

The MSP's ultimate guide to security offerings

Security offering is no longer a luxury service — it's an expectation. But more than that, it means your business can **become incredibly profitable, see steady returns and drive meaningful growth.**

This isn't just a bold claim, though. It's backed by data.

The [2025 MSP Benchmark Survey](#) found that MSPs earning net profit margins of 15% or more ranked enhanced security services among their top three sources of revenue. In contrast, those with lower margins did not.

This isn't a coincidence. **Security is one of the most reliable ways for MSPs to increase revenue and protect their bottom line.**

The [2024 Datto State of the MSP Report](#) came to the same conclusion: top-performing MSPs lead with cybersecurity. Services like endpoint detection and response (EDR), email security and managed detection and response (MDR) aren't just extra features but client-retention powerhouses and sales differentiators.



Your clients expect security

Cyberattacks aren't slowing down. If anything, they're accelerating, and artificial intelligence (AI) is helping cybercriminals move faster and look more convincing than ever before.

- AI-generated phishing emails can look like they came from your client's CEO
- Ransomware-as-a-Service (RaaS) kits let attackers launch campaigns in minutes
- Deepfake audio is being used to impersonate executives during phone calls

It's no surprise that your clients are concerned and are looking for someone they can trust to keep their business safe. MSPs who step up and take on that role stand to gain.

This checklist provides simple steps you can take to move from being a traditional IT support provider to a go-to managed security expert.

Step 1: Define the type of solutions you need

Ask yourself:

What do managed security service providers (MSSPs) offer that I don't?

What threats are my clients most worried about?

MSSPs go beyond basic antivirus and firewalls. A modern security stack includes:

Endpoint detection and response (EDR)

Managed detection and response (MDR), also known as managed security operations center (SOC)

Advanced email security and phishing protection

24/7 monitoring and response for threats

Patch management and zero-day protection

Top threats MSP clients face (Datto 2024 report):

Phishing emails: 64%

Business email compromise: 61%

Malware/viruses: 59%

Password compromise: 56%

Endpoint threats: 51%



Step 2: Find the right security vendor

You don't have to struggle with building your own security stack, but you do need a trusted vendor who can help you build it affordably. Look for vendors that offer:

Multitenant tools built for MSP workflows

24/7 security operations center (SOC) services for scaling your response

Proven integrations with your current stack (RMM, PSA, etc.)

Affordable pricing that still enables margin growth

Ongoing training and reliable support

Vendors like [Datto](#) offer security solutions purpose-built for MSPs, such as Datto EDR, Datto AV and Datto MDR/managed SOC.



**Your goal: Build a stack
that prevents, detects and
responds to these threats.**

Step 3: Train your team

Before rolling out services to clients, make sure your team is fully up to speed.

- Provide product training with your vendor
- Build internal SOPs for onboarding and response
- Certify technicians where needed, especially for SOC tools
- Align your team on how to position and support each new service



Tip: Focus messaging on peace of mind, always-on protection and business continuity, not just technical features.

Step 4: Market your new capabilities

If you don't tell people, they won't know. And if you only tell them once, they'll probably forget. To get real traction, you'll need to promote your security services consistently across the channels your clients already pay attention to. Easy ways to get the word out:

- Add a Security Services page to your website
- Include security offerings in onboarding materials and pitch decks
- Announce new services in newsletters and prospect emails
- Write blog posts about common security risks and simple best practices
- Share easy tips on LinkedIn or Facebook, like how to spot a phishing email
- Create a short video explaining how your services protect against ransomware, reduce downtime or data loss
- Host a webinar or run targeted ads to reach new prospects

Step 5: Build social proof

Credibility builds trust, and trust drives growth. Once your clients start seeing value, turn their feedback into assets.

- Ask happy customers for testimonials
- Create short case studies that highlight real results
- Use quotes in presentations, email campaigns and your website

Security is the smartest move you can make right now

The MSPs seeing the most growth are the ones who've added security to their core offerings. This isn't just a smart business move, it's a critical step in meeting client expectations and staying competitive. Want to know which solutions belong in a modern, effective MSP security stack and who can help you deliver them? Hear from your peers and learn more about how to make your security stack stronger by downloading our eBook:

The security stack that makes IT stronger

<https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/>

datto
A Kaseya COMPANY