

An MSP's Blueprint for Profitably Selling Bundled Services



Contents



Bundled BCDR Pushes Legacy BDR Over the Edge

Why Bundle Your BCDR Services?

Does Your Stack Support the Strategy?

Part 1: Selling Your Commitment to Security

Step 1: Assess Your BCDR Services.

Step 2: Create Ideal Service Bundles.

Step 3: Sell BCDR Expertise.

Part II: Stack Optimization from a La Cart to All-in-One

Step 4: Assess Your BCDR Stack

Step 5: Prepare to Evolve.

Step 6: Consolidate BCDR Solutions.

Step 7: Find the Perfect Vendor

Next Steps: Implementing the Bundled BCDR Blueprint

Bundled BCDR Pushes Legacy BDR Over the Edge

The tipping point for optional, piecemeal backup, using multiple vendors, products, billing and admin procedures, support channels, onboarding tasks, ongoing maintenance, and recovery plans (whew!) has officially been hit.

High-performing MSPs are streamlining **business continuity and disaster recovery** (BCDR) by consolidating and standardizing on all-in-one solutions from a single vendor. By reducing the technical and administrative debt of over-complicated and disparate vendor systems, MSPs are cutting overhead costs, accelerating recovery, and delivering uniform data protection for all clients.

While the business and security benefits of modernizing your IT stack are obvious, the catalyst for the updated approach is based on the demands of **our cybersecurity landscape**. Small-to-medium-sized businesses (SMBs), including MSPs, are constantly targeted with sophisticated and frequent attacks.

As an MSP, you are a business owner who must meet clients' changing needs while optimizing your stack to deliver complete data protection. This is where strategically planning your bundled offerings can help your business mature and see profit growth while delivering on your SLAs.

Keep Reading To...



Discover the positive impact of a bundled services strategy for MSP owners, heads of sales, CTOs, and technicians.



Leverage BCDR simplicity as part of a mutually beneficial sales approach that directly addresses real client concerns with the cybersecurity you know they need.



Determine if your current tech stack supports the strategy and see what's required from vendors and solutions for implementation to be successful.

An Overview of the Cybersecurity Landscape:




- **83%** of breaches involve external actors, and **95%** are financially motivated.
- **74%** of breaches include a human element via error, privilege misuse, stolen credentials, or social engineering.
- **Top 3 ways attackers access data:** Stolen credentials, phishing, and exploitation of vulnerabilities.
- **24%** of breaches involve ransomware – making it the top threat action hackers use.
- **> 50%** of social engineering incidents rely on Business Email Compromise – or pretexting attacks – which have almost doubled in the last year.

Resource:

[Verizon 2023 Data Breach Investigations Report](#)

Why Bundle Your BCDR Services?

Moving from break/fix, backups only, and optional cybersecurity to customizable, comprehensive, and bundled BCDR simplifies complexity, reinforces data protection, and supports MSP profits. As a result, MSP leaders are embracing the shift for various reasons.

-  **MSP Owners love the consolidated structure** required for efficient bundled services because it inherently speeds operations, reduces recurring costs, and grows margins.
-  **MSP Heads of Sales and Marketing love the differentiated value** of bundled services – easy-to-understand, all-in-one security with predictable, straightforward pricing for peace of mind.
-  **MSP CTOs and Technicians love the productivity, focus, and cost-efficiency** of a standardized stack with hands-free automation to reduce tech debt, lower labor costs, accelerate restoration, and allow techs to master proficiency with a single solution.



Does Your Stack Support the Strategy?

Not all solutions can fulfill a bundled services strategy due to limited use case fulfillment, required manual interventions, and vendors focused on more than just MSPs. To achieve anticipated outcomes, your BCDR stack has to do more than just backup.

You need:



Flexibility to solve various use cases, including those with and without an appliance, using just one solution and vendor.



Billing predictability to accommodate immutable storage, long-term retention, and varying service level agreements (SLAs) with margin protection.



Data protection features to ensure BCDR efficiency, cost-effectiveness, and rapid and reliable recovery for clients.

Stack Your Stack Right

With a Reference Architecture (RA) design, top-performing MSPs are **2x as profitable** as average-performing MSPs.

[Get the RA Overview for MSPs](#)

In a nutshell...

- **Packaging BCDR services**
Ensures complete client data protection and safeguards MSPs from liability, *instead of relying on backups alone or à la carte security.*
- **Standardizing BCDR stacks**
Delivers the consolidated infrastructure necessary for profitably selling cybersecurity, *instead of juggling multiple solutions and vendors.*
- **Selling BCDR bundles**
Lets sales, marketing, and techs drive campaign optimization, revenue, and product innovation, *instead of elements of BCDR from scattered vendors.*

Part I: Selling Your Commitment to Security

Designing bundled security offerings specifically for your MSP means each package must consider your MSP's capabilities and the client's compliance requirements, industry standards, budgets, preferences, environments, and risk factors. The following steps walk you through the process of creating secure BCDR bundles that attract clients by catering to end-user needs.

Step 1: Assess Your BCDR Services

What do clients **THINK** they need?

The following 6 questions summarize SMB cybersecurity priorities:

1. Do you protect all of my data?
2. Am I safe from ransomware?
3. If something bad happens, will my business still run?
4. How do I know if it's working?
5. Will I pass my audits and maintain cyber insurance?
6. Is this affordable?

If You Can't Say "Yes" ...

It's always a good time to explore the market. Use this MSP guide to **choose the best solution and vendor** for achieving your goals.

[Get the BCDR Buyer's Guide](#)

What do you **KNOW** clients need?

Respond to those 6 questions by highlighting how your BCDR bundle addresses each need. For example, with **x360Recover**, you can say...

- 1. Yes, I protect ALL your data!** Image-based backups protect all data by default, so everything on the system is covered and cannot be easily excluded.
- 2. Yes, you are safe from ransomware!** Being secure by design, not configuration, means that fundamental safety features for **immutable backups** are always on and cannot be misconfigured.
- 3. Yes, your business will keep running!** Business continuity for all, with or without an appliance, ensures flexible recovery options to keep businesses moving.
- 4. Yes, you will see it is working!** Automated, on-by-default, in-depth, daily **backup integrity testing** monitors and alerts, provides screenshot verification, and ensures backup health with self-adapting and self-healing technology.
- 5. Yes, you pass audits and be insured!** Highly detailed and automatic **reporting capabilities** provide evidence of BCDR procedures and outcomes to easily satisfy audits, compliance, and insurance requirements and ensure client confidence.
- 6. Yes, it is affordable!** In an apples-to-apples comparison, we are less expensive than the alternative – legacy backup and the fears and risks that come with it – and we're also less expensive than other true BCDR competitors.

Step 2: Create Ideal Service Bundles



Establish minimum client security standards.

MSPs can no longer allow clients to forgo necessary data protections while promising business continuity. New and expanding breach notification laws, government requirements, industry demands, and cyber insurance must-haves are raising the threshold for cybersecurity, and both clients and MSPs are in the hot seat.

- **Protect everyone** by demanding a baseline of BCDR protection using current SMB cyber threats, not individual risk tolerance.
- **Reinforce security** to efficiently meet competitive SLAs and protect your MSP from liability when an under-protected client can't recover.
- **Avoid conflicts** with clients who were given the opportunity – and took it – to opt out or misconfigure complete BCDR and suffer data loss as a result.



Differentiate bundles based on use cases.

As you build your security bundles using minimum client standards, consider how the following factors influence BCDR use case fulfillment for more clients.

- **Demographics:** Budget, size, and industry or vertical.
- **Environment:** Endpoint backup, appliance-free BDR, turnkey BDR, and public cloud backup.
- **Compliance:** Retention, storage, and immutability needs.
- **Reporting:** Proof of BCDR best practices for audits, compliance, and insurance.
- **SLA:** RTO and RPO.

Hear from a Peer:

Swapping transactional customer relationships with BCDR bundled security:

“When I first started, losing, turning away, or cutting ties with clients seemed like crazy talk. Now, I realize it’s imperative to stay healthy and protect ourselves. I’m responsible for my employees, their livelihoods, and their families. If I’m reckless with who and how I engage – and let our clients put us at risk – that is on me.”

– Dennis Cockrell,
Founder/CEO at EIT Networks

Step 3: Sell BCDR Expertise



Build trust.

Assert your authority as a cybersecurity expert and guide that prioritizes data protection ahead of profits. Showcase your security bundles as evidence of your commitment to their business.



Educate.

An MSP's job is to continuously inform clients about the threats to their business and the consequences of reactive disaster recovery. The more clients understand, the more willing they are to act on your guidance toward proactive cybersecurity.



Be Transparent.

SMBs must understand the “why” behind an MSP's BCDR bundles and security standards. Not all SMBs will appreciate your high standards at first. Still, after discussing the criticality of features and the potential fallout of an incident, most are thankful for the simplicity of pre-determined, all-inclusive security bundles.

Ready to Grow Sales?

Enjoy 3 resources in 1 for campaign, search, ad, and event optimization using targeted verticals, budget-friendly strategies, and actionable takeaways.

[Get the Sales and Marketing Playbook](#)

Hear from a Peer:

Streamlining stacks to standardize and optimize BCDR management:

“We had about 25 different backup vendors, and we were spread too thin. You can't focus on any one vendor or product. There are different training plans, different product support, compression is different, retention is different, and they all do different things. We wonder how we did it at 25.”

– Neil Hawkins,
COO at LANAIR Technology Group

[Get the Whole Story](#)

Part II: Stack Optimization from À La Cart to All-in-One

Now that you see how a bundled BCDR approach strengthens client security, MSP protection, and sales and marketing strategies, it's time to realize the design with a robust solution and dedicated vendor. Continue these steps to understand how your stack needs to be structured, what features make it easy, and who to partner with for success.

Step 4: Assess Your BCDR Stack



What is the REAL cost of your vendors?

Ask yourself the following 3 questions to accurately assess the true cost of your stack:

- 1. How many different processes** do you adhere to for billing, support, client onboarding, tech training, maintenance, and disaster recovery – per vendor and solution?
- 2. How many different solutions** do you use to fulfill BCDR client use cases?
- 3. How many different sales strategies and marketing campaigns** must you develop to gain an ROI on each solution?

With each new vendor and solution added, MSPs must increase their required labor costs. And the enduring tech skills gap makes finding, hiring, and retaining IT expertise a long and expensive process. While technical labor costs are often a priority, many MSPs don't realize the administrative burden of juggling disparate, time-consuming processes based on inefficient vendor demands.

Lastly, a historical sticking point for most SMBs – including MSPs – is growing net new revenue and expanding contracts with current clients. Creating, launching, and optimizing individualized product marketing materials and sales support demands the attention of a dedicated team to track and manage multiple campaigns simultaneously. Ask yourself...



What OBSTACLES are preventing profitability?

As you analyze the cost of your stack, identify the bottlenecks and inefficiencies blocking profitability. The most common barriers stem from the number of processes, solutions, and selling techniques required to manage a sprawling stack.

- 1. How does the number of vendors and solutions in your stack impact** MSP profitability, sales revenue, and technician productivity?
- 2. What vendors and solutions are causing** the identified obstacles?
- 3. What type of vendors and solutions are missing** that would increase efficiency?

Step 5: Prepare to Evolve.



Act on vendor red flags.

Vendor shakeups through acquisitions and mergers force providers to widen their focus to larger markets. MSPs commonly experience longer response times, changing account reps, fewer feature releases and updates, discontinued products, higher prices, more limits, and a decline in MSP-specific resources. These **service downgrades prevent MSP innovation** leaving you stuck with legacy manual tasks that increase costs, threaten security, and frustrate technicians. Move on quickly or risk going down with the ship.



You deserve more.

Confronting the reality of a partner no longer committed to the original agreement you aligned on justifies the consolidation effort. Once that's acknowledged, you can get the most out of a good vendor or suffer in silence with a bad one. **A good partner for MSPs is a 100% MSP dedicated vendor** that understands and ensures client and MSP protection with easy-to-digest reporting,

innovative automation, responsive and frequent product launches and upgrades, done-for-you resources, and a mutually beneficial partner program. These are the protections and features that should be available to all MSPs.



Think long-term.

Some MSPs feel overwhelmed by standardizing and offloading vendors, but **moving vendors is a short-term inconvenience with long-term payouts.** Avoid having to re-stack often by partnering with vendors with a demonstrated commitment to solving evolving MSP pain points. Has use case fulfillment expanded without adding to management costs? Is the product a one-trick pony or an all-in-one solution with broadening capabilities? Are you confident in your vendor's business structure, associations, and historical actions? High-value vendors prioritize MSP security, scalability, and business growth for a lasting relationship.

Hear from a Peer:

Leveraging automation and bundled BCDR for higher margins:

“Simplifying processes by consolidating into one vendor allows us to automate many low-value tasks. Now, I can use my team for high-value, customer-facing things rather than just managing a bunch of backups.

...At a minimum, we make a 35% gross margin on our Axcient stack. Typically, though, it's closer to 50% because we bundle local and cloud backup into all of our managed services agreements.”

– Luis Alvarez, CEO at Alvarez Technology Group

[Get the Whole Story](#)

Step 6: Consolidate BCDR Solutions.

Utilize your BCDR services and stack assessments, ideal bundle designs, and identified obstacles to plan your path to consolidation and selling security bundles. Keep or find BCDR solutions that check these 5 boxes to maximize simple and profitable bundled services as you whittle stack complexity.

Made for MSPs

Solutions designed and developed exclusively for MSPs offer the most **targeted benefits to help MSPs now and in the future**. These solutions are secure by design, directly addressing the number one cause of data loss – human error – with failsafe features that replace manual requirements with pre-configured, always-on data protection.

Flexible use case fulfillment

The more client use cases an MSP can solve with a single solution, the more efficient your stack will be. Standardization is ideal for growing with current clients and attracting new SMBs. Cover various environments with multiple **deployment options** in one solution – including endpoint backup, hardware-free BDR, full-service BDR, and public and private cloud protection.

Proactive protection

Secure-by-design solutions rely on modern innovations like always-on, automatic features to reinforce cybersecurity. They accelerate productivity, reduce labor costs, and lower risks with hands-off backup checks, immutable data, **pooled storage**, and **automated disaster recovery and DR testing**. With these protections in place by default, MSPs **stay one step ahead of attackers and accidental data loss**, preventing business interruptions no matter what.

Unconditional security

When proactive protection is built into a BCDR solution, everyone gets **robust cybersecurity, regardless of budget or pricing tier**. Data protection should always be primary, and automatic protections that meet your MSP's minimum client security standards ensure business continuity for all – including your MSP.

Transparency

Proof of BCDR capabilities, cybersecurity infrastructure, and testing outcomes is required to satisfy audits, compliance standards, and insurance policies. **In-depth, auto-generated, and customizable reporting and dashboards** make it easy to support external needs while gaining client trust. Don't wait for a disaster to show the value of your solutions. Give **clients regular updates** in easy-to-understand formats to drive new sales, **upsells, and cross-sells** as part of your ongoing sales cycle.

See How Your MSP Peers Are Consolidating

Solve vendor sprawl with these MSP-driven strategies for meeting most use cases with one solution.

[Get the 6 BCDR Must-Haves ebook](#)

Step 7: Find the Perfect Vendor

The last puzzle piece to efficient bundled security services is the vendor you choose to partner with. Beyond having the BCDR solutions required for data protection, vendors should be painless, profitable, and proven.



Painless data protection for fewer headaches.

- Easy to use.
- Easy to sell.
- Easy to do business with.
- Easy to talk to someone.
- No term contracts with auto-renewals.
- No having to master multiple vendors.
- No “ridiculous” licensing models.
- No frustration with support or services.



Profitable simplicity for higher revenue.

- Reduces technical labor costs.
- Delivers > 50% gross margins.
- Simplifies your MSP.
- Helps your MSP grow.
- No surprise storage overages and fees.
- No monitoring and verifying chains.
- No data bloat and reseeded.
- No failed backups and replications.



Proven business enablement never lets you down.

- Always there when you need it.
- Proven value through reporting.
- Recovery, no matter what.
- Meet competitive SLAs.
- No broken solutions.
- No unhappy surprises.
- No unresponsive vendors.
- No fear.

Hear from a Peer:

Increasing monthly revenue by \$12,000 with the right vendor:

“I’m making six figures more than I was last year on backup savings alone. ...My advice for other MSPs is to quit dragging your feet. Schedule a demo with Axcient. Try it somewhere. Put it on an internal server. Stop with the 15 different solutions and training nightmares. Just come to Axcient, and they’ll show you how to do it right.”

– Todd Maddex, President of Tampa Bay Tech Solutions

[Get the Whole Story](#)

Next Steps: Implementing the Bundled BCDR Blueprint

Moving forward with this strategy starts with finding solutions and vendors that can make it a reality. Axcient **x360Recover** is a secure-by-design, complete BCDR solution that enables bundled services using multiple deployment options, immutable data, automated security features, and the support of an MSP-only provider. See how we can support your MSP:

Schedule a 1:1 Demo

Request a BCDR Quote

Start Your Free 14-Day Trial

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 4,800 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