

Axcient AirGap Technology Overview

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 they’ve accomplished their malicious goal – so they stop pursuing corruption – but, in reality, the data is stored on isolated tiers of storage.
- Human factor controls limit authorized individuals who can create a deletion requests within the Axcient organization. This is separated from authorized individuals who can actually fulfill the deletion requests.
- Human two-factor authorization is required to verify the deletion request made using audible confirmation that the deletion request is valid. Even if the deletion request is malicious, in the event that phone, email and support systems are compromised, the request won’t be processed without audible approval.
- Time gaps between when deletion requests are created, verified and executed give partners time to see and stop any malicious activity. The amount of time between processes vary so that patterns cannot be recognized and replicated.

The Benefits of Axcient AirGap for MSPs:

- **Adaptive:** AirGap is adaptive, e.g., allows pending windows updates to apply properly, and has automatic remediation and runs a self-healing backup if a filesystem is detected as having an issue.
- **Cost-effective:** Significantly increase your BDR return on investment (ROI) by eliminating the risk of ransomware and potential ransom payments, loss of data, regulatory fines, downtime costs and damage to your business reputation.
- **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 Axcient’s 24/7/365 Support Team, or utilize Virtual Office for self-managed recovery and virtualization.
- **Choice and flexibility:** Choose the installation, storage environment, and restore process that works best for your business?
 - Direct-to-Cloud hardware-free BDR.
 - Pre-installed on-site BDR appliance.
 - Build your own hardware using Axcient installation media.
 - Offsite replication of backups to the Axcient Cloud or BYODC (Bring your Own Data Center).
 - Self-host to a private cloud. Restore backups from either cloud.

WHAT IS AIRGAP?

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

Axcient 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 clients’ backup files.

AirGap is enabled by default for all Axcient partners as part of the x360Recover solution, and has been independently tested by Core Security and FRSecure to show that even if an attacker breaches your security, your data is safe.