

The Cybersecurity MSP Buyer's Guide

How to Evaluate and Select Partners for Managing Cybersecurity

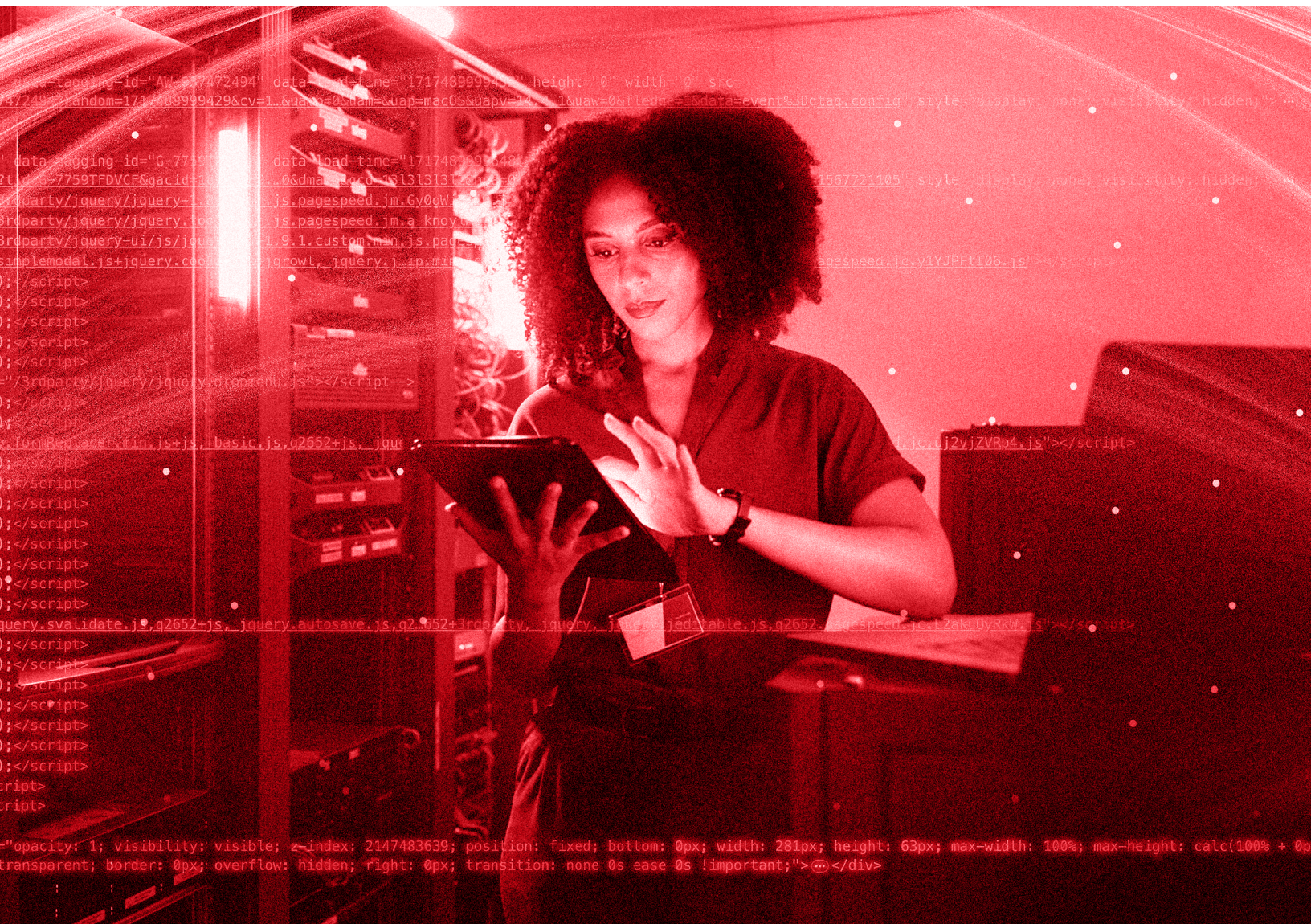


Table of Contents

Introduction	2
Understanding What You Are Buying	3
Identifying Key Provider Differentiators	5
Comparing Cybersecurity Costs: Partner or Build	7
Regulatory Compliance and Cyber Insurance	8
Evaluation Checklist: 22 Essential Questions	10
How to Read a Service Provider Security Proposal	11
Red Flags and Green Flags	13
Best Practices for Moving Forward	14
Partnering with NexusTek	15
Next Steps	15

The selection of a managed service provider (MSP) for cybersecurity is one of the most important decisions a business leader can make today. It is also one of the most confusing.

The market is crowded with providers. Many of them promise comprehensive protection, 24/7 coverage, and seamless tool integration. And most buyers, especially at small and mid-size businesses, do not have the internal expertise to separate genuine capabilities from marketing language.

Finding the right provider, however, is imperative. Globally, the average cost of a data breach is \$4.99 million.¹ For a small or mid-sized business, a single attack could lead to regulatory fines, reputational damage, revenue losses, and operational disruptions that could be difficult to recover from.

This guide provides the framework for evaluating and selecting a service provider for cybersecurity. Learn how to distinguish between various types of providers, spot key service differentiators, assess costs for these services, and ask the right questions when meeting with providers. With this framework, you can take the first steps toward finding a provider that effectively protects your organization while streamlining compliance.

INTRODUCTION

Understanding What You Are Buying

Not all providers offer the same types of cybersecurity services. Understanding the distinctions can help you simplify decision-making.

Three Main Provider Types:

- 1. Managed Service Provider (MSP) with Security Capabilities:** An MSP manages your overall IT environment, including your hardware, software, network, and security tools. A full-service MSP with security capabilities can also manage patching, monitoring, endpoint protection, and compliance documentation. For small and mid-size businesses that want a single partner to handle IT and security together, an MSP is often the right type of provider.

Typically, an MSP does not offer dedicated threat hunting by specialist security analysts. Nor will it necessarily offer a security operations center (SOC) focused on attack detection and response.
- 2. Managed Security Service Provider (MSSP):** An MSSP specializes in security monitoring and alerting. This type of provider watches your systems for suspicious activity and sends alerts when something looks wrong. But your team handles the response. MSSPs primarily focus on the operational management of security tools and alerting rather than actively responding to threats. If you have an internal IT team that can respond to alerts, an MSSP can add a useful monitoring layer. If you don't, the alerts alone will be insufficient.
- 3. Managed Detection and Response (MDR) Provider:** An MDR provider goes beyond alerting. This type of provider investigates, confirms, and responds to threats. MDR providers typically offer 24/7 threat hunting and response using advanced tools and technologies. They can address the internal cybersecurity skills shortage that makes it difficult for mid-size organizations to manage rising threats alone. Often the primary difference between an MSSP and an MDR provider is the human in the loop: MDR providers offer analyst judgment, not just automated alerting.

Which Model Do You Need?

When evaluating the different types of providers, consider these factors:

Internal IT Capacity

If you have no dedicated IT staff, you need a partner that handles the full IT environment, including security. If you have some internal IT personnel but no security specialists, you might select an MSP or an MDR provider.

Risk Profile

A bank handling sensitive customer data might face different types of threats and have different vulnerabilities than a manufacturer. Organizations in regulated industries—such as financial services, healthcare, and government—also have additional burdens compared with companies in other fields. Understanding your risk profile should help you narrow down your options, especially as you begin to compare offerings by seemingly similar providers.

Budget and Bandwidth

More comprehensive coverage costs more. Meanwhile, services that leave some management to you will require more internal resources and better coordination with providers. Choose a provider that offers the right balance of coverage and management responsibility.

Clarifying Shared Responsibility

No matter which type of provider you select, you probably won't completely offload cybersecurity responsibilities. The provider might own detection and response actions. You would own decisions, approvals, and internal controls.

Unfortunately, the dividing line is not always clear. And the gap between what you thought they covered and what they do cover can become a serious vulnerability. So, before you sign any contract, make sure you clearly define responsibilities. By understanding who owns what, you can avoid those gaps that attackers are eager to exploit.

Identifying Key Provider Differentiators

There are several factors that distinguish strong cybersecurity providers from those that will leave you exposed.

24/7/365 Coverage with Human Analysts

Threats appear around the clock. Your provider must be able to protect your organization by making key decisions on any day, at any hour.

If you ask a prospect whether they offer 24/7 monitoring, almost all will say yes. Be more specific: Ask if there would be a human analyst available to make a judgment call at 2 AM on a Saturday.

Some providers might offer only automated coverage after normal business hours. Automation is great for handling known patterns. But it handles novel patterns poorly. Human judgment is often critical for containing an incident before it becomes a full breach.

Proactive Threat Hunting

Most security tools wait for something to go wrong before they notify anyone. Proactive threat hunting means your provider is actively looking for signs of compromise inside your environment and will notify you before a tool generates an alert.

This proactive approach is important because sophisticated attackers can move quietly through systems for days or weeks before doing damage. By the time a tool produces an alert, attackers will already be poised to capitalize on vulnerabilities they've found. A provider that hunts proactively is more likely to find a threat before it becomes a crisis.

Integration with Your Existing Environment

Some providers require you to replace existing security tools to use their service. Others integrate with what you already have. As part of your provider evaluation, determine whether you will need to make additional technology investments before using their service. Be sure to factor in any additional purchases and integration work when comparing the real costs of each engagement.

Look for a provider that can plug your existing tools into its SOC and add its own only where gaps exist.

Compliance Documentation

Many providers will claim to support multiple security or privacy frameworks, but not all can prove it. If your business must comply with HIPAA, PCI DSS, CMMC 2.0, or another framework or regulation, make sure the provider can truly give you the support you need. Instead of solely asking whether they support the framework, ask them whether they can produce the specific documentation an auditor will ask for—and request an example.

Clear Incident Response Authority

During an active cybersecurity incident, taking action quickly is critical. That speed requires clarity about who is authorized to do what. Make sure you define which actions the provider can take during an incident without calling you first. Conversely, define which actions require your explicit approval.

Keep in mind that if the provider must get your pre-authorization for key actions, incident response can slow significantly. A provider that is pre-authorized to take action can contain a threat while you are being notified.

Transparent TCO

The base contract price is rarely the full cost of the provider relationship. Ask specifically what triggers additional fees. Common hidden costs include:

- Per-incident investigation hours billed separately from monitoring
- Onboarding and implementation fees not included in the subscription price
- Tool licensing costs that appear after you have committed to the engagement

When you are making cost decisions, be sure to compare the cost of engaging providers to the cost of building equivalent capabilities in-house. Include analyst salaries, tool licensing, and training. That comparison can often give you the perspective you need when evaluating TCO.

Buying Experience

The buying experience is often a predictor of the engagement experience. If the sales process is organized, specific, and honest about trade-offs, that is a positive signal. If a prospective provider avoids hard questions, is light on specifics, and tries to force quick decisions, that should be a warning for how the engagement will go.

Comparing Cybersecurity Costs: Partner or Build

To fully evaluate the cost of any one cybersecurity provider, it's essential to compare those costs with the primary alternative approach to managing cybersecurity: building in-house.

Building In-House

What would it cost to implement internal security capabilities that are comparable to what you would access through a cybersecurity provider? There are multiple components to that calculation:

- **Analyst salary:** Hiring a single experienced security analyst could cost between \$80,000 and \$120,000 per year in salary alone, before benefits and management overhead. For around-the-clock monitoring, you would need multiple analysts.
- **Training and certification:** The threat landscape changes constantly. You need to provide continuous training to ensure analysts remain effective over time.
- **Tool licensing:** Factor in tool licensing costs for endpoint detection and response, security information and event management (SIEM), vulnerability scanning, and other capabilities you need to complete a modern security stack. These tools carry per-seat or per-device licensing costs that scale with your organization.
- **Replacement hiring:** Cybersecurity professionals are in high demand. If you lose a key analyst, for whatever reason, you face the hiring costs for a contractor or permanent replacement.

Beyond the monetary costs of building a team and implementing tools, you will need to weigh the risks associated with an in-house model. For example, if you experience turnover in the middle of a security incident or during a critical compliance period, you could experience delays in remediation or completion of compliance tasks.

And despite your best efforts to create a complete team with all the right tools, you might still have coverage gaps. Many small and mid-size organizations experience gaps in after-hours coverage, holiday coverage, or during periods of staff transition. Those gaps create real security vulnerabilities for your business.

Maintaining the Status Quo

Of course, you always have the option of maintaining the status quo. But that too has a cost.

A single successful ransomware attack can cost hundreds of thousands of dollars. Beyond the cost of recovering systems and restoring data, you might experience lost productivity and lasting reputational damage. In addition, regulatory fines for a HIPAA or PCI violation can reach into the millions. For most organizations, a single breach or regulatory fine would be much greater than the yearly cost of partnering with a cybersecurity provider.

Regulatory Compliance and Cyber Insurance

If your business handles sensitive customer data or carries cyber insurance, you'll need to evaluate how cybersecurity providers can support your particular compliance and insurance requirements.

Differences Between Compliance and Security

Compliance means you have met a documented set of requirements at a particular point in time. Security means you are protecting your organization with active, monitored defenses.

Compliance and security reinforce each other, but neither guarantees the other. Because compliance frameworks establish only a baseline for security, you might achieve compliance with a particular framework but still suffer a breach. Conversely, you might implement strong security capabilities but still fail an audit because your team did not adequately maintain necessary documentation.

You need both compliance and security. And the right cybersecurity provider should help you with both.

Security and Privacy Frameworks

Depending on your industry and business, you might need to comply with one or several major security and privacy frameworks.

Framework	What It Covers
NIST Cybersecurity Framework 2.0 (NIST CSF 2.0)	• The most widely used voluntary framework for managing cybersecurity risk across industries • Ensure that providers tell you which version they follow
HIPAA	• Required for healthcare organizations and their business associates • Covers the protection of patient health information • Requires documented administrative, physical, and technical safeguards
NYDFS 23 NYCRR 500	• New York's cybersecurity regulation for financial services companies • One of the most detailed state-level cybersecurity regulations in the United States, with specific requirements for access controls, encryption, incident response, and annual certification
CMMC 2.0	• Necessary for companies doing business with the US Department of Defense • Requires third-party certification at higher levels and cannot be self-attested
SOC 2 Type II	• A voluntary audit report that demonstrates an organization has effective controls for security, availability, processing integrity, confidentiality, and privacy • Many enterprise customers and partners now require their vendors to provide this audit report
PCI DSS	• Required for any organization that accepts, processes, stores, or transmits credit card information

A cybersecurity provider might claim to support these or additional frameworks. But ask the provider to show you sample documentation they have produced for a client under your specific framework.

Cyber Insurance

In the past few years, cyber insurance providers have tightened their requirements significantly. The cybersecurity provider you choose directly affects whether you can obtain coverage, what it costs, and whether a claim pays out when you need it.

Before issuing or renewing a policy, insurers now commonly require:

- **Multi-factor authentication (MFA)** on all remote access and admin accounts. Make sure your cybersecurity provider can help you implement and document the use of MFA.
- **A documented incident response plan** with named roles and tested procedures. You need more than a plan that exists on paper: It must be tested and documented.
- **Regular security awareness training** for employees, with documentation that it occurred.
- **Endpoint detection and response tools** actively running on all devices. These tools must be not only deployed but confirmed as active and monitored.
- **Privileged access management controls** in place. You must document who can access which systems and provide logs of access activity.
- **Documented backup and recovery processes** that have been regularly tested.

Implementing these controls and processes is not optional. If a provider does not help you build, maintain, and document these controls, an insurer could deny a claim on the grounds that you did not maintain adequate security hygiene. When evaluating a provider, ask them specifically how they can help you meet and document the controls your cyber insurer requires.

Evaluation Checklist: 22 Essential Questions

Bring this set of 20 essential questions (with a few clarifying points) to every provider evaluation session. A strong provider will welcome the opportunity to supply answers.

Evaluation Category	NexusTek Evidence
Detection and Response	• Do your analysts work 24/7/365, or is after-hours coverage automated with no human in the loop? • Would you proactively hunt for threats inside our environment, or would you only respond when an alert is triggered? • What is your mean time to detect (MTTD) and mean time to respond (MTTR)? Can you provide historical performance data, not just a target range? • How do you handle alert fatigue? What is your false positive rate? How do you prioritize which alerts get human attention? • What types of threats do you cover? Specifically, what known attack signatures and unknown behavioral patterns? • How do you use AI in detection and response, and which actions require human review? • Is our data used to train your AI models, and where is it processed and stored?
Integration and Fit	• Will your service work with the tools we already have, or will we need to replace them to use your service? • Is there an additional cost to integrate with our existing systems? • Will we need to make any additional technology investments beyond the contract price to gain full coverage? • Who handles ongoing configuration and optimization of the tools in our environment: your team, our team, or both?
Cost and Contract	• What is included in the base contract price, and what specifically triggers additional fees? • Are incident response hours billed separately when a real threat is confirmed, or are they included? • What are the exit terms? How much notice is required? What data do we get back? And in what format? • Can you provide a total cost of ownership (TCO) comparison that accounts for what it would cost to build equivalent capability internally?
Compliance and Cyber Insurance	• Which compliance frameworks do you support? Can you provide sample documentation? • Can you help us meet and document the specific controls that our cyber insurer requires? • Have you worked with businesses in our industry facing our specific regulatory requirements? • How do you handle changes to regulatory requirements? Do you notify clients proactively and update your service delivery accordingly?

Evaluation Category	NexusTek Evidence
Accountability and Service Boundaries	• During an active incident, what actions can your team take without our explicit approval? What requires us to sign off first? • How would you communicate with me and my leadership during an incident? Who calls whom, by what channel, and on what timeline? • What does onboarding look like? How long until we have full coverage from contract signature?

How to Read a Service Provider Security Proposal

Examining a proposal from a cybersecurity service provider is a key part of the evaluation process. Make sure the proposal provides several essential elements, then carefully review service level agreements (SLAs), contract terms, and the onboarding process.

Essential Proposal Elements

A complete proposal from a credible provider includes:

- A clear scope of services, with explicit statements about what is and is not covered
- Defined SLAs with specific MTTD and MTTR commitments
- A description of the onboarding process with a timeline and defined milestones
- Named points of contact for account management and incident escalation
- A compliance and reporting section that describes what documentation you will receive and how often
- Pricing that itemizes what is in the base fee and what triggers additional charges

If any of these elements are missing, ask for them before you sign. If a provider cannot produce the information you need in the proposal stage, you will likely run into problems once you are a client.

SLA Terms to Scrutinize

MTTD: On average, how long does it take for the provider to detect an incident? Ask for historical data, not just a commitment.

MTTR: How long does it take from detection to active response? A provider that detects quickly but responds slowly only solves half the problem.

Coverage hours: Is the SLA for business hours only, or 24/7/365?

Escalation paths: Who receives the call when something serious happens? Is there a named role and a direct line, or a general support queue?

Contract Terms to Review Carefully

Data ownership at exit: Make sure the contract clearly states what data you will receive, in what format, and in what timeframe once the relationship ends. Make sure you own your security logs and incident data. Getting them back should not require negotiation.

Notification obligations: If your provider detects a breach, how quickly are they required to notify you? Some frameworks require breach notification within 72 hours.

Liability caps: Most contracts cap the provider's liability for damages—and that cap is often significantly below the typical cost of a breach. Factor that gap into your cyber insurance coverage decision.

The Onboarding Plan as a Signal

Ask a prospective provider to walk you through their onboarding process in detail before you sign. Their response tells you a lot about how the organization will operate once you are a client. A provider with a well-documented, milestone-based onboarding process has done this many times and has discovered what works. A provider that describes onboarding in vague terms and says it typically takes “a few weeks” is improvising.

Beyond foreshadowing your future relationship, the onboarding process will help you understand whether you can stay secure during the transition period. A disorganized onboarding process might mean you are vulnerable before you gain full coverage.

Red Flags and Green Flags

Certain signals from a prospective MSP can help you decide whether to move forward with an engagement. Here are a few sample red and green flags.

Signal	Red / Green Flag	NexusTek Evidence
Vague or ranges-only response time commitments	Red flag	The provider cannot be held to a measurable performance standard
No named compliance certifications, only general claims	Red flag	Compliance support may not hold up under audit scrutiny
SOC is outsourced with no disclosed partnership	Red flag	You cannot evaluate the actual response team you are buying
Pricing significantly below market with no clear explanation	Red flag	There are potential coverage gaps or capability trade-offs
Cannot produce a sample audit report on request	Red flag	Reporting capability is not operationally ready
Requires full tool replacement before coverage begins	Red flag	Expect added cost, a longer transition, and reduced protection in the interim
Cannot explain where AI makes decisions	Red flag	Automated actions may lack human accountability
Named framework certifications with documentation available on request	Green flag	Compliance support is real and auditable
Published MTTD and MTTR with historical performance data	Green flag	The provider is accountable to measurable outcomes
Clear escalation path with named roles and contact protocols	Green flag	Incident response is documented
References from organizations in your industry and at your size	Green flag	The provider has relevant operational experience
Transparent onboarding timeline with defined milestones	Green flag	Implementation support is planned and repeatable
Proactive conversation about cyber insurance requirements	Green flag	The provider understands the full business context, not just the technical one
Integrates your existing tools into its SOC	Green flag	Prior investments stay productive and onboarding moves faster
AI supports analysts, with human review on critical actions	Green flag	Speed improves without sacrificing judgment

Best Practices for Moving Forward

Conducting a thorough evaluation of cybersecurity providers is worth your time and effort. The right provider will be a trusted partner that understands your environment, risk tolerance, and regulatory obligations. That partner can help you significantly reduce risks and recover rapidly if incidents occur.

1. Know What You Have Today

Before you talk to any provider, spend 30 minutes answering these questions honestly:

- What security tools are currently running in our environment, and are they actively monitored?
- Do we have a documented incident response plan, and has anyone tested it?
- Does our current cyber insurance policy have specific requirements, and are we meeting them?

Starting with this baseline assessment will help you determine whether provider offerings will fit your situation. A good provider will take your honest answers to these questions and present services that will fill the gaps.

2. Use the Checklist

Bring that 22-question checklist to every provider meeting. Don't skip the compliance and cyber insurance questions, even if they feel out of place in an early conversation. The providers that respond well to those questions are the ones worth your time.

3. Require Documentation

Every provider will tell you they support your compliance framework, offer 24/7 responses, and integrate with your existing tools. Ask each one to show you evidence, such as a sample audit report, historical MTTD and MTTR data, or a reference from a business in your industry. The best providers will have no trouble producing the evidence you need.

4. Treat the Evaluation Experience as Data

By the time you approach a final decision, you will have had several interactions with each provider. You should know by then whether they are organized, responsive, and honest under pressure. Use that evaluation experience as information to inform your buying decision.

5. Don't Let Perfect Be the Enemy of Good

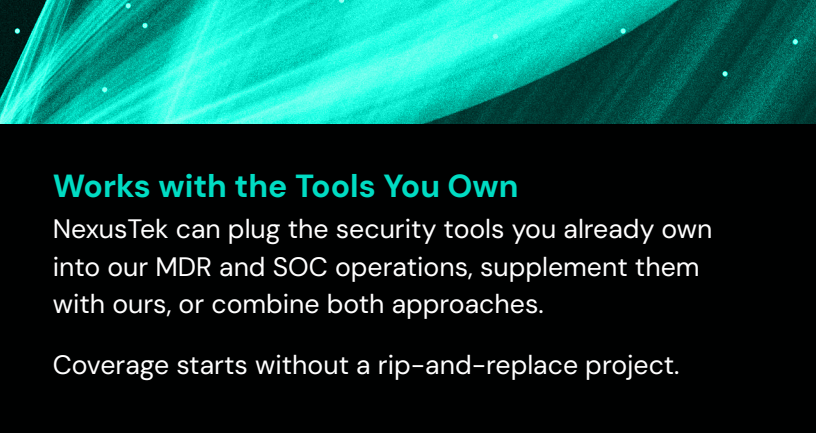
Small and mid-size businesses sometimes stall with cybersecurity service provider decisions because there are so many factors to consider. Keep in mind that your goal is not to find the perfect provider. It is to find a strong, credible partner that will work well with you. That partner should help protect your organization and maintain compliance now while strengthening security and compliance over time as the provider learns your environment. Holding out for perfection will only leave your organization exposed.

Partnering with NexusTek

NexusTek offers managed IT and cybersecurity services to more than 1,200 active customers across 48 states, Canada, Mexico, and Europe. Our Advise → Implement → Manage methodology provides a proven path for developing a tailored security strategy, deploying necessary solutions, and establishing ongoing management to keep your organization secure and compliant.

Our comprehensive security service offerings include:

- Security awareness training
- Managed cybersecurity
- Vulnerability management
- Infrastructure security
- Identity and access management
- Cybersecurity monitoring
- Cybersecurity assessments
- Zero Trust Network Access



Works with the Tools You Own

NexusTek can plug the security tools you already own into our MDR and SOC operations, supplement them with ours, or combine both approaches.

Coverage starts without a rip-and-replace project.

In delivering these services, we have built a verifiable track record that demonstrates the strength and longevity of our client partnerships. With an average six-year client relationship, we have achieved a 98% customer satisfaction rating across the customer base. And we have appeared on the CRN MSP500 list for multiple consecutive years, a recognized industry benchmark for managed service provider performance.

Next Steps

To help you get started with the evaluation framework detailed in this guide, NexusTek offers a no-obligation security assessment. A NexusTek specialist will walk through your current cybersecurity posture; identify the security, compliance, and cyber insurance gaps most relevant to your business; and give you an honest picture of where your risks are—all without a sales pitch.

With that assessment and this guide, you'll be well prepared to thoroughly evaluate cybersecurity service providers—and to find a partner that can help you strengthen security and maintain compliance.

READY TO GET STARTED?

→ **Schedule a Consultation with NexusTek**
www.nexustek.com/contact-us

References

1. IBM, [Cost of a Data Breach Report 2026: The AI tipping point](#), July 2026