eBook

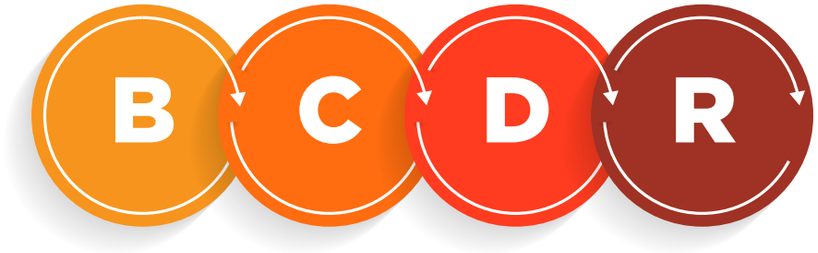
Axcient

How to Choose the Best BCDR Solution for Your MSP

Introduction

What is BCDR and Why is it Critical?

- **Understand the impact of tech stack complexity** on your technical team's ability to respond and recover quickly to meet SLAs and maintain client relationships.
- **Consider the economic advantages of simplifying BCDR management** to increase margins, the lower total cost of ownership (TCO), and drive profitability.
- **Recognize the impact of a vendor's business goals on your MSP** to ensure that your needs are prioritized, their roadmap is aligned, and stable support is always available.
- **Get a downloadable, done-for-you BCDR checklist** to quickly and easily compare solutions based on BCDR best practices for security, usability, and profitability.



Business continuity and disaster recovery (BCDR) is absolutely critical to MSPs and their SMB clients because it is the linchpin for business survival in today's cybersecurity landscape. Sophisticated and targeted cyberattacks, high-frequency human error, and dispersed remote endpoints have reduced backups alone to a legacy strategy that's sure to result in restore failure. Comprehensive BCDR is the security-first approach to surviving and thriving after data loss events.

Fortunately or unfortunately, not all BCDR solutions are created equal. To wade through your options and weigh your choices appropriately, MSPs need to understand all the factors impacting BCDR effectiveness in order to choose the right one. This eBook breaks down the most important factors to consider when exploring BCDR solutions and vendors.

Table of Contents

Versatility

BCDR versatility breeds ease of management and technician mastery for rapid and reliable recovery and profitability. Having one solution that can satisfy multiple use cases simplifies an MSPs' stack so you can dedicate more time to value-added tasks instead of vendor management requirements. Rather than juggling the demands of multiple vendors in regards to training, onboarding, support, billing, and recovery – standardize on an all-in-one BCDR solution to reduce the resources necessary for management.

Bottom Line…

✓ **Choose a solution that includes various deployment options** to satisfy a variety of use cases – including endpoint backup, hardware-free BCDR, full-service BCDR to a turn-key appliance and cloud, and public or private cloud backup.

✗ **Avoid a solution that limits use cases by infrastructure or data size,** which then requires you to increase tech stack complexity and management resources – thus inflating total cost of ownership (TCO).

"Since we started standardizing, we started seeing profitability. We've been able to grow exponentially, and now we're at a level we never thought possible. The more we simplify, the more profitable we get."

Neil Hawkins, Partner, and COO at LANAIR Group, LLC

Learn More

- Reference Architecture and its Impact on MSP Maturity, Efficiency, and Profitability
- How the Cybersecurity Landscape Killed Backups
- When to Deploy What? Appliance vs Cloud Use Case Guide

Choice and Flexibility

Appliance and cloud infrastructure limitations can force MSPs to unnecessarily add to their stack, compromising the available profit potential possible with an all-in-one, versatile solution. “Bring Your Own” (BYO) policies both support stack simplicity and attract clients who can reduce costs by reusing existing hardware or their own private cloud or data center. Depending on the vendor and how MSPs package BCDR services, BYO can also open the door for hardware leasing options to further reduce client costs.

Bottom Line…

- ☑ **Choose a solution with BYO choice and flexibility,** including Bring Your Own Device (BYOD), Bring Your Own Cloud (BYOC), and leasing options to enable and empower clients while increasing your competitive advantage in the channel.
- ☒ **Avoid a solution that forces the use of the vendor’s hardware and cloud** to prevent unnecessary client costs, discouraging clients, or requiring the addition of another vendor.

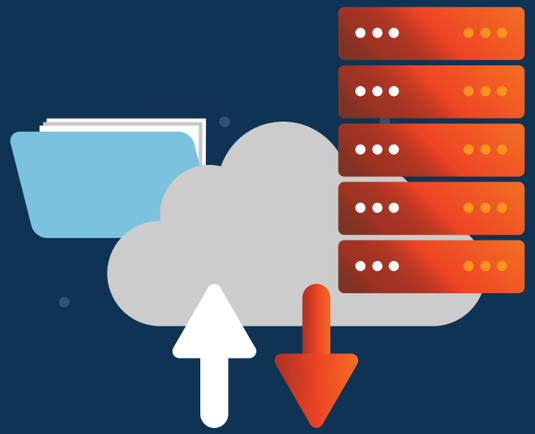
“BYOD has been extremely beneficial for our smaller clients who can’t spend thousands of dollars on a device. Sometimes, we’re able to find equipment for much less while ensuring business continuity with an on-prem appliance.”

George Lakiotis, CEO and vCIO of Symmetric IT Group

Learn More

- Cloud vs. Appliance-Based BDR Guide: When to Deploy What?
- 5 Reasons MSPs are Offering Private Cloud Deployment (and you should too!)
- Local Cache for Fast Recovery Without the Pricey Hardware

Backup Technology



Channel-focused BCDR solution providers apply innovation in automation and usability to reduce pain points for MSPs. How a BCDR solution backs up data is critical to efficiency, cost, storage and retention, and, most importantly, recovery. It comes down to chain-based or chain-free. Inverse-chain or chain-based backups are considered "legacy" because the infrastructure is risky, labor-intensive, and jeopardizes BCDR altogether.

Modern chain-free backup technology enables MSPs with automatic backup integrity verification, pooled data storage, secure retention, long-term compliance, and near-instant recovery. No chains means no chain maintenance, cloud reseeds, data loss, data bloat, storage overages, or wasting time with manual tasks.

"Because recovery points have such a small storage footprint, we can provide much greater granularity and retention with chain-free backups than other backup solutions. We don't have the same issues as other solutions, like chain management (retiring/rebasing), and the storage impact considerations that need to be made when taking new full backups."

Craig Dowell, Backup Admin at LANAIR Group, LLC

Axcient

Backup Technology

Bottom Line…

- ☑ **Choose a solution built on chain-free backups** to significantly reduce costs and empower technicians while efficiently delivering near-instant recovery.
- ☒ **Avoid a solution that uses inverse-chain or chain-based backups** to bypass storage limitations, overages, and surprise fees; chain maintenance and cloud reseeds; and additional software requirements for full recovery capabilities.

Learn More

- Why Should You Care How Your Backups Work?
- Chains Explained: Why You Need Chain-Free Backup
- Axcient Includes Pooled Storage at a Flat Fee for All MSP Partners

Critical Capabilities

Beyond the basics, BCDR solutions should come equipped with a host of always-on features and 24/7/365 support designed specifically for today's MSPs. For example, ransomware and phishing should be addressed with anti-data deletion technology. To meet competitive service-level agreements (SLAs), the recovery point objective (RPO) needs to be 15-minutes or less, and the recovery time objective (RTO) should be less than 1 hour. Additionally, self-managed DR testing should be available to prove DR readiness as part of incident response planning, along with runbooks to increase recovery speeds with automatic deployment plans for virtualization.

> "With automatic backup verification, we can manage by exception. If we get an alert, we deal with it. Otherwise, we just sit back and relax knowing the system works."
>
> **Luis Alvarez,** President, and CEO at Alvarez Technology Group

Bottom Line…

- ✓ **Choose a solution provider dedicated to the channel** to get the unique capabilities, regular product updates, and support you need to deliver uninterrupted BCDR.
- ✗ **Avoid vendors that fail to prioritize MSPs** among their broader customer base and may lose touch with what's required for comprehensive BCDR or charge additionally for critical capabilities.

Learn More

- An MSP Playbook for Best Practices in Disaster Recovery Planning and Testing
- RPO and RTO: Two Critical Components of BCDR Success
- Survey Results: Do the Vendors in Your Stack Check the Top 3 Boxes?

Axcient

Security and Compliance

Ask BCDR vendors for third-party, independent assessments to validate the efficacy and reliability of BCDR features, as well as cloud and data center security. At a minimum, MSP vendors should be SOC 2 certified, data centers should be SSAE or SOC certified, and solutions must support an MSPs compliance with HIPAA and GDPR. Solutions will also need to meet the requirements of any specific verticals your MSP serves. After confirming that solutions can meet compliance standards, MSPs need to know what's necessary to do so. For example, how much time, labor, storage, and additional cost is required for long-term data retention?

Bottom Line…

- ✓ **Choose a vendor with multiple forms of security and compliance proof** and tools for easy long-term compliance management – such as chain-free backups and ample flat fee storage.
- ✗ **Avoid a vendor that can't back up security and compliance claims,** such as those that rely on inverse, forward, or reverse chain-based backups, which share the same shortcomings and require chain management in order to meet years-long compliance standards.

"Compliance guarantees allow us to continue to operate in the medical vertical and command higher margins. Compliance is a primary competitive advantage."

Alan Helbush, President and CEO at Where to Start, Inc.

Learn More

- How Confident Are You in Your BCDR Solution and Why?
- Powering Reliable BCDR with Cloud and Data Center Security
- What is SecurityScorecard, and Why Should MSPs Care About Vendor Scores?

Price

When it comes to pricing BCDR solutions, you have to incorporate "soft costs," including onboarding, training and certification, maintenance, on-site visits, support and troubleshooting, storage, additional software, and billing. The time and resources that go into managing a BCDR solution can significantly impact profitability than the solution's price tag. Beware of complicated, tier-based pricing structures, and always investigate the asterisks on storage capacity and feature coverage. Instead, look for simple flat-rate pricing per protected machine, per month, for predictability without surprise overages.

Bottom Line…

- ☑ **Choose a solution with simple, predictable pricing,** flat fee pricing per device or server, and versatility to enable standardization – thereby reducing TCO for margin and profit growth.
- ☒ **Avoid a solution with complex, tiered pricing,** "fine print" storage limits, and one-trick pony capabilities to prevent falling victim to vendor sprawl.

"It's nice to have everything under one x360 umbrella. One, the pricing is good. Two, I have direct data that our ticketing for failed backups and issues has dropped. I'm spending a quarter of the time now that I was before on trouble tickets and stuff like that regarding backups."

Ryan Keele, CIO at Midwest Computech

Learn More

- MSP Security Trends Correlate with Profit Growth
- Why Use Four Vendors When You Can Save, Simplify, and Protect with Just One?
- Use Reference Architecture to Boost Profits Through Operational Maturity

Conclusion: Next Steps…

Now that you know what factors to evaluate when vetting BCDR solutions, you can choose the best vendor and product for your MSP. Even if you have a BCDR solution that you're happy with, consider exploring your options to see what you might be missing. Vendor shakeups, lightning-speed innovation, and economic uncertainties constantly evolve the cybersecurity landscape. Respond accordingly to stay competitive in the channel.

Use the downloadable BCDR Solution Checklist on the following page as a guide for analyzing your current solution or testing something new. Vendors should eagerly respond to product demo requests and free trials so you can get an inside look at their solutions.

READY FOR YOUR FIRST OPTION?

Review this competitive matrix to see how x360Recover favorably compares to other BDR vendors in the channel.

Axcient x360Recover is the most comprehensive and cost-effective BCDR solution made specifically for MSPs and their SMB clients. With just one solution and one vendor, MSPs can meet a range of client needs based on budget, environment, infrastructure, and compliance requirements. Simply your tech stack to significantly cut costs, reduce downtime, and streamline management.

Schedule a 1:1 Demo or Start Your Free 14-Day Trial Now!

Table of Contents

BCDR Solution Checklist for MSPs

The following checklist contains business continuity and disaster recovery (BCDR) solution must-haves. Use this as a guide to analyze and compare BCDR solutions and vendors to choose the best BCDR solution for your MSP.

VERSATILITY

- ◯ Does the solution provide endpoint backup?
- ◯ Does the solution provide hardware-free BCDR?
- ◯ Does the solution provide full-service BCDR to a turn-key appliance and cloud?
- ◯ Does the solution protect servers in public clouds?
- ◯ Does the solution protect servers in private clouds?
- ◯ Is there an option for a local backup with hardware-free BCDR?
- ◯ Does the solution support Windows, VMware, Hyper-V, and IaaS for all use cases?

CHOICE AND FLEXIBILITY

- ◯ Is BYOD (Bring Your Own Device) available?
- ◯ Can you lease hardware from the vendor?
- ◯ Is BYOC (Bring Your Own Cloud) available?
- ◯ Can you replicate backups to the vendor's cloud?
- ◯ Is BYODC (Bring Your Own Data Center) available?

BACKUP TECHNOLOGY

- ◯ Is the solution built on chain-free image-based backup technology?
- ◯ Does the solution include built-in automatic backup integrity checks on all drives?
- ◯ Does the solution include built-in robust or pooled storage at a flat fee and retention without restrictions or tiers?

BCDR Solution Checklist for MSPs

CRITICAL CAPABILITIES

- ◯ Does the vendor cater exclusively to MSPs?
- ◯ Is 24/7/365 support included?
- ◯ Does the solution include built-in anti-data deletion technology?
- ◯ Does the solution include built-in self-managed disaster recovery (DR) and DR testing?
- ◯ Does the solution include automated runbooks?
- ◯ Is the recovery point objective (RPO) 15-minutes or less?
- ◯ Is the recovery time objective 1-hour or less?

SECURITY AND COMPLIANCE

What was the vendor's score on the most recent SecurityScorecard rating? _____

- ◯ Does the vendor utilize third-party, independent security testing?
- ◯ Is the vendor SOC 2 certified?
- ◯ Is the solution HIPAA compliant?
- ◯ Is the solution GDPR compliant?
- ◯ Is the vendor's data center certified by the SSAE or SOC?

PRICING

How much does storage cost each month? _____

What are the storage limitations? _____

What are the data retention limitations? _____

If leasing hardware is an option, what is the monthly cost? _____

What is the cost to buy new hardware? _____

How long does it take to onboard new clients? _____

How long does it take to train technicians? _____

How long does it take to certify technicians? _____

See how Axcient **x360Recover** provides comprehensive BCDR **without the local appliance.** Using **Chain-Free technology,** Axcient allows MSPs to standardize, simplify management, and lower costs while delivering best-in-class security with built-in, always-on features like **AutoVerify, Virtual Office,** and **AirGap.**

Start a Free 14-Day Trial Today

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.

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

Axcient