Microsoft 365 Data Protection

Even the Cloud Experiences Storms

veeam Cloud & Service Provider Platinum

CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com

Introduction

Cloud to Cloud

With well over 320 million business users active each month, Microsoft 365's cloud-based email and applications serve as the critical business infrastructure for hundreds of thousands of organizations. Email, collaboration, cloud storage, and more are all used daily as an integral part of business operations.

Most organizations tend to focus on the delivery of a cloud service – and Microsoft 365 is no exception. Microsoft provides a Service Level Agreement, which focuses on guaranteeing service uptime. But, many organizations forget about the data held within Microsoft 365. Emails represent sales, operational directives, contain intellectual property, etc. The data stored in the cloud involves every part of your business including marketing, development, finance, sales, accounting, and more.

With so many organizations depending on Microsoft 365, and with the SLA only concerned with uptime, the question should be raised "Who's protecting your data in Microsoft 365?"

The assumption with Microsoft 365 (and any cloud provider, really) is that the data housed there is always accessible, available, and current. But what about protection against data loss, data corruption, cyber attack, human error, or natural disasters? Organizations with traditional on premises technology are keenly aware they are responsible for their own data protection. Backups of email alone typically exist from the conversation somehow changes. Microsoft is solely concerned about service delivery, and Microsoft 365's services don't include data protection.

Every organization needs to ensure an ability to recover. Proper backups are necessary, along with retention policies to meet compliance and/or eDiscovery requirements – all part of a long-term data protection strategy. But, in a world where organizations rely on the cloud, and the perception is that there's little risk in losing your active business data, do you really need to add Microsoft 365 in your data protection strategy?

The short answer is a resounding yes. Take the example of a ransomware infection on a single workstation running the OneDrive for Business client. The encryption of local files will be replicated to the cloud, potentially impacting an entire department. No matter where your data resides, organizations need their own means by which to recover from a loss of any kind. Even when data is in the cloud, having a data protection plan is a necessity.

So, who's responsible for data protection when it comes to Microsoft 365?

In this whitepaper, we'll look at the realities of data protection within Microsoft 365, what kinds of data protection is necessary for organizations today, and how cloud-to-cloud backup can help meet the need.

Clouded Protection:

The Realities of Microsoft 365's Data Safegaurds

To best understand Microsoft's position around data protection within Microsoft 365, we need to look at who is responsible. There are two parts to the responsibility equation: data and the service.

They need to be broken apart and addressed separately. Microsoft is clearly responsible for the service. Their SLA denotes they willingly accept responsibility to maintain service availability. Data, however, isn't Microsoft's responsibility.

Many organizations just naturally assume it is since the data resides on their servers. But, Microsoft makes it clear1 the responsibility of data protection falls to the organization.

Microsoft's safeguards revolve around the following practices:

1. **Redundancy** – Microsoft has built in redundancy at the data center level. Hardware and power are all designed to protect against failures. Redundancy also exists at the data level. Data is constantly replicated across geographically separate data centers.

2. **Monitoring** – All services and systems are continuously inspected, allowing Microsoft to proactively take action to ensure service delivery.

3. **Resiliency** – This includes automatic load balancing of systems, as well as automatic and manual failover.

4. **Backups** – Yes, you read that right. Microsoft does backup its data centers. However, (and this is an important caveat) the backups are only for internal use to recover their data centers and are not for customer use.

So, you can see Microsoft's focus is purely to keep the service running. There is functionality within Microsoft 365 that feels like it provides some level of data protection we should address.

What About Archiving?

Exchange Online does provide archiving, so you might be tempted to rely on that. First off, remember that archiving isn't a backup. It's an immutable copy of certain email retained for long durations of time. Same thing goes for Legal Holds in Exchange Online.

How about Recovering Deleted Items?

There are Recycle Bin-type features in services such as Exchange Online, SharePoint Online, and OneDrive, but those features are for the very smallest of losses (e.g. a single email/document/etc.) and are not viable to recover from a scale loss of data, systems, applications, or location.

Microsoft 365: Not in the Data Protection Business

At the end of the day, Microsoft 365 is not a backup product; it's a productivity platform. So, relying on any functionality within the platform as your means of recovery (whether it be their data redundancy, or recovering deleted items) leaves your organization with the same level of risk. What's needed is a means of data protection that meets your organization's business requirements.

Brewing Storms:

The Data Protection Needs of Organizations Today

To remain competitive, successful organizations are serious about their data recoverability and business continuity. Plans that take into account even the most remote loss (such as all of Microsoft 365 going down, or data within becoming corrupted), with steps to mitigate the loss as quickly as possible. And, while improbable, your organization needs to ensure it stays operational should data loss or corruption occur.

Microsoft 365 Experts: CyberFortress and Veeam

The protection of data in Microsoft 365 is foundational to ensuring a critical part of your business can be recovered. Organizations wanting to backup and recover Microsoft 365 data for retention and recoverability purposes need to take steps to include this data as a part of their DR strategy. CyberFortress and Veeam together help organizations to protect data, applications, and operations with industry leading software and expertise.

Look for insights from CyberFortress and Veeam throughout this eBook!

CyberFortress and Veeam Insights: Using Native Functionality

Smaller organizations with basic recovery requirements can't take advantage of the embedded functionality. But those organizations wanting the ability to recover significantly more than just one email or document should look at Microsoft 365 like they would if it existed on-prem. Proper backups of the data, along with a recovery strategy are needed. CyberFortress and Veeam can help to design a plan that protects all your critical data in Microsoft 365.

Meet the 3-2-1 Backup Rule

This is cardinal rule #1 for all backups. *3 copies of your data, 2 different mediums, 1 copy offsite*. Let's see how Microsoft 365 stacks up.

3 **Copies of your Data** – One of your 3 copies is the copy in production. So, your production Microsoft 365 instance is that one copy. You still need 2 more copies. Having your data in Microsoft 365 fails the first test.

2 **Different Mediums** – Given there's only a single copy in production, Microsoft 365 also fails this test.

1 **Offsite** – while the cloud is generally considered offsite when planning recovery, it's because there is an on-prem production copy. So, being that Microsoft 365 solely exists in the cloud, you'd need another copy "offsite" from Microsoft to pass this test.

Daily, Granular Recovery

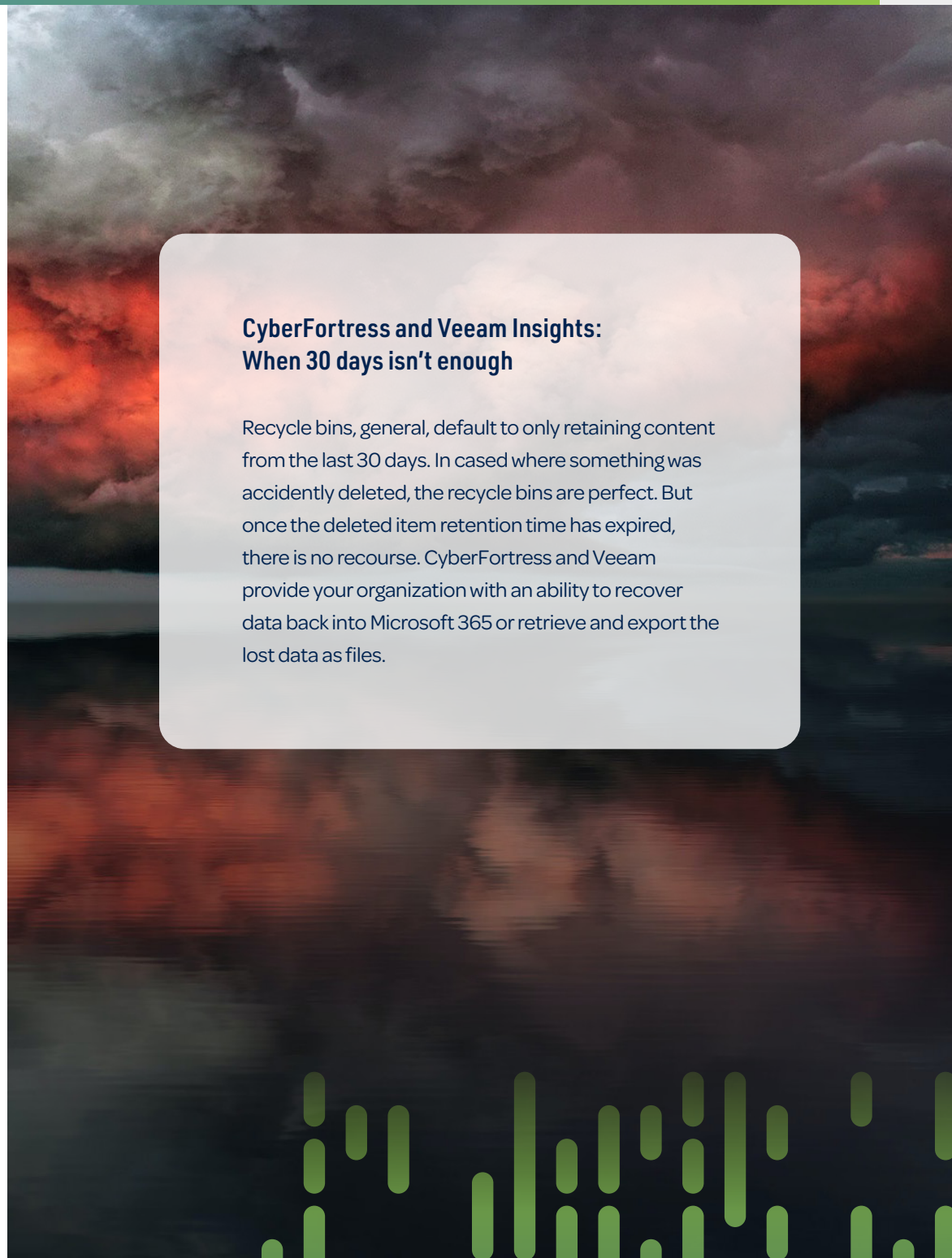
The focus here isn't to recover the services hosting your data; that's Microsoft's job. The organization needs a way to granularly recover any subset of your email, files, documents, etc. – down to a single instance – on a daily basis. We say daily because, even with recovery bin technology, the file/email/etc. that was there yesterday, may be purged today and gone forever in the eyes of Microsoft.

Your Own Copy of Data

While a remote possibility, the need to move off of Microsoft 365 – to another cloud provider or even back onpremises – can occur. Having copies of your data facilitates any migration deemed necessary due to acquisition, service level issues, costs, etc.

Being the Master of Your Data Protection Destiny

It's really simple. Think about this if Microsoft 365 were on prem; the organization would be responsible for backups and a data protection strategy, right. Even with Microsoft 365 residing in the cloud, the separation of duties still exists: Microsoft needs to ensure the applications and services run, and you need to backup and protect your data. Even the simple litmus tests we listed above all demonstrate that your data is nowhere near protected. You need to take steps to ensure your organization's data is backed up and recoverable outside of Microsoft 365.



CyberFortress and Veeam Insights: When 30 days isn't enough

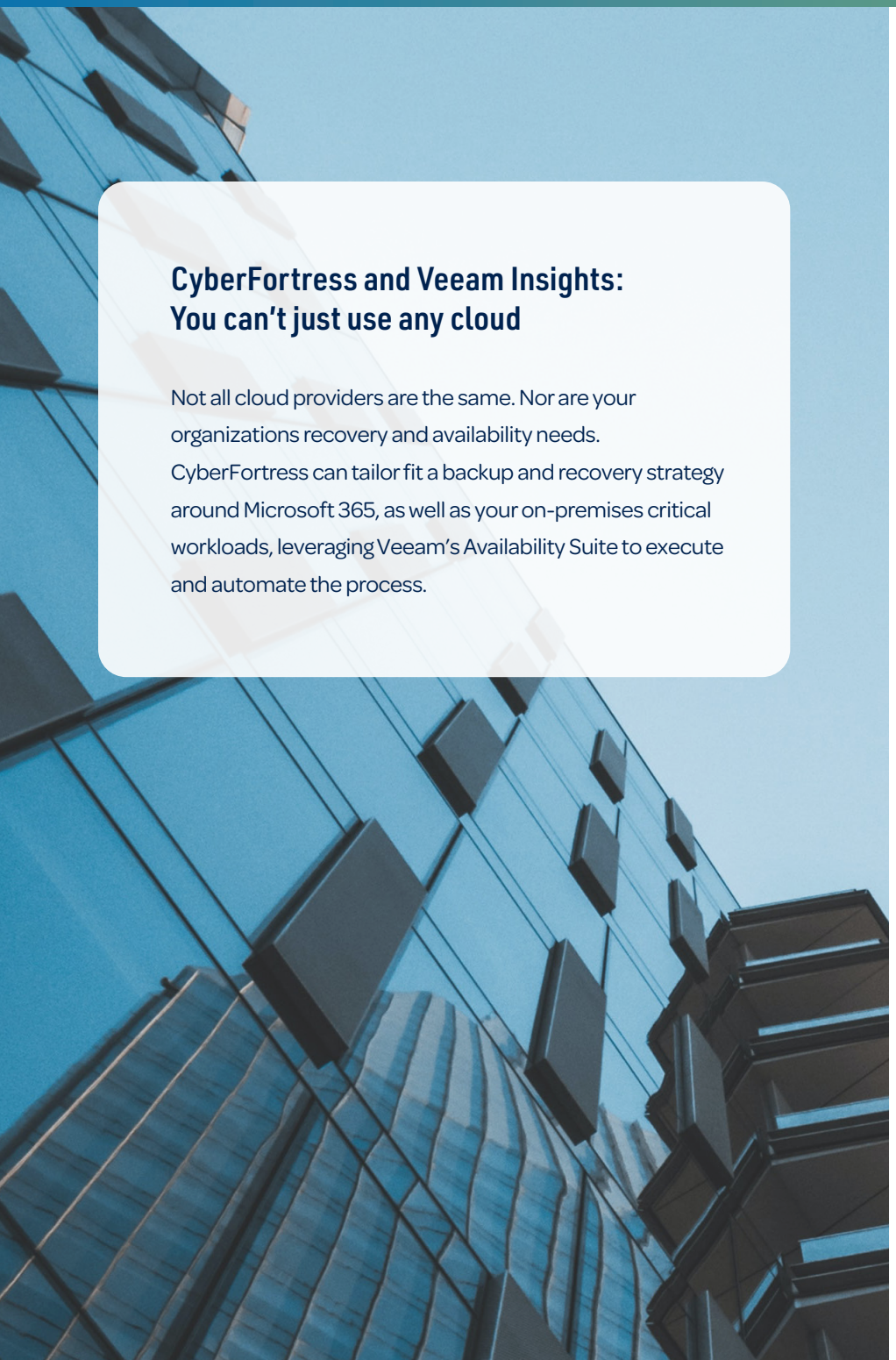
Recycle bins, general, default to only retaining content from the last 30 days. In cased where something was accidently deleted, the recycle bins are perfect. But once the deleted item retention time has expired, there is no recourse. CyberFortress and Veeam provide your organization with an ability to recover data back into Microsoft 365 or retrieve and export the lost data as files.

Clear Skies:

Leveraging Cloud-to-Cloud backup to protect Microsoft 365

So, what's the right way to protect data on Microsoft 365?

The simple answer is you need to backup your Microsoft 365 data. It really is that easy. It's when you begin looking at how you'll accomplish this, that things can get a bit more complicated. First off, it should be said, it is technically possible to backup Microsoft 365 to on-premises storage. But why would you? If your organization is leveraging a cloud vision, it begs the question *why would you use on-premises data protection?* Doing so puts your data in a single physical location and runs the risk of a lack of redundancy.



CyberFortress and Veeam Insights: You can't just use any cloud

Not all cloud providers are the same. Nor are your organizations recovery and availability needs. CyberFortress can tailor fit a backup and recovery strategy around Microsoft 365, as well as your on-premises critical workloads, leveraging Veeam's Availability Suite to execute and automate the process.

Why Cloud-to-Cloud?

Cloud-to-Cloud (C2C) backups keep with the cloud vision of availability, accessibility, and redundancy of services. Backed up Microsoft 365 data is highly available, making your data protection efforts equal to the service level efforts of Microsoft 365. It meets the 3-2-1 rule, hosting multiple copies of your data "offsite" from Microsoft 365, and removes the organization's reliance upon Microsoft 365 to protect its' data.

Which Cloud Should You Use?

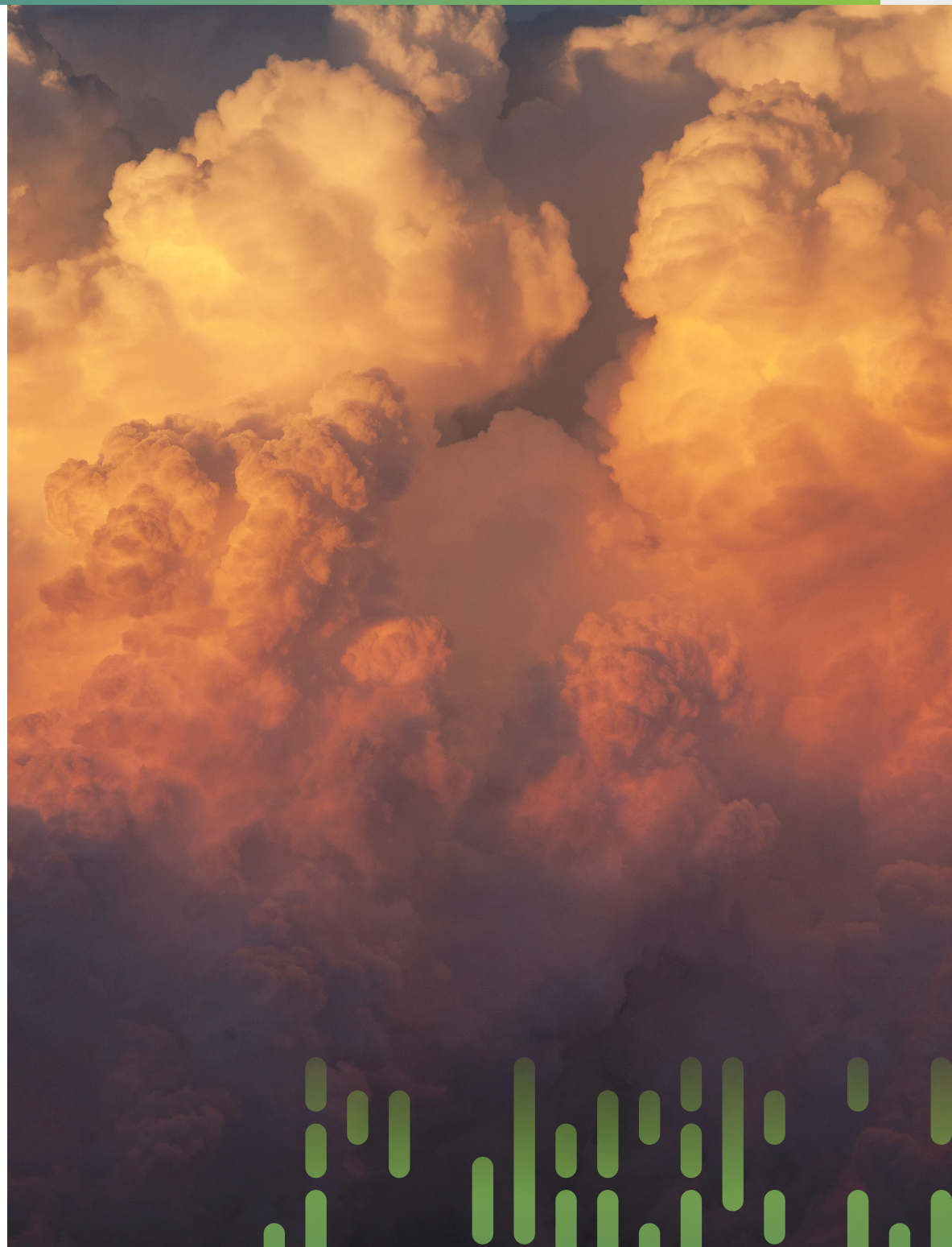
The data in Microsoft 365 represents, in many cases, a majority of your business operations. You can't simply back it up to the least expensive cloud storage and call it a day. But it's more than just a question of whose cloud storage should be used.

In similar fashion to the notion that your data protection methCyberFortress should align with your cloud vision, the same alignment rings true when considering how you should go about cloud backups. You chose Microsoft 365 so that the management of the service would be handled by experts dedicated to ensuring its availability and performance. In the same way, backups of this critical data set should rest with a partner that has similar levels of expertise in the backup and recovery of your Microsoft 365 data, and whose cloud infrastructure rivals that of Microsoft's. By doing so, you can rest assured that your organization's ability to recover Microsoft 365 data is in equivalent hands.

Protecting Your Microsoft 365 Data in the Worst Storms

At this point, it's clear that Microsoft isn't concerned with the protection of your organization's data. Like your on prem data, it's necessary to establish a plan and a means by which to backup and recover Microsoft 365 data in the midst of scenarios involving ransomware, data deletion, or data corruption.

By leveraging C2C data protection through a trusted partner, you follow your organization's cloud vision, ensuring the recoverability of your most critical operational data in Microsoft 365, no matter the storm.



Microsoft 365 Data Protection

Even the Cloud Experiences Storms

veeam Cloud & Service Provider Platinum

CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com