

EBOOK

An MSP's Guide to Profitably Selling Bundled Security



Contents

Introduction: How to Right-Size Bundled Backup and Security Offerings 3

Why Bundling Drives Growth and Protection 4

 Bundling BCDR Services.....4

 Bundling Monitoring and Security Services 4

 Bundling Backup and Security Services 5

 Does Your Stack Support the Strategy? 5

Part I: Selling Your Commitment to Security 6

Part II: Stack Optimization from Á la Carte to All-in-One 11

Next Steps: Implementing Bundled Security 15



Introduction: How to Right-Size Bundled Backup and Security Offerings

Piecemeal backup has reached its breaking point for MSPs actively looking to grow their businesses. Managing multiple vendors, products, billing and admin procedures, support channels, onboarding tasks, ongoing maintenance, and recovery plans is no longer sustainable.

High-performing MSPs are streamlining business continuity and disaster recovery (BCDR), endpoint detection and response (EDR), and security information and event management (SIEM) by consolidating and standardizing on a comprehensive security package. By reducing the technical and administrative debt of over-complicated and disparate offerings and vendor systems, MSPs are cutting overhead costs, accelerating recovery, and delivering uniform data protection for all clients.

MSPs face constant pressure to meet evolving clients' changing needs while optimizing their stack to deliver complete security and data protection. This is where strategically planning your bundled offerings for clients can help your business mature and see profit growth while delivering on your SLAs.

In this guide, you'll learn how to:



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



Leverage BCDR and cybersecurity 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 own current tech stack supports the strategy and see what's required from vendors and solutions for implementation to be successful.

Why Bundling Drives Growth and Protection

Bundling the protections your clients need simplifies sales while strengthening security outcomes. For clients who understand the seriousness of data loss and cyberattacks, a comprehensive package is often an easy decision. For others, education is essential, especially for those with budget concerns or who are skeptical of the value.

Clients operating without comprehensive protection put their business, end-users, and MSP at risk. Growing regulations and the court of public opinion are holding service providers accountable for data breaches. As cybersecurity experts, it's an MSP's job to deliver the appropriate level of security required to withstand today's attacks.

When a client suffers an intrusion, attack, or data loss incident, the impact can be devastating for both the client and the MSP. Fines and penalties are one thing, but a public record of a breach under your watch can have a lasting negative impact on your reputation. This is why many mature MSPs refuse to take on clients unwilling to accept their standard package of data protection and security services. Others may offer more flexibility but require clients to sign an acknowledgment of risk and liability in the event of data loss.

By setting clear expectations and reinforcing the value of bundled security, MSPs close deals more effectively and protect their clients, reputation, and long-term growth.

Bundling BCDR Services

Moving from break/fix and backup-only models to customizable, comprehensive, and bundled BCDR simplifies complexity, reinforces data protection, and supports MSP profits: **MSP owners** benefit from streamlined operations, reduced costs, and improved margins.

- **Sales and marketing** teams gain a clear, differentiated offering with simple, predictable pricing.
- **Technical teams** benefit from standardized tools, automation, reduced tech debt, and faster recovery.

Bundling Monitoring and Security Services

Bringing EDR and SIEM into a unified, managed security offering reduces alert fatigue, improves threat detection, and enables faster, more coordinated response. Instead of juggling siloed tools, MSPs gain a cohesive security posture that is easier to manage and more valuable to clients.

- Stronger, faster threat detection and response: Correlating endpoint activity with SIEM data provides deeper context, reducing false positives and enabling quicker, more accurate remediation.
- Operational efficiency and scalability: A unified monitoring and security stack minimizes [tool sprawl](#), streamlines workflows, and allows teams to manage more clients without increasing headcount.
- Clearer value for clients: Bundled security services are easier to position and sell, offering comprehensive protection with simplified pricing and measurable outcomes.

An MSP's Guide to Profitably Selling Bundled Security

Why Bundling Drives Growth and Protection

Bundling Backup and Security Services

Security and backup are no longer separate conversations because modern resilience requires both prevention and recovery. Bundling BCDR with EDR and SIEM creates a complete cyber-resilience solution that protects, detects, and restores, all within a single strategy.

- **Complete protection across the attack lifecycle:** Prevent endpoint threats with EDR, detect and respond across endpoints, identities, SaaS environments, and networks with SIEM, and recover quickly with BCDR, closing gaps that attackers exploit.
- **Improved client outcomes and reduced risk:** Faster detection combined with reliable recovery minimizes downtime, data loss, and financial impact from cyber incidents.
- **Higher-margin, stickier services:** A comprehensive bundle increases contract value, reduces churn, and positions the MSP as a strategic partner rather than a point solution provider.

Does Your Stack Support the Strategy?

Not all solutions can fulfill a bundled services strategy. To achieve anticipated outcomes, your BCDR and security stack must do more than just basic monitoring and backup.

You need:

- Flexibility to solve various use cases with as little tool sprawl as possible to ensure successful monitoring and response.
- 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.
- The right endpoint detection and event monitoring tools for your current and desired future client mix.

Key takeaways

Packaging security and BCDR services **ensures complete client data protection** and safeguards MSPs from liability, instead of relying on backups alone or á la carte security.

Standardizing BCDR and security stacks delivers the **consolidated infrastructure necessary for profitably selling cybersecurity**, instead of juggling multiple solutions and vendors.

Selling security bundles lets sales, marketing, and techs **drive campaign optimization and revenue**. Plus offering innovation, instead of security elements and disparate features from scattered vendors that may not integrate well with each other.

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 current security and BCDR services

Before you can build effective bundled offerings, you need a clear understanding of how your current services stack up and your clients' expectations. This step helps you align perceived needs with the security and data protection you know they actually require.

What do clients THINK they need?

These eight questions summarize

[SMB cybersecurity](#) priorities:

1. Do you protect all of my data?
2. Will you detect breaches proactively or respond proactively?
3. Am I safe from ransomware?
4. If something bad happens, will my business still run?
5. How do I know if it's working?
6. Do my security products integrate with each other?
7. Will I pass my audits and maintain cyber insurance?
8. Is this affordable?



An MSP's Guide to Profitably Selling Bundled Security

Part I: Selling Your Commitment to Security

What do you KNOW clients need?

When responding to clients, highlight how your cybersecurity and data protection bundled offering addresses each need.

For example, with [x360Recover](#), you could say:

1. **Yes, it protects 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, ransomware protection is included!**

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 insurance audits!**

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.



An MSP's Guide to Profitably Selling Bundled Security

Part I: Selling Your Commitment to Security

With [ConnectWise Managed EDR™](#) and [ConnectWise SIEM™](#), you could say:

1. Yes, it protects ALL your endpoints and users!

Advanced endpoint detection and response combined with SIEM visibility ensures coverage across devices, identities, and behaviors, so threats can't hide in overlooked gaps.

2. Yes, you are protected from modern threats!

Behavioral detection, threat intelligence, and 24/7 monitoring identify ransomware, fileless attacks, and zero-day activity before they can cause damage.

3. Yes, your business will stay operational!

Rapid detection and automated response capabilities contain threats quickly, minimizing downtime, and preventing incidents from escalating into business disruptions.

4. Yes, you will see it is working!

Centralized dashboards, real-time alerts, and clear reporting provide full visibility into security events, responses, and overall security posture.

5. Yes, you can meet compliance and insurance requirements!

Comprehensive logging, retention, and reporting across endpoints and environments help satisfy regulatory frameworks, cyber insurance mandates, and audit requests.

6. Yes, it is scalable and profitable!

A unified, managed approach to EDR and SIEM reduces tool sprawl, improves operational efficiency, and enables MSPs to deliver high-value security services at scale.

If you can't say "yes" then it's a good time to explore the market. Use these MSP guides to **choose the best solution and vendor** for achieving your goals.

[The BCDR Buyer's Guide for MSPs | ConnectWise](#)

[EDR and SIEM: Why You Need Both | ConnectWise](#)

Step 2: Create ideal service bundles

With a clear view of client needs, the next step is designing bundled offerings that balance protection, profitability, and scalability. This means establishing baseline security standards and tailoring bundles to meet a range of client environments and requirements.

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 security and protection using current SMB cyberthreats, 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 choose to opt out or misconfigure complete BCDR or security that results in a breach or data loss.

Differentiate bundles based on use cases

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

- **Demographics:** Budget, size, and industry or vertical.
- **Environment:** Endpoint backup, cloud or appliance backup needs, hybrid environments, and public cloud use.
- **Compliance:** Retention, storage, access, and immutability needs.
- **Reporting:** Proof of security and data protection best practices for audits, compliance, and insurance.
- **SLA:** Detection time, [recovery time objective \(RTO\)](#), and [recovery point objective \(RPO\)](#).

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 and CEO at EIT Networks

Step 3: Sell BCDR and security expertise

Even the strongest bundles won't succeed without trust and clear communication. In this step, you'll focus on positioning your MSP as a security expert and guiding clients toward proactive, protection-first decisions.

Build trust

Assert your authority as a cybersecurity expert and guide that prioritizes cyberattack and 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 bundles and security standards. Not all SMBs will appreciate your high standards at first. 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.

HEAR FROM A PEER:

Streamlining stacks to standardize and optimize 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

Part II: Stack Optimization from À la Carte to All-in-One

Now that you see how a bundled security approach strengthens client security, MSP protection, and sales and marketing strategies, the next phase is 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 security stack

Once your bundles are defined, it's time to evaluate whether your current stack can support them. This step helps uncover hidden costs, inefficiencies, and operational barriers that may limit profitability and scalability.

What is the REAL COST of your vendors?

Ask yourself these three questions to accurately assess the true cost of your stack:

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

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.

With each new vendor and solution added, you 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 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:

1. **How does the number of vendors and solutions in your stack impact** MSP profitability, sales revenue, and technician productivity?
2. **What obstacles are caused by vendors and solutions?**
3. **What type of vendors and solutions are missing** that would increase efficiency?
4. **Do my vendors support my business growth**, and do they have a strong partner program?

Step 5: Prepare to evolve

After identifying gaps in your stack, the next step is planning for change. This means recognizing when vendors no longer support your growth and making strategic decisions that set your MSP up for long-term success.

Act on vendor red flags

Migration and changing solutions are unpleasant. You can get the most out of a good vendor or suffer in silence with several bad ones. If your security or BCDR vendor shows signs of stagnation, it's a signal to reassess the partnership, including limited product development, infrequent enhancements, or a roadmap that hasn't meaningfully evolved. In a threat landscape that changes daily, standing still is falling behind. Likewise, vendors that fail to invest in partner programs, training, and channel events may not be equipped to support your growth or help you differentiate in the market.

MSPs should align with vendors that are actively innovating and committed to their partner ecosystem, ensuring you can deliver modern, competitive, and profitable security solutions.

Think long-term

Moving vendors is a short-term inconvenience with long-term benefits. Avoid frequent re-stacking by partnering with vendors that demonstrate a 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?
- Is your vendor investing in native and third-party integrations that really work and save you time?

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

Step 6: Consolidate BCDR and security solutions.

With your strategy and direction defined, you can begin simplifying your stack. This step outlines the key capabilities to look for in solutions that support efficient, scalable, and profitable bundled services.

Use your cybersecurity services and stack assessments, ideal bundle designs, and obstacles from above to plan your path to consolidation and selling security bundles.

To maximize simple and profitable bundled services as you whittle stack complexity, keep or find BCDR, EDR, and SIEM solutions that check these five boxes:

Made for MSPs

Solutions designed and developed for MSPs offer the most **targeted benefits to help MSPs now and in the future**. You need tools that are set up for how you do business. These solutions directly address the number one cause of data loss: human error. They are secure by design, with failsafe features that replace manual requirements with preconfigured data protection for MSPs, providing always-on data protection that is set up and priced to support the managed services business model.

Flexible use case fulfillment

The more client use cases you 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 and flexibility in one vendor, including endpoint threat detection and backup, hardware-free and cloud-based BDR, full-service security monitoring, and public and private cloud-friendly protection.

Proactive protection

Secure-by-design solutions rely on modern innovations such as always-on, automatic features to reinforce cybersecurity. These important **features shouldn't cost extra or be hidden behind complicated tiered solutions and pricing**. They accelerate productivity, reduce labor costs, and lower risks with hands-off monitoring and dependable alerting, backup checks, immutable data, ample and pooled storage, significant automation, and smart use of AI. With these protections in place by default, MSPs stay one step ahead of attackers and accidental data loss, preventing business interruptions.

Unconditional security

When proactive protection is built into security and data protection solutions, everyone gets robust cybersecurity, regardless of budget or pricing tier. This proactive protection is a must-have, not a nice-to-have. Client infrastructure security and data protection should always be a primary concern, and automatic protections that meet your MSP's minimum client security standards ensure business continuity for all, including your MSP.

Transparency

Proof of BCDR and security capabilities, cybersecurity infrastructure, and testing outcomes is required to meet audit requirements, compliance standards, and insurance policies. **In-depth, auto generated, and customizable reporting and dashboards** make it easier 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.

Step 7: Find the right vendor for you

The last step toward efficient bundled security services is the vendor you choose to partner with. Beyond having the EDR, SIEM, and BCDR solutions required for data and threat protection, select proven vendors with consistent support.

Look for vendors that deliver value across three key areas:

Data protection and security with fewer headaches

- ☐ Simplifies your MSP
- ☐ Easier to use and sell
- ☐ Easier to do business with
- ☐ Stress-free alert management
- ☐ No need to master multiple vendors
- ☐ No convoluted licensing models
- ☐ No extra fees for important features

Profitable simplicity for higher revenue

- ☐ Reduces technical labor costs
- ☐ Delivers > 50% gross margins
- ☐ Helps your MSP grow
- ☐ Enhanced with SOC and NOC services
- ☐ Right-priced security for any client budget
- ☐ No surprise overages or fees
- ☐ No monitoring and verifying backup chains

Proven business enablement

- ☐ Proven value through reporting
- ☐ Recovery, no matter what
- ☐ Meet competitive SLAs

Hint: ConnectWise checks all the boxes above

HEAR FROM A PEER:

Requiring endpoint threat detection to monitor, detect, and respond to cyberthreats across all your managed endpoints:

"For us, having 24/7 monitored EDR or MDR is not an option, it is a requirement. One of the biggest benefits of [ConnectWise MDR has] been enabling us to step into the managed security services market without having to build out an entire 24/7 SOC."

Adam Harling
Managing Director, Netitude

Next steps: Implementing Bundled Security

Moving forward with this strategy starts with finding solutions and vendors that can make it a reality. ConnectWise cybersecurity and data protection is an enterprise-ready tech stack trusted by MSPs of all sizes. Get the software, services, and support you need to sell and secure your clients 24/7.

[x360Recover](#) from Axcient™, a ConnectWise company, is the only vendor with patented chain-free backups that reduce risk to your backup data. As the industry's only multi-patented chain-free, image-based BCDR that guarantees independent, automatically verified backups for fast and more reliable recovery without the risk, complexity, or fragility of chain-based tools, it enables bundled services using multiple deployment options, immutable data, automated security features, and the best support team in the channel. See how [x360Recover](#) can support your MSP:

- ⇒ [Watch an on-demand x360Recover demo](#)
- ⇒ [Start your free 14-day x360Recover trial](#)
- ⇒ [Talk to the data protection team](#)

Cybersecurity solutions from ConnectWise have everything you need, including [ConnectWise Managed EDR™](#) and platform-powered [ConnectWise SIEM™](#), to start capturing a piece of the security services revenue opportunity, with the most complete cybersecurity platform on the market today, providing everything you need to keep your clients secure and boost profits. See a live demo to learn how we do it:

- ⇒ [Get a ConnectWise SIEM 3.0 live demo](#)
- ⇒ [Watch an on demand Managed EDR demo](#)
- ⇒ [Talk to the security team](#)

