The MSP's Guide to Evaluating Security Vendors

How to pick partners who can protect your clients and boost your bottom line.

HUNTRESS

Table of Contents

Introduction

The MSP's dilemma

For managed service providers (MSPs), there's an all-too-familiar scenario: a flashy demo, a smooth sales pitch, and an unbeatable price from a cybersecurity vendor. But fast-forward six months, and your biggest client suffers a breach. That's when the finger-pointing begins, and along with it comes the loss of trust, time, and money. Welcome to the expensive trap of "shiny object syndrome," something MSPs simply can't afford to ignore anymore.

Cybersecurity is more complicated than ever. Threats evolve daily, clients expect stronger protection, and new vendors pop up faster than you can vet. As an MSP, you're stuck in the middle, expected to be the expert who always makes the right call every time.

The stakes are obviously high. The vendors you choose directly affect your reputation. If a security tool fails, your clients won't blame the vendor. They'll blame you.

But when you pick the right partner, you can stand out, boost efficiency, and earn solid, long-term client trust.

To help you avoid "shiny object syndrome," we've put together this ebook, which provides an easy-to-follow framework for cutting through vendor marketing noise and choosing cybersecurity partners that can actually protect you and your clients.

For MSPs, choosing the right vendor is everything

Your risk: Every bad vendor decision puts you at risk of:

- Losing clients
- Compliance failures
- Tech debt
- Employee churn
- Major breaches that damage your business

Your opportunity: The right vendor becomes your competitive advantage, allowing you to win bigger deals, retain clients longer, and sleep better at night.

Consider these realities:

94%

of nearly all small and medium-sized businesses now lean on MSPs for their cybersecurity[1]

30%

of breaches involve third parties, even by conservative estimates[2]

84%

of MSPs say clients expect them to handle cybersecurity and IT infrastructure[3]

Choosing the right vendor is a big deal because MSPs are trusted advisors. Your clients expect you've done your homework on every technology you suggest. To them, a vendor's flaws are your flaws. And when something goes wrong, guess who's getting that call at 2am?

YOU!

HUNTRESS

The Security Vendor Evaluation Framework

Business alignment

Before even jumping into features and functionality, ask yourself one key question: "Does this cybersecurity vendor really understand how MSPs make money?"

With that in mind, focus on vendors who:

- ☐ Have dedicated channel support teams to meet your specific needs
- ☐ Understand the importance of multi-tenant requirements
- ☐ Offer pricing models designed for MSPs (e.g., predictable, scalable, and per-endpoint)
- ☐ Have dedicated channel support teams to meet your specific needs

Keep an eye out for red flags like vendors treating MSPs as regular customers or lacking a clear channel strategy.

HUNTRESS

Technology and integration

Your security stack needs to work as a unified system, not a collection of isolated platforms for each tool.

Essential technical criteria to consider:

- ☐ Comprehensive coverage (endpoints, networks, identities, cloud)
- ☐ Proprietary technology (avoid OEM models that add unnecessary complexity)
- ☐ Advanced detection rules and analytics capabilities
- ☐ Native multi-tenancy support for MSP operations

Remember, the best vendors don't just sell software. They give you a technology foundation on which to build your services.

HUNTRESS

Security posture and compliance

You can't protect your clients with vendors who can't protect themselves.

Essential vendor evaluation checklist:

Certifications verified

- ☐ SOC 2 Type II
- ☐ ISO 27001
- ☐ Industry-specific compliance (e.g., HIPAA, GDPR, Essential Eight)

Incident history reviewed

- ☐ Transparent communication about past incidents
- ☐ Clear remediation steps and lessons learned
- ☐ No pattern of recurring security issues

Data governance policies

- ☐ Clear data handling procedures
- ☐ Geographic data residency requirements met
- ☐ Appropriate data retention policies

Third-party validation obtained

- ☐ Independent security audits
- ☐ Penetration testing results
- ☐ Current SOC reports available

Breach notification procedures

- ☐ Clear SLAs for incident communication
- ☐ Defined escalation procedures
- ☐ Customer notification protocols

But this is about more than checking boxes. It's about making sure your vendor meets the same security standards you promise your clients.

HUNTRESS

Operations and support

When a threat hits at 3am, you want a cybersecurity partner who's alert, ready, and knows how to act fast.

What really matters from a vendor:

- ☐ **24/7 SOC availability:** It's not just about monitoring. You need real-time, human-driven analysis and response.
- ☐ **Clear SLAs:** Response times, breach notifications, uptime guarantees—everything should be spelled out.
- ☐ **Strong escalation processes:** When things are urgent, how quickly can you reach decision-makers?
- ☐ **Fast remediation:** Containing and resolving threats quickly is everything.
- ☐ **Evolving threat detection:** Are they constantly improving at spotting and stopping risks?

The difference between a good security vendor and a great one is how they handle a crisis. The best security vendors turn challenges into opportunities to build trust and prove their worth.

HUNTRESS

Channel partnership

True partnerships go beyond technology. They focus on building solid business relationships.

What to look for in a real partner:

- ☐ Training programs built for MSPs, covering both technical and sales skills
- ☐ Dedicated channel account managers who've got your back
- ☐ Support for joint campaigns and lead generation to grow your business
- ☐ Marketing development funds and co-marketing opportunities that actually help
- ☐ Competitive pricing to keep your margins healthy

The best vendor partners feel like an extension of your team, not just another supplier.

HUNTRESS

Proof and validation

Trust, but verify. Every vendor says they're the best, but you need proof before making a decision.

How to make sure they deliver:

- [ ] Ask for references from MSPs with similar clients
- [ ] Competitive pricing to keep your margins healthy
- [ ] Check out case studies that show real, measurable security results
- [ ] Try a pilot program to see their value in action before committing
- [ ] Look for independent third-party reviews for an unbiased take

For an even better perspective, talk to MSPs who've worked with specific vendors for at least 18 months. They'll give you the full story.

HUNTRESS

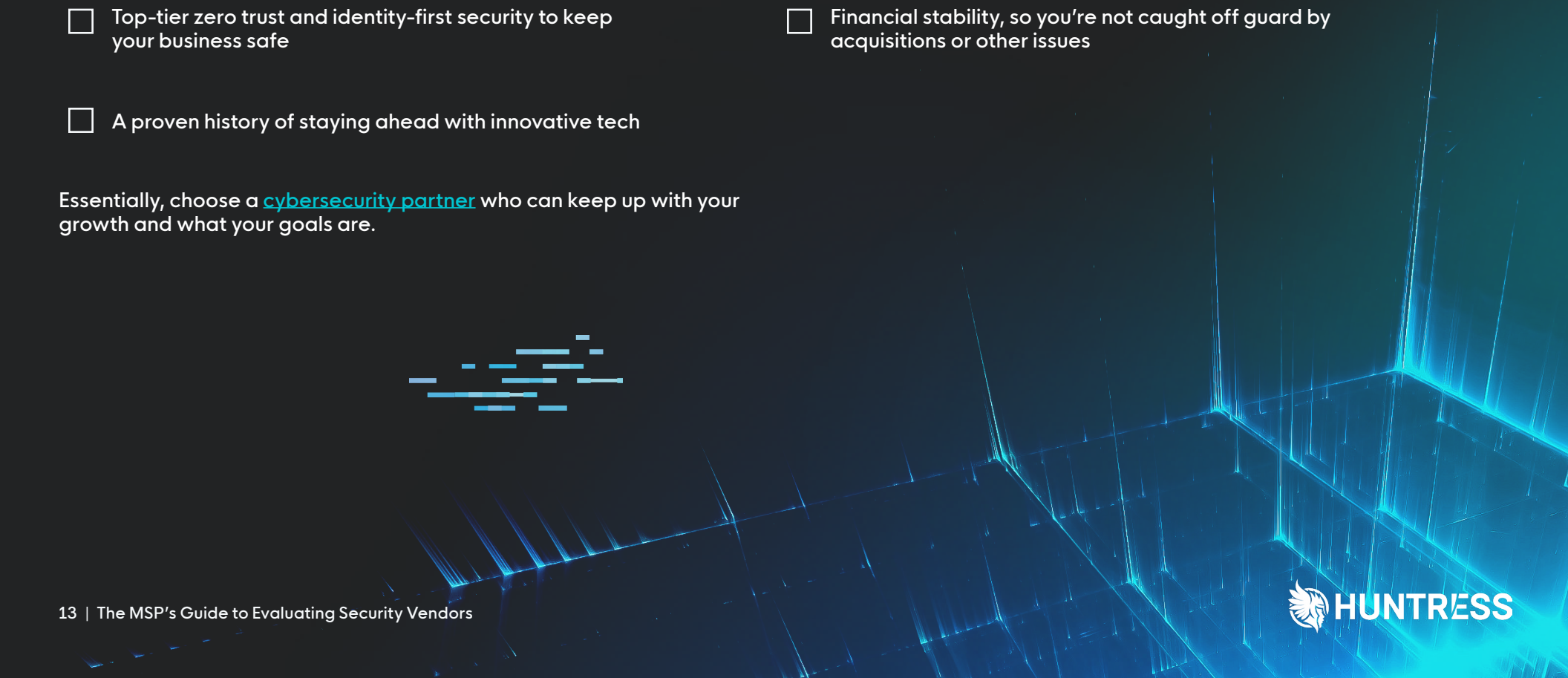
Scalability and future readiness

Look for partners who can grow with your business.

What to look for:

- [ ] A solid AI and automation game plan to make things smoother and cut costs
- [ ] Top-tier zero trust and identity-first security to keep your business safe
- [ ] A proven history of staying ahead with innovative tech
- [ ] The ability to scale, whether you're a small startup or a large enterprise
- [ ] Financial stability, so you're not caught off guard by acquisitions or other issues

Essentially, choose a cybersecurity partner who can keep up with your growth and what your goals are.



HUNTRESS

Choosing the Right Vendor for You

Cybersecurity vendor red flags that should make you walk away

Some warning signs you shouldn't ignore:

Slow support response

If they're hard to reach during the evaluation phase, imagine how frustrating it'll be after the sale.

No regular updates

In cybersecurity, outdated tools are a big risk. Staying current is a non-negotiable!

Lack of transparency

If they won't share SOC reports or incident histories, they might be hiding something.

No multi-tenant strategy

This shows they don't really get how MSPs operate.

Suspiciously low pricing

If it sounds too good to be true, it probably is.

Lack of roadmap

If they can't give you a roadmap, they might not be aligned with your future goals.

HUNTRESS

An ongoing process:

Why a single evaluation isn't enough

Evaluating vendors isn't a one-time thing. With cybersecurity constantly evolving, both vendor capabilities and threats are always changing. To keep a strong partnership going, here are some key things to look for:

- Annual re-evaluations using a clear scorecard
- Quarterly business reviews with transparent performance metrics
- Annual re-evaluations using a clear scorecard
- Vendors who provide free **Not For Resale (NFR) licenses** so you can fully test their tools

Speaking of NFR licenses, the best vendors know how important hands-on experience is when MSPs are evaluating security tools.

By offering solid NFR programs, vendors show confidence in their product and commitment to supporting the MSP community.

HUNTRESS

Building a stronger security community, together

Here's something you don't hear from vendors often: the security community is at its best when everyone has the right tools. When one MSP strengthens their defenses, the whole ecosystem benefits from shared threat intelligence and collective security insights.

That's why the best vendors focus on programs that support the entire MSP community. They understand that your success boosts everyone's overall security posture.

HUNTRESS

Your next steps

The vendor evaluation framework is a practical guide you can start using right now. Start by reviewing your most important vendor relationships, then work through the rest of your tech stack.

In cybersecurity, there's no room for mistakes. The decisions you make today will determine whether you're building a resilient, thriving practice or constantly struggling to put out fires.

Neighborhood Watch Program

Want to see what truly great vendor partnerships look like? Join the Huntress Neighborhood Watch Program. You can get hands-on experience with a fully equipped security platform designed just for MSPs. When you join, you'll get:

Free NFR licenses for our entire security suite

24/7 AI-assisted SOC support by an elite team of threat analysts

Early access to exciting new features from our suite of products

By joining, you'll strengthen your own defenses and help protect the entire community. When MSPs are better protected, everybody wins.

Join the Huntress Neighborhood Watch Program today.

HUNTRESS

Sources cited

1. Rachel Banks, "Why SMBs Need to Reassess the Cyber Expertise of Their Service Providers," Cybersecurity Magazine, November 7, 2024. https://cybersecurity-magazine.com/why-smbs-need-to-reassess-the-cyber-expertise-of-their-service-providers/

2. Verizon. 2025 Data Breach Investigations Report (DBIR). 2025. https://www.verizon.com/business/resources/Td94/reports/2025-dbir-data-breach-investigatios-report.pdf

3. Emma Woollacott. "Pressure Mounts on MSPs as Enterprises Flock to Managed Cybersecurity Services." ITPro, July 8, 2025. https://www.itpro.com/security/pressure-mounts-on-msps-as-enterprises-flock-to-managed-cybersecurity-services

HUNTRESS

About Huntress

Huntress is a global cybersecurity company on a mission to make enterprise-grade products accessible to all businesses. Purpose-built from the ground up, Huntress' technology is specifically designed to continuously address the unique needs of security and IT teams of all sizes. From Endpoint Detection and Response (EDR) and Identity Threat Detection and Response (ITDR) to Security Information and Event Management (SIEM) tools and Security Awareness Training (SAT), the platform provides targeted protection for endpoints, identities, data, and employees, delivering trusted outcomes and valuable peace of mind.

Its 24/7, AI-assisted Security Operations Center (SOC) is powered by a team of world-renowned engineers, researchers, and security analysts, dedicated to stopping cyber threats before they can cause harm. Huntress is often the first to respond to major hacks and incidents, with its expert security team sharing real-time tradecraft analysis and actionable advisories with the community. Currently safeguarding over 4 million endpoints and 7 million identities, Huntress empowers security teams, IT departments, and Managed Service Providers (MSPs) worldwide to protect their businesses with enterprise-grade security accessible to everyone.

As long as hackers keep hacking, Huntress keeps hunting. Join the hunt at www.huntress.com and follow us on X, Instagram, Facebook, and LinkedIn.

HUNTRESS