

# Quest Platform Management Virtual Summit 2020

## Office 365 & Azure AD Enterprise Recovery Tips for IT Pro's

Speaker: Marc Koeneman

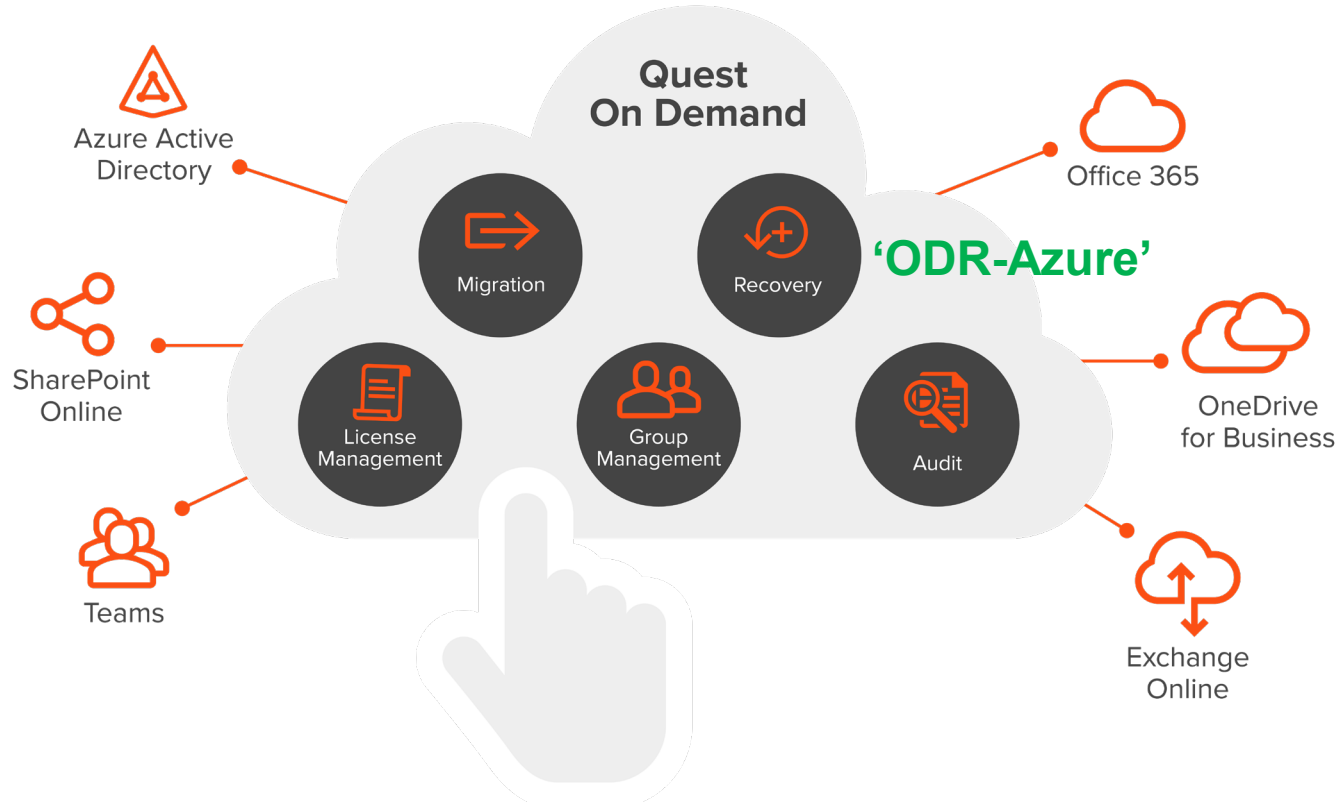
Sales Consultant Quest Netherlands



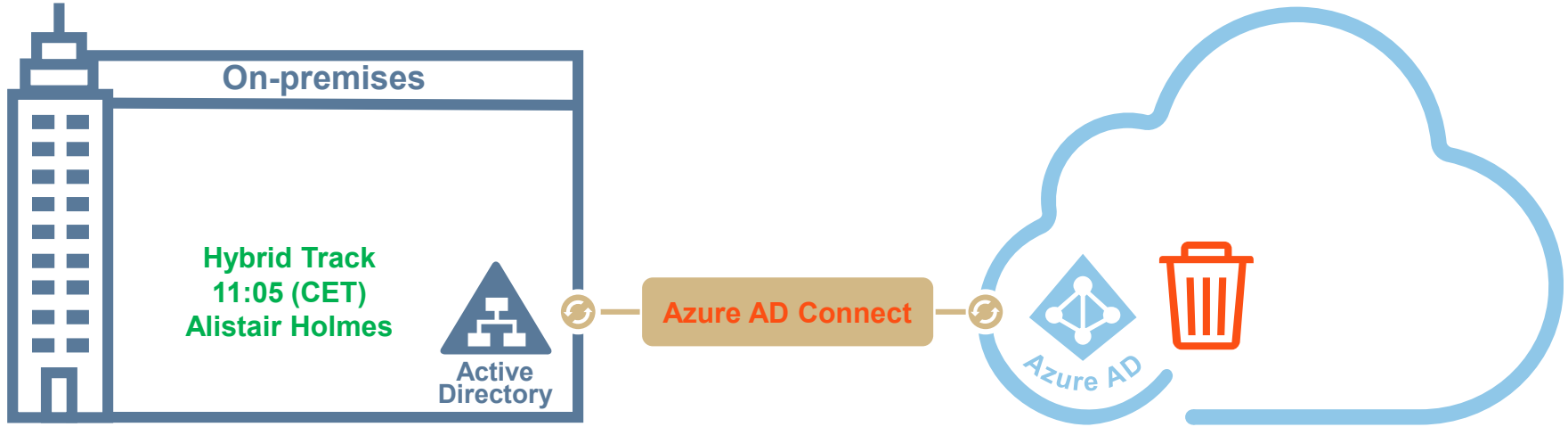
# Agenda

- **Quest On Demand**
- **Hybrid environments**
- **Use Case scenario's**
  - Groups
  - Users
  - Applications
  - Settings
- **Short Demo**
- **Final Thoughts...**

# Quest® On Demand



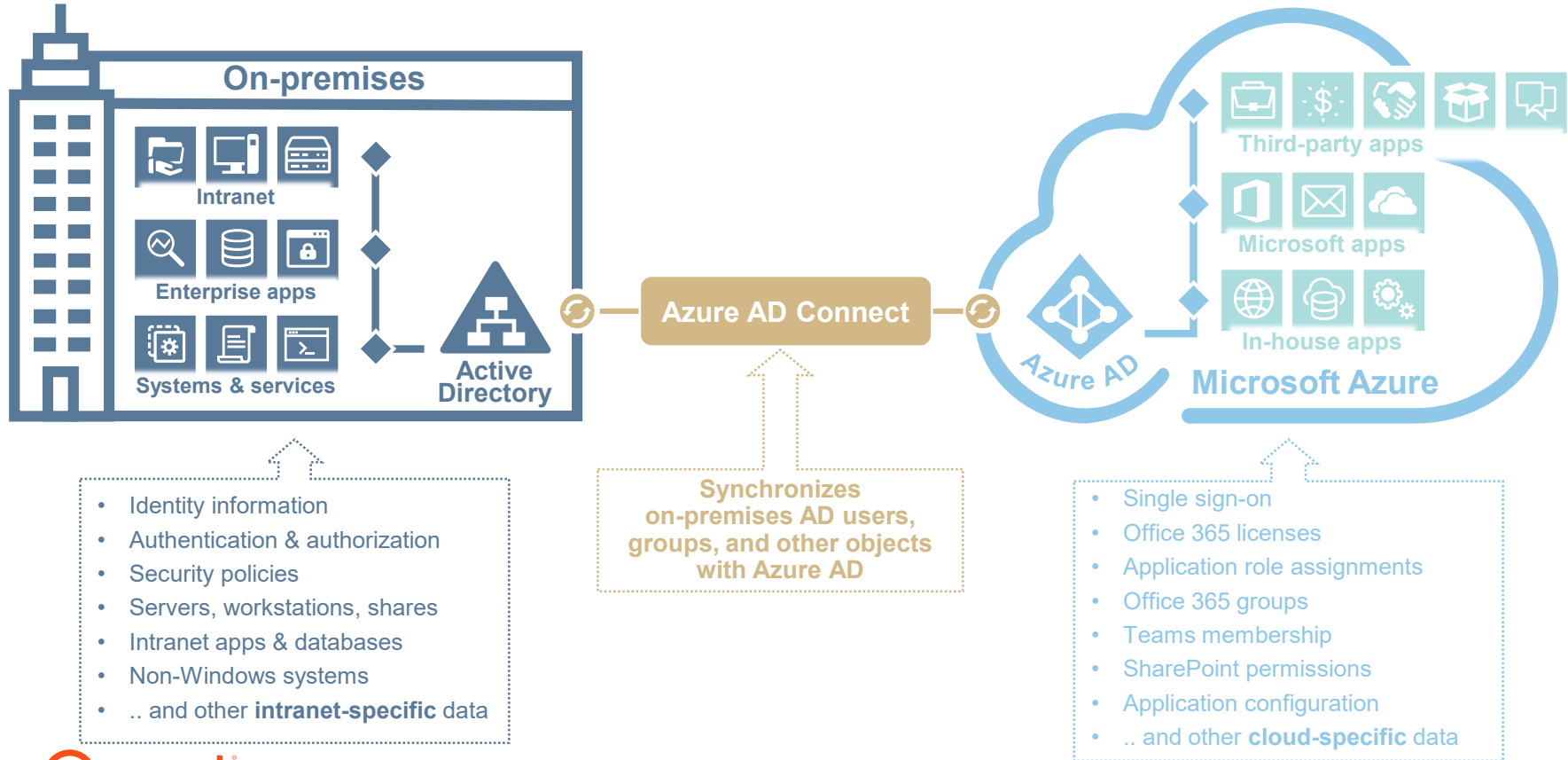
# Hybrid environment overview



# Poll 1 / 3

- What setup do you have:
  - 1) Cloud Only (Azure AD/O365)
  - 2) Hybrid (On Prem AD + Azure AD/O365)
  - 3) On Prem Only (On Prem AD Only)
  - 4) Other

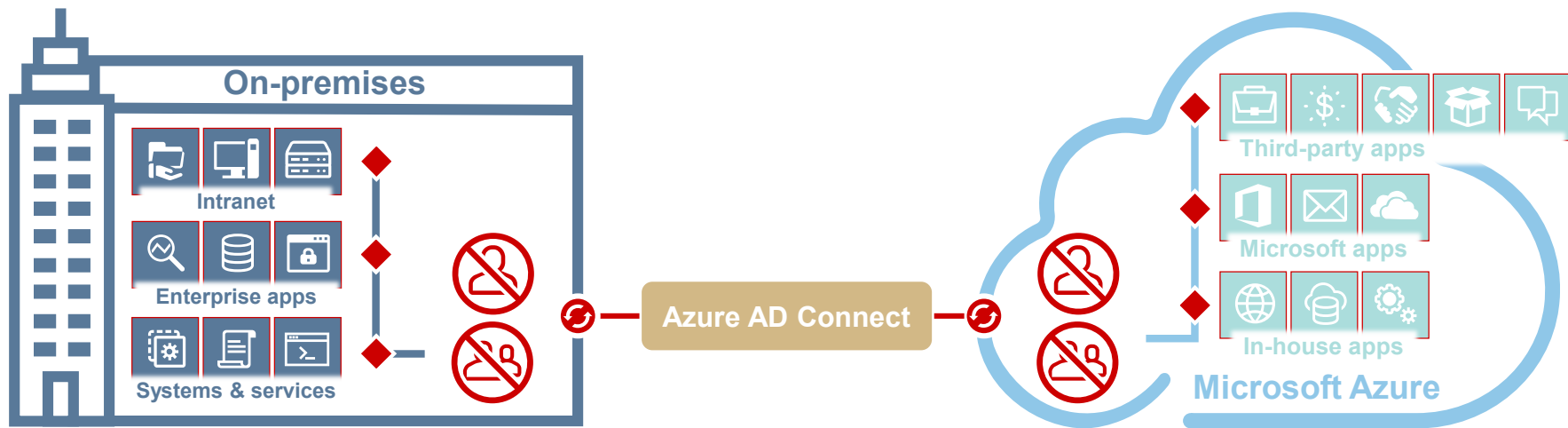
# Hybrid environment






# Poll 2 / 3

- **Do you think you have a proper recovery plan for your Azure Active Directory?**
  1. Yes
  2. No
  3. Do we actually need one?

# What if I **delete** a hybrid user or group?

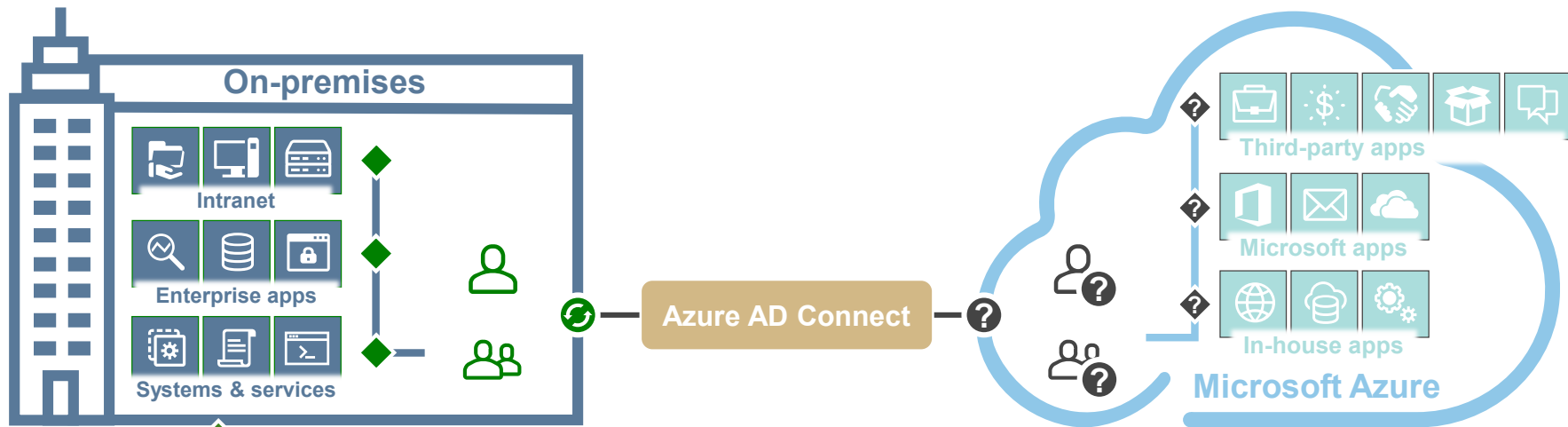


**Azure AD Connect will do its job and deletes the pair in Azure AD:**

-  **All cloud-specific account properties are lost.** Including license assignments, applications and data access.
-  By default, synchronization runs **every 30 minutes**. There's a pretty good chance it's done before you roll back the changes.
-  Removing the account from sync **automatically deletes** the matching Azure AD user. This might happen if you accidentally change the OU.



# Oops, it was the **wrong one!**



Q

Fortunately, I have up-to-the-date **RMAD backup**.  
Can I restore from it and wait for Azure AD Connect to sync the cloud?

A

**SUCCESS IS NOT GUARANTEED!**  
On-premises AD doesn't have cloud data.

Restoring  
a hybrid  
group ▶

Restoring  
a hybrid  
user ▶

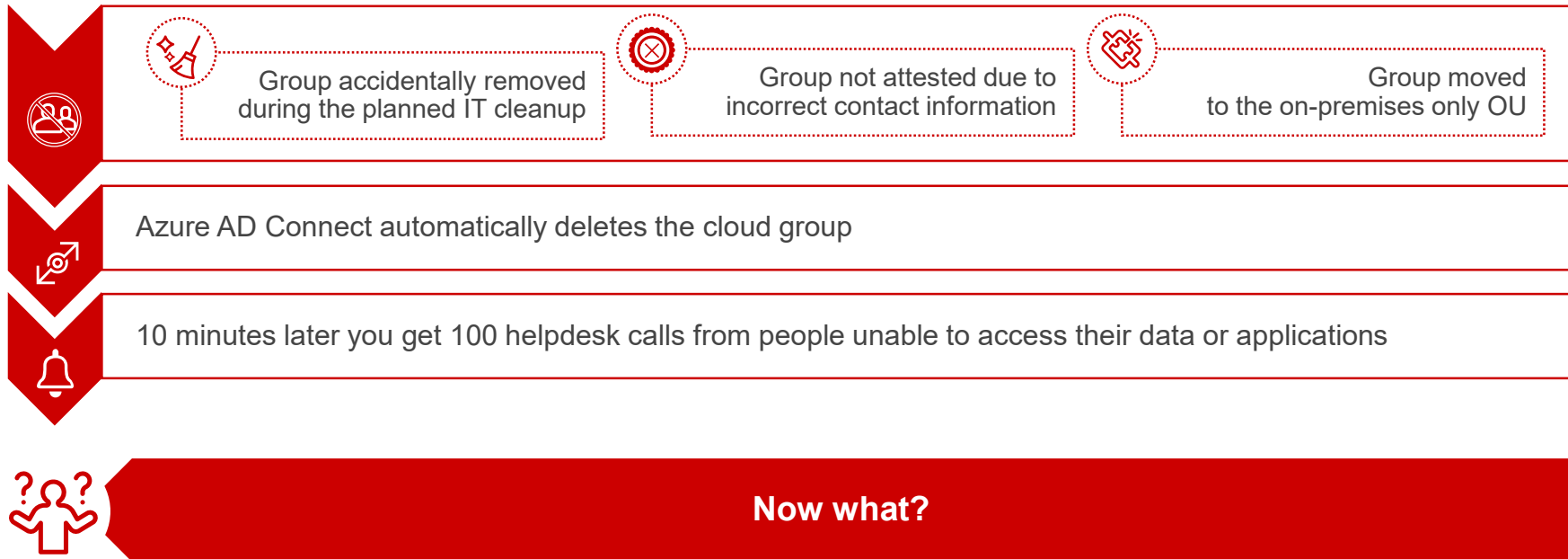


# Restoring a hybrid group

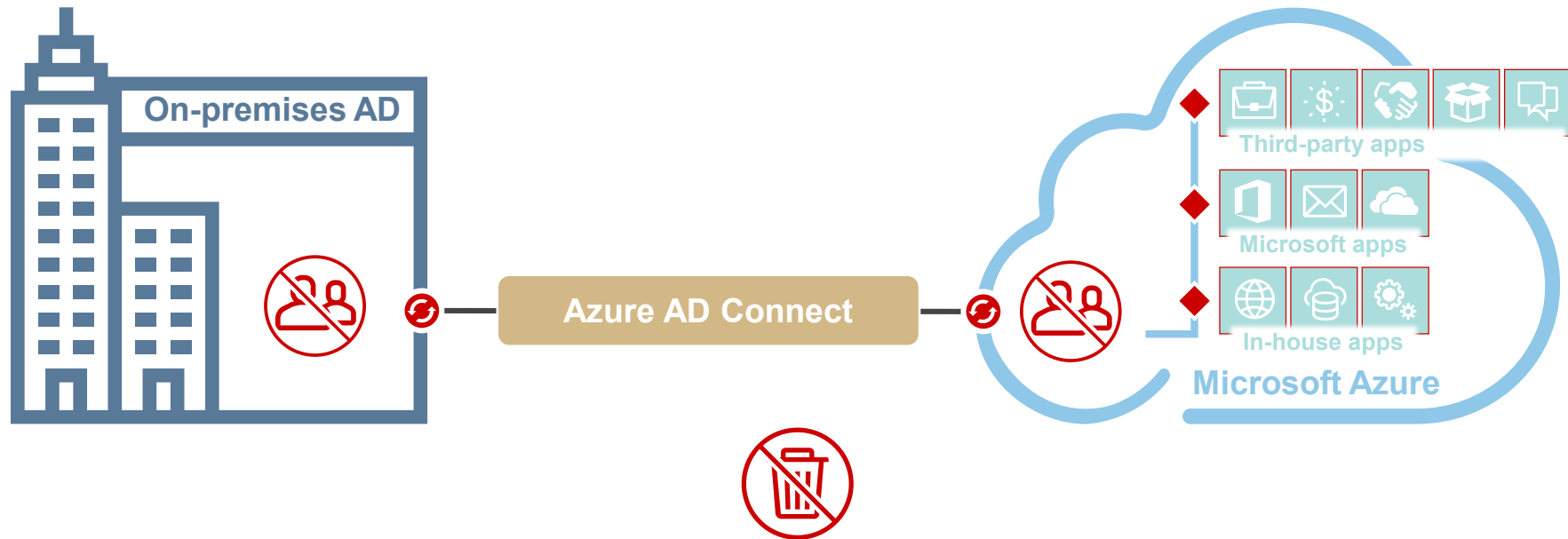
without  
On Demand Recovery

Quest

# Accidental deletion of a hybrid group



# Azure AD groups are **permanently deleted!**

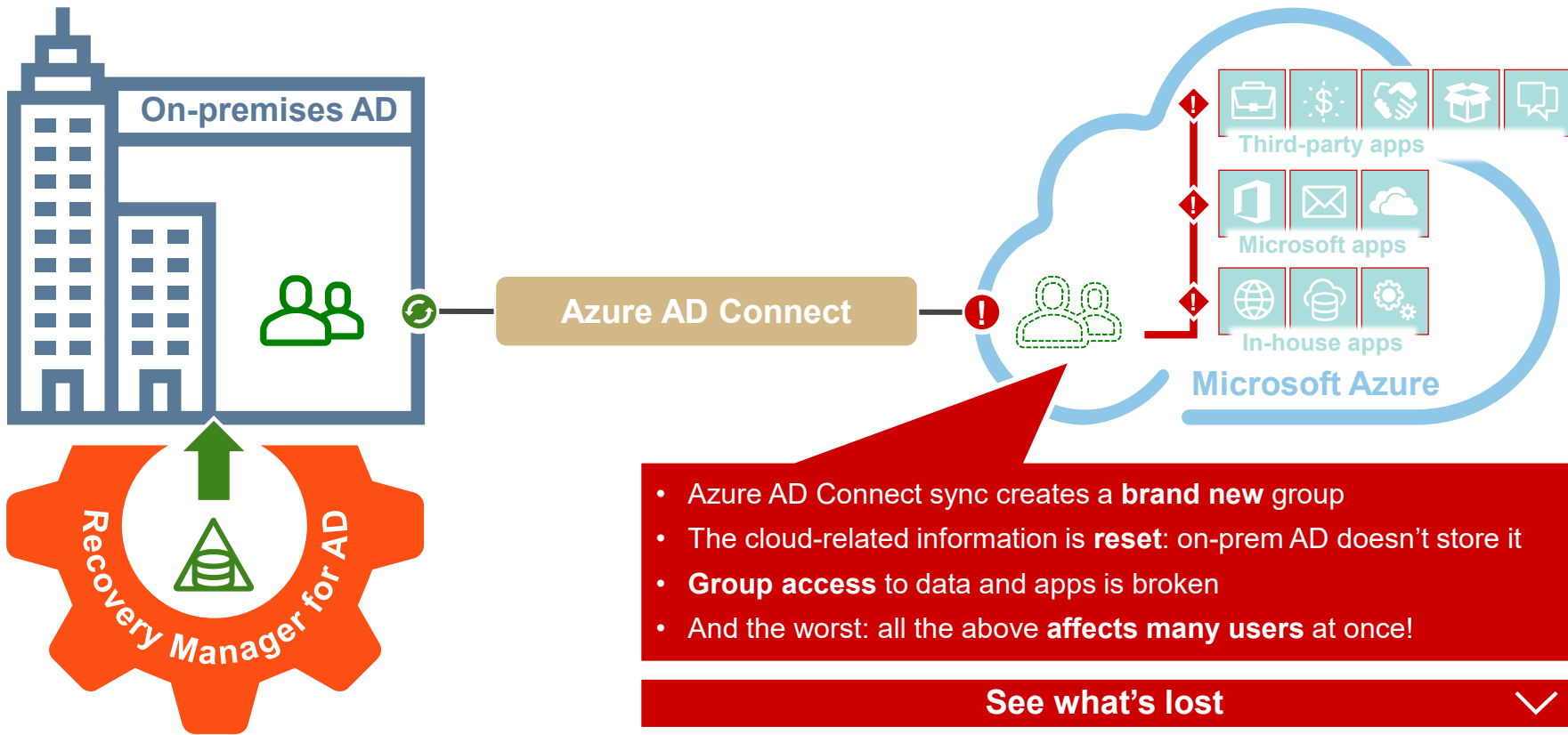


## Deleted groups

Deleted Microsoft 365 groups will be shown here for 30 days before the group and its associated data are permanently deleted. If you need to, you can restore a Microsoft 365 group and its data within this period. **All other group types are permanently deleted immediately.**

The

# Restoring a group



# What's lost without On Demand Recovery?

## Cloud data restored with On Demand Recovery

vs

## Without On Demand Recovery

- ✓ Applications Role assignments
- ✓ Conditional Access Policies
- ✓ Office 365 Licenses
- ✓ SharePoint Group membership
- ✓ Membership in the cloud-only groups

Azure AD Recycle bin is of no use, it **doesn't work with these groups**



Azure Active Directory Connect causes **issues**



On-premises changes might result in **damaging cloud environment**



Troubleshooting is **too complex**



# Hard-delete Office 365 or Teams group

Affected data, restored by On Demand Recovery

vs

Challenges & limitations of the native tools



Group Membership and Owners



Application Role assignments



Conditional Access Policies

Complex relations between groups and Office 365 apps



Group management complexity



Broken membership cannot be restored from Recycle Bin



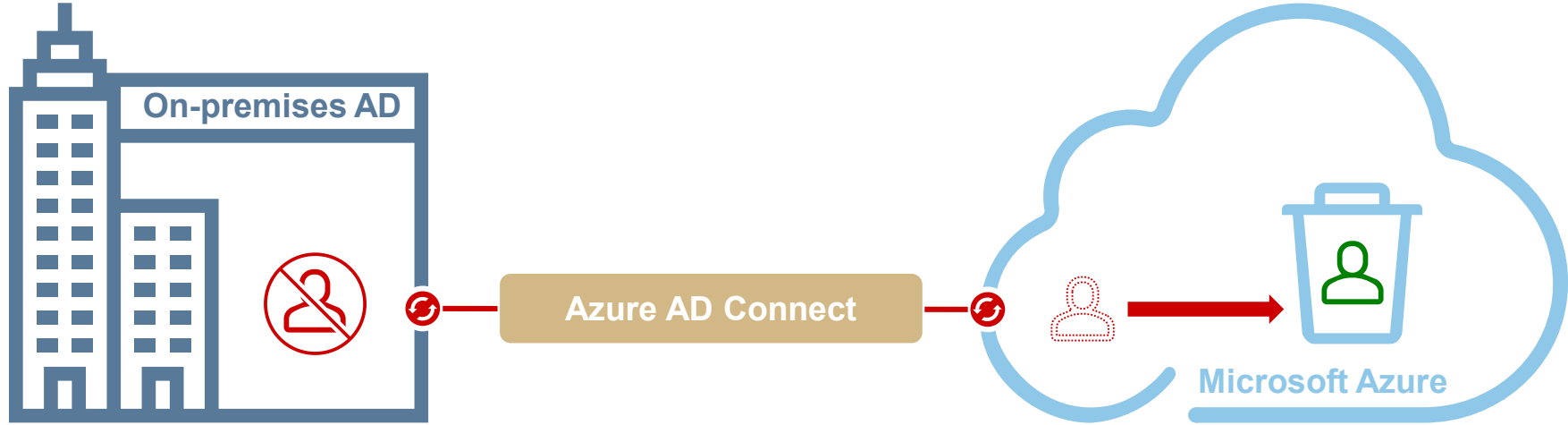
# Restoring a hybrid user

without  
On Demand Recovery



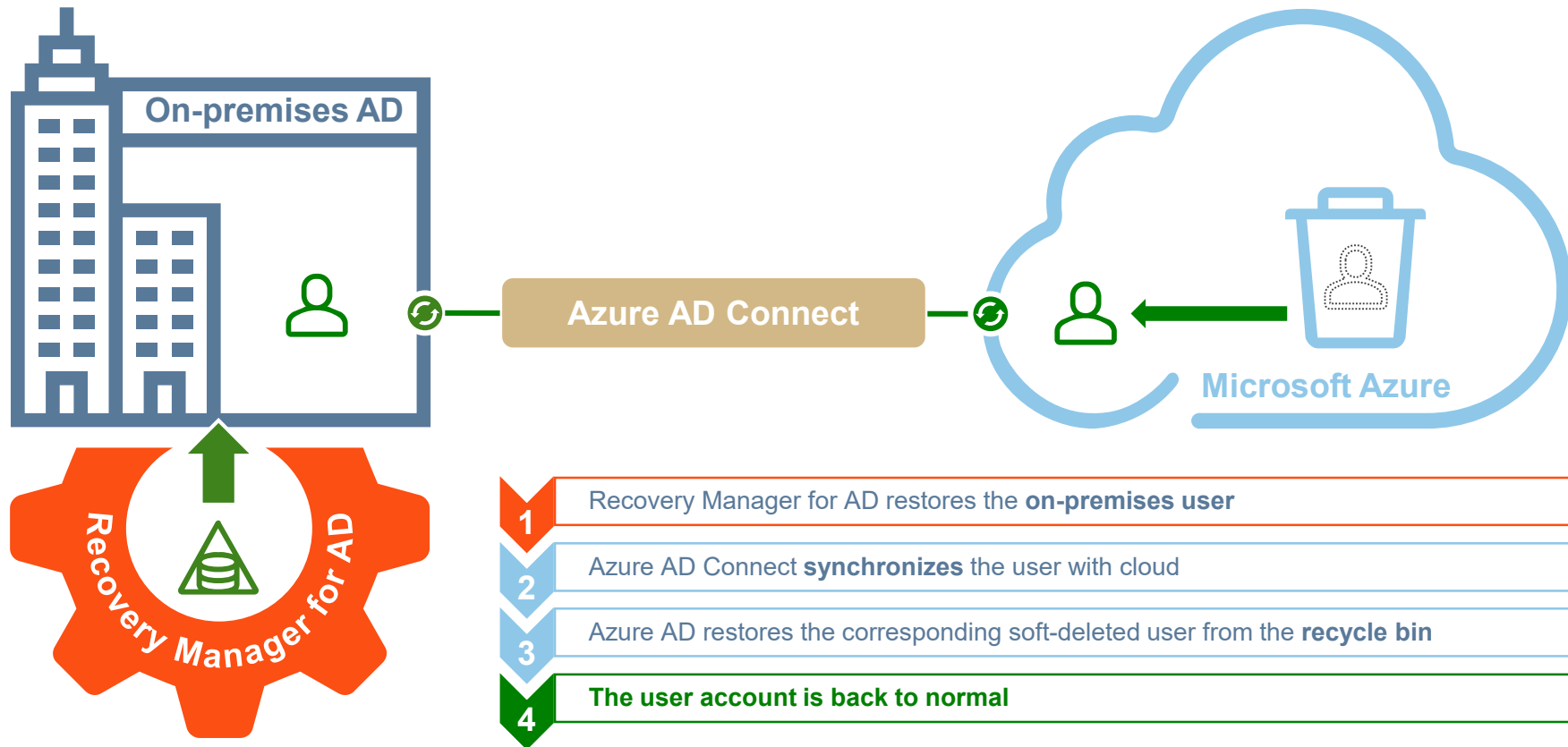


# Good news: Azure AD has a “user recycle bin”

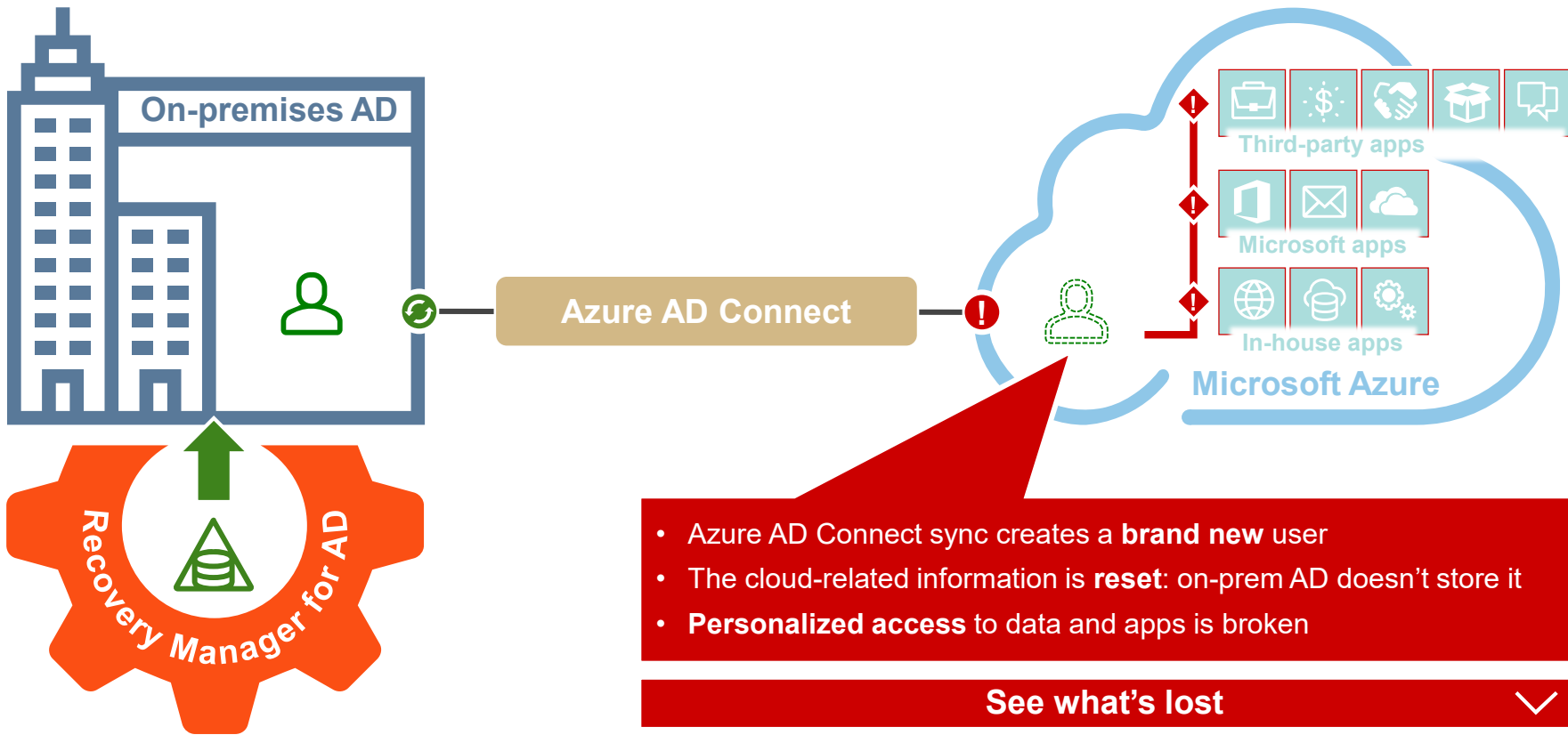


By default, Azure AD keeps the deleted user in “soft-deleted” state for 30 days

# Restoring a soft-deleted user



# Restoring a **permanently deleted** user



# What's lost without On Demand Recovery?

## Cloud data restored with On Demand Recovery

vs

## Without On Demand Recovery

- ✓ Office 365 licenses
- ✓ Mailbox
- ✓ Application role assignments
- ✓ Office 365 groups & Teams membership
- ✓ Multi-factor authentication & password reset configuration
- ✓ Azure AD Roles membership
- ✓ Conditional Access Policies rules
- ✓ Custom properties for cloud applications
- ✓ SharePoint Group membership

Synchronizing with Azure AD Connect won't help, on-premises AD **doesn't** contain this data



Bulk restores are **tedious** & **error-prone**



Manual restore might be **very difficult** without the required knowledge



# Hard-delete B2B or B2C user

Affected data, restored by On Demand Recovery

vs

Challenges & limitations of the native tools



Registration info: email, phone, geo



Office 365 groups & Teams membership



Multi-factor authentication & policies

Incident publicity might result in **reputational risks**



Broken channels of communication might cause the **business interruption**



Bulk restores are **hard**



# Delete application

Affected data, restored by On Demand Recovery

vs

Challenges & limitations of the native tools

- ✓ User and groups in role assignments
- ✓ SAML configuration
- ✓ User Attributes and claims
- ✓ Permissions
- ✓ Conditional Access Policies
- ✓ Application Configuration

Recycle bin **doesn't hold** this data



Azure Active Directory Connect **doesn't help**



**No way to automate** configuration with PowerShell



Manual re-configuration is **(too) complex**



Third-party apps (SFDC, Concur, etc.)



Microsoft apps



In-house apps

# Delete Conditional Access Policies (CAP)

Affected data, restored by On Demand Recovery

vs

Challenges & limitations of the native tools



All properties



Include and exclude lists of users and groups



Named Locations

Consider the example:

1. Users from Europe need to have MFA configured (CAP with MFA)
2. Only users from Europe can access Azure applications. (CAP)

## Scenario:

CAP or MFA policy is (accidentally or maliciously) deleted

MFA settings and other CAP settings can not be restored...

Risk of sensitive data leak



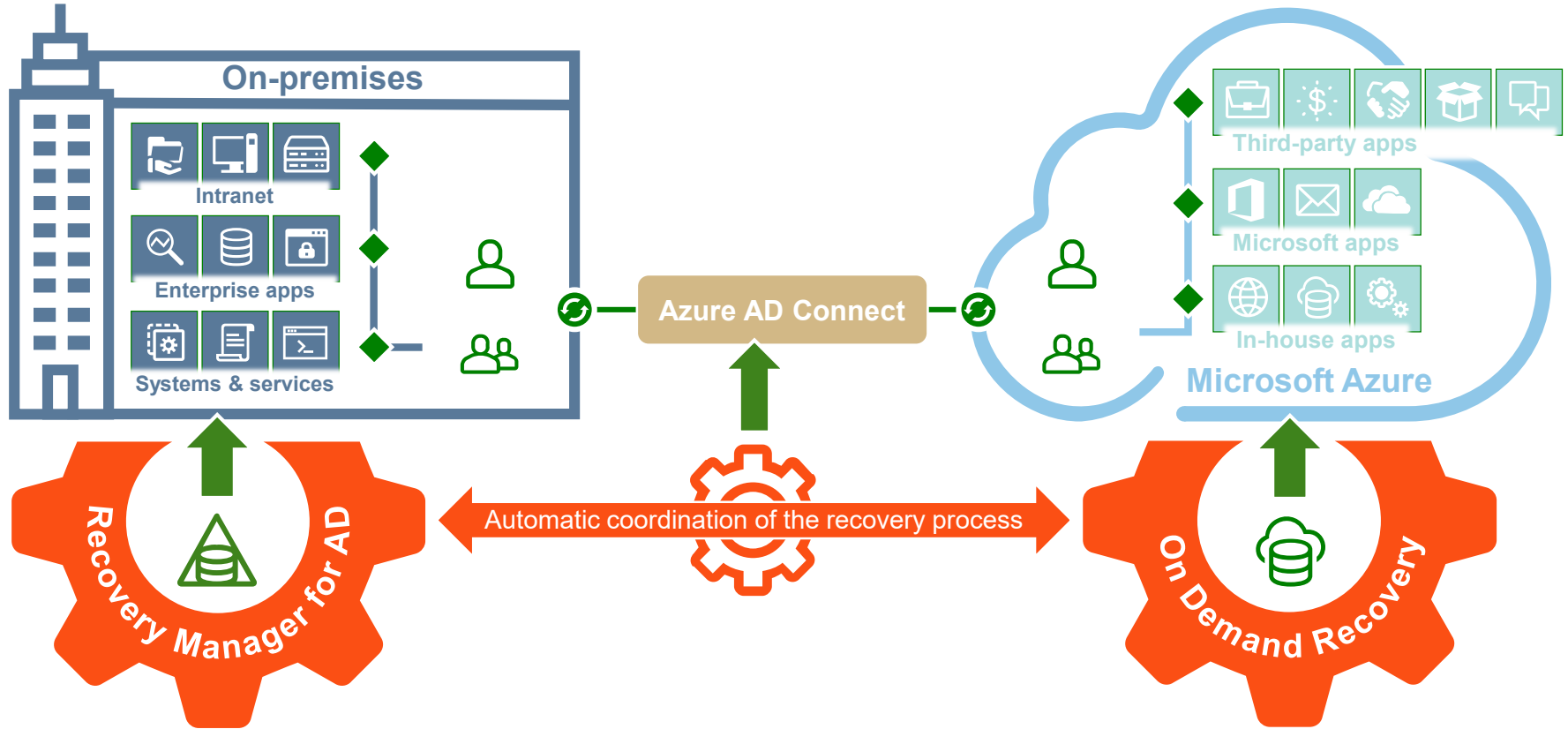
No way to export and import policies



Cannot be restored from Recycle Bin

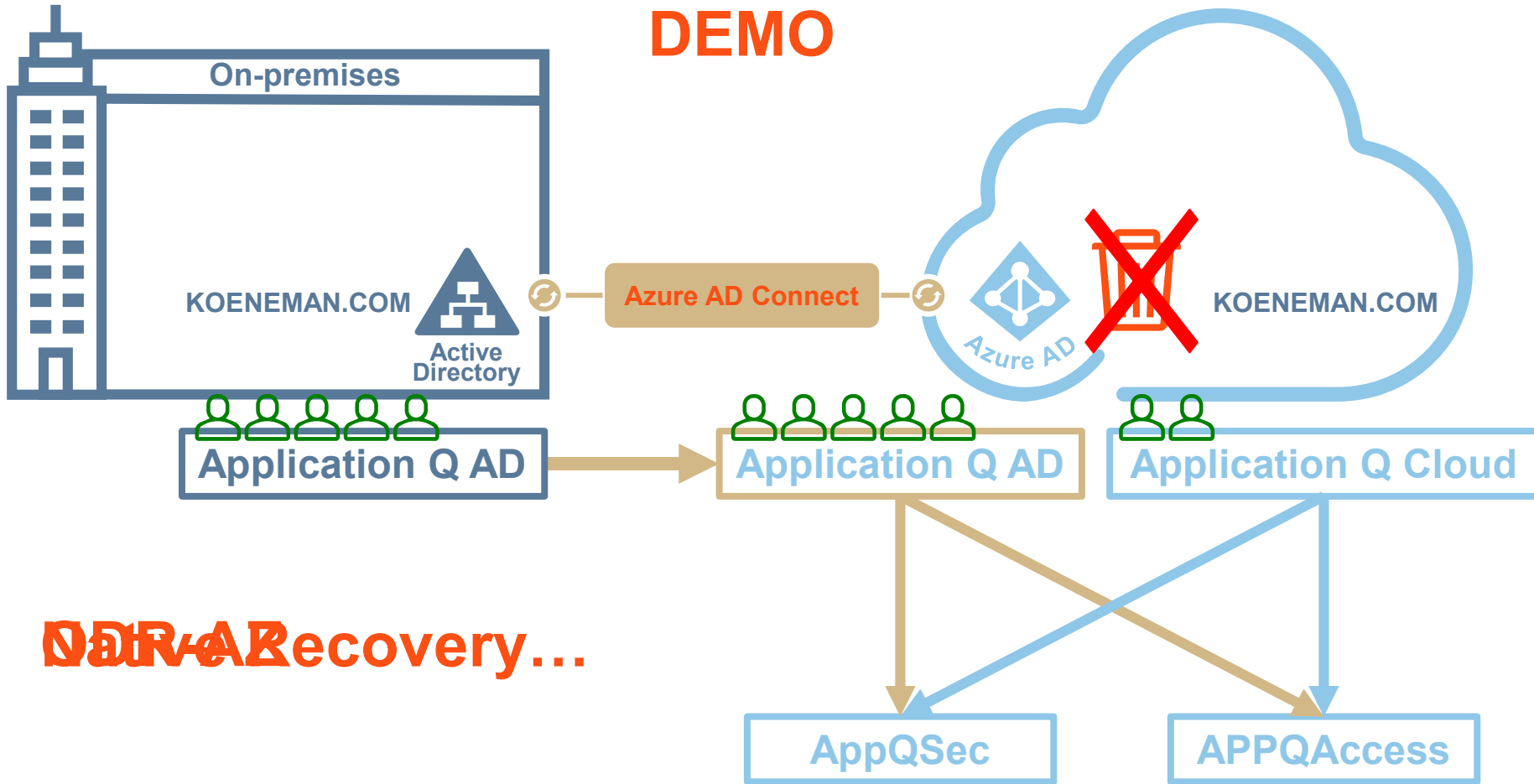


# Hybrid recovery solution





# DEMO

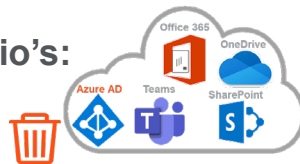


~~DR~~ Recovery...

Quest

# Final Thoughts

- On Demand earns ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2019 Certifications
- Presentation is about Hybrid, but think about Cloud Only scenario's:
  - No automatic re-creation of AD objects by AA-Connect
  - No real 'Backup' of Azure AD information
- Recycle bin is for 'deletions' to be undone....  
But where do 'changes' go?  
Also consider malicious changes...



Your options are:



quest<sup>TM</sup>

# Poll 3 / 3

- Do you **STILL** think you have a proper recovery plan for your Azure Active Directory?
  1. Yes
  2. No
  3. ~~Do we need one?~~

# Azure AD recycle bin limitations



Only keeps deleted objects for 30 days



No reporting to identify or search what you need to restore



You can't restore specific user attributes or Application, MFA and Conditional Access Policy configurations



Some objects cannot be recovered at all – AAD groups, group membership, hard deletes



You can't restore in bulk without PowerShell



You can't restore objects across tenants



Restore multiple objects and attributes at one time

# QUESTions?

Active Directory & Office 365 management  
End-to-end support for your next Microsoft  
challenge

For more information on O365, Hybrid O365 check out our solutions pages:

<https://www.quest.com/solutions/microsoft-platform-management/>

Feel free to reach out to me with any questions.

[Marc.Koeneman@quest.com](mailto:Marc.Koeneman@quest.com)

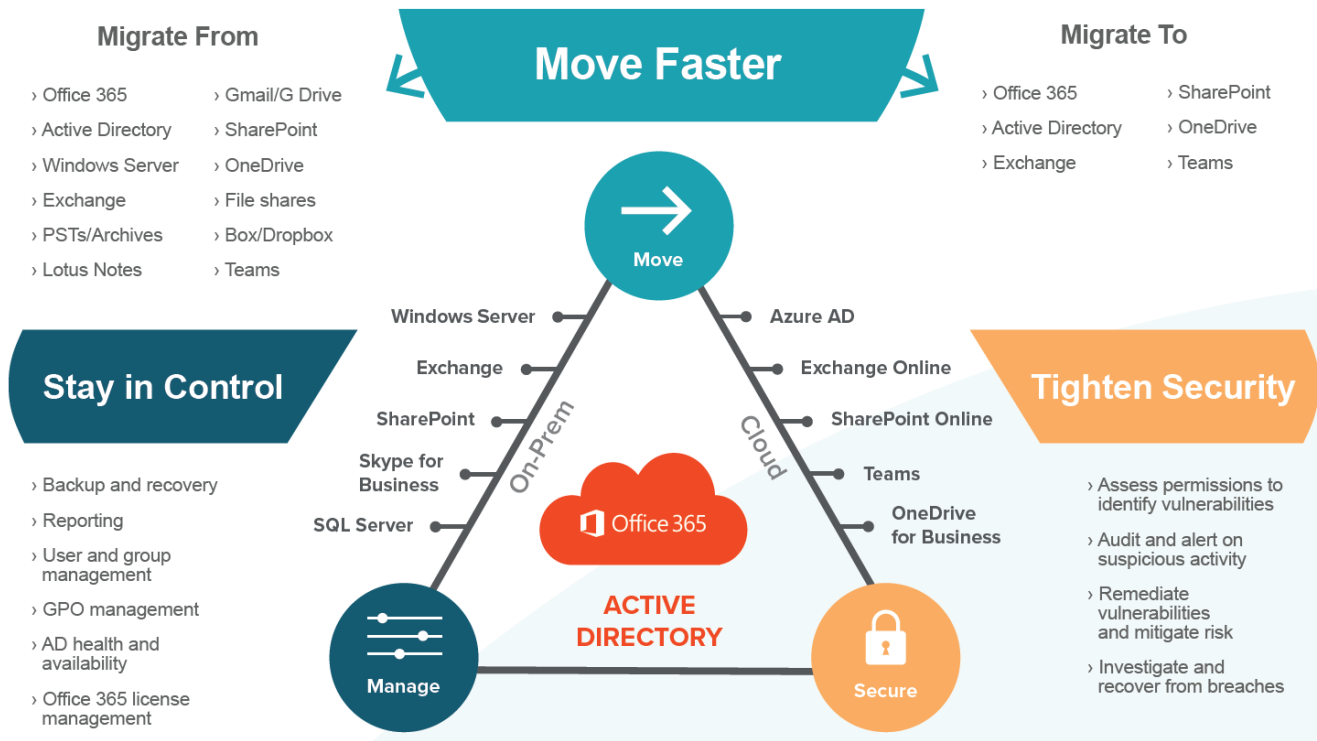
Free Trials:

<https://quest-on-demand.com/>

Quest

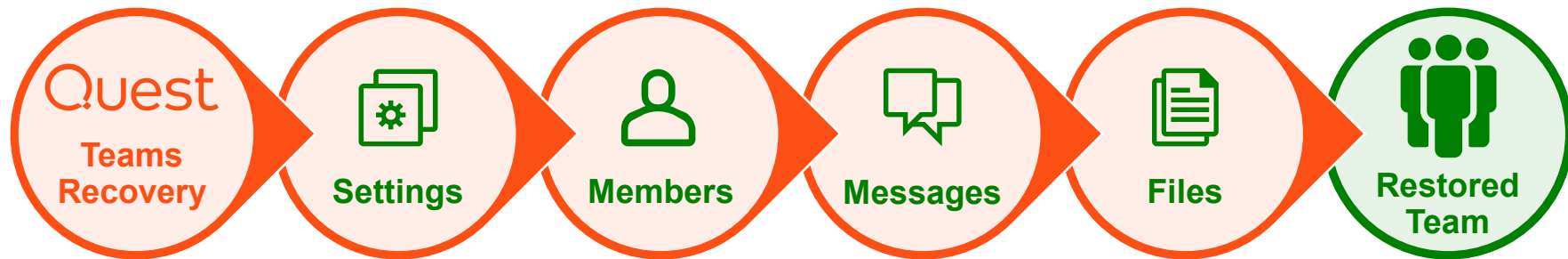
Where Next Meets Now.

# We can do - Much - More!



# Restoring a Team

**ODR- Teams:** Granularly and securely restore Team content, references and configuration



- RTM – November 20, 2020
- GA – December 11, 2020



# Features

- Backup/restore Teams configuration(Settings, Members, Guests and Owners)
- Backup/restore Teams Channel conversations(Channel posts, replies, URL links with preview, Inline Images, Emojis, @user mentions, gifs, memes, stickers, thumbnail reach card attachments, attached media files and docs)
- Backup/restore Teams SharePoint files
- Incremental hourly backups for Teams conversation
- Restore from recycle bin of Teams and SharePoint data
- Automatic backup