Axcient

Cloud vs. Appliance:

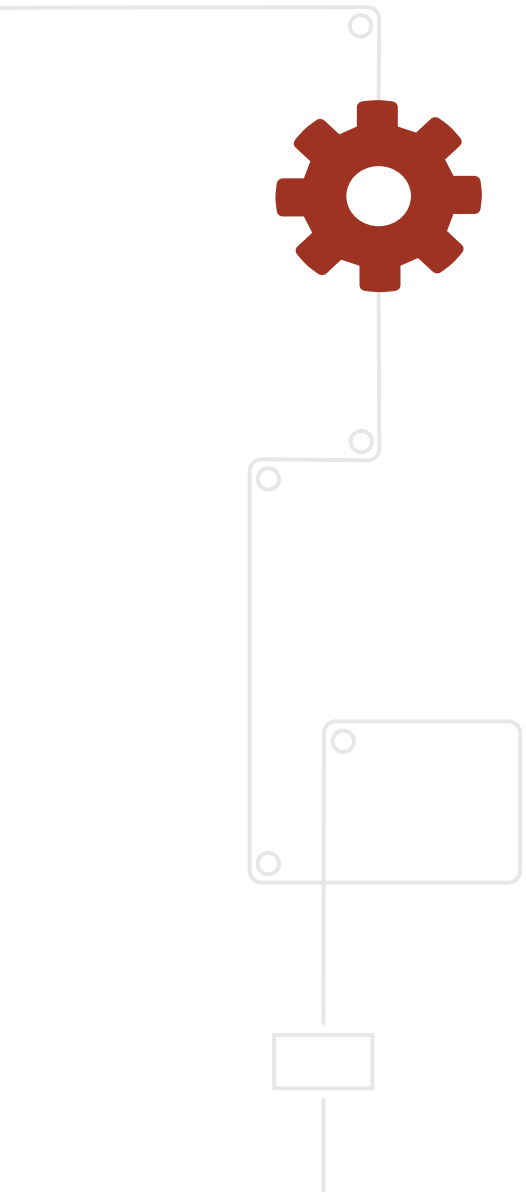
BDR Deployment Playbook

When to Deploy What?

MSPs have deployment considerations when choosing between a cloud-first infrastructure with hardware-free cloud backup versus an appliance-based backup. Ideally, an all-in-one backup and disaster recovery (BDR) solution allows MSPs to meet all client needs with just one vendor – including endpoint backup, hardware-free BDR, turnkey BDR, and public or private cloud backup. With that said, even if MSPs have already consolidated vendors on a multi-deployment platform, you still need to tailor the architecture to individual clients.

Does your MSP know…

- When should you use Direct-to-Cloud hardware-free backup versus appliance-based backup?
- What critical factors need to be addressed?
- How do built-in features impact either deployment option?



Cloud-Based BCDR Deployment

Hardware-free backup was created to protect remote endpoints without the expense, hassle, maintenance, on-site visits, and limitations of appliances. Cloud backups are sent directly to one or more secure clouds for accidental deletion or disaster recovery of anything from a single file to an entire system. Cloud-based, comprehensive business continuity and disaster recovery (BCDR) solutions are well-suited for today's remote environments, protecting employees from the risks of unprotected at-home infrastructures and public Wi-Fi connections.

When cloud-based BCDR is best:

- When clients want something other than a dedicated turnkey appliance due to cost or distributed IT.
- When protecting virtual machines (VMs) in the cloud or for clients who don't want local backups, use a third-party, public cloud backup to separate backups from production and avoid complete downtime.
- When protected machines roam to different networks – for example, endpoints are not on the same local area network (LAN).
- When using an inexpensive local USB or NAS device as a local cache to speed recovery and reduce failback times.
- When cloud-based recovery is suitable for protecting servers without a local USB or NAS restoration acceleration device or a local cache, or if it is acceptable for restore speeds to be limited by internet speed.
- When protecting desktops or laptops, with or without a local USB or NAS recovery acceleration device
- When leveraging existing devices – including NAS devices, USB disks, and Windows-based BDR devices.

Cloud-deployment considerations and challenges:

- **Does your cloud backup solution accept local backups separate from cloud backups?** Is an internet connection required for backups? Is backup speed dependent on internet connection speed?
- **Are you backing up data during the restore process?** Depending on bandwidth, the initial backup could take days or weeks. Can cloud BDR restores run concurrently with the existing backup vendor or Windows backup until the initial backup is complete?
- **What is the RTO promised to clients?** Fast local recovery with a local cache requires the internet to download the encryption key and recovery point indexes. More than 99.9% of data will come from the local cache.
- **Can a local Hyper-V desktop or server access a local cache?** A local cache as an acceleration layer can be critical for fast virtualization.
- **Do you have spare hardware on hand?** Maintaining extra recovery appliances with Hyper-V preloaded can be a lifesaver when clients don't have hardware for local virtualization.

Hardware-Based BCDR Deployment

Traditional appliance-based BCDR supports on-premise backup for clients who need or want it. When clients need BDR hardware support, there are important use cases to remember as you tailor backup processes.

When appliance-based BCDR is best:

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

Hardware deployment considerations and challenges:

- **Appliances are required at each client site.** All-in-one vendors typically offer their own turnkey appliances, compatible x86 hardware, or a Hyper-V/VMware VM that can be deployed via a bootable installer ISO. Hardware-agnostic vendors can repurpose existing x86 hardware (servers, desktops, and some competitive BDR units) with a vendor-specific appliance or vault.

- **Local recovery is not dependent on the internet,** so no data is downloaded for local recovery. Performed via an appliance web-based graphical user interface (GUI), local recovery is often completed via the vendor's portal or locally through a web browser or the Windows Recovery Center application.

- **Physical seeding of the initial backup is possible but not required.** Incremental backups can be replicated to the cloud, even while a physical seed drive is in transit.

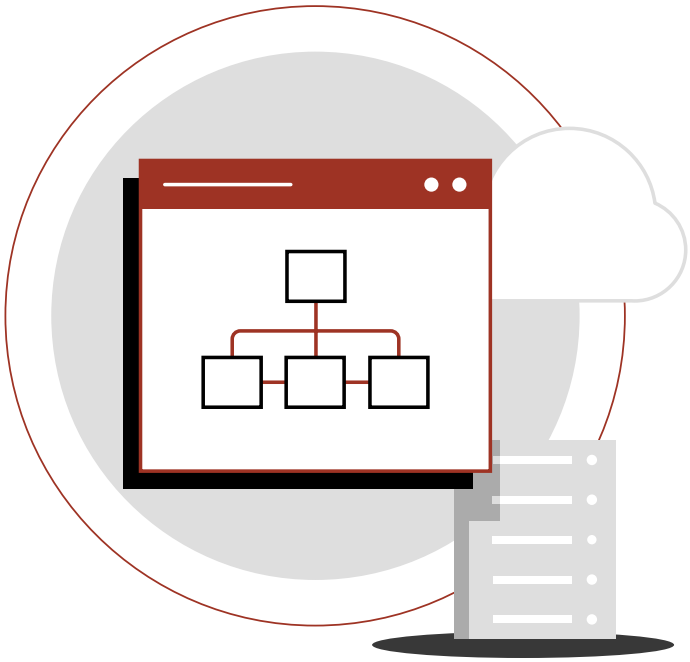
Can Your MSP Do Both?

Despite individual client preferences, MSPs need specific automated features to lower costs, improve efficiency, and boost profits when deploying in the cloud or with hardware. Partner with an evolving solution provider with a proven record of responding to MSP-specific, unpredictable, and changing threat vectors.

Avoid legacy technology that is not tailored to the channel and MSPs' pain points. Conversely, dedicated MSP vendors ensure uninterrupted business continuity if the MSP or your clients need to remediate after accidental or malicious data deletion.

Before you deploy, answer these questions:

- Are you using chain-free or chain-based backup, and how does that impact **management ease** and accessibility?
- How will client data be **tested to ensure recovery**?
- How will you deliver on your RTO and RPO **promises in SLAs**?
- How will you meet the 3-2-1-1 backup rule? Specifically, **immutable data** for ransomware-readiness?
- Are you automating backup integrity testing and verification? If not, **why not?**
- Can you **prove data protection and recovery testing** to clients and insurance providers?
- How simple is **cloud virtualization when it's imperative** to keep the business running?
- Can you **self-manage virtualization and disaster recovery**, or need vendor support?
- Can rapid virtualization provide **business continuity**? How does that affect costs and stressors?
- How do your answers impact **downtime and recovery speed**?



Cloud and Hardware-Free Deployments, Just for MSPs

x360Recover Security + Unmatched Flexibility

Axcient x360Recover for comprehensive BCDR adapts and expands to meet a wide range of MSP use cases with the simplicity of consolidated efficiency. Protect data in Windows, VMware, Linux, MacOS, the public cloud, and IaaS models with all-in-one BCDR for disparate client budgets, environment preferences, and compliance demands.

Regardless of how it is deployed, x360Recover's speed and responsiveness to ransomware and other cyber threats contain layers of reinforced data protection. Both deployment options ensure business continuity with a 15-minute RPO and less than 1-hour RTO. x360Recover Direct-to-Cloud (D2C) was created exclusively for MSP flexibility and choice. With Axcient's patented Chain-Free backup technology, MSPs get automated backup integrity testing, minutes-long virtualization, and pooled storage for a flat fee, making x360Recover an intelligent choice for MSP profitability.

Leveraging these always-on features, MSPs can replace juggling vendors across siloed solutions with provable data security and the value of deployment choice. Bring your own device (BYOD), bring your own cloud (BYOC), or customize a hybrid solution to expand BCDR services without increasing budget or labor.

Cloud and Appliance Agnostic BCDR

Start saving immediately with the option to repurpose existing BDR devices or hardware, data center, or cloud. Axcient's BYOD and BYOC policies invite MSPs to purchase or lease Axcient equipment or replicate to the Axcient Cloud.

Focusing exclusively on MSP-specific pain points, x360Recover goes beyond traditional BDR. MSPs get backup, business continuity, and disaster recovery within a user-friendly single pane of glass.

BYOD options:

- Build or repurpose existing hardware as a local BDR appliance.
- Purchase a turnkey BDR hardware and software bundle directly from Axcient.
- Lease hardware from Axcient.

BYOC options:

- Use the secure and compliant Axcient Cloud.
- Use your own private cloud through your data center.
- Use a public cloud.
- Use the Axcient Cloud and your private cloud to retain multiple off-site copies.

With Axcient, MSPs can design the best service for their customers to support optimal total cost of ownership (TCO) and customer SLAs. Depending on SMB requirements and industry-specific use cases, this level of choice and flexibility is critical for adequate data protection. Furthermore, it supports efficient consolidation of solutions to reduce stack management complexity for technical teams – thereby reducing TCO with fewer solutions and vendors to manage.

Cloud-Based BCDR

Use x360Recover Direct-to-Cloud (D2C) to backup all remote endpoints, desktops, laptops, servers, workstations, and Microsoft Azure data directly to the secure Axcient Cloud, your private cloud, or the public cloud without any pricey appliances. Hardware-free delivers significant savings by eliminating high appliance costs and complexity, including on-site visits, ongoing maintenance, unexpected failures, and stressful limitations.

With x360Recover D2C, MSPs deliver rapid and reliable recovery across dispersed workforces regardless of how data is lost—whether through ransomware or other cyberattacks, accidental deletion, or a natural disaster. Proprietary Chain-Free image-based backups are sent directly to the Axcient Cloud to quickly recover anything from a single file to an entire system. Created for today's remote environments, D2C protects employees from the risks of less sophisticated at-home infrastructures and public Wi-Fi connections.

Local Cache Acceleration

Local Cache is an extension of x360Recover D2C that simplifies protecting critical systems and data from any physical or virtual Windows or Linux server, desktop, or laptop. While Axcient strongly encourages Local Cache, it is optional and independent of D2C backups, ensuring backup data security.

- **Rapidly restore lost or missing files** without waiting to download from the cloud.
- **Limit downtime** with accelerated bare metal restores directly from the Local Cache.
- **Secure data by default** with always-on Local Cache encryption.
- **Lower costs** can be achieved using inexpensive local storage or skipping utilizing a cache altogether.

How quickly can you recover? Use Axcient's RTO Calculator to find out.

Appliance-Based BCDR

MSPs can offer x360Recover with an appliance for clients seeking a conventional BDR system. Of course, there's no one-size-fits-all BDR solution for MSPs, so Axcient offers both deployment options within a single solution. If clients have bandwidth issues and the MSP has committed to a short RTO, choosing from Axcient's BDR appliance options is best.

Where you buy matters - turnkey simplicity

There are plenty of places for MSPs to purchase hardware, and Axcient is committed to providing MSPs with more value than legacy hardware. Flexible and turnkey appliances ensure that MSPs can reliably protect client data and maintain recovery readiness. Axcient's BDR appliances cover most MSP use cases and are customizable for seamless integration with the x360Recover product. The end result is a plug-and-play solution optimized for your customer's environment.

BDR appliance options

Purchase or lease Axcient BDR appliances using the BDR appliance ordering system in the x360 Portal. Equipped with a modern UI, appliance ordering is wizardized and simple, even when purchasing several appliances simultaneously. All Axcient turnkey BDR appliances express storage sizes in terms of recommended usage, so MSPs can easily choose the right size by simply looking at the BDR name or usable size.

Priced for savings

Axcient's bundled appliances offer exceptional value for MSPs. Upfront hardware costs can affect MSP finances, so Axcient appliances are priced to deliver up to 22% savings over leasing. Order your BDR appliances and pay your way…

- **Upfront Purchase:** Maximize savings with a one-time purchase.
- **Three-Year Lease:** Lease the appliance for a minimum of 3 years, with the option to return it or buy it outright to fully own it.

Built-In Features for Both Deployment Options

Regardless of which deployment option best fits 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 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.

Axcient x360Recover Critical Features:

- Chain-Free backup technology eliminates the need for periodic or manual reseeding.
- Pooled storage provides predictable billing without the chance of surprise overages or fees.
- AirGap anti-ransomware and data deletion 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 with runbooks enables self-managed disaster recovery with a minutes-long RTO and near-instant virtualization in the cloud.
- Flat-fee pricing per protected machine, per month + 30 free days per year per protected machine of cloud virtualization.

Unified Data Security with Unmatched Flexibility

If you're not an Axcient partner, use the options below to see how your MSP can protect what matters with any deployment method.

Schedule a 1-on-1 Demo

Try Axcient for Free for 14 Days

Get a BCDR Quote

Additional Resources

- Recovery Playbook for Axcient x360Recover
- QBR Handbook for MSPs
- MSP Blueprint for Profitably Selling Bundled Services
- DR Planning and Testing Best Practices for MSPs
- 5 Critical Pieces of a Good Security Playbook

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 5,200 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

Axcient

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