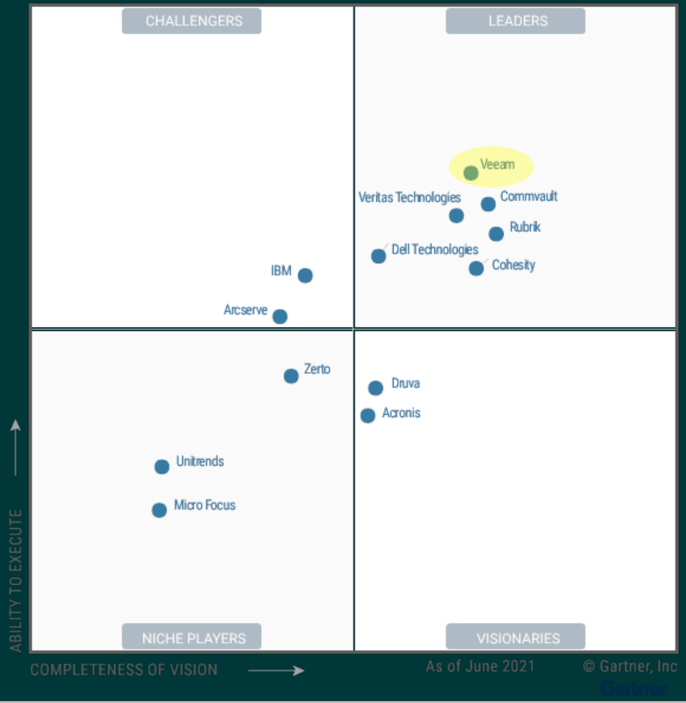
5 Reasons Why Office 365 Backup is Critical

Chris Tong

Sr. Systems Engineer | Veeam

Veeam is the Leader

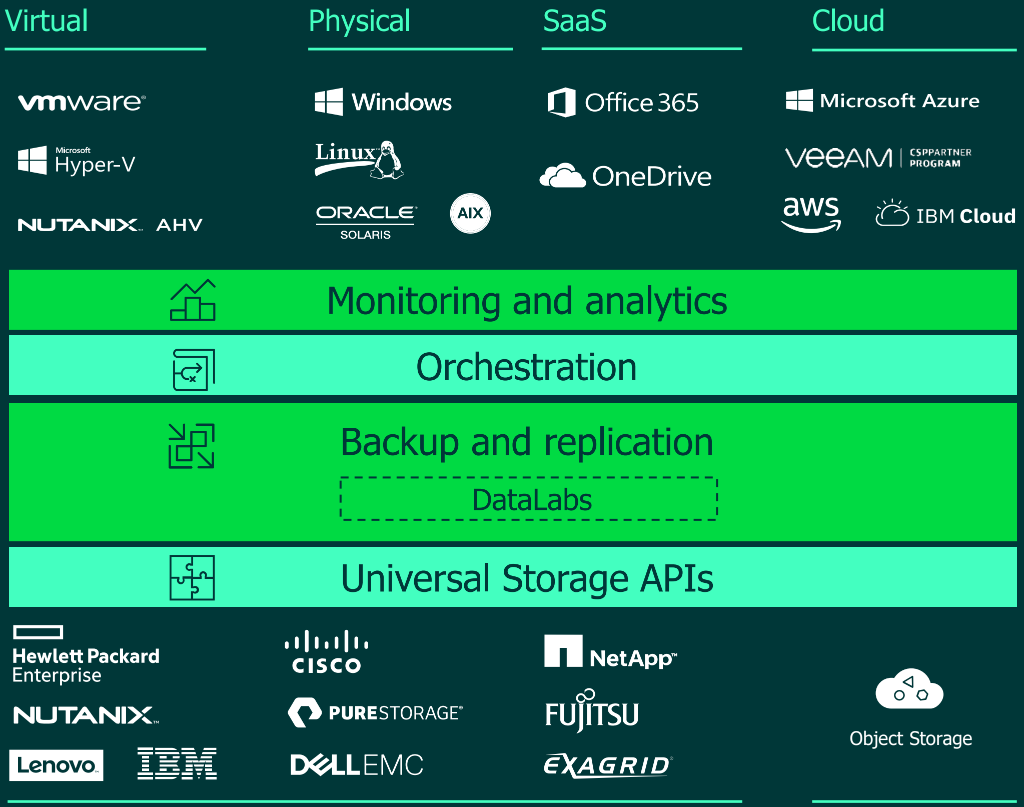
Gartner: 2021 Magic Quadrant for Data Center Backup and Recovery Solutions



Gartner®

2021 (5 years in a row): “Gartner Magic Quadrant for Data Center Backup and Recovery recognizes Veeam as a Leader.”

A Single Platform for Cloud, Virtual and Physical



Virtual

vmware

Microsoft Hyper-V

NUTANIX AHV

Physical

Windows

Linux

ORACLE SOLARIS

AIX

SaaS

Office 365

OneDrive

Cloud

Microsoft Azure

veeAM | CSPPARTNER PROGRAM

aws

IBM Cloud

Monitoring and analytics

Orchestration

Backup and replication

DataLabs

Universal Storage APIs

Hewlett Packard Enterprise

NUTANIX

Lenovo

IBM

CISCO

PURESTORAGE

DELLEMC

NetApp

FUJITSU

EXAGRID

Object Storage

5 Reasons WHY

you need an Office 365 backup

Accidental deletion

Retention policy confusion / gaps

Internal security threats
Malicious insiders / departing employees

External security threats
Ransomware / rogue apps

Legal and compliance requirements

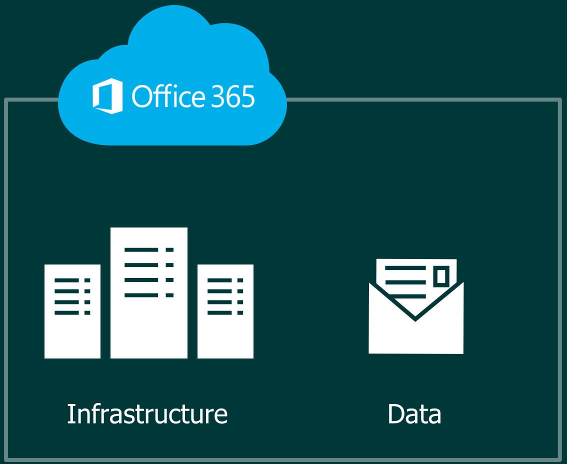
Archived video webinar: The six reasons for Microsoft Office 365 backup
https://www.veeam.com/videos/six-reasons-office-backup-14845.html

Why do I need a backup?

Microsoft takes care of it.

Customer perception

Microsoft takes care of everything



Why do I need a backup?

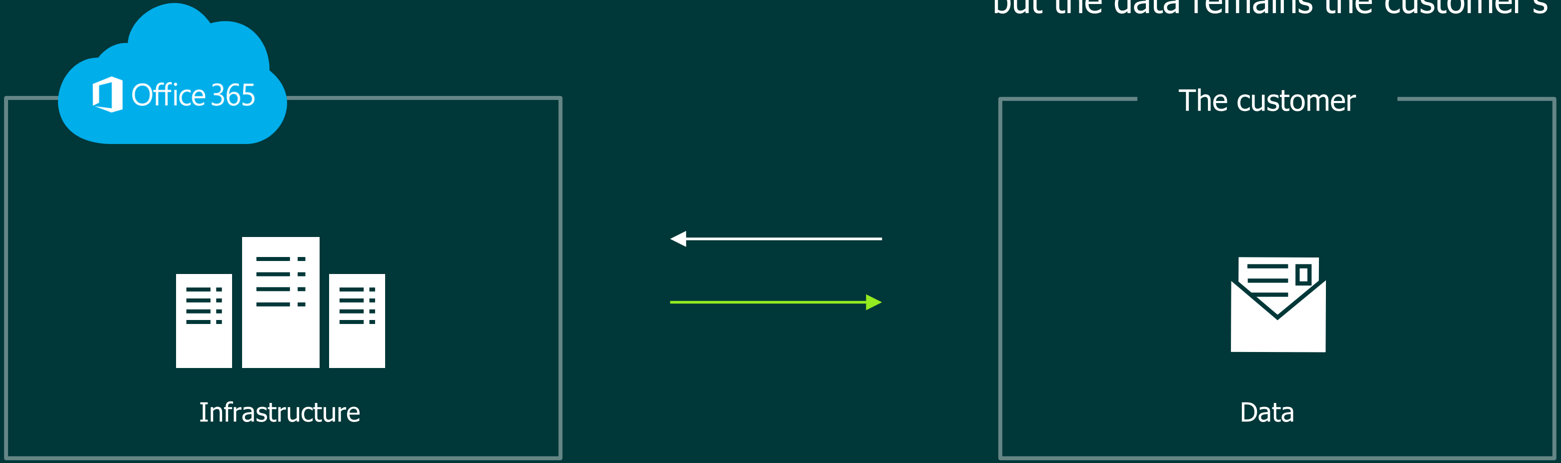
Microsoft takes care of it.

Customer perception

Microsoft takes care of everything

Customer reality

Microsoft takes care of the infrastructure,
but the data remains the customer's responsibility.



Uptime of Office 365

Protection and long-term retention
of Office 365 data

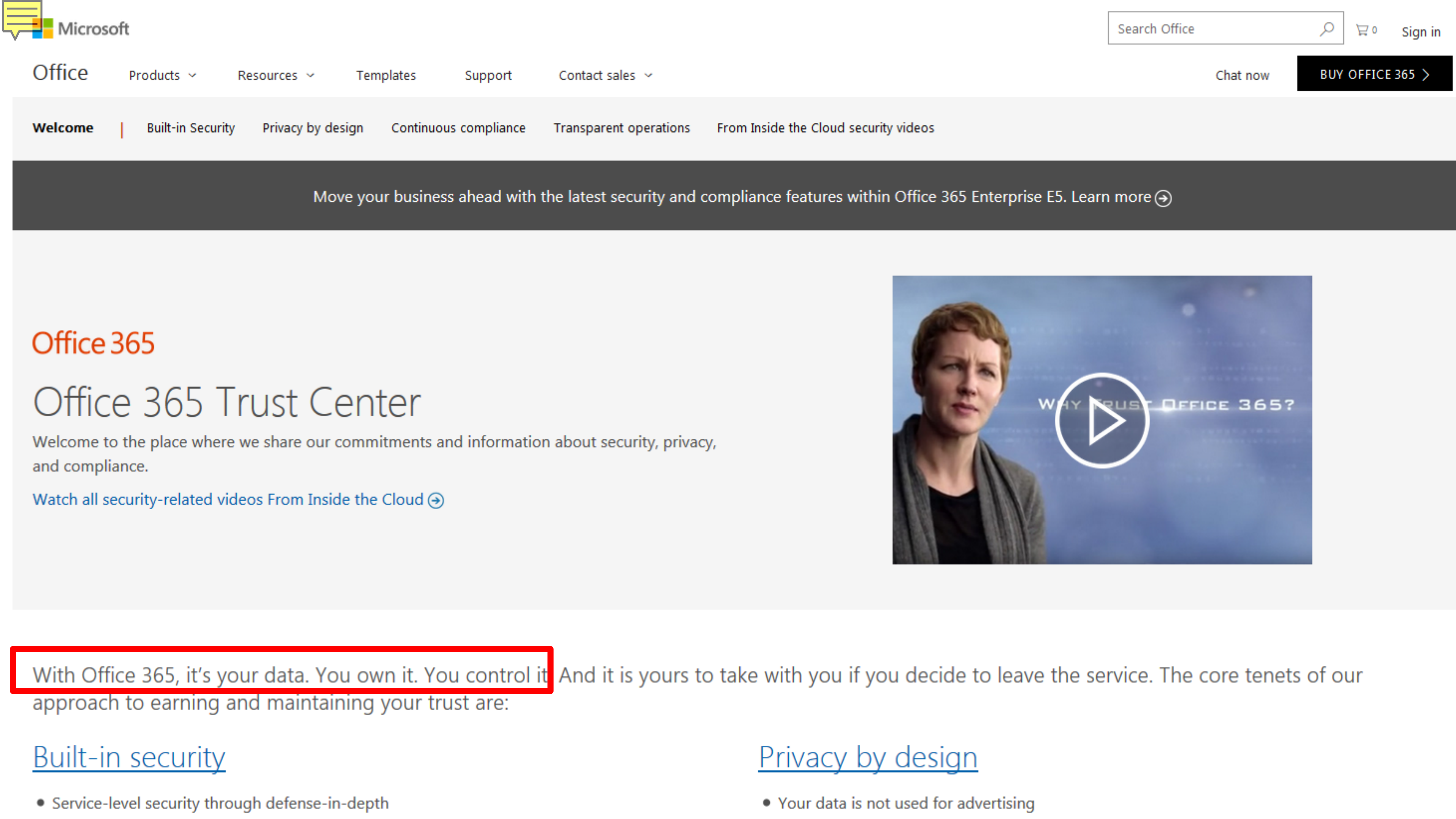
"Back up your SaaS data – because most SaaS providers don't."

FORRESTER®

"There's an assumption that if the data is in SaaS, it's automatically backed up, but that's not the case. Just because it's in the cloud doesn't mean that you don't have to back it up. You are still responsible for protecting the data, making it recoverable and archiving it, especially email."

ESG
Enterprise Strategy Group

Sources: Forrester Research, Back Up Your SaaS Data – Because Most SaaS Providers Don't, 2018



Move your business ahead with the latest security and compliance features within Office 365 Enterprise E5. Learn more

Office 365

Office 365 Trust Center

Welcome to the place where we share our commitments and information about security, privacy, and compliance.

Watch all security-related videos From Inside the Cloud

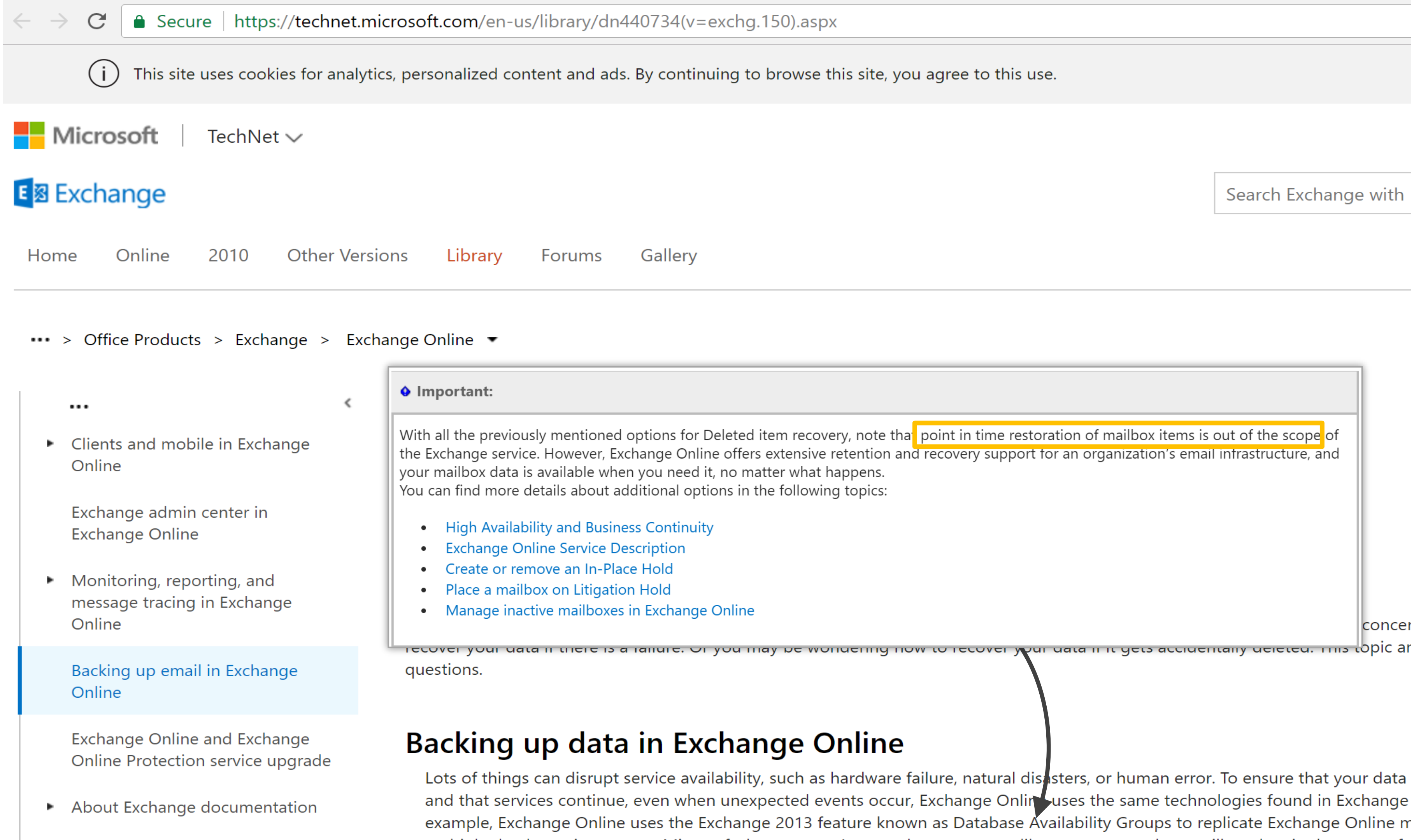
With Office 365, it's your data. You own it. You control it And it is yours to take with you if you decide to leave the service. The core tenets of our approach to earning and maintaining your trust are:

Built-in security

- Service-level security through defense-in-depth

Privacy by design

- Your data is not used for advertising


Secure
https://technet.microsoft.com/en-us/library/dn440734(v=exchg.150).aspx
Microsoft
TechNet
Exchange
Search Exchange with
Home
Online
2010
Other Versions
Library
Forums
Gallery
... > Office Products > Exchange > Exchange Online
Clients and mobile in Exchange Online
Exchange admin center in Exchange Online
Monitoring, reporting, and message tracing in Exchange Online
Backing up email in Exchange Online
Exchange Online and Exchange Online Protection service upgrade
About Exchange documentation

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use.

Important:

With all the previously mentioned options for Deleted item recovery, note that point in time restoration of mailbox items is out of the scope of the Exchange service. However, Exchange Online offers extensive retention and recovery support for an organization's email infrastructure, and your mailbox data is available when you need it, no matter what happens.
You can find more details about additional options in the following topics:

- High Availability and Business Continuity
- Exchange Online Service Description
- Create or remove an In-Place Hold
- Place a mailbox on Litigation Hold
- Manage inactive mailboxes in Exchange Online

concer

recover your data if there is a failure. Or you may be wondering how to recover your data if it gets accidentally deleted. This topic ar questions.

Backing up data in Exchange Online

Lots of things can disrupt service availability, such as hardware failure, natural disasters, or human error. To ensure that your data and that services continue, even when unexpected events occur, Exchange Online uses the same technologies found in Exchange example, Exchange Online uses the Exchange 2013 feature known as Database Availability Groups to replicate Exchange Online m

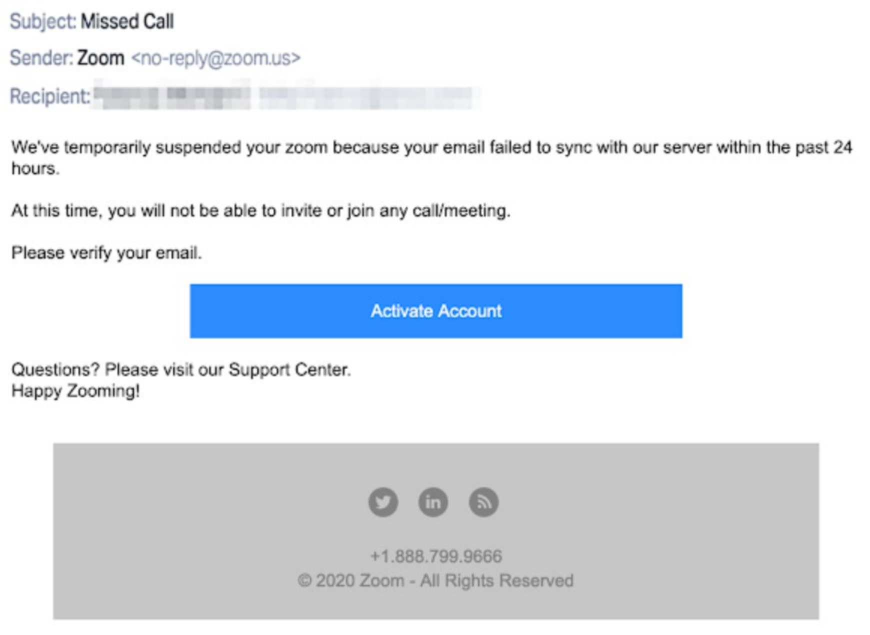
Hacking News on 2020

Microsoft Office 365 Users Targeted By a New Phishing Campaign Using Fake Zoom Notifications

- The phishing messages spoof an official Zoom email address and are intended to imitate a real automated Zoom notification.

- As soon as the users click the "Activate Account" button, they are redirected to a fake Microsoft login page through 'an intermediary hijacked site'.

- On the phishing landing page, they are asked to include their Outlook credentials in a form intended to exfiltrate their account subtleties to attacked controlled servers.



Subject: Missed Call

Sender: Zoom <no-reply@zoom.us>

Recipient: [redacted]

We've temporarily suspended your zoom because your email failed to sync with our server within the past 24 hours.

At this time, you will not be able to invite or join any call/meeting.

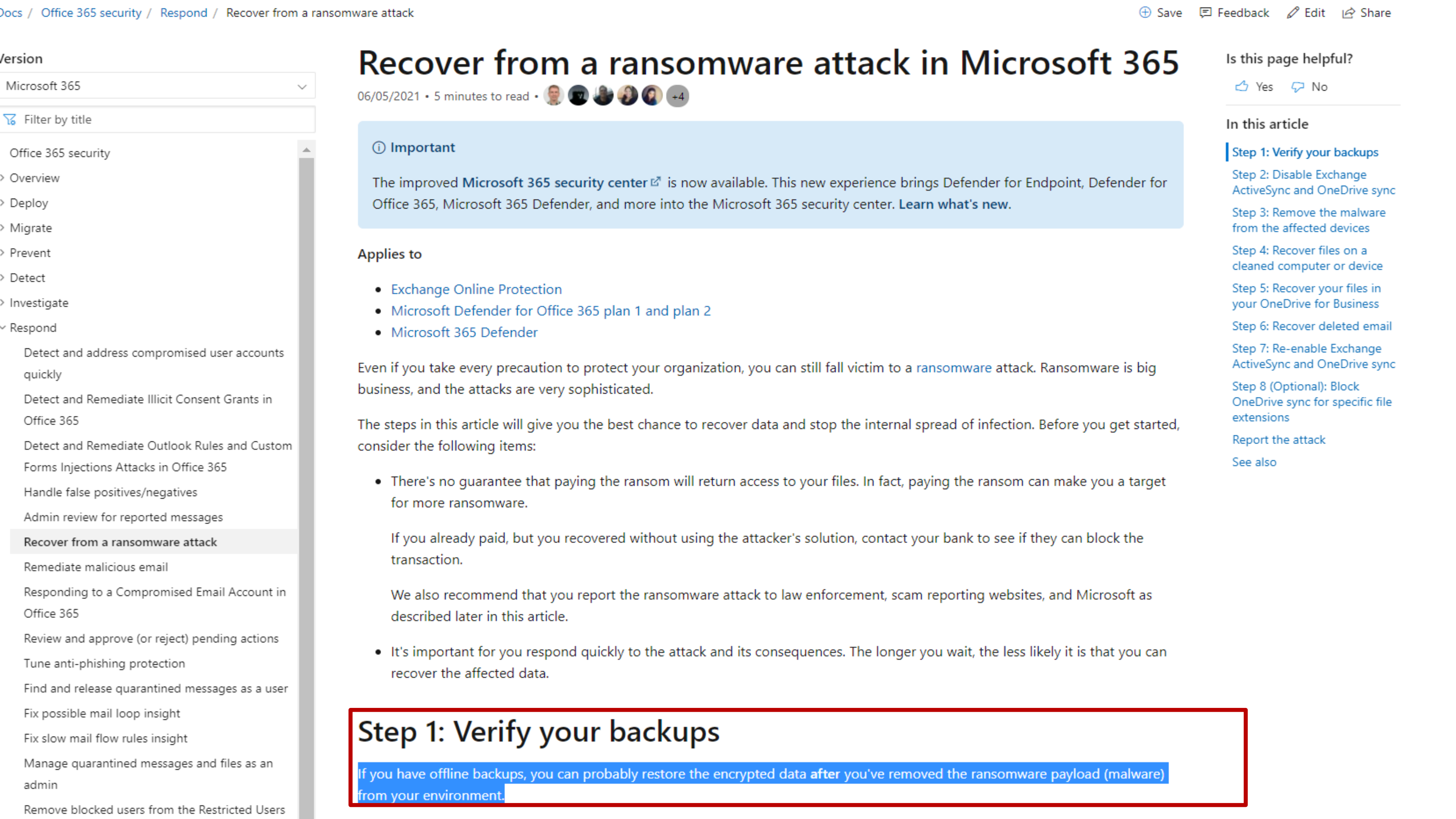
Please verify your email.

Questions? Please visit our Support Center.
Happy Zooming!

+1.888.799.9666
© 2020 Zoom - All Rights Reserved

https://www.ehackingnews.com/2020/07/microsoft-office-365-users-targeted-by.html

▶



Version
Microsoft 365
Filter by title
Office 365 security
Overview
Deploy
Migrate
Prevent
Detect
Investigate
Respond
Detect and address compromised user accounts quickly
Detect and Remediate Illicit Consent Grants in Office 365
Detect and Remediate Outlook Rules and Custom Forms Injections Attacks in Office 365
Handle false positives/negatives
Admin review for reported messages
Recover from a ransomware attack
Remediate malicious email
Responding to a Compromised Email Account in Office 365
Review and approve (or reject) pending actions
Tune anti-phishing protection
Find and release quarantined messages as a user
Fix possible mail loop insight
Fix slow mail flow rules insight
Manage quarantined messages and files as an admin
Remove blocked users from the Restricted Users

Recover from a ransomware attack in Microsoft 365

06/05/2021 • 5 minutes to read • +4

> ⓘ **Important**
>
> The improved **Microsoft 365 security center** is now available. This new experience brings Defender for Endpoint, Defender for Office 365, Microsoft 365 Defender, and more into the Microsoft 365 security center. **Learn what's new.**

Applies to

- Exchange Online Protection
- Microsoft Defender for Office 365 plan 1 and plan 2
- Microsoft 365 Defender

Even if you take every precaution to protect your organization, you can still fall victim to a ransomware attack. Ransomware is big business, and the attacks are very sophisticated.

The steps in this article will give you the best chance to recover data and stop the internal spread of infection. Before you get started, consider the following items:

- There's no guarantee that paying the ransom will return access to your files. In fact, paying the ransom can make you a target for more ransomware.

  If you already paid, but you recovered without using the attacker's solution, contact your bank to see if they can block the transaction.

  We also recommend that you report the ransomware attack to law enforcement, scam reporting websites, and Microsoft as described later in this article.

- It's important for you respond quickly to the attack and its consequences. The longer you wait, the less likely it is that you can recover the affected data.

Step 1: Verify your backups

If you have offline backups, you can probably restore the encrypted data **after** you've removed the ransomware payload (malware) from your environment.

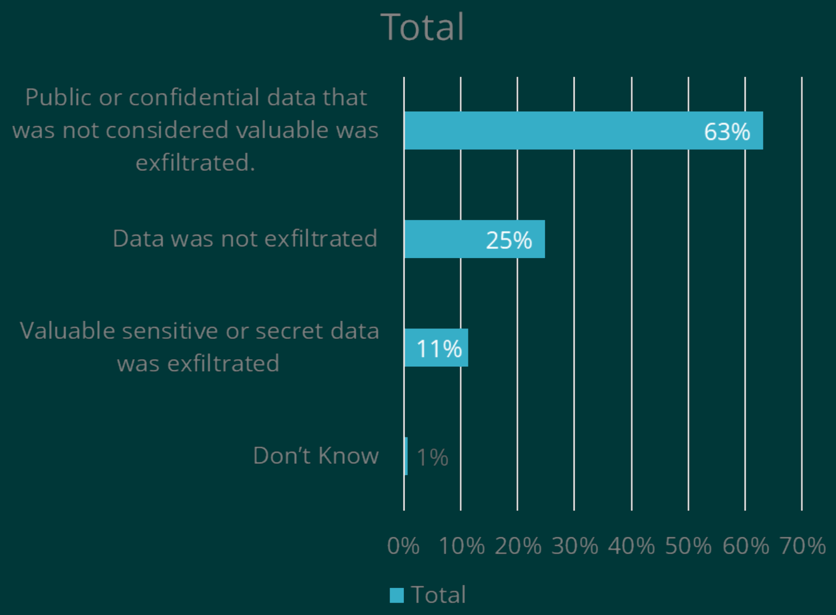
Is this page helpful?
Yes No

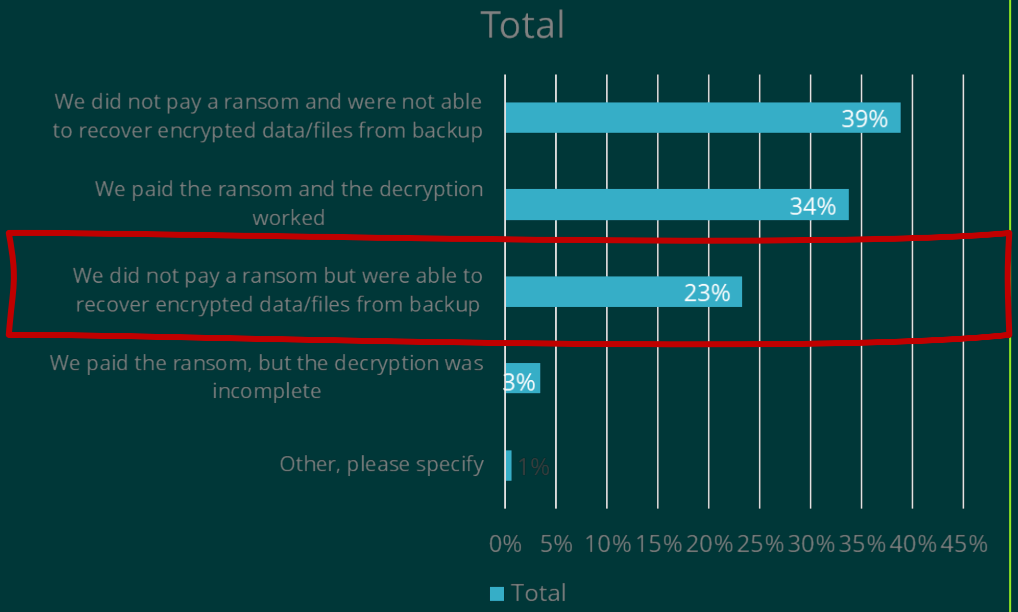
In this article

What Role do Backup Technologies Play in Organizations' Recovery From Ransomware Attacks?

Q. For your most recent ransomware incident, which of the following occurred?

Q. For your most recent ransomware incident, which of the of following occurred?





IDC #EUR148149921 (August 2021)
Source: IDC's *Future of Enterprise Resilience Wave 6 Survey*, 2021, Internal, July 1-15, 2021 (n = 430)

Veeam Backup *for Microsoft Office 365*

Veeam Backup *for Microsoft Office 365* eliminates the risk of losing access to your Office 365 data including Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams.

Securely backup to any location including on-premises or cost-effective cloud object storage and:

Protect your Office 365 data

from accidental deletion, security threats and retention policy gaps

Quickly restore individual Office 365 items and files

with industry-leading recovery flexibility

Meet legal and compliance requirements

with efficient eDiscovery of Office 365 backup data

veeAM

Planning your Office 365 Backup

Infrastructure components

There are three core components of this solution — backup server, backup proxy and backup repository.

Backup Server

The backup server is the central configuration and control component. It is responsible for setting up and managing other components, job scheduling, tasks coordination and more.

Backup Proxy

The backup proxy is the workhorse behind the scenes which conducts all the read and write activities. It provides an optimal route for backup traffic and enables data transfers to happen efficiently.

Backup Repository

The backup repository is the location where Office 365 data is stored. It uses a database format (JET DB) that is directly mounted to the proxy for local repositories.

Infrastructure Planning

Typically, the size of an environment dictates the deployment model. The size of an environment is not necessarily related to the number of Microsoft Office 365 users to protect. Instead, it’s based on the number of objects to protect.
The following objects are supported:

Microsoft Exchange

Primary mailboxes

Archive mailboxes

Shared mailboxes

Public folders

Resources mailboxes

Microsoft SharePoint

Collaboration sites

Communication sites

Personal sites

Microsoft OneDrive for Business

OneDrive for Business accounts

Microsoft Teams

Teams groups

Teams channels

Teams posts

Teams chats

Teams files

Teams tabs

Deployment options

Your Veeam Backup *for Microsoft Office 365* deployment can run in on-premises, private and public cloud environments. The prerequisites and how these components work for each environment are very similar.

On-premises deployments

Public cloud deployments

Supported storage

Veeam Backup *for Microsoft Office 365* support a variety of different storage options. Backup repositories are supported on the following types of storage:

Object storage

DAS
(Directly attached storage)

SAN
(Storage area network)

NAS
SMB (Server Message Block 3.0 and higher)

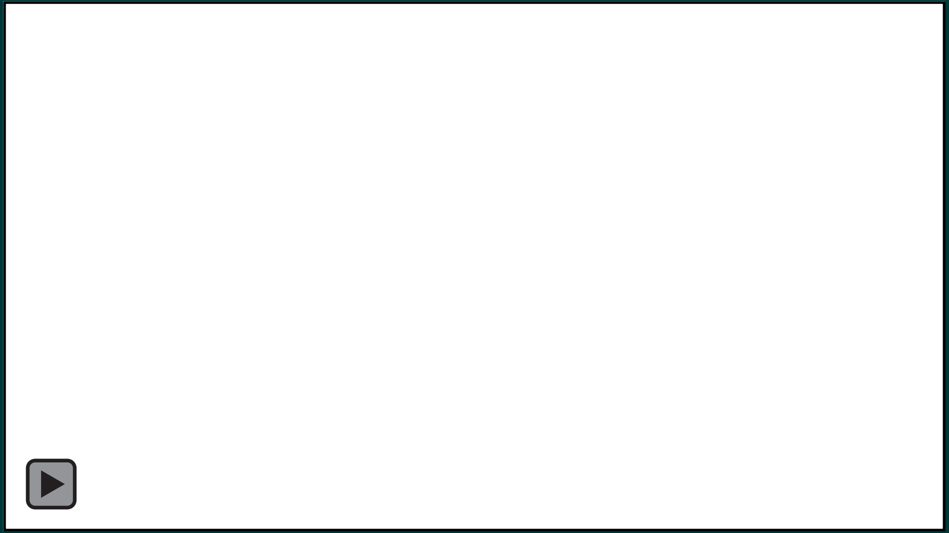
How to Backup and Restore M365 objects with Veeam

Creating a backup job

Creating a backup job

Creating a backup job in Veeam Backup *for Microsoft Office 365* is an easy, wizard-driven process.
There are 6 steps you will need to follow for the backup job setup:

1. Launch the New Backup Job wizard
2. Specify a backup job name
3. Select objects to back up
4. Select objects to exclude
5. Specify a backup proxy and repository
6. Specify scheduling options



Veeam Explorers

Veeam Explorers for Microsoft Exchange, Microsoft SharePoint, OneDrive for Business and Teams are designed to search and recover data between online, on-premises and hybrid Office 365 deployments.
There are 40 total restore options available.

Veeam Explorer *for Microsoft Exchange*

To explore and recover Microsoft Exchange mailboxes, folders, messages, tasks, contacts and items.

Veeam Explorer *for Microsoft SharePoint*

To explore and recover Microsoft SharePoint sites, libraries and items.

Veeam Explorer *for Microsoft OneDrive for Business*

To explore and recover Microsoft OneDrive for Business items and folders.

Veeam Explorer *for Microsoft Teams*

To explore and recover Microsoft Teams teams, channels, tabs, posts and files.

Veeam Explorers assist the architecture with the following tasks and use cases:

- In-place and out-of-place restores
- Browse content
- Search for content

How to restore 1-2-3

There are 3 major steps for restoring Office 365 data with Veeam. In this example we'll show how to restore data of a Teams file.

1. Launch the Restore wizard and select restore scope
2. Choose whether you want to use modern or basic authentication.
3. Authenticate into your Microsoft Office 365 organization.

Key Difference Makers

There are some key benefits that Veeam Backup *for Microsoft Office 365* can provide over other vendors. Many backup vendors do not offer the flexibility or functionality necessary to tailor data protection to specific business needs.

Complete Flexibility

Maintain ownership of data by choosing any infrastructure that fits your business need and change it whenever required with support for nearly any cloud or hardware platform.

Customizable Backup No Vendor Lock-in

Maintain control by delivering the appropriate level of protection to different users according to the business value of their data.

Many Recovery Options

Minimize business downtime by recovering data in the way that makes the most sense, no matter the kind of data loss.

Licensing

Subscription per user

Veeam Backup *for*
Microsoft Office 365

Support for…

Exchange Online and
on-premises Exchange

SharePoint Online and
on-premise SharePoint

OneDrive for Business

Teams for Business

…included in one solution.

Production 24/7 Support included

VEEAM

Sales & Technical Inquiry

Contact Us and get a FREE 30-day trial

Chris Tong

Sr. Systems Engineer | Veeam
chris.tong@veeam.com

Kathy Wong

Territory Manager | Veeam
Kathy.wong@veeam.com
+852 559 88761