VEEAMON 2023

Wait, You're Still Not Protecting **Microsoft 365 Data?**

Edward Watson

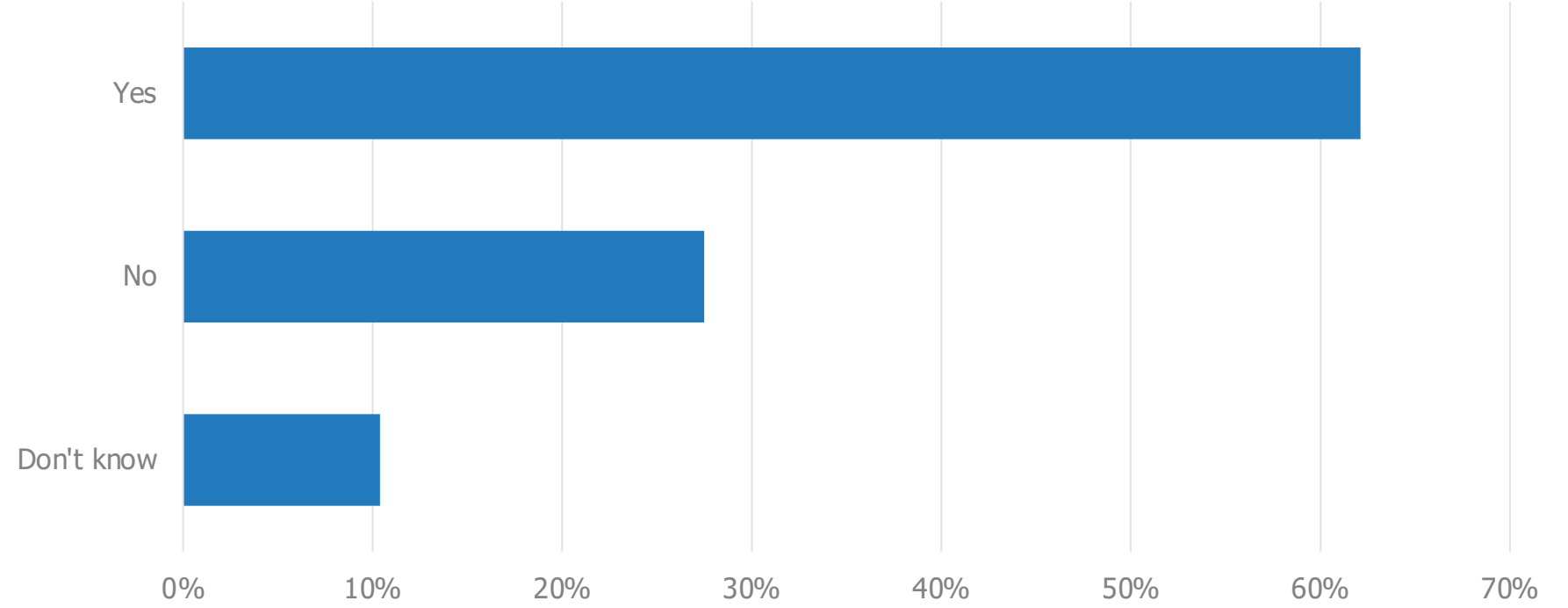
Principal Product Marketing Manager

Archana Venkatraman

Research Director, IDC

Cloud services are becoming primary data environments for digitally mature organizations

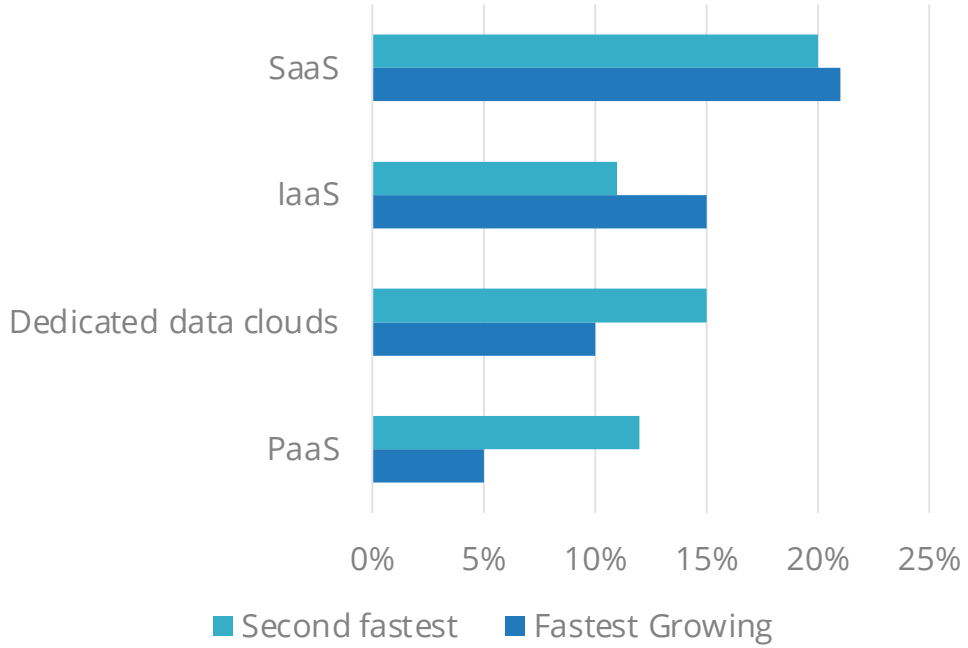
Is more than 50% of critical data in cloud for your organization? Mature cloud users



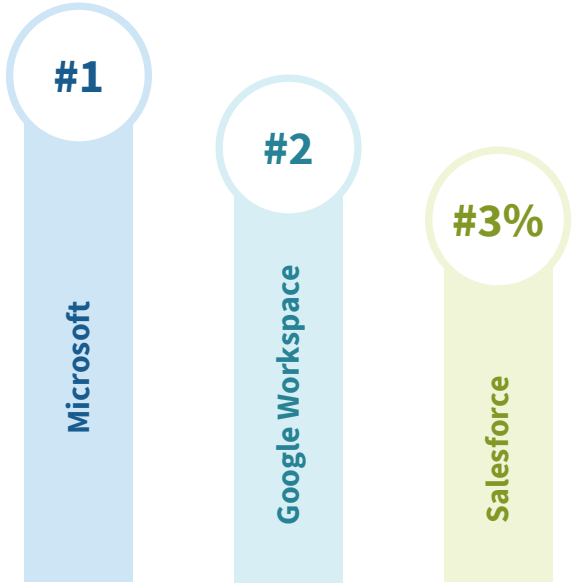
Source: IDC CloudOps Survey, 2023

Data growth in SaaS environments is fastest

Q. In which of these environments would you say is your organization's business data growing fastest?



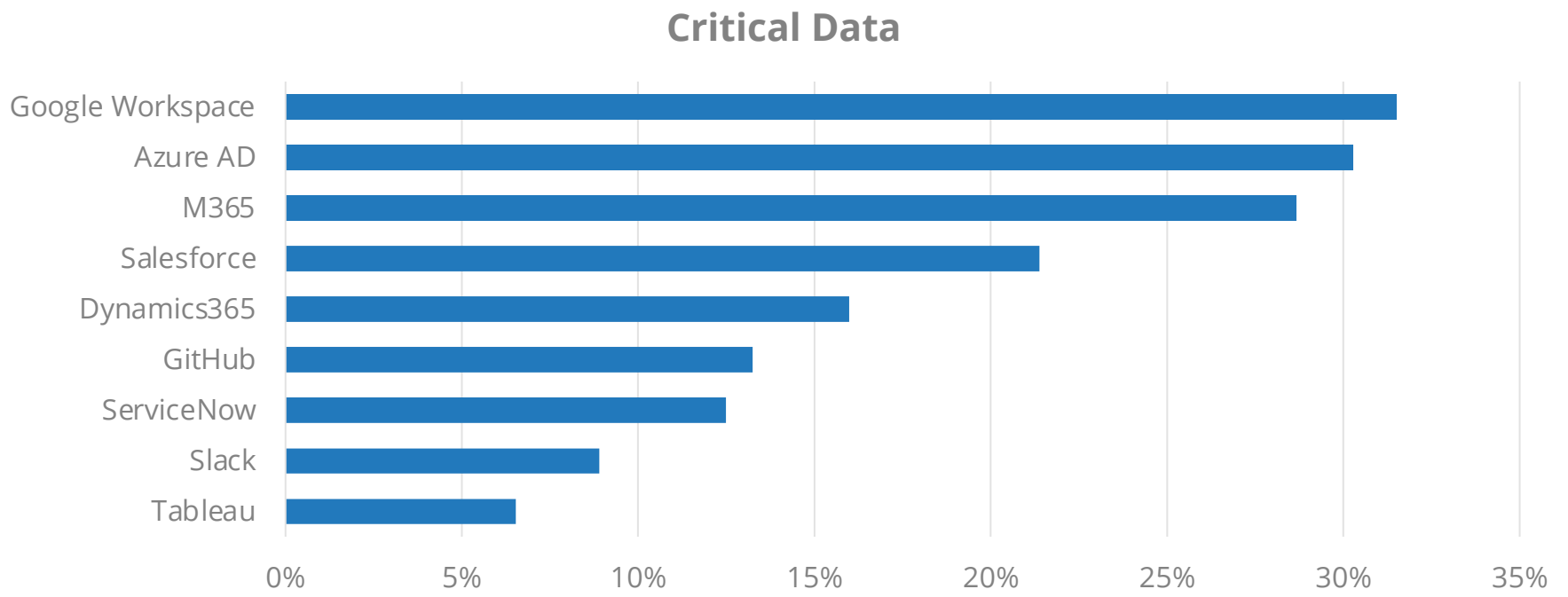
Most strategic SaaS services for your organization



Source: IDC CloudOps Survey, 2023, IDC Multicloud Survey, 2022

Critical data in SaaS environments

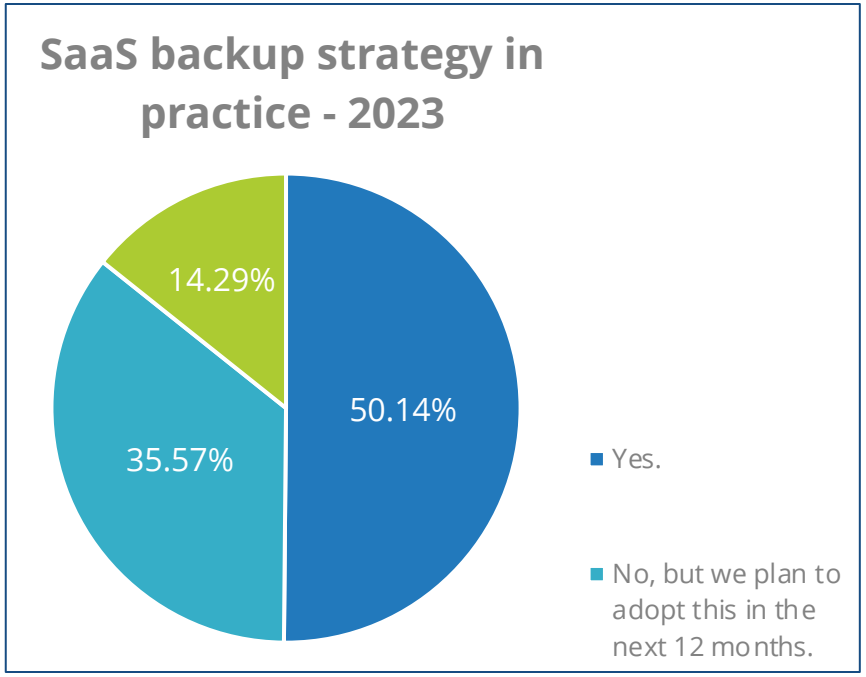
Q. Which of these SaaS environments do you see as home to business-critical data?

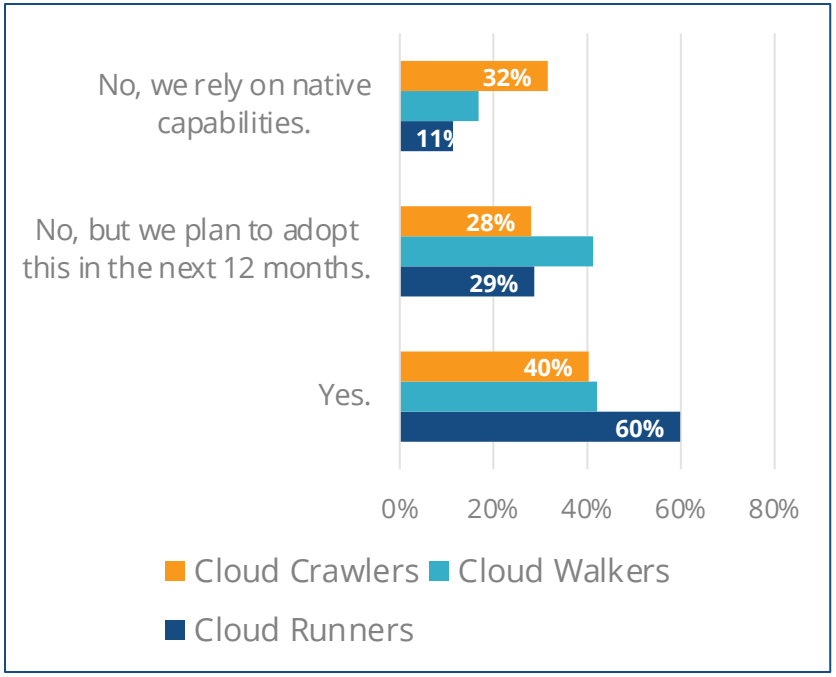


Source: IDC CloudOps Survey, 2023

Dedicated SaaS backup: 86% of organizations have or plan to adopt SaaS backup…do you?

Q. Does your organization have dedicated backup, restore and recovery strategies for data in SaaS environments?

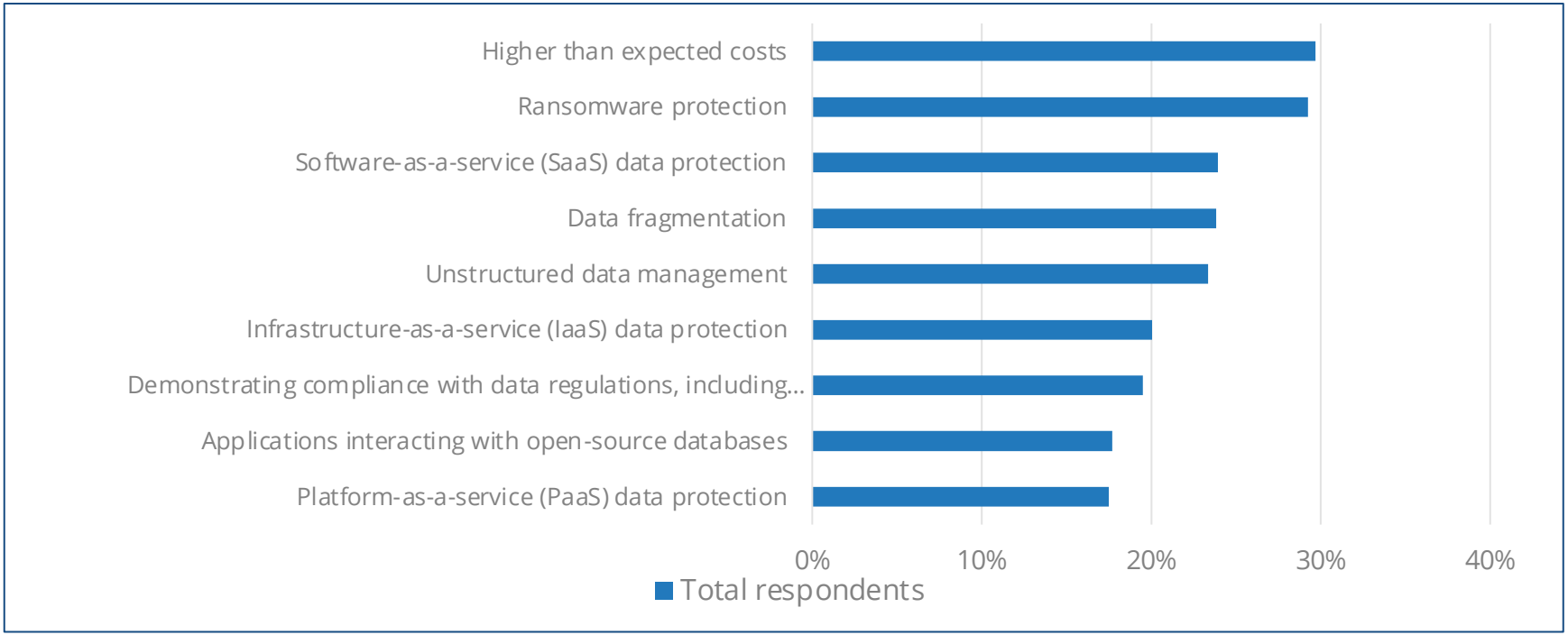




Source: IDC CloudOps and Cloud Governance Survey, 2023

SaaS data protection a rising challenge

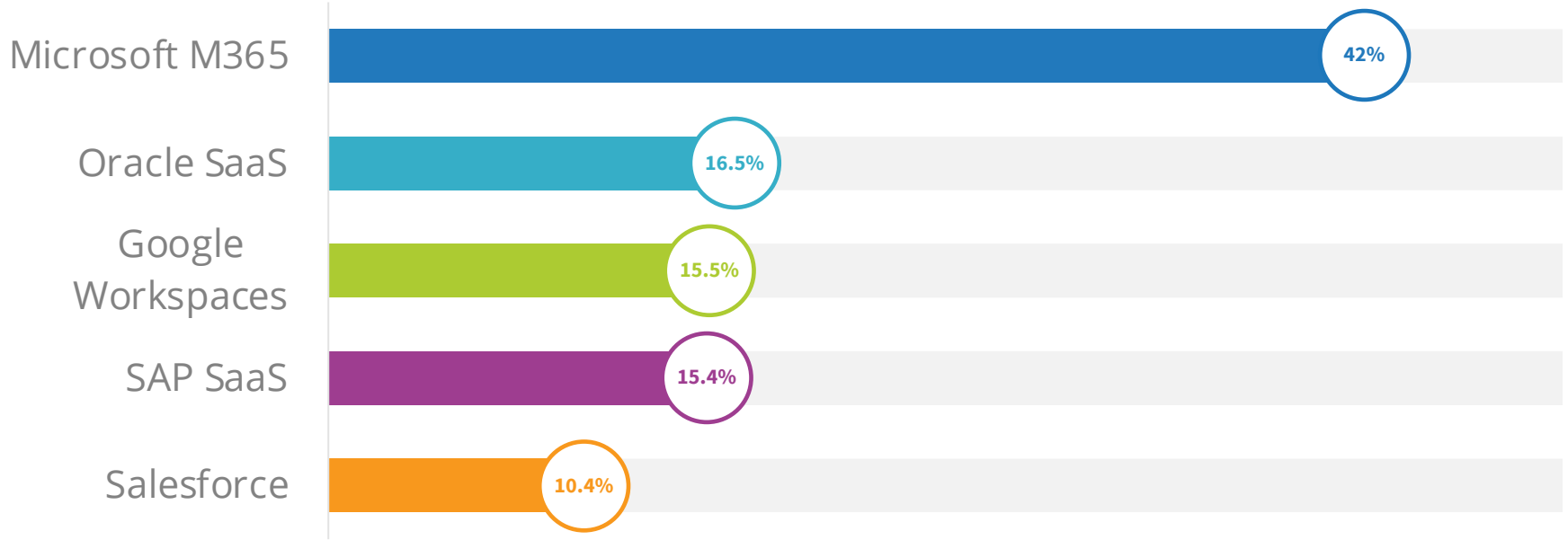
Q. What are the most challenging areas for data protection in your organization



Source: IDC CloudOps and Cloud Governance Survey, 2023

Data loss fears in SaaS environments remain high

Q. In which of the SaaS and PaaS environments currently in use in your organization are you most concerned about data loss, accidental deletion? [Choose all that apply]



Source: *IDC's European Multicloud survey, 2021 (N=925)*

Data loss scenarios in SaaS environments

- Ransomware
- Accidental deletion
- Cloud platform outages
- Reliance on default retention
- Data corruption
- Lack of access to historic data

Ransomware is one of the biggest cyberthreats bringing existential risks to organizations

Cyberattacks, especially ransomware is becoming an existential risk to business survivability.

In 2022 alone:

- **Two thirds of global organizations** experienced ransomware attacks.
- The average ransom in **2022 was close to $300,000 for financial organizations followed by healthcare and life sciences organizations** at around $250,000.

It results in:

- Financial loss.
- Loss of business reputation and trust.
- Non-compliance and data breaches.
- Loss of business, opportunities due to downtime and service interruption.
- Tightening regulations and speed of breach notification.
- Supply chain vulnerabilities.

Ransomware in numbers

10%

Did not pay ransom after experiencing attack

41%

Prevented attack with

SIEM

XDR

CASB

UEBA

49%

Have witnessed cyber insurance premium increase

#1

Source of compromise is a drive-by compromise in which malicious adversaries gain access over the normal course of internet browsing

22%

Valuable, sensitive or secret data was exfiltrated

50%

Experienced data loss

59%

Experienced business disruption for few days to few weeks

52%

Backup and DR strategy failure

Source: EMEA FERS, March 2023, Wave 2, N=540

SaaS, especially M365 Backup, is imperative to meet the four data resiliency priorities identified by the C-Suites

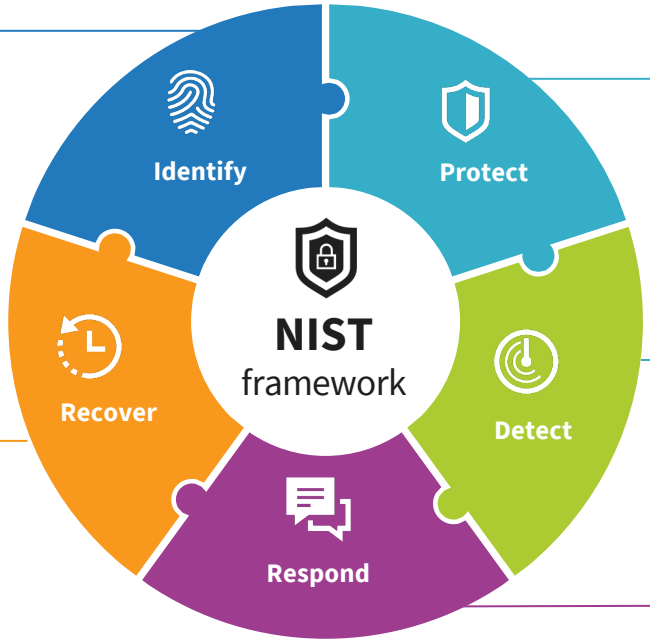
IDC Digital Transformation Futurescape, 2021

Roots of resilience: NIST Framework, EU's NIS 2 Directive, EU's DORA, WEF Cyber Resilience Index

The five functions of the NIST Cybersecurity Framework

Includes

- Identify physical and software assets to establish the basic of an asset management program.
- Identify established cybersecurity policies to define the governance program, as well as legal and regulatory requirements.
- Identify asset vulnerabilities, threats to internal and external organizational resources, and risk response activities as a basic for risk assessments.
- Identify a risk management strategy, including establishing risk tolerances.



Includes

- Identify management and access control protections.
- Ensure staff awareness and training, including role-based and privileged user training.
- Establish data security protection consistent with the organization's risk strategy.

Includes

- Ensure detection of anomalies and events and understanding potential impact.
- Implement continuous security monitoring capabilities.
- Maintain detection processes to provide awareness of anomalous event.

Includes

- Implement recovery planning processes and procedures to restore system and assets.
- Implement improvements based on lessons learned and review existing strategies.
- Coordinate internal and external communications during & following recovery.

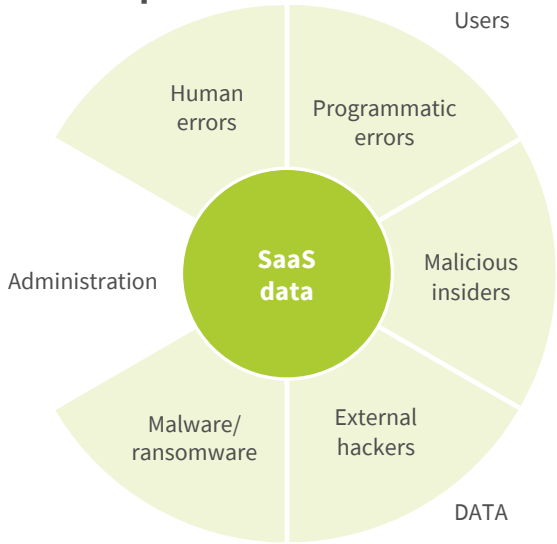
Includes

- Ensure response planning processes are executed during and after an incident.
- Manage communications with stakeholders and law enforcement during and after event.
- Conduct analysis, including forensics, to ensure effective response and to support recovery activities.

SaaS Shared Responsibility Model: value of backup

Responsibility	SaaS	PaaS	IaaS	On-Prem	
Information and data	■	■	■	■	**Responsibility always retained by customer**
Devices (mobile and PCs	■	■	■	■	
Accounts and identities	■	■	■	■	
Identity and directory infrastructure	▨	▨	■	■	**Responsibility varies by service type**
Application	□	▨	■	■	
Network controls	□	▨	■	■	
Operating system	□	□	■	■	
Physical hosts	□	□	□	■	**Responsibility transfer to cloud provider**
Physical network	□	□	□	■	
Physical datacenter	□	□	□	■	

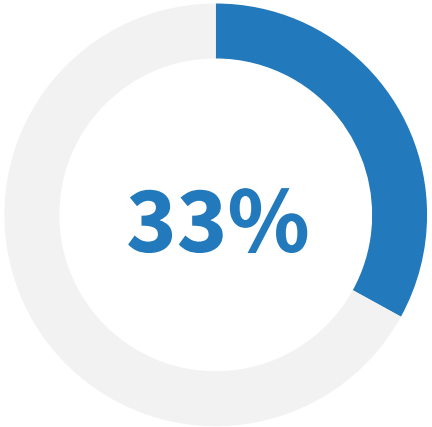
□ Cloud vendor ■ Customer



Provider's responsibility

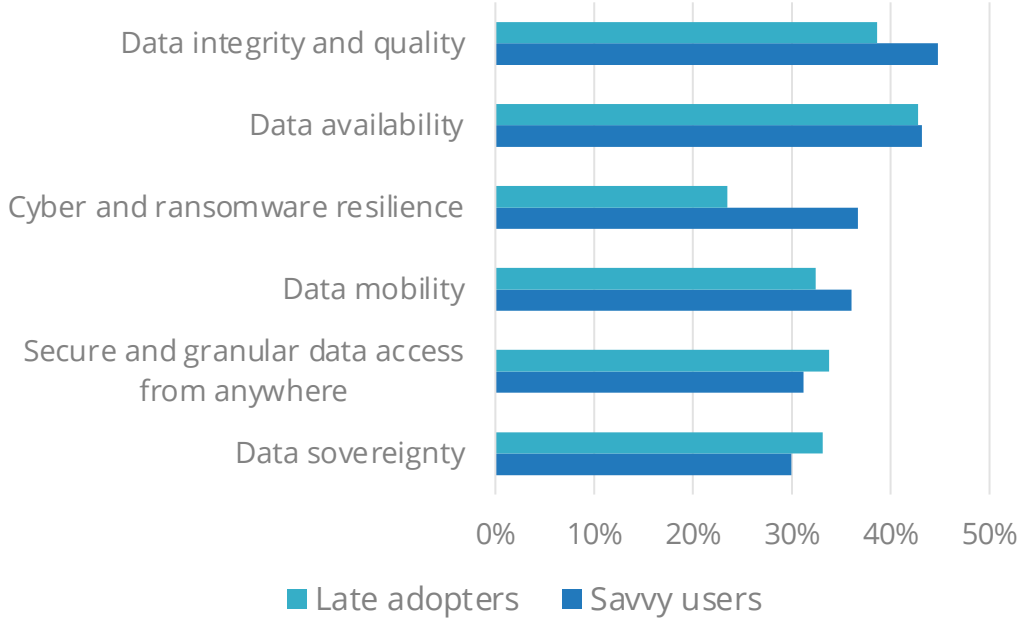
- Hardware failure.
- Software failure.
- Power outages.
- Physical intrusion.
- Operating system.
- Network.
- Natural disaster.

Data protection investment trends for 2023 and beyond: SaaS and cloud-native most resilient environments for investment. Are you ready?



Of mature cloud adopters plan to increase data protection related investments in SaaS environments

Q. What capabilities are essential for your organization for successful cloud data management and governance?

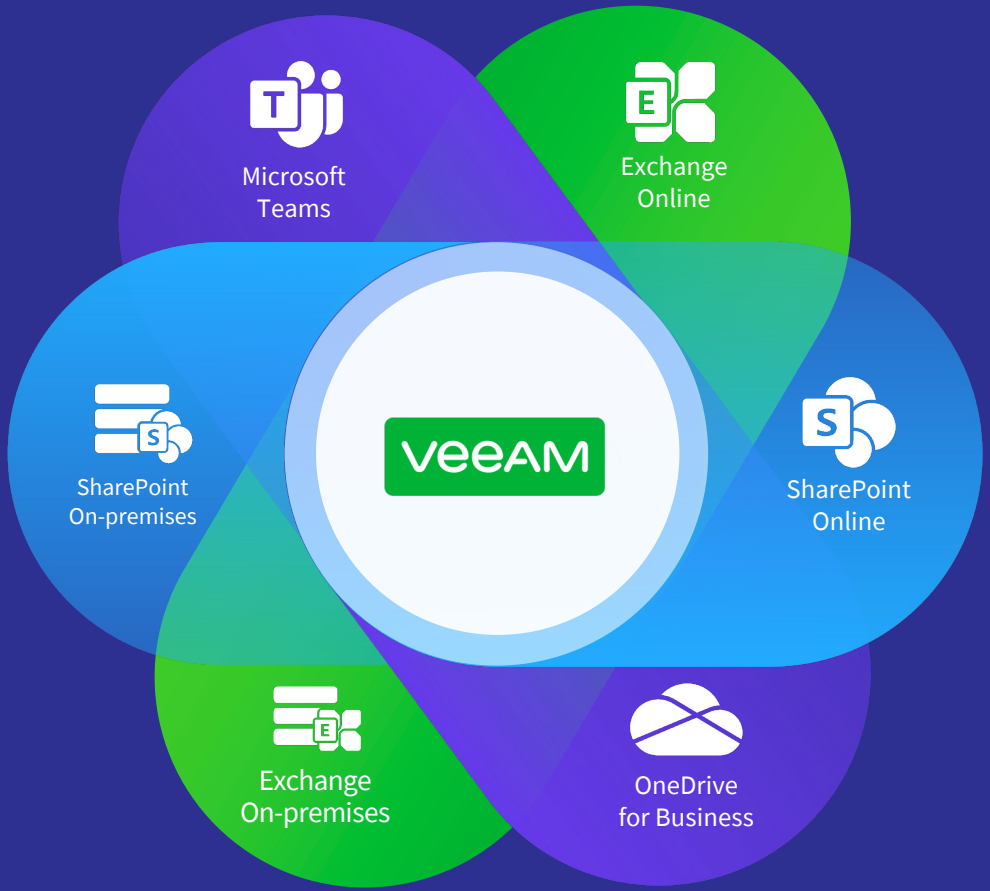


Source: IDC CloudOps Survey, 2023

M365 Data Protection Platform investment: what features are must-haves

Veeam® Backup
for *Microsoft 365*

Eliminate the risk of losing your Microsoft 365 data



Veeam Backup
for Microsoft 365

Capabilities

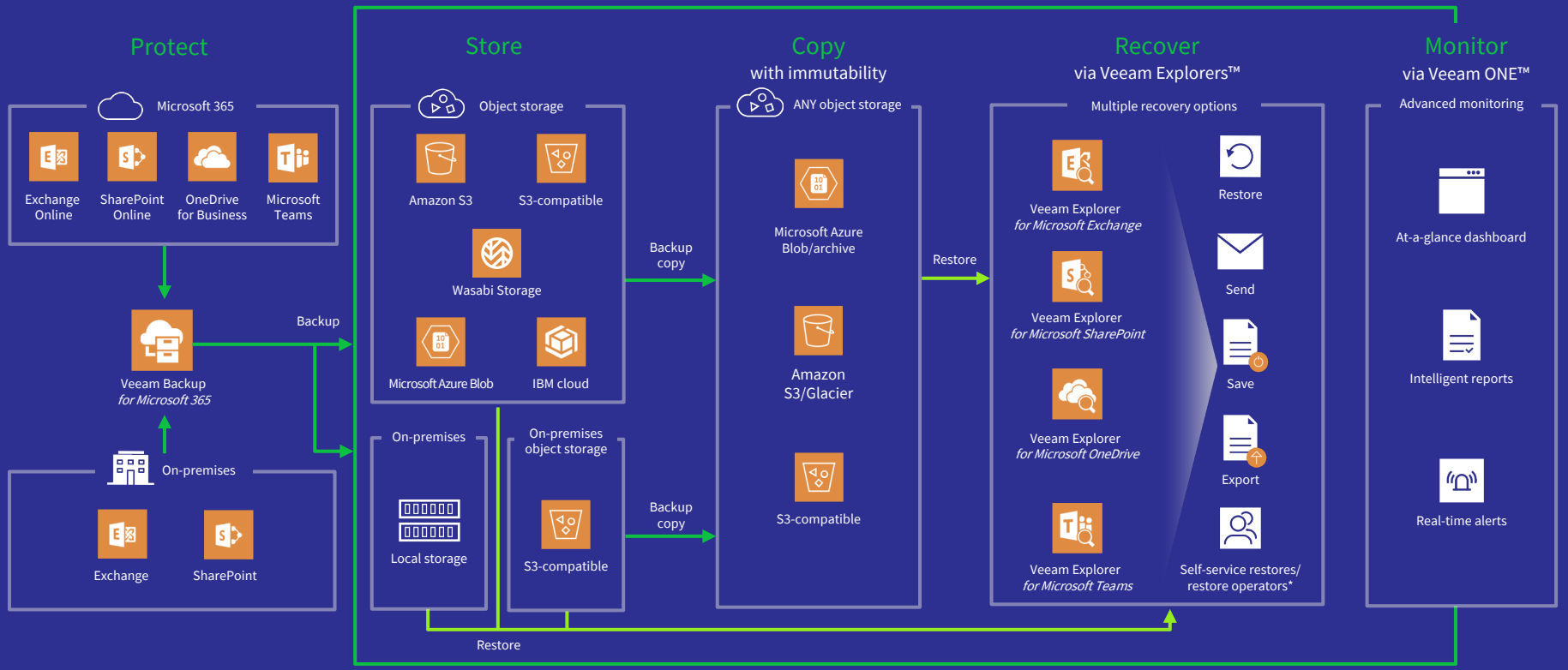
- Protect Microsoft 365 data.
- Quickly restore individual items and files.
- Meet legal and compliance requirements.

Veeam Backup
for Microsoft 365

Difference makers

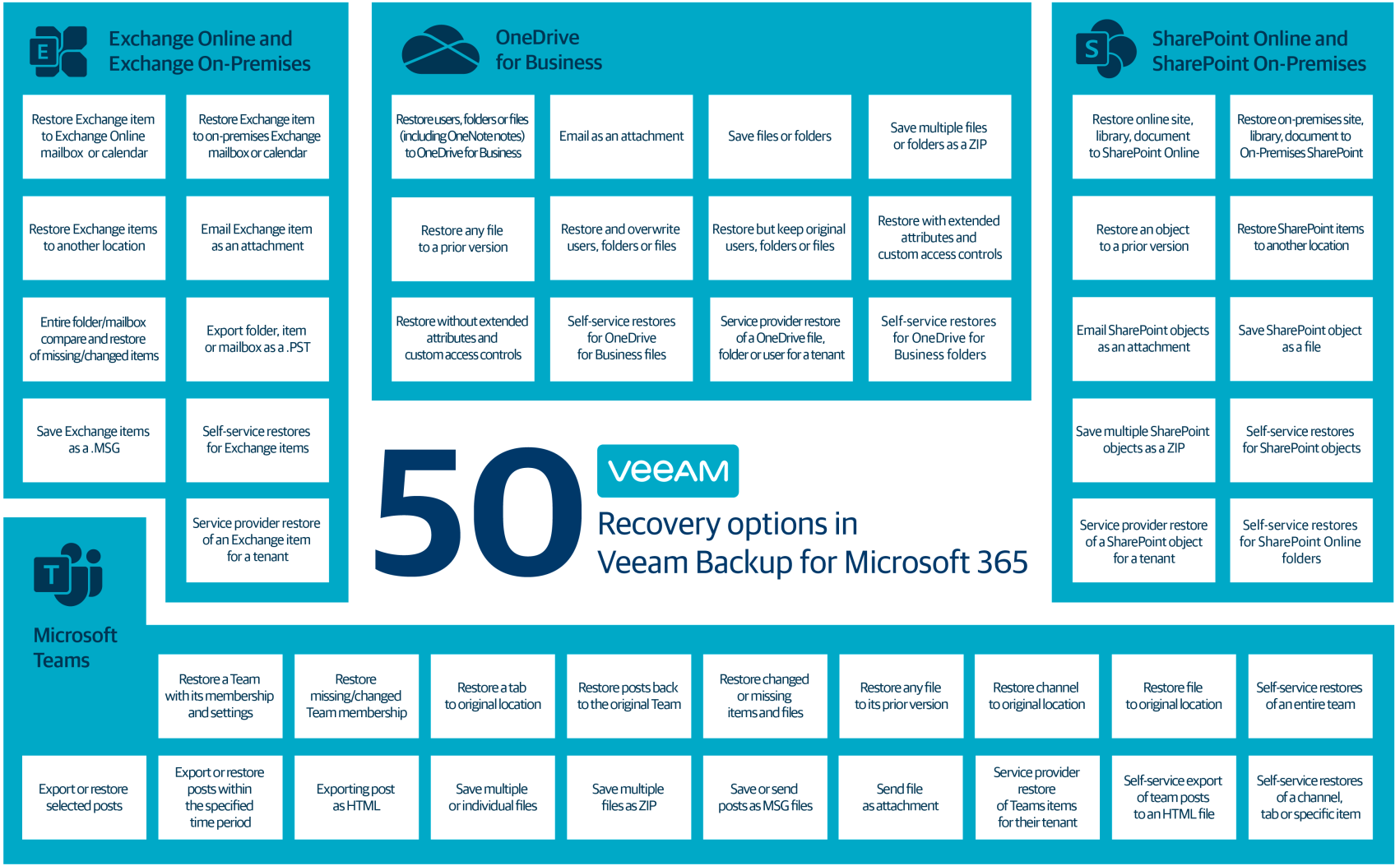
- Infrastructure freedom.
- Backup control.
- Recovery flexibility.

NEW Veeam Backup *for Microsoft 365* v7



*The Self-Service Restore Portal only supports Microsoft 365 organizations using modern app-only authentication.

VeeAMON 2023


Exchange Online and Exchange On-Premises
Restore Exchange item to Exchange Online mailbox or calendar
Restore Exchange item to on-premises Exchange mailbox or calendar
Restore Exchange items to another location
Email Exchange item as an attachment
Entire folder/mailbox compare and restore of missing/changed items
Export folder, item or mailbox as a .PST
Save Exchange items as a .MSG
Self-service restores for Exchange items
Service provider restore of an Exchange item for a tenant
OneDrive for Business
Restore users, folders or files (including OneNote notes) to OneDrive for Business
Email as an attachment
Save files or folders
Save multiple files or folders as a ZIP
Restore any file to a prior version
Restore and overwrite users, folders or files
Restore but keep original users, folders or files
Restore with extended attributes and custom access controls
Restore without extended attributes and custom access controls
Self-service restores for OneDrive for Business files
Service provider restore of a OneDrive file, folder or user for a tenant
Self-service restores for OneDrive for Business folders
SharePoint Online and SharePoint On-Premises
Restore online site, library, document to SharePoint Online
Restore on-premises site, library, document to On-Premises SharePoint
Restore an object to a prior version
Restore SharePoint items to another location
Email SharePoint objects as an attachment
Save SharePoint object as a file
Save multiple SharePoint objects as a ZIP
Self-service restores for SharePoint objects
Service provider restore of a SharePoint object for a tenant
Self-service restores for SharePoint Online folders
50
VEEAM
Recovery options in Veeam Backup for Microsoft 365
Microsoft Teams
Restore a Team with its membership and settings
Restore missing/changed Team membership
Restore a tab to original location
Restore posts back to the original Team
Restore changed or missing items and files
Restore any file to its prior version
Restore channel to original location
Restore file to original location
Self-service restores of an entire team
Export or restore selected posts
Export or restore posts within the specified time period
Exporting post as HTML
Save multiple or individual files
Save multiple files as ZIP
Save or send posts as MSG files
Send file as attachment
Service provider restore of Teams items for their tenant
Self-service export of team posts to an HTML file
Self-service restores of a channel, tab or specific item

Microsoft 365 backup solution checklist

Features

Back up Exchange Online/on-premises

Back up SharePoint Online/on-premises

Back up OneDrive for Business

Back up Microsoft Teams

Flexibility and choice

Deploy on premises or in the cloud

Utilize any storage target you want

No lock-ins, switch storage anytime

Flexible job configurations

Innovation

Simple UI, powerful features

Implement customer feedback

Easy tools for eDiscovery

Scale

Handles large number of users

SMB friendly

Backup proxies

Integration

Natively integrated with Microsoft 365

Large ecosystem of service providers

Integrated with hyperscale clouds

S3-compatible

Breadth of service

Wide range of workloads within a platform - cloud, physical, virtual

NEW Veeam Backup *for Microsoft 365* v7

Immutable backup copies

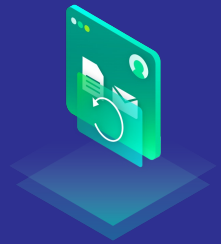
Protect against ransomware attacks with immutable backup copies on ANY object storage

Advanced monitoring

At-glance dashboard, real-time alerts and intelligent reports through integration with **Veeam ONE**

Increased control for BaaS

Tenants have more backup, monitoring and restore options with deeper integration with **Veeam Service Provider Console**



Self-service restore portal enhancements

Self-service restore portal now has support for Microsoft Teams and MORE!

No third-party backup vendor protects more data

15M+

protected Microsoft 365 users

Gartner®
Veeam is a Leader in the
2022 Gartner Magic Quadrant

Gold
Microsoft Partner
Five plus years in partnership
with Microsoft

VEEAMON 2023

Take action

Read up or share

Technical guide on how the #1 Microsoft 365 backup solution works!

#1 Office 365 Backup Guide by Veeam

Chapters

2

Direct link: https://go.veeam.com/guide-backup-office-365

See for yourself

Trial download: **FREE for 30 days**

Direct link: https://go.veeam.com/backup-office-365

VEEAMON 2023

Deploy as a service or manage it yourself.

Veeam gives you options.

On-premises | In the cloud | As-a-service


Thank you!
VEEAMON 2023