## **Entra Backup Campaign-in-a-Box Objection Handling Guide**

## **🛡️ Objection Handling Guide: Overcome Resistance with Confidence**

### **📌 What This Is**

This quick-reference guide is built to help MSP sales team members handle the most common objections you'll hear when introducing Entra backup. Whether you're talking to a loyal client or a new prospect, pushback is normal—especially when the risk isn’t obvious.

The key is to stay calm, stay curious, and **reframe the conversation around business continuity, security, and client peace of mind**—not backup jargon. These talk tracks help you do just that.

### **🔁 Common Objections & Confident Responses**

### **❓ “We’ve never had a problem with access before.”**

**Response:**

“That’s actually why this is the perfect time to put protection in place. Most businesses only think about this *after* something breaks—when someone accidentally deletes a setting or a hacker locks them out. We want to make sure you never have to experience that kind of disruption.”

### **❓ “Microsoft already backs this up, don’t they?”**

**Response:**

“Microsoft protects your files and emails—but not the settings that control who can log in, what they can access, or how your system stays secure. Once something is deleted, it’s gone after 30 days—and there’s no simple rollback. That’s the gap we’re helping you close.”

### **❓ “This feels like overkill. Do we really need another layer?”**

**Response:**

“That’s a fair question—and one we hear a lot. But this isn’t about adding complexity. It’s about covering a part of your system that most businesses don’t realize is vulnerable. A single misstep or attack could lock you out—and without backup, recovery can be slow or impossible.”

### **❓ “I’m already backing up Microsoft 365. Isn’t that enough?”**

**Response:**

“That’s a great start—and you’re ahead of many. But 365 backup covers files, email, and calendars. What we’re talking about here is **identity and access protection**—the system behind your logins. If that breaks, even your backed-up files won’t help if no one can sign in to access them.”

### **❓ “Can’t we just fix things manually if something happens?”**

**Response:**

“Sometimes. But in many cases, you won’t know exactly what was changed—or how to put it back. And in the middle of an outage, you don’t want your team stuck guessing. This solution gives you snapshots, comparisons, and a way to restore exactly what was lost.”

### **❓ “We trust our internal team—they’re careful.”**

**Response (Internal Error Use Case):**

“Totally fair—this isn’t about pointing fingers. But even experienced staff can accidentally change or delete the wrong setting, especially during user onboarding or offboarding. One slip can lock out the whole team. This backup gives you a safety net in case that ever happens.”

### **❓ “We already have cybersecurity tools. Isn’t that enough?”**

**Response (Cyberattack Use Case):**

“Most security tools focus on keeping attackers out—but if they get in, they often go straight for your login system. We’ve seen cases where attackers disable MFA, delete users, or change access policies. With this in place, you can restore clean access settings fast—and avoid extended downtime.”

### **❓ “We don’t really have compliance requirements.”**

**Response (Compliance Use Case):**

“Even if you’re not in a heavily regulated industry, your clients might be—and they’ll expect a fast, reliable recovery if something goes wrong. Plus, having backup of login and access settings helps with internal audits and shows you’ve taken responsible steps to protect your business continuity.”

### **❓ “We’re not a big company—why would we be targeted?”**

**Response:**

“Actually, small businesses are often easier targets. Attackers know you may not have the same layers of protection, and access systems are a soft spot. Whether it’s a misclick or a malicious login, we want to make sure your business doesn’t go dark.”

### **❓ “We’ve already invested a lot in IT—can this wait until next year?”**

**Response:**

“Totally understand—you want to be smart about where you invest. But this is one of those cases where waiting could cost far more. If a single mistake or attack locks out your systems, the downtime, lost productivity, and recovery time could outweigh the cost of protection many times over. This is a small step with big impact.”

### **❓ “Isn’t this just an upsell?”**

**Response:**

“It might feel that way, but honestly—it’s a gap in Microsoft’s coverage that more and more businesses are just now realizing exists. We wouldn’t offer this if we didn’t think it was essential. This is about giving you full coverage for the systems that keep your business running.”