Axcient

Incremental Vault Recovery from Axcient

What is Incremental Vault Recovery?

Vault recovery has always been available on x360Recover, but with the addition of incremental vault recovery, MSPs can recover faster and with less risk of data loss.

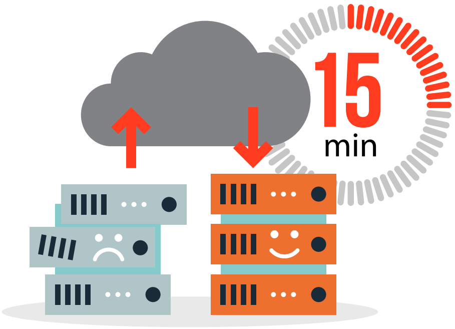
When an appliance is lost or damaged, or you're switching a protected system from x360Recover Direct-to-Cloud (D2C) mode to appliance mode, **incremental vault recovery significantly speeds up this process.** This enhancement to standard vault recovery enables seamless manual incremental failback to an appliance with minimal downtime:

→ During cloud failover, MSPs can recover protected data on a vault and move it back to an appliance in multiple passes.

→ Until the final pass, D2C backups continue to run on the vault, so you maintain an uninterrupted set of backups while actively fixing the appliance and recovering cloud data.

→ When you're ready, switch back to appliance mode to merge the cloud data and the final snapshot.

Incremental vault recovery is available on x360Recover v.12.3.0 and higher via the x360Portal without any additional costs or fees.



When Should MSPs Use Incremental Vault Recovery?

Incremental vault recovery fulfills three main MSP use cases:

1. To quickly fail back to an appliance from a cloud virtualization.
2. To smoothly transition from D2C to an appliance without missing any backups.
3. To effortlessly migrate from any traditional third-party BDR appliance to x360Recover.

Use Case #1: Virtual Office Failback to an Appliance

The Scenario: You need to virtualize a protected system in the cloud.

The Problem: Recovering systems back to an appliance can be a long, arduous, and resource-intensive process with high costs and long downtime.

The Solution: Incremental vault recovery provides a painless path to restore in just 3 steps:

1. **Run backups in Virtual Office,** the cloud failover feature in x360Recover. Virtual Office lets MSPs start VMs in the Axcient Cloud of one or more protected devices to temporarily replace all impacted production infrastructure.
2. **Perform incremental vault recovery** to recover the backup data from the vault to the appliance. This process occurs in the background.
3. **Shut down Virtual Office and complete the final pass of snapshots** to the appliance.

Use Case #2:
Backup Continuity After an Appliance Failure

The Scenario: You need to repair or replace a failed hardware appliance.

The Problem: After a hardware failure, clients might be left without backup protection, thereby threatening business continuity and disaster recovery.

The Solution: Incremental vault recovery enables backup continuity within the efficient, user-friendly x360Portal in just 4 steps:

1. **Convert the protected system to Direct-to-Cloud mode** to maintain backups and send them to the vault while you fix the failed appliance.
2. **Perform incremental vault recovery** to copy the protected system data back to the appliance. Some notes…
   - → The first pass copies the base image and all recovery points on the vault to the appliance. Backups continue to run, and new recovery points continue to be created on the vault.
   - → You can choose the starting point for the appliance data by selecting a specific recovery point as the appliance's base image (oldest snapshot). When space is limited, you don't have to replicate ALL historical data from the vault back to the appliance.
   - → Once the initial pass is complete, you can perform additional incremental passes to collect and copy snapshots from the vault to the appliance.
3. **Complete the final pass of snapshots** to the appliance. This automatically stops D2C mode on the protected system in the vault.
4. **Reconfigure x360Recover to point to the appliance** and configure replication on the appliance to the vault.

Use Case #3:
Repurpose Third-Party BDR Appliances

The Scenario: You want to reuse your client's existing, third-party BDR hardware as an x360Recover appliance.

The Problem: During an appliance migration, MSPs risk backup disruptions and potential loss that threaten SLA requirements for retaining backup history.

The Solution: Incremental vault recovery and Axcient's hardware-agnostic BYOD policies make it safe and simple to repurpose devices in just 4 steps:

1. **Deploy x360Recover Direct-to-Cloud** (D2C) to send backups to the cloud vault in parallel with the existing solution. Continue parallel backups until…
   - → The first base image backup is complete.
   - → There is sufficient backup history in the cloud to satisfy minimum SLA requirements.
2. **Reload the device as an x360Recover appliance and deploy.** Uninstall third-party backup agents from the protected systems since they are no longer backing up to that appliance.
3. **Perform incremental vault recovery** to seamlessly retrieve data from the protected system's vault down to the appliance without interruptions.
4. **Reconfigure x360Recover to point to the appliance** and configure replication on the appliance to the vault.

Why Should MSPs Use Incremental Vault Recovery?

No rip and replace. Just a few clicks within the x360 Portal to reconfigure deployment modes.

No missing data or backups. D2C backups continue in the vault so you can fail back from D2C to an x360Recover-ready appliance without any loss.

No device limits. x360Recover is hardware agnostic, so clients can easily repurpose existing hardware devices to conserve costs and delight clients.

No complexity. This frictionless path to cloud failover, deployment transitions, and appliance migration prioritizes simplicity for data protection and backup continuity without delays.

See how incremental vault recovery can accelerate and secure failback, recovery, and migration to and from an appliance.

Get a 1:1 demo day: axcient.com/schedule-a-demo/