AirGap: An Added Layer of Security to Your Data Protection Strategy

Why AirGap?

Cybercriminals realize that SMBs are relatively unprotected compared to enterprises.

In fact, one-third of SMBs only use free, consumer-grade cybersecurity tools, and one in five have no endpoint security at all. Not only are they making it easy to access their data, but they're failing to ensure complete recovery and data restoration. So while the initial payout on an enterprise attack may be larger, hackers have figured out that smaller attacks can be more lucrative, especially with the weaker defenses used by SMBs. Additionally, even though law enforcement is improving their ability to get all or some of these ransom payments back, and despite growing federal interest in counter ransomware tactics, there are not enough resources to investigate the thousands of SMB incidents that occur each year. **This is where the added layer of AirGap becomes beneficial.**

What is Airgap?

AirGap is part of your layered security approach that includes MFA, strong password policies, firewalls, spam filtering, phishing detection, and data redundancy.

AirGap saves and protects a snapshot of your data so it can be restored in the event of a malicious or accidental deletion. It's your last line of defense when there's a cyberattack on your backup files.
Core Security and FRSecure have independently tested AirGap to show that even if an attacker breaches your security, your data is safe.

How does AirGap work?

- AirGap technology separates backup requests from the actual backup mechanics to prevent malicious deletion using the following unique features.
- "Honeypots" give bad actors the illusion that they've achieved their malicious goal – so they stop pursuing corruption – but, in reality, the data is stored on isolated storage tiers.
- Human factor controls limit authorised individuals who can create deletion requests within your organization. This is separated from authorised individuals who can actually fulfill the deletion requests.
- Human two-factor authorisation is required to verify the deletion request made using audible confirmation that the deletion request is valid. Even if the deletion request is malicious, iif phone, email, and support systems are compromised, the request won't be processed without audible approval.
- When deletion requests are created, verified and executed, time gaps give partners time to see and stop any malicious activity. The amount of time between processes varies so patterns cannot be recognized and replicated.

The Benefits of AirGap

- **Adaptive:** AirGap is adaptive, e.g., allows pending windows updates to apply properly, has automatic remediation, and runs a self-healing backup if a filesystem is detected as having an issue.
- **Preventative:** Reduce accidental deletions and ransomware threats with multiple validations required to delete Protected System backups.
- **Worry-free:** Your data is safe no matter what with native snapshots of Protected Systems stored in a safe location, separate from your actual filesystem.
- **Almost instant recovery:** Quickly get back to business with one call to your MSP to initiate the process of recovery

hello@it.ie