



# Choosing the Right IT Partner

2026 buyer's guide // for small and mid-size businesses in North Georgia

Your IT partner is one of the most consequential vendors you will hire. The wrong choice means slow response, surprise invoices, security gaps you find out about during an audit or a breach, and a years-long rip-and-replace cycle when you finally switch. The right choice is a team that quietly keeps the business running, the numbers predictable, and the risks handled.

This guide walks through what actually matters when you evaluate a Managed Service Provider (MSP), the questions that separate real operators from sales teams, and the red flags that save you a painful 12 months.

**\$137–\$427**

per minute of IT downtime for a typical small business

**30%**

of data breaches now involve a third-party vendor

**\$10.22M**

average U.S. data breach cost in 2025

## Why the choice matters

Three numbers frame the decision. Downtime costs a small business somewhere between \$137 and \$427 per minute once you count lost productivity, missed orders, and the scramble to catch up. The Verizon 2025 Data Breach Investigations Report found that third-party involvement in breaches has doubled year over year: your vendors are now one of the most common ways attackers get in. And the IBM Cost of a Data Breach Report pegs the average U.S. breach at \$10.22 million.

Your IT partner touches all three. They set how fast you recover, how much access your other vendors have, and how hard it is for an attacker to reach anything important. Treat the selection accordingly.

<sup>1</sup>Industry reporting on SMB IT downtime costs, 2025.

<sup>2</sup>Verizon 2025 Data Breach Investigations Report.

<sup>3</sup>IBM Security, Cost of a Data Breach Report 2025.

# What to look for in an IT partner

---

Seven criteria, in rough order of how much they will matter in the first year.

## 1. Proactive management, not break-fix

- ✓ **Monitoring and maintenance happen on a schedule:** Patches, backups, and security checks run whether you call or not. If the only time you hear from your MSP is after you submit a ticket, you are paying for a help desk, not a partner.
- ✓ **Preventive projects are on the calendar:** Hardware refresh cycles, license renewals, and end-of-life operating systems are tracked in a plan you can see, not a spreadsheet in someone's head.

## 2. Fast, human response

- ✓ **Responses in minutes, not hours:** Critical issues get a real person on the line quickly, not an auto-reply promising a callback within a business day. Ask for the specific response time commitment and what "critical" means to them.
- ✓ **Local on-site coverage when it matters:** Remote tools fix most things, but a dead switch, a flooded server closet, or a new-hire workstation deployment still wants boots on the ground. Confirm who shows up, how quickly, and from where.

## 3. Cybersecurity depth and insurance alignment

- ✓ **Security is baked in, not an add-on:** Endpoint Detection and Response (EDR) on every device, phishing-resistant multi-factor authentication (MFA), immutable backups, and 24/7 monitoring should be part of the standard offer. If security is a separate upsell, you are buying half of what you need.
- ✓ **They speak your insurer's language:** Modern cyber insurance renewals require MFA, EDR, tested backups, and security awareness training. A good MSP fills out your renewal questionnaire, does not flinch, and tells you where the gaps are before the carrier does.

## 4. Full-stack range of services

- ✓ **Workstations, servers, network, cloud, and email under one roof:** Splitting IT across three vendors creates finger-pointing. One partner means one phone number for anything that plugs into power or runs on a screen.
- ✓ **AI and automation are part of the conversation:** If your MSP cannot tell you how to safely use Microsoft Copilot, where to draw the line on employee use of free AI tools, or how to automate a recurring task in your business, the scope is too narrow for 2026.

## 5. Industry fit and real references

- ✓ **They have worked with businesses like yours:** Manufacturing, fabrication, construction, professional services, and healthcare all have different compliance, uptime, and floor-level reality. Ask for references in your industry and actually call them.
- ✓ **Case studies that name specific outcomes:** "We helped them with IT" is a pamphlet. "We cut their ticket volume by 40 percent in six months and moved them off a failing server" is a case study.

## 6. Clean onboarding and off-boarding

- ✓ **A documented onboarding plan with dates:** The first 60 to 90 days should be mapped: discovery, documentation, agent deployment, baseline security controls, and the first review. Vague onboarding is vague ownership.
- ✓ **You own your environment, not them:** Ask in writing who owns domain names, Microsoft 365 tenants, firewall configurations, and documentation. If you ever switched, could you take it all with you? If the answer is "it's complicated," the answer is no.

## 7. Transparent pricing and contracts

- ✓ **Flat, per-user or per-device pricing you can model:** Per-user or per-device flat fees make budgeting predictable. Hourly break-fix billing rewards slow fixes. Avoid contracts that mix the two without clear rules.
- ✓ **No surprise project minimums or automatic renewals:** Out-of-scope work gets a written estimate before the hours start. Contracts renew month-to-month after the initial term, or with clear written notice. Multi-year lock-ins with auto-renew and 90-day-exit windows are a red flag.

## Ten questions to ask on the sales call

---

The answers tell you more than the pitch. Take notes and compare.

### 1. What is your typical response time for a critical ticket, and what counts as critical?

*You want a specific answer measured in minutes, and a clear definition of priority levels.*

### 2. Who will we actually work with day to day?

*Great sales reps, unknown technicians is a common disconnect. Meet the engineer who will own your environment.*

### 3. How do you handle after-hours emergencies?

*Is there a 24/7 on-call engineer, or does an overnight outage wait until Monday?*

### 4. Walk me through your onboarding for a business like ours.

*Specificity matters. Vague onboarding leads to vague ownership.*

### 5. What security controls are included in the base package?

*MFA, EDR, email security, backups, training, patching. Each one that is an upsell is a gap on day one.*

### 6. How do you support a cyber insurance renewal?

*You want a partner who fills out the questionnaire, reviews it with you, and flags gaps before the carrier does.*

### 7. Can I see a sample of the monthly report I will receive?

*If they cannot show you a real report with real metrics, they probably do not produce one.*

### 8. How do you handle our data and access on offboarding?

*You need to know you can leave cleanly, with your data, your tenants, and your documentation.*

## 9. Who are three current clients I can call as references?

*Ideally in your industry or region. A partner with nothing to hide hands over the list.*

## 10. What does a typical escalation path look like when something is broken?

*You want a clear chain: ticket to technician to engineer to leadership, with expected timelines at each step.*

## Red flags to watch for

---

Any one of these is a reason to dig deeper. Two or more and you keep looking.

- ⚠ **Vague response commitments:** "We respond fast" without a specific number means no commitment. "Responses in minutes, not hours" is a commitment.
- ⚠ **Pricing that skips security:** A lower headline price that excludes MFA, EDR, backups, or security training is not cheaper, it is incomplete.
- ⚠ **Ownership fog:** You cannot get a straight answer on who owns your Microsoft 365 tenant, your domain, or your firewall configs. This becomes painful fast if you ever switch.
- ⚠ **Multi-year contracts with punitive exits:** Long lock-ins, automatic renewals, and short exit windows are a way to keep you through the pain instead of earning the renewal.
- ⚠ **No written documentation of your environment:** If they cannot show you a network diagram, asset inventory, and password vault for your business after month three, they are flying blind and so are you.
- ⚠ **Gift-card or kickback-style promos in their sales pitch:** A free tablet or gift card at signing is not the value you should be evaluating on. Read the annual cost.
- ⚠ **One-size-fits-all packages:** A 12-person law firm and a 40-person fabrication shop do not need the same stack. Packages are fine, but they should flex to your reality.

## How the right partner actually changes things

---

In the first 90 days, a good MSP stabilizes the environment: monitoring deployed, backups verified, endpoints locked down, the scariest gaps closed. In the first year, the ticket volume drops, surprise outages get rare, and you stop being the one who has to remember that the server license is expiring.

By year two, the conversation shifts. Instead of firefighting, you are planning: a cleaner Microsoft 365 setup, automation that takes a manual process off someone's plate, a hardware refresh that doesn't require emergency capex, an AI pilot your team can actually trust. Good IT moves from a line item you grudgingly pay to a lever you pull when you want the business to do something it couldn't do before.

## About PeachByte

---

PeachByte is North Georgia's managed IT partner for businesses that want to stop thinking about IT. Founded in 2022 and based in Adairsville, we manage 200+ endpoints across the region and respond in minutes, not hours. We are deliberately a small, senior team: our clients know us by name, we know their environments by heart, and we show up on-site when the situation calls for it.

Our clients are manufacturers, fabricators, contractors, professional services, and industrial operators who cannot afford for the technology to be the reason the work stops. One partner, one bill, one phone number for workstations, servers, network, email, cybersecurity, backups, vendor coordination, and the AI tooling that is increasingly part of the stack.

We cover Adairsville, Cartersville, Calhoun, Dalton, Rome, and Marietta on-site, and the rest of North Georgia remotely.

### Your next step

Start with a free IT review: a 60-minute walk-through where we benchmark your environment against the criteria in this guide and hand you a written roadmap of what to fix first. The findings are yours to keep whether or not we work together.

Book a free strategy call at [peachbytesolutions.com](https://peachbytesolutions.com), or dial 470-529-1421.

### Sources

1. Industry reporting on small-business IT downtime costs, 2025 (per-minute estimate, SMB range).
2. Verizon, 2025 Data Breach Investigations Report. [verizon.com/business/resources/reports/dbir](https://verizon.com/business/resources/reports/dbir).
3. IBM Security, Cost of a Data Breach Report 2025.