HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS

Entra ID Recovery: Two Truths and Some Lies

Paul Robichaux

Microsoft MVP

Sr Director of Product Management, Keepit

About me…

- Sr Director of Product Management @ Keepit
- Microsoft MVP, 2002-present
- Keeper of 2 beagles + Pancake the cat
- Commercial multi-engine rated pilot

Two truths and a lie… let’s get started

Spot the lie…

- I have been interviewed on CNN
- I have driven the Formula 1 race course in Monaco
- I once ate 32 McNuggets at a single sitting

Agenda

What does “backup” even mean?

Setting healthy boundaries

What Microsoft says about backup

Restore vs recovery

What does “backup” mean?

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

What does backup even mean?

- Classical definition: “3-2-1”
  - 3 copies of the data (original + 2)
  - 2 different media types
  - 1 copy offsite

- In the cloud world, does this make sense?
  - Different media types?
  - What’s “offsite”?
  - What about immutability?

Modernizing our definition

- Let’s keep “3-2-1” but modernize it
  - Still 3 copies of the data (original + 2)
  - 2 different storage security boundaries
  - 1+ copies immutable
- These are minima, not maxima
  - More copies, more security boundaries, and more immutable copies are all good
- Let’s talk about security boundaries…

Quick show of hands…

Q1: does keeping a backup copy in the same cloud as your production system represent a real backup?

Q2: are you familiar with the EU NIS2 directive?

Q3: have you heard of Mango Sandstorm’s Storm-1087? How about Storm-0501?

Setting healthy boundaries

A truth about security boundaries

- Remember the Immutable Laws of Security?
- Law #3: “if a bad actor has unrestricted physical access to your computer, it’s not your computer any more.”
- In a cloud world, that can be reworded: **“if a bad actor has unrestricted access to your cloud, it’s not your cloud any more.”**
- A hybrid cloud extension of your on-prem environment probably isn’t a security boundary
- Another logical partition in the same service as your production cloud also probably isn’t a security boundary

What Microsoft says

What Microsoft says about backup

Spot the lie…

- “We probably won’t lose all of your data at the same time.”
- ”You share responsibility for your data protection with your cloud vendors.”
- “Our native data protection is good enough; you don’t need third-party tools.”

The truth about Microsoft and backup

- Microsoft’s native data protection is quite good
  - Multiple distributed copies
  - Logical undelete / recovery
- But that protection isn’t evenly distributed across workloads!
  - E.g. list the Entra ID objects that can be soft-deleted vs those that cannot
- Microsoft doesn’t enter markets on a whim
  - 90+% of enterprise M365 customers have no backup at all
  - Clear threat from cloud-focused ransomware at scale
- **Bottom line: Microsoft is validating the need to back up data.**

The truth about Microsoft and backup

- Microsoft's native data protection is quite good
  - Multiple distributed copies
  - Logical undelete / recovery
- But that protection isn't evenly distributed across workloads!
  - E.g. list the Entra ID objects that can be soft-deleted vs those that cannot
- Microsoft doesn't enter markets on a whim
  - 90+% of enterprise M365 customers have no backup at all
  - Clear threat from cloud-focused ransomware at scale
- **Bottom line: Microsoft is validating the need to back up data.**

Restore vs recovery

Restore vs Recover

- Let’s try a thought experiment…

Quick show of hands…

Q1: How many of you back up M365 today?

Q2: How many of you back up Entra ID today?

Q3: Which of those two environments would you rather lose, Entra or M365?

Disaster reality

- It’s not enough just to put all the data back where it was before!

- “Recovery” through restoration is a **necessary first step**, but it’s not everything

- Users depend on the end-to-end environment to be functional

Prioritization

- Not all of your data is created equal
- If you don’t know what’s most important, you cannot provide an acceptable recovery interval

- Prioritization hurts…
- …Not prioritizing hurts more, and lasts longer.

- ”So I have 1.2 petabytes of SharePoint data…”

And what about Entra?

- Consider what threats you’re trying to protect against
  - Mishap
  - Malice
  - Mistake
  - Migration
- Mitigation of each of those threats may require a different mix of protection
- But really, everyone should at least be backing up CAPs.

HYBRID IDENTITY PROTECTION conf24 NEW ORLEANS

Pro questions for a happier life

- What data items do you need to return to normal-ish?
  - The answer cannot be “all of it”
  - Think “minimum needed to resume operations”

- Are you backing up your important M365 data?
  - …but see previous tip

- What would an end-to-end MVP recovery look like for you?

- How does your IdM strategy play against these requirements?

- Are you comfortable with your data protection boundaries?

Questions?