EXECUTIVE BRIEF

Cloud Protection Trends in the Americas 2021

In August 2021, Veeam® published the research findings from an independent analyst survey of 1,550 unbiased IT Decision Makers involved in cloud-powered production IT, including Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS) and/or Containers. 503 of the research respondents were in the Americas. The entire report can be downloaded from vee.am/CPT21report.

One of the most transformative modernizations of "production" IT is the utilization of cloud-based services in lieu of or in supplement to traditional servers within data centers. The Cloud Protection Trends Report for 2021 (CPT21) summarizes a recent global survey of **1,550** unbiased organizations across **14** countries to understand their approaches towards cloud-based production IT today — and the ramifications for their data protection strategies moving forward, including:

- The realities of hybrid cloud
- Disaster recovery to cloud-hosted infrastructure
- SaaS-based applications, such as Microsoft (Office) 365
- Containers

The research findings found that "the cloud" is not new to most organizations; over **40%** of all respondents have been using production services in the cloud for more than 24 months. In fact, organizations in the Americas are more likely to use the cloud as part of their DR strategy and to use cloud-infrastructure as a secondary site compared to the rest of the world. North America in particular is also more likely to use different clouds for protection rather than production. For most organizations, the strategy and the requirements for choosing a protective cloud-based production data are defined by the central IT operations team, but there were significant variations by type of cloud resource regarding the strategies and personas for protecting the data:

- **For cloud-hosted servers** (i.e., Infrastructure as a Service or IaaS), now hosted within hyperscale clouds, the same team responsible for backing up on-premises data center servers are more frequent and responsible for backing up cloud-hosted servers (**65%** of organizations); compared with the cloud administrators.
- **For cloud-hosted applications** (i.e., Software as a Service or SaaS), the SaaS administrators were instead more likely responsible for protecting their SaaS data (e.g., Office 365), instead of core IT or backup administrators.
- **For cloud-hosted containers,** one of the component administrators — e.g., the storage administrators of the underlying storage or the database administrators of the cloud-hosted database — were most likely to protect that aspect of the container framework, but not the rest of the framework.

65%

of cloud-hosted servers brought online in 2020 were "migrated" from the data center — the rest were new workloads.

59%

of organizations stated that their data protection strategy and requirements were defined by their central IT operations team, compared with **35%** by their backup administrators.

58%

of Office 365 environments are backed up by their Office 365 administrators, compared with **36%** by their IT operations or backup administrators.

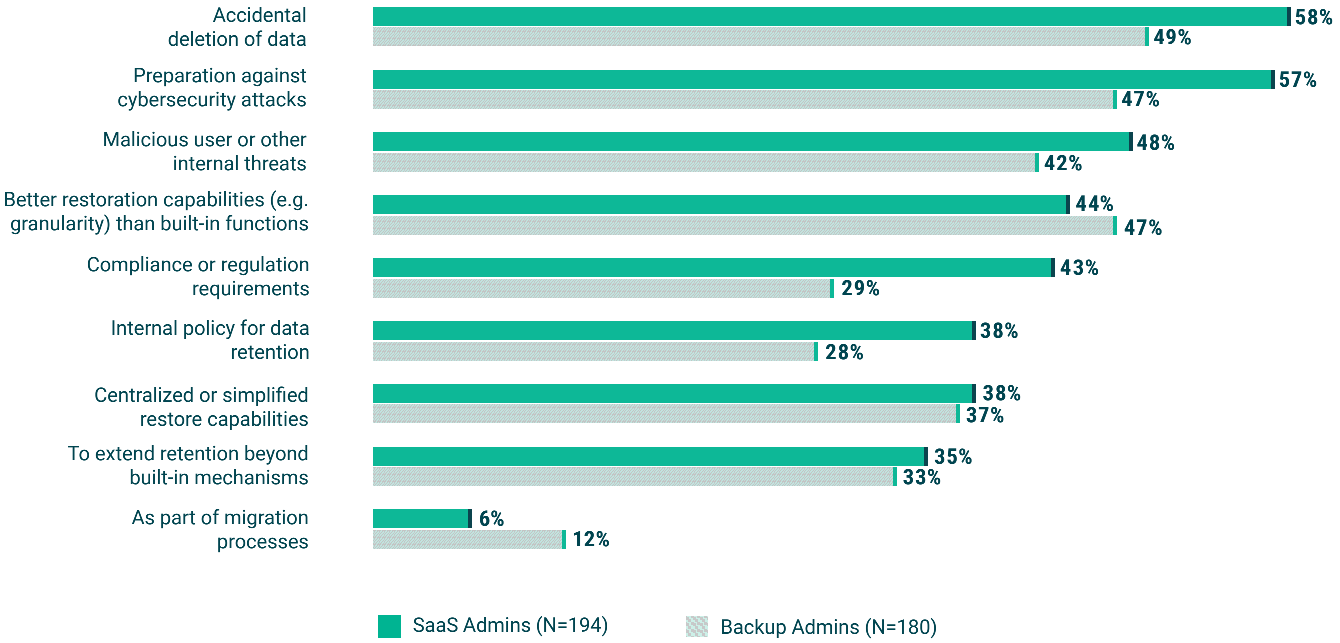
52%

of organizations back up their Office 365 environments as part of their ransomware preparedness strategy.

In a perfect world, this means that the same data retention requirements, often defined by outside regulatory compliance mandates or internal operational policies, would be consistently applied to data on-premises within modern data centers and within the myriad of clouds that production data can now reside within. For many organizations, this has not proven to be the case, neither now in hybrid clouds, nor even in the days past when database administrators would use Oracle RMAN to dump/scrape backup data, while email administrators relied solely on storage snapshots or built-in transactional replication.

One of the more interesting findings in considering the dichotomy of data protection strategy definers (IT operations) and the various application/platform teams is that organizations in the Americas are more likely to have decision makers evenly distributed among influencers and stakeholders. These individuals are responsible for enacting the backups and restores, requiring consistency in understanding why backups are necessary, even with natively resilient cloud architectures.

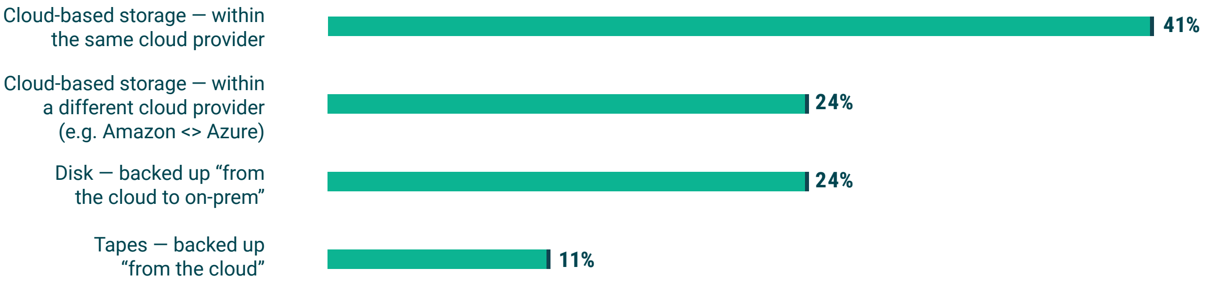
Figure 3.3 What are your primary reasons for protecting the data from Office 365?



From the Cloud Protection Trends report, Figure 3.3 shows alignment and understanding between the SaaS administrators and the backup administrators on why Office 365 data needs to be protected. Of particular importance is the top response by Office 365 administrators to protect against accidental deletion, which one might presume that the built-in recycle bin would address. Similarly, both Office 365 and backup administrators recognize how third-party backup can supplement with built-in restoration capabilities.

Recognizing external threats like ransomware and other cyberattacks, as well as regulatory mandates that require long-term retention (regardless of on-premises or cloud-hosted), is reassuring to see alignment on, since either or both groups will inevitably be involved in enacting the data protection and recovery of this near ubiquitous workload across modern IT. This research project asked similar questions of Containers and PaaS administrators, as well as those responsible for IaaS deployments.

For cloud backup data you are retaining for one year or longer, where do you store those backups?



Other key findings generated from this research, but not published in the report, were an enlightenment of where should long term data be retained from cloud-based production data. Since North American organizations are most likely to pull their data back from the cloud, it is important to understand that, while half of organizations store their long-term data within the same cloud provider as the production data (e.g., Office 365 backed up to Azure), there is notable interest in storing data "across clouds" or "back to on-prem."

This scenario essentially reverses what many organizations do to store long-term copies of data center data in cloud object storage. In this case, by retaining backup copies of cloud production data within the data center, organizations can satisfy distance and separation best practices and even produce tapes for governance or air gap purposes.

The Veeam perspective

While the Cloud Protection Trends Report uses unbiased data and analysis, the report does include Veeam's perspective in boxes like this. When assessing the Executive Summary data and the diversity of roles and methods that can be involved in protecting cloud-hosted data, consider that Veeam has native backup solutions for hosted servers on Amazon, Azure and Google, as well as Veeam Backup *for Office 365* and for Kubernetes via Kasten by Veeam.

Click here to view the complete research Global report

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