## **Entra Backup Campaign-in-a-Box Quick Pitch Guide**

## **💬 Quick Pitch Guide: Talk Tracks for Everyday Conversations**

### **📝 Description**

Simple, straight-to-the-point responses to common client questions about why Entra backup matters—so MSP reps can speak clearly, confidently, and without technical jargon.

### **🎯 Purpose**

To help MSPs **frame the value of identity protection** (without needing to say "Entra") in client calls, emails, or QBRs—especially when explaining why this is a new and necessary offering.

### **✅ Fast 30-Second Value Pitch**

“We’re now offering a new service that backs up your login and access system—the part that controls who gets into email, files, and apps. If something goes wrong, Microsoft only gives you 30 days to recover it. We help you recover faster, avoid lockouts, and keep your business running.”

### **🔥 Key Client Questions & Talk Tracks**

### **❓ “Why do I need this?”**

**Talk Track:**

“We’re seeing more businesses run into issues where a user or setting gets deleted or changed—and it locks them out of their Microsoft tools. Microsoft doesn’t fully back up that part of the system, which means recovery can be slow or even impossible. This new service gives you a safety net, so your team stays online, even if something goes wrong.”

### **❓ “Doesn’t Microsoft already back everything up?”**

**Talk Track:**

“Microsoft backs up your email and files—but **not** the system that controls your logins and access. If that data is deleted, it’s gone after 30 days. Our solution fills that gap, so you’re covered on all fronts.”

### **❓ “Is this really necessary? We’ve never had an issue.”**

**Talk Track:**

“That’s a fair question—and honestly, most businesses say the same thing… right up until something goes wrong. We’re seeing three big issues hit companies hard:

* **Simple mistakes**—like deleting a user or changing a setting—can lock out your whole team.
* **Hackers** are now targeting login systems to shut businesses down and demand ransom.
* And if you’re in a regulated industry, **compliance requires recoverability**—and Microsoft doesn’t cover this part of the system.

This backup isn’t about fixing a past issue—it’s about making sure you’re protected before one happens.”

Additional talking points:   
  
“We’ve seen where a small business was hit with a targeted cyberattack that compromised their Microsoft login system. The attackers changed access policies, locking out employees and disabling MFA. Without a backup of those settings, recovery was manual and slow—causing hours of downtime and business disruption. That is the last thing I want for you.”

“Microsoft's own documentation makes it clear—they don’t offer long-term backup or easy recovery for the access layer. After 30 days, deleted objects are gone. Most clients only realize this when it’s too late.”  
  
“We’ve seen clients experience lockouts due to accidental deletions or misconfigured access settings in Microsoft 365. Without backup, recovery is slow, manual, or sometimes impossible.”

“We’ve seen scenarios where internal staff members within our client base with elevated permissions accidentally changed a user access setting while onboarding a new hire. It locked multiple team members out of email, Teams, and files for nearly a day. Without a backup of those access settings, there was no fast way to undo the change.”

### **❓ “How is this different from our existing backup?”**

**Talk Track:**

“Traditional backup covers things like email, files, and calendars. This service protects **who can log in, what they can access, and how your system stays secure**—which is just as important, but often overlooked.”