Centrend
Volume 25
Monthly Newsletter
# THE TECH CHRONICLE
April 2025 www.centrend.com Thursday

## WHAT'S INSIDE?





# Beyond Antivirus: 5 Overlooked IT Security Layers SMBs Need in 2025

Let's face it—antivirus alone won't cut it anymore. For years, small and mid-sized businesses (SMBs) have leaned on antivirus software like a digital security blanket. But cyberthreats in 2025 are faster, sneakier, and far more dangerous than they used to be. Ransomware doesn't knock before it locks up your systems. Phishing scams don't look suspicious anymore—they look like your boss. And your antivirus? It's only one layer of defense.

If you're still relying on it as your main line of protection, your business could be one click away from disaster.

At ***Centrend***, we work with organizations like yours every day—ones that want real protection, not just the illusion of it. So here's what many SMBs are overlooking when it comes to IT security in 2025.

### 1.Multi-Factor Authentication (MFA): Your Login's Secret Weapon

Strong passwords are great—until they're guessed, phished, or leaked in a breach. That's where MFA steps in.

MFA adds an extra step (like a text or app notification) to prove a user's identity. Even if a password gets stolen, MFA blocks unauthorized access.

**Why SMBs skip it:** It seems like a hassle or "only for the big guys."

*Beyond Antivirus: 5 Overlooked IT Security Layers SMBs Need in 2025…*

**Why you need it:** 90% of breaches start with compromised credentials. MFA can stop most of them dead in their tracks.

### 2. Endpoint Detection & Response (EDR)

Think of EDR as antivirus with a brain—and a memory. It doesn't just try to stop threats. It watches what's happening on every device, learns from behavior, and helps you respond to attacks in real time.

**Why SMBs skip it:** It sounds expensive or too complex.

**Why you need it:** EDR tools catch things antivirus can't—and often spot threats before they cause real damage.

### 3. Patch Management: The Easy Fix Everyone Ignores

Cybercriminals love out-of-date software. Why? Because it's full of known vulnerabilities. And most breaches come from systems that just weren't patched.

**Why SMBs skip it:** Updates feel like a low priority, or they don't want to disrupt daily operations.

**Why you need it:** Unpatched systems are like unlocked doors. Good patch management closes them.

### 4. Security Awareness Training: The Human Firewall

Even with the best tech in the world, one distracted employee can click the wrong link and let a hacker in.

Regular, engaging training helps your team recognize threats like phishing, social engineering, and spoofed websites. And no—*one boring video a year doesn't count.*

**Why SMBs skip it:** It's seen as a "nice to have," not a must.

**Why you need it:** Your team is your front line. If they don't know what to look for, your systems are already at risk.

### 5. Offsite & Immutable Backups: Your Ransomware Insurance Policy

Even the best defenses can fail. What matters then is how fast you can recover.

Backups that are stored offsite and cannot be altered (a.k.a. immutable) give you a lifeline. If ransomware hits, you don't have to pay—you just restore.

**Why SMBs skip it:** "We back up to a local drive—that's enough, right?"

**Why you need it:** If your backups are connected to your network, ransomware can encrypt those too. Immutable = untouchable.

Final Thought: Don't Wait for a Breach to Take This Seriously

Cybersecurity in 2025 isn't about if you'll be targeted. It's about how well you're prepared when it happens. SMBs are increasingly in the crosshairs because they often lack layered protection.

At **Centrend**, we specialize in giving small businesses enterprise-grade security that fits their budget—and actually works.

**Ready to move beyond antivirus?** Let's chat about how you can strengthen your defenses without overwhelming your team.

**Schedule a free consultation** today at **centrend.com** or call us directly at **774 241-8600.**

# Managed IT vs. In-House: What Growing Businesses Are Choosing in 2025

Growing a business in 2025 means navigating hybrid work, cloud everything, nonstop cybersecurity threats — and the constant pressure to do more with less.

One of the biggest questions business leaders face as they scale is: **"Should we build an in-house IT team or partner with a Managed IT provider?"**

The answer isn't one-size-fits-all. But more and more growing businesses are leaning toward **Managed IT Services**, and it's not just about cost—it's about agility, expertise, and peace of mind.

Let's break it down.

*Managed IT vs. In-House: What Growing Businesses Are Choosing in 2025...*

### What's the Difference?

- **In-House IT** means hiring your own staff to manage technology, security, support, and strategy.
- **Managed IT Services** (like those offered by Centrend) provide a full team of outsourced experts who proactively manage your IT infrastructure, security, helpdesk, and more for a flat monthly rate.

Both have their pros. But here's why Managed IT is taking the lead in 2025.

### 1. Breadth of Expertise—Without the Overhead

Hiring one or two in-house IT pros may seem practical, but it's hard for a small team to cover everything—cybersecurity, networking, cloud, compliance, helpdesk, backups, and strategy.

Managed IT gives you a **whole team of specialists** for less than the cost of a single full-time hire. You're not paying one salary—you're accessing decades of collective experience.

### 2. 24/7 Support, Without Burning Out Your Team

In-house IT staff can't be on-call around the clock (and if they are, they'll burn out fast). Managed IT teams monitor your systems 24/7, respond to issues immediately, and often fix problems before you even know they exist.

Business doesn't stop after 5 p.m.—**neither should your IT support.**

### 3. Stronger Cybersecurity, Built-In

Cybersecurity has gotten too complex for a generalist to manage alone. Managed IT providers stay ahead of the latest threats and deliver layered protection—firewalls, EDR, patch management, offsite backups, compliance reporting, and more.

At Centrend, we include advanced security tools as part of our managed services, **not as expensive add-ons.**

### 4. Predictable IT Costs, Scalable as You Grow

Hiring and retaining IT talent is expensive—and unpredictable. Salaries, benefits, turnover, training... it adds up fast.

With Managed IT, you get **flat-rate pricing**, no surprise bills, and services that scale as your business grows. It's budget-friendly and growth-ready.

### 5. You Stay Focused on What Matters

When your IT just works—and someone else is managing the risk—you and your team can stay focused on customers, sales, operations, and innovation.

**No more tech headaches. No more fire drills. Just smart, stable, secure IT.**

### So What Are Businesses Choosing in 2025?

Here's the trend we're seeing:

- **Small teams (10–100 employees)** are choosing Managed IT for full coverage and fewer headaches.
- **Mid-sized businesses** often keep a small internal IT presence—but rely on Managed Services for cybersecurity, strategy, and scaling support.
- **Fast-growing companies** are switching to Managed IT to move faster without hiring delays or skill gaps.

### Is Managed IT Right for Your Business?

If you're still deciding between hiring or outsourcing—or wondering if your current IT setup is future-ready—we're here to help.

Centrend specializes in helping growing businesses in Massachusetts and beyond get the IT support, strategy, and security they need to thrive.

Book a free strategy session or give us a call at **774 241-8600.** Let's figure out what makes the most sense for *your goals.*

# How AI Updates Are Revolutionizing SMB Operations

AI is no longer just for big corporations. In 2025, small and mid-sized businesses are using AI to streamline operations, boost productivity, and stay competitive—without the need for massive budgets.

AI is transforming decision-making by analyzing data in real time, providing insights, and predicting trends that help business leaders make smarter choices faster. Whether it's forecasting sales, tracking inventory, or identifying customer issues early, AI helps you stay ahead.

Automation is another key benefit. AI tools handle routine tasks like emails, meeting summaries, and customer support, freeing up time for employees to focus on more strategic work.

AI is also revolutionizing customer service, with advanced chatbots and virtual assistants offering personalized, 24/7 support. SMBs can now provide the same level of service as larger enterprises—without the extra overhead.

On the security front, AI-powered systems detect and respond to threats in real time, offering powerful protection for businesses of any size. These systems monitor for unusual behavior, stopping risks before they escalate.

The best part? Many of these AI tools are already built into software you're probably using, like Microsoft 365, Google Workspace, and CRMs—making it easier than ever to get started.

At **Centrend**, we help growing businesses leverage AI to work smarter, stay secure, and drive growth—without the tech overwhelm.

Ready to learn how AI can support your business? Book a free consultation or call at **774-241-8600**

# From Security Risks to Compliance Issues: The True Cost of Using Old Tech

Still running outdated software or relying on aging hardware? It might seem like a way to save money—but in 2025, **old tech is one of the biggest hidden risks to your business.**

Here's why holding onto outdated systems can end up costing more than upgrading:

### 1. Security Vulnerabilities

Old tech doesn't get security patches, making it a prime target for hackers. One unpatched machine can be all it takes to let ransomware into your network.

### 2. Compliance Problems

Industries like healthcare, finance, and legal must meet strict compliance standards. Unsupported systems often fail audits and can result in **fines, lawsuits, or lost contracts.**

### 3. Productivity Losses

Outdated systems are slower, less reliable, and prone to crashing. That adds up to lost time, frustrated employees, and **real dollars out the door.**

### 4. Hidden Costs

Keeping old tech running often costs more than replacing it—between extra support, downtime, and emergency fixes, you'll feel it in your IT budget.

### 5. You're Falling Behind

Modern apps, cloud services, and security tools often don't integrate with legacy systems. That means missed opportunities for efficiency, automation, and growth.

**Bottom line?** Old tech isn't just a nuisance—it's a liability.

At **Centrend**, we help growing businesses identify tech risks and plan smart upgrades without breaking the bank.

Let's chat: Book a free assessment or call **774 241-8600.**

# Why MFA Isn't Enough Anymore

If you've added Multi-Factor Authentication (MFA) to your logins, you've taken a critical step toward protecting your business. It's one of the most effective ways to block unauthorized access—no argument there.

But here's the uncomfortable truth: **MFA alone won't keep your company safe in 2025.**

Cybercriminals have caught up. They're bypassing MFA, launching smarter attacks, and targeting companies that think they're already protected. As your business grows, so do your risks—and your security strategy needs to grow with it.

Let's break down why **MFA isn't enough anymore**, and what advanced threat protection really looks like for modern, growth-focused companies.

### The MFA Myth: "We're Covered Now."

When businesses implement MFA, there's often a false sense of total security. And we get it—adding that second factor feels like locking the door and installing a deadbolt.

But here's what many business owners don't know:

- **Phishing kits can now bypass MFA** using real-time man-in-the-middle tactics.
- **SIM swapping and push fatigue attacks** (where attackers flood a user with MFA prompts until they accept one) are on the rise.
- **Social engineering** and deepfakes are being used to trick users into giving up codes or approving access.

MFA *reduces* risk, but it's no longer a guaranteed wall. Hackers are finding the cracks—and exploiting them.

### So What Is Advanced Threat Protection?

Advanced Threat Protection (ATP) is more than one tool—it's a *strategy*. It layers multiple defenses to detect, block, and recover from threats before they can do real damage.

Here's what growing companies need to add to their MFA setup:

### 1. Behavior-Based Threat Detection

Tools like Endpoint Detection & Response (EDR) go beyond simple antivirus. They analyze what users and devices are doing—flagging suspicious behavior in real time. Think of it as a digital security guard that never sleeps.

### 2. AI-Driven Email Protection

Email is still the #1 attack vector. Modern ATP solutions use artificial intelligence to scan emails for suspicious content, malicious attachments, and phishing links before they reach inboxes. Standard spam filters won't catch these—AI will.

### 3. Zero Trust Architecture

In a Zero Trust model, no user or device is trusted by default—even inside your network. Access is granted based on verification, location, behavior, and other risk factors.

It's "never trust, always verify" on every level—and it's quickly becoming a must-have for forward-looking businesses.

### 4. Security Awareness Training

Advanced security isn't just tech—it's also people. Regular, up-to-date training empowers your team to recognize phishing, social engineering, and other attacks before they click or respond.

Your users are your weakest link or your strongest defense—depending on how prepared they are.

### 5. Immutable Offsite Backups

If a ransomware attack slips through, the last line of defense is your backup. But if your backups can be altered or deleted, they're useless.

ATP strategies include immutable, offsite backups that can't be tampered with—so you can restore quickly without paying a ransom.

### Final Thoughts: Growth Shouldn't Outpace Security

The truth is, hackers don't care how big your company is. In fact, they often prefer SMBs and fast-growing companies because they know security often lags behind.

MFA is a great start. But if that's where your protection ends, you're still vulnerable.

At **Centrend**, we help growing businesses go beyond basics. From real-time threat monitoring to AI-powered email filtering, we build layered defenses that scale with your success.

**Let's get your company protected for 2025.**

Schedule your free IT security consultation today or call us at **774-241-8600.**