Cloud vs. Appliance-Based BDR Guide: When to Deploy What?

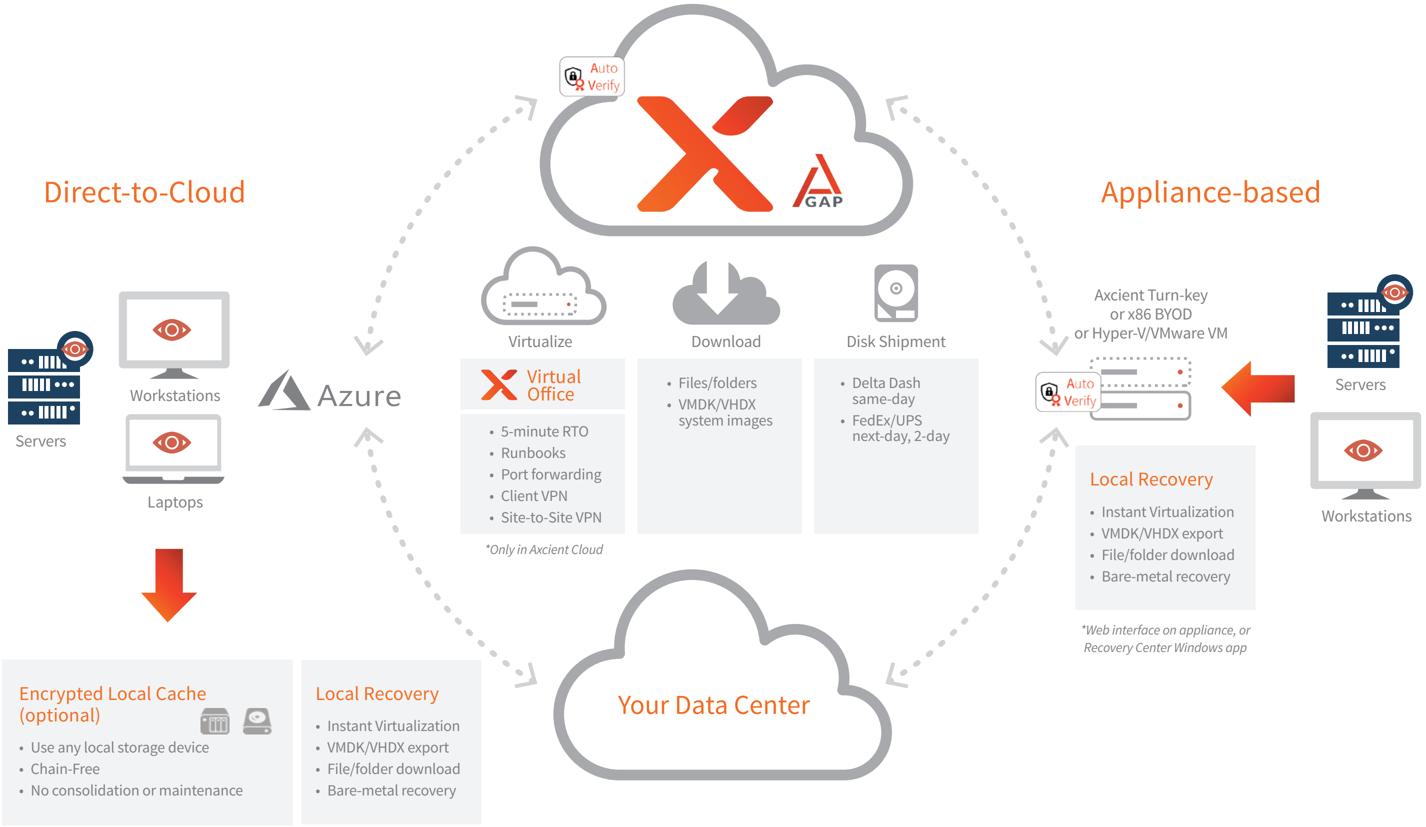
Deployment considerations when deciding whether to use hardware-free cloud backup versus appliance-based backup.

Axcient's business continuity and disaster recovery (BCDR) solutions provide MSPs and their clients choice and flexibility.

Our all-in-one x360Recover solution allows MSPs to meet all client needs with just one vendor – endpoint backup, no-appliance BDR, turn-key BDR, and public or private cloud backup. But, with all of these deployment options under one roof, how do you choose the best infrastructure for each client?

MSPs must consider:

- **When to use Direct-to-Cloud hardware-free backup versus appliance-based backup.**
- **What deployment considerations need to be taken into account.**
- **How built-in features explicitly designed for MSPs enhance either deployment option.**



Virtual Office

- 5-minute RTO
- Runbooks
- Port forwarding
- Client VPN
- Site-to-Site VPN

*Only in Axcient Cloud

- Files/folders
- VMDK/VHDX system images

- Delta Dash same-day
- FedEx/UPS next-day, 2-day

Local Recovery

- Instant Virtualization
- VMDK/VHDX export
- File/folder download
- Bare-metal recovery

*Web interface on appliance, or Recovery Center Windows app

Encrypted Local Cache (optional)

- Use any local storage device
- Chain-Free
- No consolidation or maintenance

Local Recovery

- Instant Virtualization
- VMDK/VHDX export
- File/folder download
- Bare-metal recovery

Download Axcient's Quick Guide to x360Recover Deployment Options

x360 Recover Direct-to-Cloud

Direct-to-Cloud: Business Continuity Without the Local Appliance

x360Recover Direct-to-Cloud (D2C) hardware-free backup was created to protect remote endpoints without the expense, hassle, maintenance, on-site visits, and limitations of appliances. Chain-Free image-based backups are sent directly to the secure Axcient Cloud for quick recovery of anything from a single file to an entire system in just an instant. Created for today's remote environments, D2C protects employees from the risks associated with less sophisticated at-home infrastructures and public Wi-Fi connections.

Direct-to-Cloud is best…

- **For clients who don't want a dedicated turn-key appliance** because of cost or distributed IT.
- **When protecting virtual machines (VMs) in the cloud,** or in other cases when local backups are not desired, use D2C for Microsoft Azure to separate backups from the production infrastructure to avoid complete downtime.
- **When protected machines roam to different networks –** for example when endpoints are not on the same local area network (LAN).
- **For protecting servers when used with Local Cache –** an optional, fully independent D2C feature that pairs D2C with an inexpensive local USB or NAS device to substantially decrease recovery and failback times.
- **If cloud-based recovery is suitable for protecting servers without Local Cache,** or if it is acceptable for restore speeds to be limited by Internet speed.
- **For protecting desktops or laptops, with or without Local Cache.**
- **When you want to leverage existing devices –** including network-attached storage (NAS) devices, USB disks, and Windows-based BDR devices.

Consider these deployment components:

- **D2C doesn't take local backups separate from cloud backups.** An Internet connection is required for backups, and the backup speed is dependent on the Internet connection speed.
- **The initial backup could take days or weeks, depending on bandwidth.** D2C can run concurrently with the existing backup vendor or Windows backup until the initial backup is complete.
- **Fast local recovery from the local cache requires an Internet connection** to download the encryption key and recovery point indexes. More than 99.9% of data will come from Local Cache.
- **Instant local virtualizations require a local Hyper-V desktop or server to access Local Cache.**
- **If the client has no hardware for local virtualization,** we recommend keeping a spare 'recovery BDR' in your MSP office with Hyper-V preloaded that you can transport to a client needing recovery.

x360 Recover

Traditional Appliance-Based BCDR

Axcient x360Recover also supports on-premise, appliance-based backup for clients that desire this infrastructure. Built on the same Chain-Free backup technology and using the same secure Axcient Cloud, x360Recover provides comprehensive local recovery and instant virtualization.

Appliance-Based BCDR is best...

- **When you need dedicated hardware on-site** for instant local failover of backed-up workloads.
- **When you need to continue local backups** even when the client's internet connection is down.
- **When you need to do local restores** even when the client's internet connection is down.
- **When you need to separate time of backups from time of replicating data to the cloud.**
- **When a client has low bandwidth,** or you need to do a physical seeding of cloud backups.
- **For protecting physical or virtual servers** that need dedicated on-site infrastructure for failover.
- **For protecting desktops in an office** where an appliance is already deployed to protect servers.

Consider these deployment components:

- **Appliance-based BCDR requires an appliance at each client site.** Use a turn-key Axcient appliance (USA only), other compatible x86 hardware, or a Hyper-v/VMware VM that can be deployed via a bootable installer ISO.
- **Existing x86 hardware (servers or desktops and some competitive BDR units) can be replaced to be an x360Recover appliance or vault.** Check the hardware compatibility list for supported hardware configurations and solutions.
- **Local recovery has no dependence on the Internet.** Zero data is downloaded for local recovery.
- **Local recovery is performed via the appliance web-based graphical user interface** (GUI) – which can be accessed via the x360 cloud portal, or locally via a web browser – or can also be performed via the Windows Recovery Center application.
- **Physical seeding of the initial backup is possible, but not required.** Incremental backups are replicated to the cloud even while a physical seed drive is in transit.

Built-In BCDR Features Make Both Deployment Options Beneficial for MSPs

Regardless of the deployment option that best fits your unique client's needs, x360Recover comes complete with various innovative features designed to lower costs, improve efficiency, and boost profits. Axcient products are regularly updated and upgraded with the latest technologies available to streamline backup management and speed-up disaster recovery. Our evolving solutions respond to today's cybersecurity landscape to ensure uninterrupted business continuity despite security breaches, human error, and natural disasters.

- **Chain-Free backup technology** eliminates the need for periodic or manual reseeding to reduce overhead dramatically.
- **Unlimited storage and retention** provide predictable billing without even a chance of surprise overages or unexpected fees.
- **Patented AirGap anti-ransomware technology** separates data deletion requests from deletion mechanics, so your data is always protected, even after a ransomware attack.
- **AutoVerify ends manual backup** verification by automatically virtualizing and running numerous tests for data corruption, ensuring your data is always ready to recover.
- **Virtual Office enables self-managed disaster recovery** with a minutes-long recovery time objective (RTO) and near-instant virtualization in the cloud.
- **Simple flat-rate pricing** per protected machine per month + 30 free days per year per protected machine of cloud virtualization.

Choose Your Deployment Option

Check out all of Axcient's x360Recover deployment options with a 14-day free trial.

This is your opportunity to get a sneak-peek at all of Axcient's features on the x360 Portal to see how your MSP can grow with Axcient. Compare x360Recover to your current BCDR to determine your average monthly savings with automation, innovation, and simple service delivery.

Start Your Free Trial Now!

ABOUT AXCIENT:
Axcient is an award-winning leader in business continuity and disaster recovery for Managed Service Providers (MSPs). Axcient x360 provides one platform for MSPs to Protect Everything™, and includes BCDR, Microsoft 365 and Google Workspace backup, and secure sync and share. Trusted by more than 3,000 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

CONTACT:
Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202
Tel: 720-204-4500 | axcient.com

FOLLOW US: