastructure focus. Unfortunately, regardless of platform, data loss scenarios still take place in Kubernetes which are not addressed by availability/replication – so organizations still need a backup solution that works against a wide range of Kubernetes application stacks and deployment methods.

Kasten K10 has been built to focus on the application, is Kubernetes native, can run in multiple cloud and on-premises clusters, and is data services aware.

Summary

Cloud-based IT is inevitable for almost every organization, though unlike every IT generation before, there is not just one "modern" architecture. In the past, nearly everyone standardized on Midrange, then NetWare, then Windows, then VMware-powered virtualization. This time, there are several "modern" scenarios including IaaS, SaaS, PaaS, and containers – each with various benefits and each with different data protection requirements.

This research shows that while central IT is still most often defining overall data protection strategy, which is especially important for consistency of governance and compliance in retaining data that may be more natively resilient in the cloud but still just as necessary to preserve.

That said, it is easy to see that differing maturations in cloud platforms' adoption are yielding differing understandings of who and how to back up production data in the clouds.

About the Authors

The industry analyses of this data was authored by the following contributors

Jason Buffington
VP, Solutions Strategy
@JBuff

Dave Russell
VP, Enterprise Strategy
@BackupDave

Julie Webb
Director,
Market Research & Analysis

To download additional materials from this research, click **HERE**

For questions on this research or its usage: **StrategicResearch@Veeam.com**

Thank you!

veeam.com