MSP BUYER'S GUIDE

How to Choose the Right Managed Services Partner for Your Organization

A practical framework for evaluating managed IT and cybersecurity providers, built for IT leaders, executives, and business owners.

Logically™

CYBER FIRST. FUTURE READY.

Logically™

CYBER FIRST. FUTURE READY.

MSP BUYER'S GUIDE

How to Choose the Right Managed Services Partner for Your Organization

A practical framework for evaluating managed IT and cybersecurity providers, built for IT leaders, executives, and business owners.

Contents

How to Use This Guide

Technology risk is accelerating. Cyberattacks are more frequent, more costly, and more sophisticated than ever. Regulatory requirements continue to expand. Talent is scarce. And the gap between IT operations and cybersecurity has become one of the most dangerous blind spots in modern business.

Choosing the right managed services partner is no longer a procurement exercise. It is a strategic decision that directly affects your organization's security posture, operational resilience, and ability to grow. This guide is designed to help you evaluate providers with clarity, accountability, and confidence.

Who This Guide Is For

Business owners, executives, and IT leaders at small and mid-market organizations who are evaluating, replacing, or expanding their managed IT and cybersecurity services.

How This Guide Is Organized

Section 1: Why Managed Services?
If you are new to managed services or want a refresher on why organizations outsource IT and security, start here. This section covers the business case and operating model.

Section 2: What the Right MSP Should Deliver
This is the core of the guide. It defines the services, capabilities, and standards your MSP must meet. If you already understand managed services, skip directly to this section.

Section 3: Not All MSPs Are Created Equal
Criteria for evaluating an MSP beyond services: accountability, expertise, operational maturity, and customer experience.

Appendix: Top Questions to Ask
A ready-to-use evaluation framework for your next MSP conversation.

The Logically Perspective

This guide is published by Logically, a cyber-first, next-generation MSP that unifies IT operations and cybersecurity into one accountable operating model supporting mid-market organizations across the U.S. Founded in 1999, Logically closes the gap between IT and security with shared visibility, coordinated response, and clear ownership. Throughout this guide, we have included our perspective on what good looks like, because we believe the right MSP should set the standard, not just meet it.

Section 1

Why Managed Services?

Every modern organization depends on technology to operate. When systems go down, data is breached, or employees lose access to critical applications; the consequences are immediate: lost revenue, operational disruption, regulatory exposure, and reputational damage. These are not edge cases—they are expected realities in today's threat and technology landscape.

This is why thousands of small and mid-market businesses outsource all or part of their IT and security operations to managed services providers. Rather than building and maintaining a full internal IT team with the depth required across infrastructure, cloud, cybersecurity, compliance, and end-user support, organizations partner with an MSP to gain access to enterprise-grade expertise, tools, and coverage for a predictable monthly investment.

What an MSP Should Do for Your Organization

At its core, a managed services provider assumes operational responsibility for your technology environment. The right MSP moves beyond reactive support models, it proactively monitors, manages, and secures your infrastructure while enabling your workforce and providing the strategic guidance you need to make informed technology decisions.

A qualified MSP should enable you to:

- **Focus on your core business** by delegating technology management to a capable, accountable partner.
- **Reduce downtime and disruption** through proactive monitoring, patching, and incident response.
- **Strengthen your security posture** with integrated cybersecurity that is embedded into every service, not layered on as an afterthought.
- **Access deep technical expertise** across infrastructure, cloud, cybersecurity, compliance, and emerging technologies like AI, without the cost and complexity of hiring internally.
- **Shift from reactive to proactive** with a partner that identifies and mitigates risk before it becomes a business problem.
- **Convert unpredictable capital expenses into manageable operating costs** with fixed-fee, subscription-based service models.

How MSPs Deliver Services

MSPs typically deliver services through two engagement models:

Recurring Managed Services

Your MSP manages all or part of your environment for a fixed monthly fee. This typically includes monitoring, patch management, help desk support, backup and disaster recovery, security operations, and ongoing infrastructure management. Service levels are defined in a service level agreement (SLA) that establishes performance standards, response times, and accountability.

Project-Based Services

For specific initiatives such as cloud migrations, security assessments, infrastructure upgrades, or compliance readiness programs, MSPs deliver services on a fixed-price or time-and-materials basis.

Why Organizations Choose Managed Services

Reduce Downtime and Maintain Business Continuity

Downtime directly impacts revenue, productivity, and customer trust. The right MSP will design resilient environments, proactively monitor for issues, and resolve problems before they cause disruption. When incidents do occur, coordinated response and clear ownership ensure faster recovery.

Access Enterprise-Grade Expertise Without Enterprise-Grade Costs

The technologies supporting your business (servers, cloud platforms, endpoints, firewalls, cybersecurity tools, collaboration systems, databases) are more complex and interconnected than ever. The talent required to manage and secure them is scarce and increasingly specialized, making external expertise essential. The global cybersecurity workforce gap alone stands at nearly 4.8 million unfilled roles[1]. MSPs provide immediate access to certified professionals across IT and security disciplines at a fraction of the cost of building an equivalent internal team.

Protect Data, Systems, and Reputation

Data is your most valuable asset. Whether it is patient records, financial data, intellectual property, or customer information, the consequences of a breach are severe. U.S. cybercrime losses exceeded $21 billion in 2025[2]. Fewer than half of small businesses have a formal cybersecurity plan[3], and only about 38% of small business leaders feel adequately prepared for an attack[3]. A qualified MSP integrates security into every aspect of IT management, not as an optional add-on, but as a foundational requirement.

[1] (ISC)[2], *Cybersecurity Workforce Study* (2025)

[2] FBI, *Internet Crime Report* (2025)

[3] Crowdstrike, *The State of SMB Cybersecurity* (2025)

Address Compliance and Regulatory Requirements

Organizations in regulated industries (healthcare, financial services, government, education) face growing compliance obligations including HIPAA, GLBA, PCI DSS, CMMC, and state-level privacy regulations. The right MSP aligns governance, risk, and compliance with your operating model, implement controls, maintain audit readiness, and demonstrates compliance on an ongoing basis.

Improve Employee Productivity

When employees cannot access their systems, applications, or data, they cannot do their work. A responsive, expert help desk is not a nice-to-have. It is a business requirement. Your MSP should resolve the majority of issues on the first interaction and provide self-service options that reduce friction and keep your team productive.

Plan for the Future

Technology decisions should align with business strategy. The right MSP provides strategic advisory services, including virtual CIO and CISO guidance, to help you define technology roadmaps, prioritize investments, and prepare for emerging challenges with clear accountability for outcomes. Your MSP should be a strategic partner, not just a service vendor.

Your Turn: Is a Managed Services Partner Right for You?

Use the checklist below to assess whether your organization would benefit from engaging an MSP. If you check three or more of these statements, a managed services partnership should be a serious consideration.

MSP Readiness Assessment			
Statement	**Applies**	**Partially**	**Does Not Apply**
Your internal IT team is stretched thin or lacks depth in key areas like cybersecurity, cloud, or compliance.	☐	☐	☐
You have experienced unplanned downtime, data loss, or a security incident in the past 12 months.	☐	☐	☐
You could not confidently pass a security audit or respond to a breach today.	☐	☐	☐
You are spending more time reacting to IT problems than proactively improving your environment.	☐	☐	☐
Hiring and retaining qualified IT and security professionals has been difficult or cost-prohibitive.	☐	☐	☐
Your IT budget is unpredictable, and you would benefit from shifting capital expenses to a predictable operating model.	☐	☐	☐
Your organization is growing, and your current IT infrastructure and support model may not scale with you.	☐	☐	☐
You rely on multiple vendors with unclear accountability, and issues fall through the cracks.	☐	☐	☐
You need 24/7 monitoring and support but cannot justify the cost of a full internal NOC or SOC.	☐	☐	☐
You want a technology partner who can provide strategic guidance, not just break/fix support.	☐	☐	☐

Logically's Take

If managing technology has become a distraction from your core mission, or if gaps between IT and cybersecurity are creating risk, delays, and lack of ownership, it is time to evaluate a managed services partner. The right MSP will not only solve today's problems but will position your organization to adapt, scale, and lead through change.

Section 2

What the Right MSP Should Deliver

Not every MSP offers the same services, and not every service is equal. The managed services market has reached a saturation point where thousands of providers offer nearly identical bundles of IT support and cybersecurity, all framed around similar promises of uptime and responsiveness. As a buyer, you need to look beyond marketing language and evaluate what your MSP actually delivers, and how.

The right MSP should provide comprehensive coverage across five core service areas, delivered through a unified operating model with shared visibility, integrated workflows, and clear ownership.

Core Service 1:

Cybersecurity

This is non-negotiable. Any MSP you engage must treat cybersecurity as foundational, not as an optional add-on or a separate engagement. Security should be embedded into every service the MSP delivers, across every endpoint, cloud workload, and network segment. The era of bolting security on top of IT operations is over.

Your MSP's cybersecurity capabilities should include, at a minimum:

- **Managed Detection and Response (MDR):** Continuous 24/7 monitoring with AI-assisted threat detection and human-led investigation, analysis, and response. Your MSP should operate an in-house Security Operations Center (SOC), not outsource it to a third party.
- **Endpoint Security:** Protection across all devices (laptops, desktops, servers, and mobile) with next-generation antivirus, endpoint detection and response (EDR), and policy enforcement.
- **Email and Identity Security:** Defense against phishing, business email compromise, credential abuse, and deepfake-driven fraud. Multi-factor authentication and identity management should be standard.
- **Network and Perimeter Security:** Managed firewall, DNS security, intrusion detection and prevention, and secure remote access.

- **Vulnerability Management:** Regular scanning, prioritized remediation, and patching to reduce your attack surface.
- **Security Assessments and Penetration Testing:** Third-party risk assessments, vulnerability testing, and security posture evaluations.
- **Incident Response and Forensics:** A documented, tested incident response plan with forensic investigation capabilities. Your MSP should be able to contain, remediate, and recover from security events quickly and decisively.
- **Security Awareness Training:** Ongoing employee education to reduce human-factor risk, including phishing simulation and compliance-focused training.

Why Cybersecurity Matters

Nearly half of MSP customers are willing to switch providers if they cannot see clear evidence of cybersecurity depth and 24/7 security support. When customers leave due to perceived security gaps, nearly 90% remove all bundled IT services along with security, immediately or shortly thereafter[4]. Cybersecurity is not just a service line; it is the foundation of the entire MSP relationship.

Core Service 2:

Cloud and Infrastructure

Your MSP should be able to design, migrate, manage, and modernize your infrastructure across on-premises, hybrid, and cloud environments. Cloud adoption increases complexity, expands attack surfaces, and introduces visibility gaps that must be actively managed.

Critical cloud and infrastructure capabilities include:

- **Cloud Migration and Modernization:** Planning and executing migrations to platforms like Microsoft Azure and AWS, as well as optimizing existing cloud investments for performance, cost, and security. If your organization has already moved to the cloud, your MSP should help you get more value from that investment, not just maintain the status quo.
- **Hybrid and Multi-Cloud Management:** Consistent management, monitoring, and security across mixed environments. More than 80% of organizations now operate in hybrid or multi-cloud configurations[5], which expands the attack surface and creates visibility gaps that must be actively managed.

[4] Barracuda, *MSP Customer Insights Report* (2025)

[5] Flexera, *State of the Cloud Report* (2025)

- **Cloud Optimization and Cost Management:** Ongoing analysis of cloud spend, resource utilization, and architecture to maximize ROI.
- **Server and Network Infrastructure:** Management of physical and virtual servers, switches, routers, firewalls, storage, and wireless infrastructure.
- **Data Center Services:** Colocation, hosting, and management of data center environments with built-in redundancy and disaster recovery.
- **Backup and Disaster Recovery:** Validated backup solutions with tested recovery procedures. Your MSP should not only back up your data but regularly prove that backups are recoverable and meet your recovery time and recovery point objectives.

The Cloud-Security Connection

Cloud adoption creates new security risks that many organizations underestimate. Nearly 70% of organizations cite tool sprawl and lack of unified visibility as major security challenges, and about two-thirds say they are not confident in their ability to detect and respond to cloud threats in real time[6]. Your MSP must integrate cloud management with cybersecurity from the start, not treat them as separate disciplines.

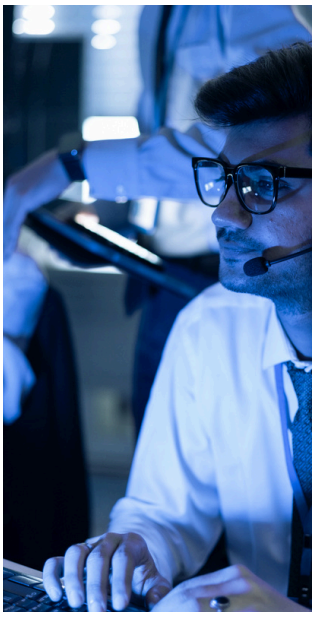
Core Service 3:

Managed IT Services

Managed IT services represent the operational backbone of your MSP relationship. These are the day-to-day services that keep your environment running reliably, your employees productive, and your systems current. Every qualified MSP should deliver these as standard capabilities:

- **24/7 Monitoring and Alerting:** Continuous monitoring of your entire environment (servers, network devices, endpoints, and applications) through a dedicated Network Operations Center (NOC). Issues should be identified and escalated before they impact your business.
- **Help Desk and End-User Support:** A responsive, expert help desk that resolves the majority of issues on the first interaction. Look for an MSP that treats the help desk as a primary resolution center, not a ticket-routing queue.
- **Patch Management:** Automated, validated patching of operating systems, applications, and firmware to eliminate vulnerabilities and ensure compliance. Your MSP should provide detailed reporting on patch status across your environment.

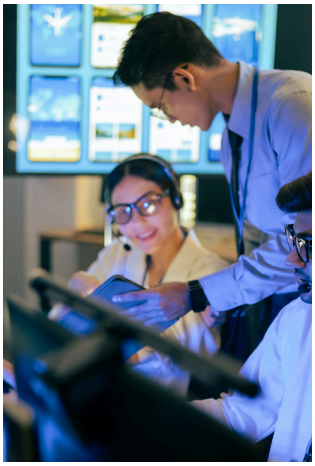
[6] Fortinet, *Cloud Security Report* (2026)



- **Remote Monitoring and Management (RMM):** Tools and automation to detect, diagnose, and resolve issues remotely, including self-healing capabilities that remediate common problems before users are affected.
- **Equipment and License Procurement:** Vendor management, purchasing, license tracking, renewals, warranty management, and end-of-life planning. A mature MSP should simplify procurement and leverage its vendor relationships on your behalf.
- **Asset Management and Lifecycle Planning:** Inventory tracking, hardware lifecycle management, and proactive replacement planning to prevent unexpected failures.
- **Reporting and Transparency:** Regular, meaningful reporting on environment health, incident resolution, SLA performance, and security posture, not just dashboards, but actionable intelligence.

Core Service 4:

Governance, Risk, and Compliance



If your organization operates in a regulated industry, or works with clients who do, governance, risk, and compliance (GRC) is not optional. Your MSP should operationalize compliance as part of daily operations, not periodic checklists, aligned to regulatory requirements.

- **Compliance Frameworks:** Support for HIPAA, GLBA, PCI DSS, SOX, CMMC, NIST, and state-level privacy regulations, among others.
- **Risk Assessments:** Regular assessments to identify vulnerabilities, quantify risk, and prioritize remediation.
- **Policy Development and Enforcement:** Assistance with developing, implementing, and enforcing security and IT governance policies.
- **Audit Readiness:** Ongoing controls validation and documentation to ensure you are prepared for audits at any time.
- **Compliance Monitoring:** Continuous monitoring and reporting to maintain compliance posture as your environment and regulations evolve.

Core Service 5:

AI Governance

AI adoption is accelerating faster than most organizations can govern it. Employees are already using public AI tools (ChatGPT, Claude, Grok, and others) often without authorization, oversight, or consistent safeguards. This creates shadow AI and unmanaged AI sprawl, where usage grows faster than IT can control. The risks are real: data leakage, compliance exposure, loss of intellectual property, and institutional knowledge embedded in personal accounts that walk out the door when employees leave. AI bans do not stop usage. They drive it underground. The organizations that win will standardize and govern AI, not prohibit it. If your MSP cannot help you navigate this, it is already behind.

Your MSP should be able to help you govern—and not block—AI's adoption, standardized use, and security. Look for a provider that can deliver:

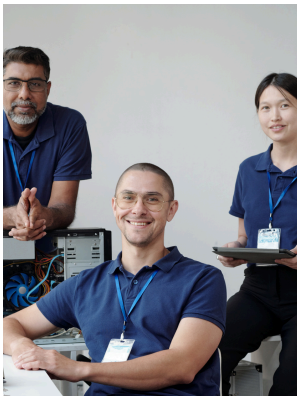
- **A Private AI Tenant:** A dedicated, auditable AI environment fully owned and controlled by your organization.
- **Usage Visibility:** Centralized monitoring and reporting on how AI tools are being used across your workforce.
- **Access Controls:** Role-based permissions and data isolation to ensure the right people access the right resources.
- **Compliance Logging:** Continuous governance and audit-ready documentation without creating friction that slows innovation.
- **Multi-Model Access:** A single platform providing access to multiple vetted and approved AI models.

This kind of service should be comprehensive in focus: including auditing of environments and determining readiness, offering data services to prepare for organizational AI transformation, providing a governed and managed tenant, providing training and enablement to upskill internal teams.

Value-Added Services

Beyond these five core services, the right MSP should also be able to address specialized needs as your organization grows and evolves. These value-added services include:

- **Strategic Advisory (vCIO/vCISO):** Executive-level technology and security guidance to align IT strategy with business objectives, define roadmaps, and prioritize investments.
- **M&A IT Integration:** Technology due diligence, integration planning, and risk alignment for mergers and acquisitions.
- **Custom Projects:** Infrastructure upgrades, application integrations, office buildouts, and other initiatives that require specialized expertise and project management. The best MSPs manage these engagements through a formal project management office (PMO) to ensure governance, accountability, and successful delivery.
- **Equipment and License Procurement:** Streamlined purchasing through a self-service portal for hardware, software, and licensing needs, simplifying vendor management and ensuring cost transparency.



An MSP That Evolves with You

The technology landscape shifts constantly, and your MSP should be shifting with it. Too many providers grow stagnant, relying on the same service catalog year after year while their clients' challenges outpace their capabilities. The right MSP actively develops new solutions in response to emerging customer needs, whether that means standing up AI governance frameworks, expanding security operations, or addressing new compliance requirements. When evaluating providers, ask how their service offerings have changed over the past two years; the answer will tell you everything about whether they can grow with you.

Your Turn: Which Services Should You Be Looking For?

Use the matrix below to evaluate which services your organization requires from an MSP. For each service, indicate whether it is required, optional, or not applicable for your environment. This will help you build a clear requirements profile for evaluating prospective providers.

MSP Service Requirements Matrix

Service	Need to Have	Nice to Have	N/A
RECOMMENDED CORE SERVICES			
Managed Detection and Response (MDR / SOC)	☐	☐	☐
Endpoint Security (EDR / Next-Gen AV)	☐	☐	☐
Email and Identity Security	☐	☐	☐
Network and Perimeter Security	☐	☐	☐
Vulnerability Management and Patching	☐	☐	☐
Incident Response and Forensics	☐	☐	☐
Security Awareness Training	☐	☐	☐
Cloud Migration and Modernization	☐	☐	☐
Hybrid / Multi-Cloud Management	☐	☐	☐
Cloud Optimization / Cost Management	☐	☐	☐
Server and Network Infrastructure	☐	☐	☐
Backup and Disaster Recovery	☐	☐	☐
24/7 Monitoring and Alerting (NOC)	☐	☐	☐
Help Desk and End-User Support	☐	☐	☐
Patch Management	☐	☐	☐
Remote Monitoring and Management	☐	☐	☐
Equipment and License Procurement	☐	☐	☐
Compliance Program Support (GRC)	☐	☐	☐
Risk Assessments	☐	☐	☐
Penetration Testing	☐	☐	☐
Audit Readiness and Reporting	☐	☐	☐
AI Governance and Enablement	☐	☐	☐
VALUE-ADDED SERVICES			
Strategic Advisory (vCIO / vCISO)	☐	☐	☐
M&A IT Integration	☐	☐	☐
Custom Projects and Implementations	☐	☐	☐
Project Management Office (PMO)	☐	☐	☐

Section 3

Not All MSPs Are Created Equal

Outsourcing your business-critical technology is a significant decision. The provider you choose will have direct influence over your security posture, operational stability, and ability to grow. Services matter, but how those services are delivered, by whom, and with what level of accountability matters just as much.

Here are the benchmarks that separate a qualified MSP from the rest.

Unified IT and Security Under One Operating Model

This is the single most important differentiator to look for. When IT operations and cybersecurity are managed by separate providers, or by separate, disconnected teams within the same provider, gaps form. Accountability blurs. Response slows. Risk grows quietly in the space between.

The right MSP unifies IT and security into a single operating model with shared visibility, integrated workflows, and clear ownership. Detection, investigation, and response should move through one coordinated process, not across multiple escalation paths, vendor handoffs, or siloed teams.

Cyber-First by Design

Security should not be a layer added on top of existing systems. It should be embedded into how technology environments are designed, managed, and supported from the start. Ask your MSP how security is integrated into every service, not whether it is offered as a separate line item.

AI-Assisted Monitoring, Human-Led Response

Automation and AI have transformed how quickly threats can be detected. Speed without context creates noise, not outcomes, and organizations are left without clear direction. The right MSP uses AI to accelerate monitoring and surface patterns, while experienced professionals lead analysis, decision-making, and response. This balance ensures faster detection, smarter prioritization, and accountable action, not opaque, black-box automation.

Proven Expertise and Certifications

Evaluate the depth and breadth of your MSP's technical bench. You need certified professionals across cybersecurity, cloud, infrastructure, compliance, and emerging technologies. Look for industry certifications (CISSP, CISM, CCSP, Azure, AWS), SOC 2 compliance, and a demonstrated track record with organizations like yours. Ask about the MSP's investment in continuous training and its ability to support emerging and critical technologies.

Operational Excellence and Process Maturity

A qualified MSP should have documented, repeatable processes that ensure consistent service delivery. Ask about ITIL adoption, operational maturity assessments, SLA compliance rates, and quality assurance programs. The best MSPs codify mature practices into automation (self-healing, automated patching, infrastructure audits) to improve performance and eliminate human error.

Resilience and Incident Readiness

Disruptions are inevitable. The question is whether your MSP is prepared. Look for a provider that embeds resilience into day-to-day operations: proactive risk reduction, tested response plans, coordinated recovery, and an internal R&D function that evaluates new threats, tools, and configurations before they impact customer environments.

A Customer Experience That Sets the Standard

Ask for proof of customer satisfaction: Net Promoter Scores, customer satisfaction metrics, retention rates. Speak with references and ask specific questions about responsiveness, communication, billing, and long-term partnership quality. The right MSP assigns dedicated experts who understand your environment and take ownership of outcomes, not a rotating cast of technicians reading from a script.

Ease of Onboarding

Whether you are outsourcing IT for the first time or switching providers, onboarding sets the tone for the entire relationship. Your MSP should have a dedicated onboarding team, a documented project plan, and a proven process for transitioning environments without disruption. Ask about timelines, milestones, and how knowledge transfer is handled.

Commercial Flexibility

Your MSP should offer flexible engagement models (bundles, a la carte services, and project-based work) with pricing that reflects your environment, not arbitrary tiers. As your organization grows, your MSP should be able to scale with you without rigid contracts or hidden costs.

Does Your MSP Need to Be Local?

One of the most common questions in MSP selection is whether geographic proximity matters. The short answer: with the right MSP, both you and your provider can be anywhere.

Managed services today are provided remotely using secure cloud tools, around-the-clock monitoring systems, and encrypted remote connections. The vast majority of day-to-day management (monitoring, patching, help desk support, security operations, and incident response) happens through remote infrastructure. Physical proximity is rarely a factor in service quality.

What does matter is scale, capability, and accountability. Local MSPs often provide a personal touch, but they may lack the depth of expertise, 24/7 coverage, or advanced security capabilities that your organization requires. National providers offer scale but are often transactional, process-driven, and impersonal. The ideal partner combines the high-touch service of a local provider with the depth, innovation, and national reach of a larger firm.

The table below compares how different MSP models typically stack up across the capabilities that matter most:

Capability	Logically	Local MSPs	National Providers
Cyber-first service model	Security embedded across all services	Primarily resale of technology vendors	Often outsourced or white-labeled
Unified IT + security operations	Single operating model	Not available	Integrated but siloed by function
24x7 in-house SOC and NOC	Fully operated by Logically	Rare or outsourced	SOC often outsourced
Threat detection and response	Proprietary XDR platform	Third-party tools	Platform-based
Executive accountability	One accountable partner	Relationship-dependent	Multi-team escalation
Strategic advisory (vCIO / vCISO)	Embedded, ongoing guidance	Limited or ad hoc	Often transactional
Commercial flexibility	Bundles, a la carte, and projects	Limited options	Rigid packaging
AI-assisted operations	Human-led, AI-assisted workflows	Minimal	Automation-led
Personalized service at scale	High-touch with national depth	High-touch, limited scale	Low-touch, transactional

Logically's Approach

Logically delivers high-touch, relationship-driven service at national scale. With a US-based 24/7 NOC and SOC, 200+ IT professionals, 50+ dedicated cyber professionals, and proprietary technology including SentryXDR and LogicAI, Logically combines the accountability and service quality of a dedicated partner with the expertise and reach of a national provider. Location does not limit capability. Operating model and commitment do.

Your Turn: What's Important to You?

Use the matrix below to assess which MSP characteristics and benchmarks matter most to your organization. This will help you weight evaluation criteria and compare providers objectively.

MSP Evaluation Criteria Matrix

Benchmark / Characteristic	Need to Have	Nice to Have	N/A
OPERATING MODEL			
Unified IT and cybersecurity under one operating model	☐	☐	☐
Security embedded across all services (cyber-first)	☐	☐	☐
AI-assisted monitoring with human-led response	☐	☐	☐
In-house SOC and NOC (not outsourced)	☐	☐	☐
Single point of accountability for all services	☐	☐	☐
EXPERTISE AND CAPABILITIES			
Certified cybersecurity professionals (CISSP, CISM, etc.)	☐	☐	☐
Cloud expertise (Azure, AWS, hybrid environments)	☐	☐	☐
Compliance and regulatory expertise (HIPAA, PCI, GLBA)	☐	☐	☐
AI governance and enablement capabilities	☐	☐	☐
Strategic advisory (vCIO / vCISO)	☐	☐	☐
Proprietary technology and innovation (XDR, R&D)	☐	☐	☐
OPERATIONAL MATURITY			
Documented processes and ITIL adoption	☐	☐	☐
Automation and self-healing capabilities	☐	☐	☐
Formal PMO for project delivery	☐	☐	☐
Proven onboarding process and dedicated team	☐	☐	☐
SOC 2 compliance	☐	☐	☐
CUSTOMER EXPERIENCE			
Dedicated account team with environment familiarity	☐	☐	☐
Transparent SLA reporting and performance metrics	☐	☐	☐
High customer satisfaction scores (NPS, CSAT)	☐	☐	☐
Proactive communication and strategic guidance	☐	☐	☐
Low customer churn rate	☐	☐	☐

MSP Evaluation Criteria Matrix			
Benchmark / Characteristic	**Need to Have**	**Nice to Have**	**N/A**
COMMERCIAL AND SCALE			
Flexible pricing (bundles, a la carte, projects)	☐	☐	☐
Environment-based pricing (not rigid tiers)	☐	☐	☐
National coverage with high-touch service	☐	☐	☐
Ability to scale services as organization grows	☐	☐	☐
RESILIENCE AND READINESS			
Tested incident response plans	☐	☐	☐
Validated backup and disaster recovery	☐	☐	☐
Internal R&D and emerging threat testing	☐	☐	☐
Business continuity planning support	☐	☐	☐

Final Thoughts

The managed services landscape has changed dramatically. The threats are more sophisticated. The technology is more complex. The stakes are higher. Risk now concentrates in the gap between IT and cybersecurity, where ownership is unclear and response is delayed.

Choosing an MSP is no longer about finding a vendor to keep the lights on. It is about selecting a strategic partner who will take accountability for the security, performance, and resilience of your technology environment, and who will help you make smarter decisions as both technology and risk continue to evolve.

The right MSP should:

- Unify IT and cybersecurity under a single, accountable operating model.
- Embed security into every service, not layer it on as an afterthought.
- Combine AI-assisted speed with human-led judgment and accountability.
- Demonstrate proven expertise through certifications, track record, and customer results.
- Deliver a customer experience rooted in transparency, proactive communication, and dedicated ownership.
- Scale with your organization and adapt as your needs evolve.

Close the Gap with Logically, the Next-Gen MSP

Logically unifies IT operations and cybersecurity into one accountable operating model, providing shared visibility, coordinated response, and clearer control. Modern IT and multi-layered security from one partner, built into an integrated operating model that attackers can't exploit and traditional MSPs can't match.

Appendix A: Top Questions to Ask When Evaluating an MSP

Experience and Expertise

- How many managed services customers do you currently support, and what is your ideal customer profile?
- How many endpoints do you manage, and what is the size and composition of your service delivery team?
- What certifications do your cybersecurity and engineering professionals hold?
- Are you SOC 2 compliant? Can you provide your most recent audit report?
- What is your experience supporting organizations in our industry and regulatory environment?

Operating Model and Accountability

- How are IT operations and cybersecurity integrated within your organization?
- Do you operate your own SOC and NOC in-house, or do you outsource any monitoring or response functions?
- Who owns accountability when an incident occurs? Can you describe your escalation and response process?
- How do you ensure shared visibility across IT and security teams?
- What proprietary technology or platforms do you bring to the engagement?

Services and Capabilities

- What services are included in your standard managed services engagement, and what is priced separately?
- What cybersecurity services do you provide, and how are they integrated with IT management?
- What cloud platforms do you support, and can you help us modernize existing cloud investments?
- How do you approach governance, risk, and compliance for regulated organizations?
- Can you support AI governance and enablement for our workforce?
- Do you provide strategic advisory services such as vCIO and vCISO?

Operational Maturity and Quality

- What SLAs do you offer, and what is your historical compliance rate?
- What is your first-call resolution rate for help desk issues?
- How do you automate routine tasks, and what self-healing capabilities do you offer?
- Describe your onboarding process. What does the first 90 days look like?
- How do you handle project delivery? Do you have a formal PMO?
- How do you validate that backups are successful and recoverable?

Customer Experience and Partnership

- How do you measure customer satisfaction, and what are your most recent scores?
- What is your annual customer retention rate?
- Will we have a dedicated account team that understands our environment?
- How frequently do you provide strategic reviews and proactive recommendations?
- Can you provide three to five references from organizations similar to ours?

Security and Resilience

- How do you approach incident response, and when was your last tabletop exercise?
- Do you have an internal R&D function that tests emerging threats and technologies?
- How do you ensure our security posture improves over time, not just stays static?
- What is your approach to threat intelligence, and how do you share it with customers?

Commercial Terms

- How is your pricing structured? Per user, per device, per environment?
- What flexibility do you offer in terms of service bundling and contract terms?
- Are there any hidden costs for on-site visits, after-hours support, or emergency response?
- How do you handle service changes as our organization grows or our needs evolve?