nexetic

BackITUP!
SECURE CLOUD

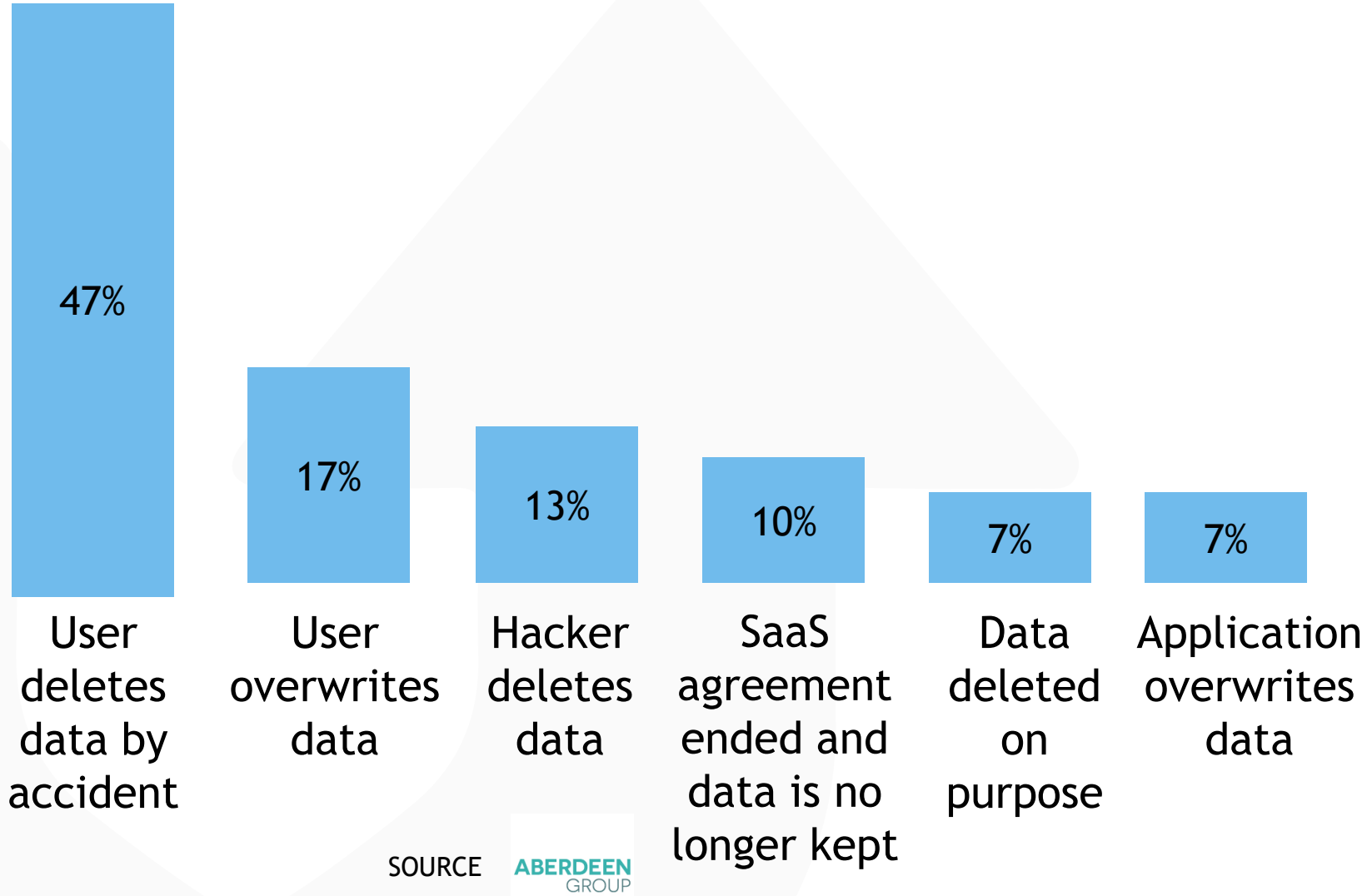
Microsoft

ALSO

Available in the ALSO Cloud


95%
“Through 2022, at least 95% of cloud security failures will be the customer’s fault.”
Gartner
nexetic

REASONS FOR DATA LOSS IN CLOUD



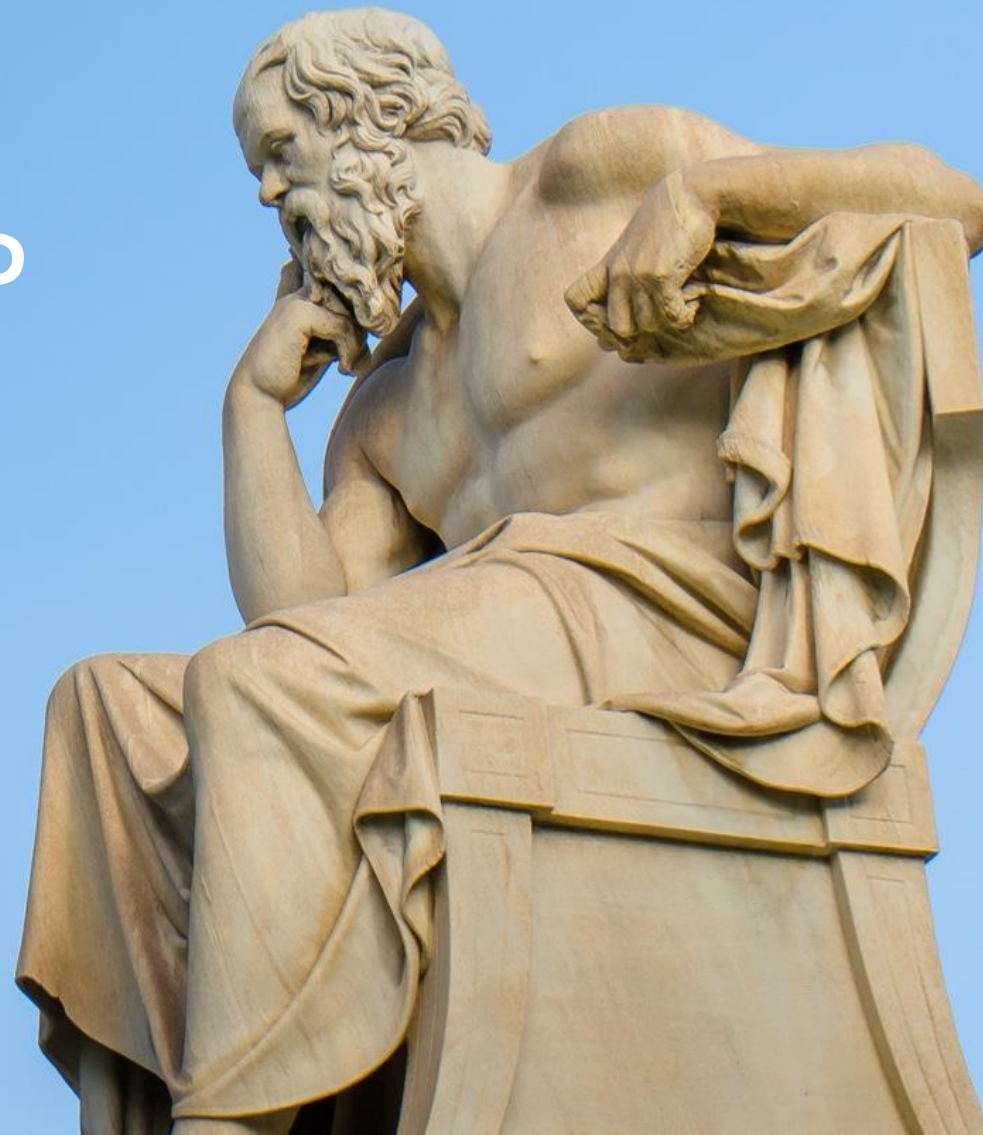
SOURCE ABERDEEN GROUP

nexetic

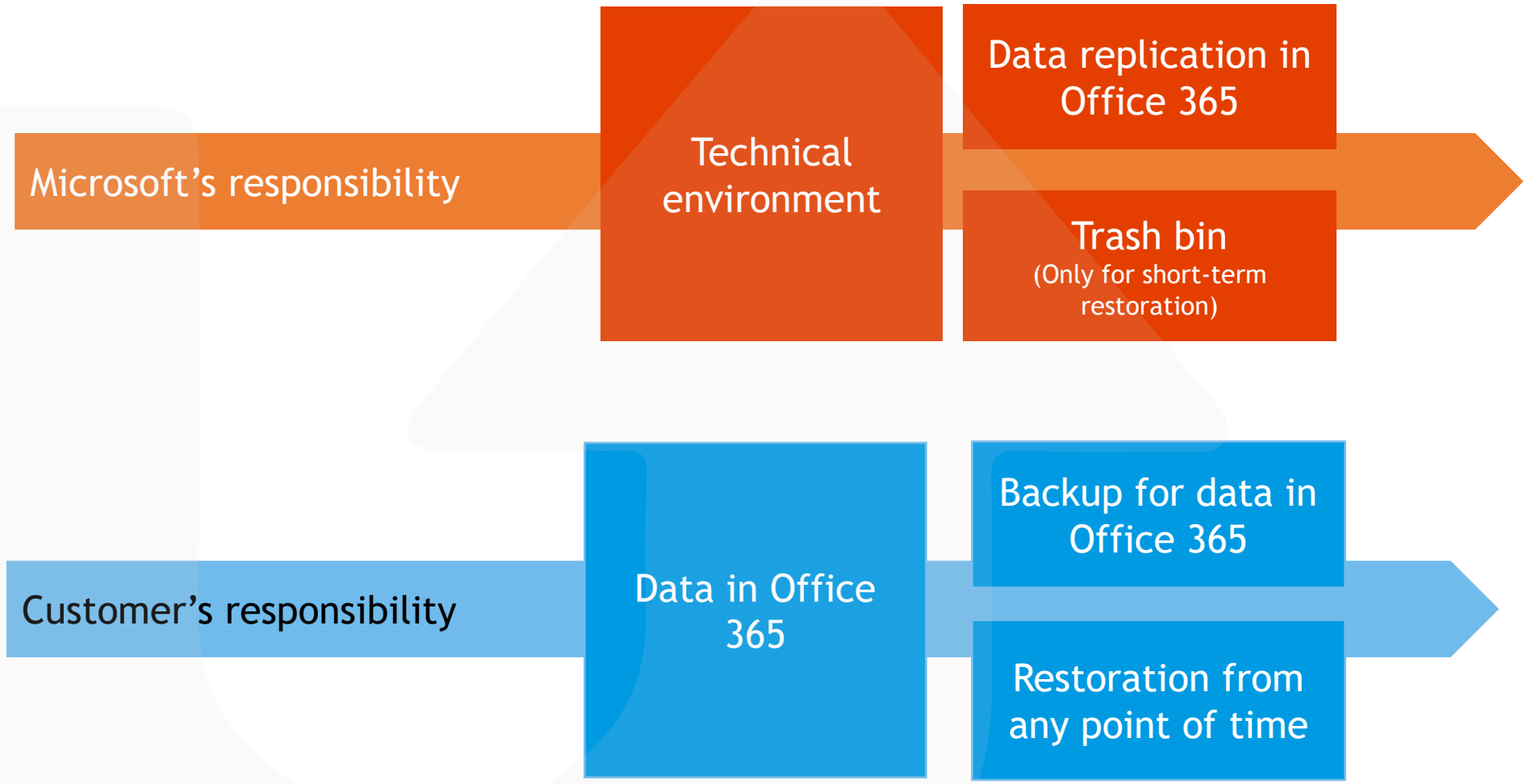
Biggest Cloud Security Threats

1. Data breaches
2. Human error
3. Data loss
4. Ransomware
5. Internal risks
6. Service interruptions

ISN’T O365’S OWN BACKUP ENOUGH?

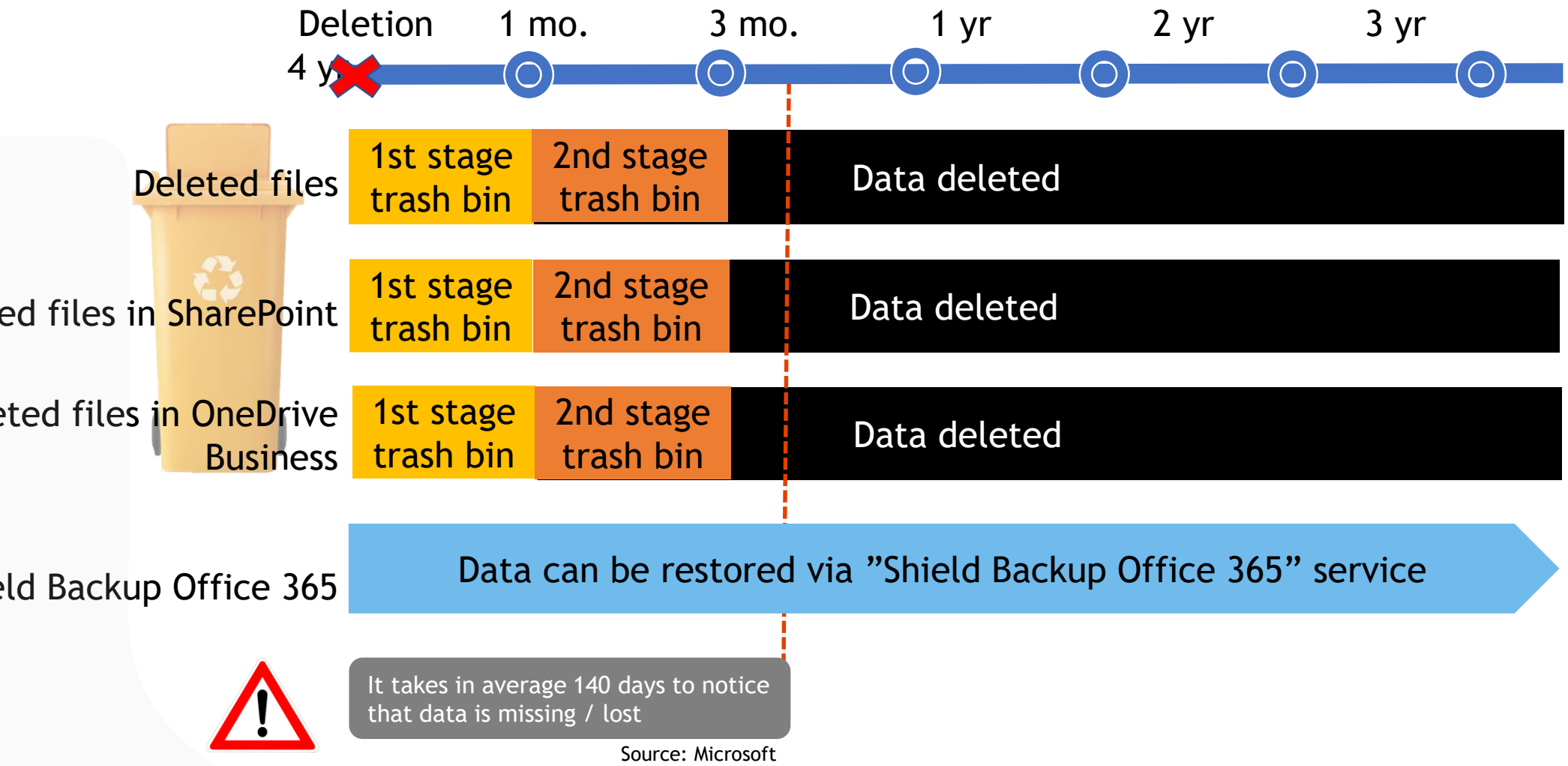


SHARED RESPONSIBILITY IN OFFICE 365



nexetic

DELETED FILES IN O365



Source: Microsoft

nexetic

RANSOMWARE AND RECOVERING

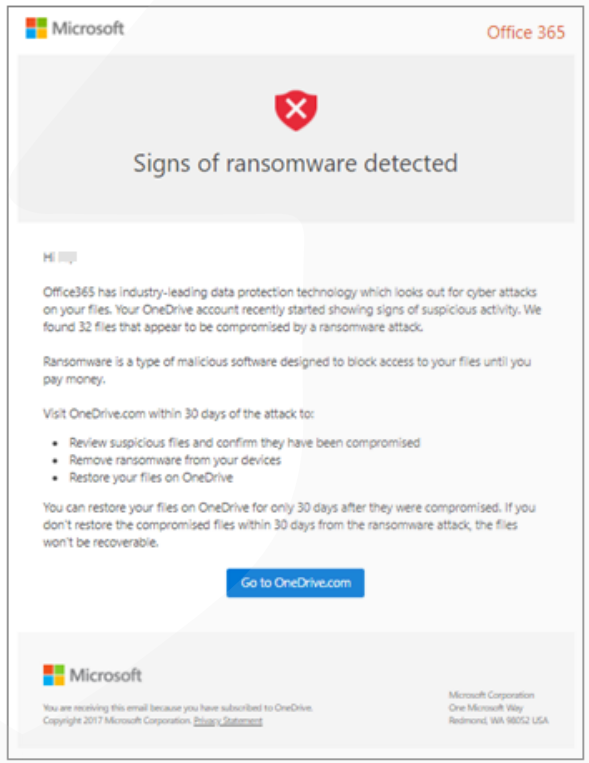
Ransomware detection and recovering your files

OneDrive

For Office 365 Home and Office 365 Personal subscribers, Ransomware Detection notifies you when your OneDrive files have been attacked and guides you through the process of restoring your files. Ransomware is a type of malicious software (malware) designed to block access to your files until you pay money.

When Office 365 detects a ransomware attack, you'll receive an email from Microsoft Office 365.

1. Click the link in the email or go to the OneDrive website, and we'll walk you through the recovery process, which includes:
2. Confirm your files are infected.
3. Clean all your devices.
4. Restore your OneDrive.


Microsoft Office 365

Signs of ransomware detected

Hi

Office365 has industry-leading data protection technology which looks out for cyber attacks on your files. Your OneDrive account recently started showing signs of suspicious activity. We found 32 files that appear to be compromised by a ransomware attack.

Ransomware is a type of malicious software designed to block access to your files until you pay money.

Visit OneDrive.com within 30 days of the attack to:

- Review suspicious files and confirm they have been compromised
- Remove ransomware from your devices
- Restore your files on OneDrive

You can restore your files on OneDrive for only 30 days after they were compromised. If you don't restore the compromised files within 30 days from the ransomware attack, the files won't be recoverable.

Go to OneDrive.com

Microsoft

You are receiving this email because you have subscribed to OneDrive.
Copyright 2017 Microsoft Corporation. Privacy Statement

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 USA

Office 365, the impact from a ransomware attack can be multiplied

Files stored in SharePoint Online or OneDrive for Business, the infected files will overwrite those files immediately on the next sync cycle, potentially impacting other users sharing the same files, even if they themselves have not been infected.

Step 1: Make sure you have a backup of your files

We cannot guarantee that you will be able to recover your data. Make sure that you have a backup as we previously discussed under the "*Regularly backup your files*" section of this blog post.

Step 2: Disable ActiveSync & OneDrive Sync

Disable Active Sync and pause OneDrive for Business Sync. If you have them enabled, it is possible that they will overwrite your files.

ActiveSync is the service that allows your Email in Exchange Online to sync to Office 365. If you suspect your email data may be targeted by the Ransomware, you should disable ActiveSync temporarily to protect the data in the cloud from being targeted. To disable ActiveSync, you can run the following script in PowerShell:

nexetic

SHIELD BACKUP
Office 365

DEMO AT NEXETIC TABLE IN THE CINEMA HALL

nexetic

MAKE IT SIMPLE

- Backup for O365 Mail
- Backup for Calendar
- Backup for Contacts
- Backup for OneDrive for Business
- Backup for SharePoint
- Stored data is encrypted with 256-bit AES encryption keys
- Only changed data is backed up

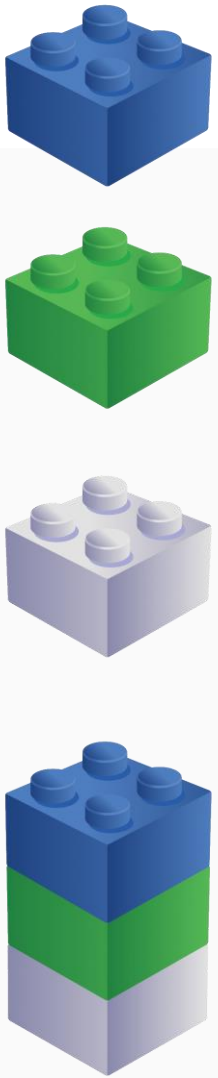
- One-click data restoration
- Automatic backup
- Possibility to start backup manually
- Full + granular backup & restore
- Restoring previous version(s)
- Archiving
- Audit log

New: OneNote + Planner + GDPR Q2-2019

SHIELD BACKUP Office 365

nexetic

BUNDLING DRIVES SALES



Microsoft Office 365

Shield Backup Office 365

Shield Backup Win + Mac

ALSO
Available in the ALSO Cloud

ALSO Cloud Marketplace is the best place to buy Nexetic licenses.

When you buy Microsoft licenses or computers from ALSO you can also buy Nexetic licenses and grow your service business.

nexetic

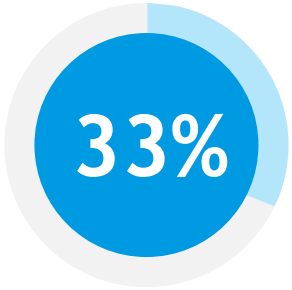
NEXETIC IN A NUTSHELL

NEXETIC IS DELIVERING CORE BUILDING BLOCKS FOR MODERN IT

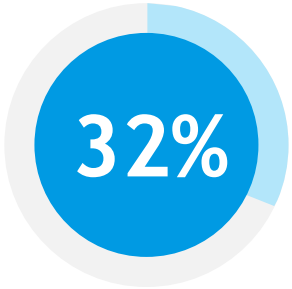
- Nexetic since 2008
- Internal support + R&D (Finland)
- Shield Backup Office 365
- Shield Backup Gsuite
- Shield Backup Win+Mac
- Shield Backup Server (Q2)

"WE PROTECT YOUR CUSTOMERS` VALUABLE DATA"

- ALSO Finland 2016
- Nexetic Scandinavia 2018
- > 500 Managed Service Providers
- MSP profit margin 25-42%
- > 4000 Business Customers



of corporate data is on endpoints



of companies have lost data on cloud

nexetic

Thank you!

nexetic

Microsoft

ALSO
Available in the ALSO Cloud