nexustek

Managed IT Services Guide

The Mid-Size Business Guide to Managed IT Services

A Practical Framework for Companies with 50 to 500 Employees

PUBLISHED BY NEXUSTEK

Table of Contents

Many mid-size organizations have outgrown the break-fix model for IT. As technology becomes a central driver for their businesses, these organizations need IT teams that can launch new tech-driven initiatives while addressing evolving cybersecurity threats. But not all have the resources to staff a full internal IT department.

Managed IT services can fill that gap. With the right managed IT service provider, mid-size organizations can meet their operational technology and cybersecurity needs while gaining strategic and leadership resources that help maximize the value of technology for their businesses.

This guide provides a framework for evaluating managed IT service providers and selecting the services that are right for your organization. Learn what managed IT covers, what it costs, how to assess providers, and what strategic offerings can augment services. With this framework, you can take key steps toward establishing a long-term partnership that delivers the technology resources you need for achieving business goals.

INTRODUCTION

Why Mid-Size Businesses Can't Afford to Go It Alone

For many organizations, technology has become the operational and strategic heart of the business. But mid-size organizations, with 50 to 500 employees, often have difficulty protecting their technology environment and moving forward with tech-led plans relying solely on their in-house teams.

Three key challenges make it particularly difficult for these organizations to go it alone:

1. **Cybersecurity threats:** Businesses with fewer than 1,000 employees face the same types of threats as larger organizations.[1] And because attackers are well aware that mid-size businesses often have fewer defensive resources than enterprises, these businesses are frequent targets.
2. **Financial impact of breaches:** The average cost of a data breach across organizations of all sizes is now $4.99 million per incident.[2] For mid-size organizations without the reserves to absorb that impact, the consequences of a breach can be existential. If a company with fewer than 500 employees experiences a breach that costs even a few hundred thousand dollars, that loss could be enough to close the business.
3. **A tight IT talent market:** Combating threats while also moving forward with new technology projects requires skilled IT workers. And finding, hiring, retaining, and managing those workers demands substantial time and money. Companies with fewer than 500 employees often can't afford to employ a sufficiently sized team with the level of skills required. As a result, they struggle to defend their organizations and successfully launch new tech-driven initiatives.

If mid-size organizations can find ways to supplement their in-house personnel, the potential payoffs can be considerable. Clearly, implementing robust cybersecurity is critical for simply staying in business. Meanwhile, organizations that align their IT strategy with broader business objectives achieve faster revenue growth than companies that treat IT as a cost center.

For many mid-size businesses, realizing those payoffs requires engaging managed IT services.

What Managed IT Services Include

Managed IT services are not limited to help desk support. When a managed IT services engagement is structured correctly, organizations can forge a comprehensive technology partnership that spans daily IT operations, cybersecurity, and strategic planning.

Here is what a well-structured managed IT relationship can cover and what your organization should look for when evaluating managed service providers (MSPs):

Service Category	What It Covers	What to Look for in a Provider
Managed help desk and IT support	Day-to-day incident resolution, user support, monitoring, and maintenance	Domestic staffing, clearly defined response service-level agreements (SLAs)
Cloud services	Migration planning, cloud hosting, environment optimization, multi-cloud management	Experience across major cloud platforms (AWS, Azure, Google Cloud), proven migration methodology
Cybersecurity	Threat detection and prevention, incident response, vulnerability management	Proactive posture, not just reactive tools; security operations depth
Data and AI infrastructure	Data architecture, analytics readiness, AI infrastructure preparation	Ability to operationalize data before AI tools are introduced
Virtual CIO (vCIO) and advisory services	Strategic IT planning, technology roadmaps, executive-level guidance	Technology leaders, not just account managers
Virtual CISO (vCISO) services	Security program ownership, compliance alignment, board-level risk reporting	Direct experience with relevant security and privacy frameworks (SOC 2, HIPAA, CMMC, NIST)
Professional services	Project-based implementation, migrations, network architecture, M&A technology support	Continuity between advisory and implementation teams
Backup and disaster recovery	Documented backup cadence, tested recovery, defined recovery time objective (RTO) and recovery point objective (RPO) commitments	Regular testing RTOs/RPOs meet critical workload recovery requirements

Some providers will try to sell you a product and hand it off to your understaffed in-house team. A better approach brings together individual services into a single, coherent, end-to-end engagement. The provider should **advise** you on strategy, **implement** solutions, and then continuously **manage** ongoing operations to help you achieve your desired outcomes. When evaluating managed IT service providers, be sure to ask them how their advisory and implementation work connects to an ongoing managed relationship.

Key Factors to Evaluate

Most mid-size businesses enter MSP evaluations without a structured framework. But doing so can result in long-term contracts with providers that don't deliver what they promised.

Examine these seven factors before engaging a managed IT services provider:

Support Availability and Response Time

When something breaks on Friday at 11 PM, what happens? Will a member of the provider's team answer the phone, and how quickly can you expect a resolution?

Ask prospective partners for documented SLOs. In particular, evaluate their track record of recorded uptime to understand their commitment to availability and resiliency. Verify that their support team is staffed domestically. Offshore support can introduce communication problems that compound when your team is under pressure.

Pricing Transparency

Hidden fees and surprise overages are among the most consistently reported areas of frustration for organizations with MSPs. In many cases, those unexpected costs appear because service thresholds were never clearly defined in the contract.

Require a clear, transparent pricing model and build a regular review into the contract. Determine exactly what is included in the platform fee and monthly per-user rate, what triggers additional charges, and how pricing will change as your business expands or contracts.

Visibility and Communication

A managed IT service provider is deeply integrated into your organization and your IT environment. The provider's team members have access to systems, credentials, and data that are central to your operations. That level of access requires clear visibility and communication.

When evaluating MSPs, make sure they will commit to policies that prevent their team from making significant changes to network environments without your knowledge. Ensure you can establish a reporting cadence and dependable point of contact, and clarify the escalation path for when something goes wrong.

Security and Compliance Capability

Regulatory requirements related to data security and privacy continue to evolve rapidly. Choosing the right managed IT service provider can help you streamline compliance. When evaluating providers, ask specifically which security and privacy frameworks they support. Discuss how they handle audit preparation and ask to see examples of their incident response documentation.

Specialization and Depth

The managed IT market is fragmented and competitive, with numerous providers offering overlapping services at similar price points. Often what differentiates providers is depth. Some might have depth in specific industries, technology stacks, or technology problems. As you assess providers, probe into the areas that matter most to your company.

Ask about their existing client base. What is the average company size for clients? In which industries do those clients operate? What types of technology challenges do clients face most frequently? Ask also about the average length of their client relationships. Long relationships mean that MSPs have had opportunities to gain valuable knowledge about particular industries and technology areas.

Backup and Disaster Recovery

Many businesses do not adequately assess backup and disaster recovery (DR) expertise when evaluating MSPs. But evaluating skill levels is essential, because when backup jobs fail, it's often because of misconfigurations or a lack of testing.

Require prospective MSPs to provide documented RTO and RPO options. Ask how frequently recovery can be tested and have them walk you through an example event. If they won't give you specifics about their backup and DR processes, you probably can't rely on them when something goes wrong.

Scalability

Your business will not look the same in three years. Your managed IT services should be able to grow and evolve with you. Evaluate whether each provider's service model scales with your headcount changes, whether the provider supports hybrid and multi-cloud environments, and whether the contract structure allows changes without penalties.

How Much Should You Expect to Spend?

Managed IT service pricing follows a relatively consistent structure of a platform fee plus per-user-per-month pricing across the market. Understanding typical costs for each service tier can help you calibrate expectations before you discuss pricing with providers.

Cost Tiers by Service Level

Service Tier	Cost per User per Month	What Is Typically Included
Basic IT support	$75 to $150[3]	Help desk access, remote monitoring, basic incident resolution
Fully managed IT (including cybersecurity and cloud management)	$150 to $300	Comprehensive IT environment management, security tools, cloud oversight
Enterprise-level IT with 24/7/365 dedicated monitoring	$300 to $500	Full-stack management, dedicated monitoring, advanced security capabilities, strategic advisory

Total Costs for Mid-Size Organizations

For a 50-person company, annual managed IT costs range from $90,000 to $180,000 depending on the service tier.[4] That range is typically less than half the total cost of building an equivalent internal IT team, especially when you account for salaries, benefits, recruiting, training, tools, and management overhead.

For organizations adding dedicated managed security services, monthly investment ranges from $5,000 to $20,000, or $60,000 to $240,000 annually. Those costs cover a full security operations team, tools, 24/7/365 monitoring, and incident response capabilities.

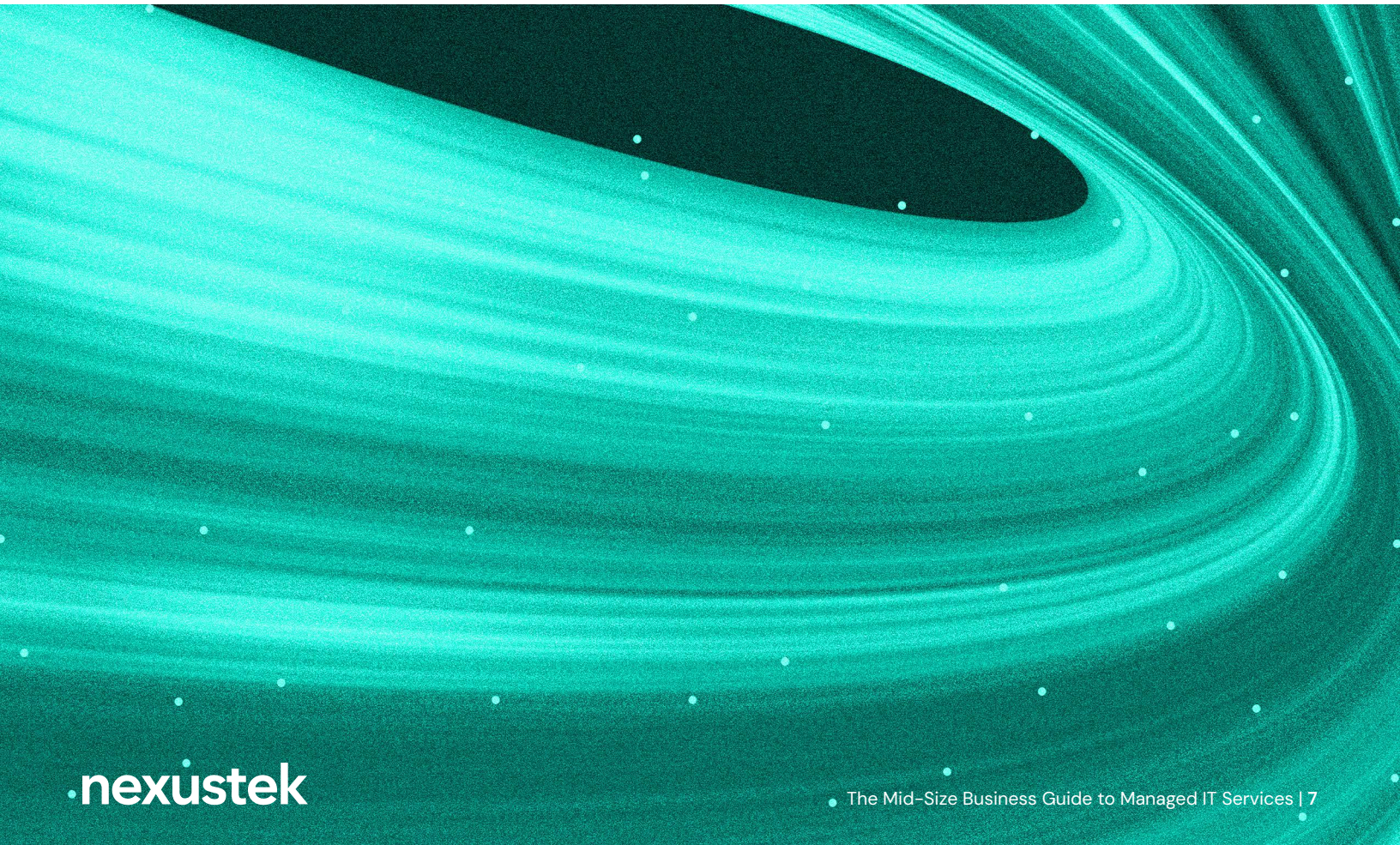
Potential Cost Savings

As you evaluate MSP pricing, factor in the potential savings you could achieve with the right provider. Organizations that move to managed IT services report average IT cost savings of 25% compared to their prior model. They achieve those savings by eliminating redundant tools, reducing recruiting and retention costs, and decreasing the operational impact of incidents. Businesses transitioning to managed IT also report efficiency improvements of 45% to 65%.

One financial services organization that invested approximately $800,000 in security automation and managed services achieved an ROI within one year. That outcome resulted from reduced IT service management costs, prevention of major incidents, and workflow automation savings.

Framing Your Cost Evaluation

Potential cost savings should not be the sole deciding factor when evaluating MSPs or choosing services. Instead, consider what level of coverage, reliability, and strategic capability your business needs. You might also estimate the costs of inaction. Do the costs of managed IT services outweigh the potential financial impact of a security breach? Are the potential revenue benefits of new tech-driven initiatives worth the costs of managed services?



How to Score Providers

Implementing an assessment framework and scoring system can help ensure you are evaluating providers consistently. Score each provider on a scale of 1 to 5 for each evaluation category. A "5" indicates the provider has clear, documented evidence for a capability or claim. A "3" means the provider made a credible claim but could not substantiate it. A "1" reflects the provider's inability to address the category at all.

Use the results to structure follow-up questions with your short list of contenders.

The Scoring Table

Evaluation Category	Weight	Questions to Ask	Score (1–5)
Support availability and response time	High	Is support available and at what times? What is the documented response SLO? What happens after hours and on holidays?	
Pricing transparency	High	Is pricing per user or per device? What triggers overage fees? Can you walk me through a sample invoice? How does pricing adjust as our business grows or shrinks?	
Security and compliance capability	High	Which frameworks do you support (SOC 2, HIPAA, CMMC, NIST, PCI)? How do you handle incident response? Beyond using specific tools, how do you manage security operations?	
Backup and disaster recovery	High	How often are backups and DR tested? What are your options for RTOs and RPOs? Can you walk me through a real recovery event?	
Communication and reporting	Medium	What is the cadence for business reviews? What visibility would we have into our environment day to day? What does the escalation path look like?	
Partnership depth and client tenure	Medium	What is the average length of your client relationship? Looking at your current client base, what are the typical company sizes and industries? What strategic partnerships and certifications do you have in place?	
Scalability and flexibility	Medium	How would your model scale as our company adds headcount? Do you support hybrid and multi-cloud environments? How does the contract handle business changes mid-term?	
Strategic advisory capability	Medium	Do you offer vCIO or vCISO services? Who staffs those roles and what is their background? How do you connect strategic planning to day-to-day management?	

Score Interpretation

Total Score Range	What It Indicates / What to Do Next
35 to 40	Strong candidate. The provider has substantiated claims across all categories. Move to reference checks and contract review.
27 to 34	Viable candidate but with gaps. Identify which categories scored below 3 and determine whether those gaps are acceptable or can be addressed in the contract.
18 to 26	Proceed with caution. Material gaps exist. Use these gaps as leverage in negotiation or as a reason to keep evaluating.
Below 18	Eliminate from consideration. A provider that can't address core categories at procurement won't improve once engaged.

How NexusTek Scores

NexusTek can provide documented evidence for deep capabilities across all evaluation categories.

Evaluation Category	NexusTek Evidence
Support availability and response time	• Support options (including 24/7/365 support) based on needs, helping ensure business continuity and security • Staffed domestically
Pricing transparency	• Clear pricing model provided during the discovery conversation
Security and compliance capability	• Proactive cybersecurity portfolio including detection, prevention, and response • vCISO services staffed by former industry security leaders
Backup and disaster recovery	• Backup and DR services available, including managed of existing customer solutions (subject to NexusTek support list)
Communication and reporting	• Approximately six-year average client relationship, which reflects high-quality communication and account management
Partnership depth and client tenure	• 1,400+ active customers • Approximately six-year average client relationship • 100+ strategic partnerships • Multiple consecutive CRN MSP500 appearances
Scalability and flexibility	• Offices in Colorado, California, and New York with network operations centers (NOCs) nationwide • Customers in 48 states, Canada, Mexico, and Europe
Strategic advisory capability	• vCIO and vCISO services staffed by former industry technology leaders • Advise → Implement → Manage methodology, which connects strategy through implementation to ongoing management

Follow-Up Questions

Once you've identified viable candidates, it's time to dig deeper, asking follow-up questions that determine whether possible limitations can be overcome. For example, you might ask:

What is your response time for a Priority 1 incident, and what is the escalation path if that SLO is missed?
Walk me through exactly what is and is not included in the platform fee and monthly per-user rate. What are the most common add-on charges your clients encounter?
How do you communicate with clients between formal business reviews?
Can you provide compliance documentation from a current client engagement?
Can you share results from a recent backup or DR recovery?
Can you provide two or three references from companies similar in size and industry to ours?
If we grow from 100 to 250 users in the next 18 months, how do the service model and contract adjust?

What Else Belongs in Your IT Strategy

Most of the initial evaluation process for MSPs centers on operational functions—and that might be all you need. But before committing to a particular provider, consider whether you could benefit from strategic assistance. Many mid-size organizations can profit from advisory and leadership services designed to move their business forward.

Virtual CIO (vCIO)

Most companies with 50 to 500 employees cannot justify hiring a full-time chief information officer. Yet operating without strategic IT leadership means technology decisions are made reactively instead of according to a plan.

A vCIO functions as your organization's senior technology strategist. They attend leadership meetings, build multi-year IT roadmaps, and translate technical decisions into language your board and finance team can act on. The vCIO produces the alignment between IT strategy and business objectives that can accelerate revenue growth.

What a vCIO does in practice:

- Builds and maintains a technology roadmap tied to the company's three-to-five-year business plan
- Presents an IT strategy and explains the company's risk posture to the executive team and board
- Manages partner relationships at a strategic level
- Identifies opportunities to reduce costs, consolidate tools, and improve efficiency
- Ensures IT investments are aligned with measurable business results

NexusTek vCIO services, available as an add-on, are staffed by individuals who have held technology leadership roles. You gain access to experienced, executive-level strategic judgment without the overhead of a full-time hire.

Virtual CISO (vCISO)

Smaller companies face the same threats as larger enterprises, but in many cases, they lack the dedicated cybersecurity leadership and capabilities to adequately defend against those threats. With the average cost of a data breach reaching $4.99 million,[5] addressing these deficiencies must be a top priority.

A vCISO is a fractional chief information security officer who can fill the gap in dedicated cybersecurity leadership for mid-size organizations. This leader owns your security program, establishing policy, conducting risk assessments, and briefing your executives on the company's threat posture. The vCISO also guides compliance efforts, serving as the accountable executive when regulators, auditors, or insurers ask who is running security.

What a vCISO does in practice:

- Builds and maintains a formal security program aligned to frameworks such as NIST, SOC 2, HIPAA, or CMMC (Cybersecurity Maturity Model Certification—a US Department of Defense framework)
- Leads risk assessments and vulnerability management programs
- Prepares the organization for audits, regulatory reviews, and cyber insurance renewals
- Translates security risk into financial and operational language for the executive team
- Owns incident response planning and tabletop exercise programs
- Serves as the named security executive in contractual relationships with clients, partners, and regulators

NexusTek has vCISO services available, allowing you to access expert, executive-level security leadership aligned with your risk profile and compliance obligations.

Strategic IT Consulting

Not all managed IT service providers offer the strategic consulting required for making significant technology decisions. If you are planning a cloud migration, assessing AI readiness, selecting an enterprise resource planning (ERP) solution, considering a network architecture overhaul, or conducting M&A technology due diligence, you will need more than standard operational services.

NexusTek offers strategic IT consulting as part of the Advise → Implement → Manage methodology. Advisory and professional services are built into the managed relationship and provided by the same team—the team that already knows your environment well.

AI Readiness Advisory

Many mid-size businesses are under pressure to adopt AI but lack the necessary foundational architecture. Before your business invests in AI tools, you need to know whether your data is clean, structured, and accessible; whether your cloud environment can support AI compute requirements; and whether your security posture can handle the expanded attack surface that is created by AI integrations.

The NexusTek AI readiness advisory is a consulting engagement that assesses whether your current infrastructure, cloud environment, and security posture can support AI tools and workflows. The NexusTek team identifies any gaps and then helps develop a plan for moving forward.

Frequently Asked Questions

When evaluating managed IT service providers, a few key questions rise to the surface repeatedly.

Q: Beyond the platform fee, how much does managed IT cost per user per month?

Pricing depends on the service tier. On average, basic IT support costs $75 to $150 per user per month. Fully managed IT, including cybersecurity and cloud management, costs $150 to $300. Enterprise-level managed IT with 24/7/365 dedicated monitoring costs $300 to $500.[6] For a 50-person company, that translates to annual costs of $90,000 to $180,000 for the fully managed tier.

Q: What is the difference between managed IT and break-fix support?

Break-fix support is reactive and transactional: When something breaks, you call a vendor, and you are billed for that specific incident. There is no ongoing relationship or accountability for preventing future incidents. Managed IT is a continuous relationship built around monitoring, maintenance, and proactive risk reduction. The goal is to catch and resolve issues before they disrupt the business. The NexusTek Advise → Implement → Manage methodology reflects the managed IT approach: The same team that advises on strategy and implements solutions also manages the environment on an ongoing basis.

Q: How do we know if our business is too small for managed IT?

Mid-size organizations face many of the same technology challenges as larger enterprises. For example, they are targeted with similar types of cyber threats and have similar aspirations for transforming parts of their business with AI. But mid-size organizations often lack the resources to adequately protect themselves and launch tech-driven initiatives. If your business depends on technology to operate, generate revenue, or protect client data, it is a candidate for managed IT, regardless of your headcount. Selecting the right service tier will enable you to address your needs within your budget.

Q: What should we look for when evaluating managed IT providers?

There are several key factors to evaluate, including whether providers offer responsive support, pricing transparency, clear visibility and communication, extensive security and compliance capabilities, specialization and depth, backup and disaster recovery, and scalability. In addition, the right providers will be able to deliver not only operational assistance but also strategy, consulting, and leadership as part of a single, integrated methodology.

Q: What frameworks should a managed IT provider support?

A managed IT provider should support the security and privacy frameworks most important for your business and your industry. Working with a provider that supports SOC 2, HIPAA, CMMC, NIST, and PCI frameworks can help your organization reduce your compliance risks.

Your Next Step

Finding a managed IT service provider can be daunting. But with an evaluation framework in place, you can methodically assess capabilities and narrow down the list of contenders.

Given the potential benefits of managed IT services, it is worth taking the time for a thorough evaluation process. A managed IT relationship is not a vendor transaction. It is a long-term operational and strategic partnership. The provider you choose will have access to your systems, your data, and the technology infrastructure that your business depends on. The decision deserves the same rigor you would apply to any significant business partnership.

Partnering with NexusTek

NexusTek was built to provide the type of trusted, long-term managed IT partnership that mid-size organizations need. We are present across the full lifecycle of your IT environment, from the initial strategy development through execution and ongoing management. We bring senior expertise to your leadership team without requiring you to hire full-time executives. And we communicate proactively, not just when something breaks.

Most providers do one of three things well: they advise, they build, or they manage. Very few do all three in a connected, reliable way.

The NexusTek Advise → Implement → Manage methodology ensures that the strategy you develop at the beginning of an engagement persists through the managed services phase. The team that helps you build the roadmap is connected to the team that implements it—and they are connected to the team managing your environment day to day. That continuity is what transforms IT from a cost center into a business accelerator.

Our track record is verifiable, not just claimed:

1,400+
customers across 48 states plus Canada, Mexico, and Europe trust NexusTek to manage their technology environments

NexusTek has earned a
98% customer
satisfaction rating across the customer base

The average client relationship is approximately
6+ years
notable in a market where provider switching and MSP frustration are well documented

NexusTek holds
100+ strategic
partnerships with leading technology providers, including AWS, Google Cloud, and Microsoft

NexusTek has appeared on the
CRN MSP500
list for multiple consecutive years, a recognized industry benchmark for managed service provider performance

Support is available
24/7/365
staffed domestically, so the person who answers when something goes wrong actually knows your environment and can address issues

Where to Start

The first step is a conversation. The NexusTek team will ask about your current environment, identify the gaps with the highest operational or security impact, and give you a clear picture of what managed IT services would look like for a business at your stage.

You do not need to have everything figured out before that conversation. The questions you are still working through are exactly what this discussion is designed to surface.

From there, you can move forward in a few different ways, depending on where you are in the process of considering managed IT services and evaluating providers.

- **Assessment:** If you want to understand your current cybersecurity exposure, request a security or compliance assessment. This assessment gives you a documented baseline and a prioritized gap analysis before you commit to anything.
- **Structured discovery call:** If you are actively comparing providers and are ready to score NexusTek against competitors, ask for a structured discovery call. Come with questions. You will receive direct, substantiated answers.
- **Roadmap conversation:** If you know you need to make changes and want to understand what a transition looks like, ask for a roadmap conversation. The NexusTek Advise → Implement → Manage model means the planning phase is not a separate engagement. It is the beginning of the relationship.

The businesses that gain the most from managed IT services are not the ones that spend the most. They are the ones that find trustworthy partners who can deliver a full range of services over a long-term relationship. With this guide, you have the framework you need to thoroughly evaluate providers.

READY TO MOVE FORWARD?

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

References

1. Verizon, 2026 Data Breach Investigations Report, May 2026
2. IBM, Cost of a Data Breach Report 2026: The AI tipping point, July 2026
3. IT Pro Consultants, Managed IT vs. In-House IT: Which Delivers Better ROI?, March 2025
4. Ibid.
5. IBM, Cost of a Data Breach Report 2026: The AI tipping point, July 2026
6. IT Pro Consultants, Managed IT vs. In-House IT: Which Delivers Better ROI?, March 2025