January 2025

TechTidbit.com

brought to you by Tech Experts

Are Your Tech Tools Helping Or Hurting Your Business?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

In the rush to stay competitive, businesses have been trying out new tech tools left, right, and center. It's great to embrace change.

But here's the thing: Having too many tools - or the wrong kind - can create more headaches than solutions.

That means lots of businesses are now stuck with a jumble of software that doesn't play nicely together, making work slower and more frustrating than it should be.

Over the past few years, companies have thrown tools at every problem:

- HR needed a way to track time off requests… there's software for that
- Finance needed help with tax compliance… another tool added to the mix
- Add in the scramble to adapt to remote work and fast growth, and suddenly, every department has its own tool

The result? A patchwork quilt of systems that just don't connect.

Now the focus is shifting to working smarter, not harder, and those cracks in your tool stack are showing. Instead of helping your team, too many disconnected tools are slowing them down. Data gets stuck in silos, workflows feel clunky, and employees are juggling software. To make matters worse, you're likely paying for tools no one's even using.

So, what can you do?

Look at the bigger picture. Think about consolidating your tool stack. Cut out the extras and focus on systems that work together smoothly. When your tools are aligned, your data flows properly and your team can do what they do best.

It's not just about saving money (though you'll probably do that too). It's about making work easier and more efficient. Automation can also help you spot inefficiencies and connect the dots between systems, so everything runs more smoothly.

If your team isn't working as efficiently as they could, before you start pointing fingers consider that your stack might be the reason.

We can help you create a tool stack that helps, not hinders, your workflow. Get in touch.

Instead of helping your team, too many disconnected tools are slowing them down. Data gets stuck in silos, workflows feel clunky, and employees are juggling software. To make matters worse, you're likely paying for tools no one's even using.

Act Now: The Clock Is Ticking For Windows 10

"But Windows 11 is here, and it's built to make your business run more smoothly. From stronger security features to smarter productivity tools, the upgrade is packed with benefits… and it's free!"

Still using Windows 10? It's time to start planning for a big change. Microsoft has announced that this October will mark the end of support for the operating system.

That means no more security updates, no bug fixes, and no technical support.

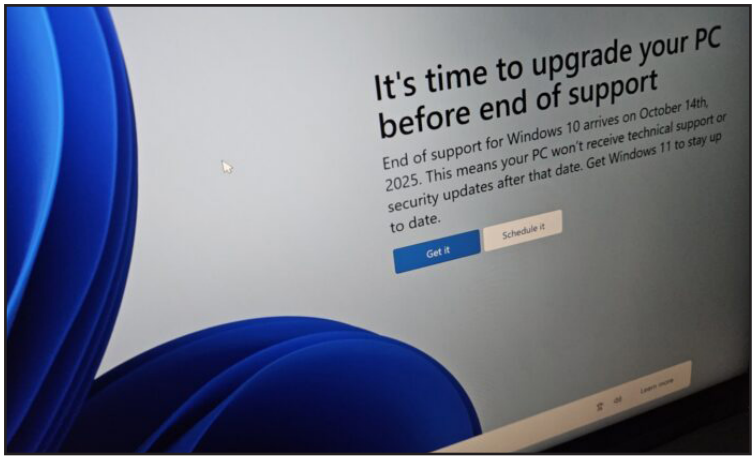
While your computers won't suddenly stop working, staying on Windows 10 after its end-of-life date could put your business at serious risk.

Without regular updates, your systems will be more vulnerable to cyber attacks.

Cyber criminals love to exploit old, unsupported systems because they know the weaknesses won't be fixed. If you handle sensitive customer data or financial information, this is a huge red flag.

On top of that, software compatibility could become a problem. New applications will be designed with Windows 11 and future systems in mind, meaning your current setup might not be able to keep up.

The result? Slower workflows or even critical tools that stop working entirely. And if something goes wrong, you'll be on your own – Microsoft won't be there to help.



But Windows 11 is here, and it's built to make your business run more smoothly. From stronger security features to smarter productivity tools, the upgrade is packed with benefits… and it's free!

Before making the move, you'll need to check if your current computers meet the requirements for Windows 11. Not all Windows 10 devices will be compatible, but it's easy to find out using Microsoft's PC Health Check tool.

If some devices don't make the cut, it might be time to invest in new hardware. While that sounds like a big step, newer machines offer better performance and security, saving you headaches down the line.

The key to a smooth transition is starting early. Back up your data, check compatibility, and plan your upgrade timeline so it doesn't disrupt your team.

Making the move now means you'll avoid scrambling later. And of course, you'll set your business up for success with a system designed for the future.

If you're feeling overwhelmed about where to begin, we can help every step of the way. Get in touch.

We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

What Is Threat Exposure Management (TEM) And Why Do You Need It?

Threat Exposure Management (TEM) is an important cybersecurity tool. It helps organizations find and fix weak spots in their digital systems. TEM outsmarts hackers before they break into your network.

Importance of TEM

Cyber attacks keep getting worse. Hackers always find new ways to break in. TEM helps businesses spot problems before they become big issues.

TEM allows you to:

- Find weak points in your network
- Fix issues quickly
- Reduce your risk of cyber attacks

How TEM works

TEM uses special software to scan your entire network. It finds places hackers could attack and helps you fix these weak spots.

Continuous monitoring
TEM keeps looking all the time. This way, you can find new problems as soon as they appear.

Risk assessment
TEM finds which weak spots are the most dangerous. This helps you fix the most important ones first.

Main parts of a TEM program

Asset discovery
This finds all devices and software on your network. You can't protect what you don't know about!

Vulnerability scanning
This looks for open weak spots in your system. It's like checking for unlocked doors and windows in your house.

Threat intelligence
This provides insights into new hacker techniques, helping you stay informed about what to watch out for.

Remediation planning
Once you find the vulnerabilities, you need a plan to fix them. TEM helps you make good choices on how to patch these spots.

Benefits of TEM for your business

Better security
Finding and fixing weak spots makes your whole system much safer and more resilient.

Cost savings
Stopping an attack before it happens can save you a lot of money. Dealing with the aftermaths of cyberattacks often comes with expensive costs.

Peace of mind
With TEM, continuous monitoring ensures your system is always under watch. This can help you worry less about cyber attacks.

What to look for in a TEM solution

A good TEM tool should:

- Be user-friendly, ensuring that all team members, regardless of their technical expertise, can easily navigate and utilize the tool.
- Provide immediate results, enabling quick and effective decision-making to address potential threats as soon as they are detected.
- Integrate seamlessly with your existing security infrastructure, enhancing overall protection by working in harmony with other security tools and systems.
- Generate clear and comprehensible reports, presenting findings in an easily digestible format that facilitates understanding and action.

Getting started with TEM

- Check your current security setup to understand your existing vulnerabilities and areas for improvement.
- Find a TEM tool that fits your needs, ensuring it aligns with your security goals and integrates well with your current systems.
- Set up the tool and start scanning your environment.
- Make a plan to fix the weak spots you find, prioritizing the most critical issues.
- Keep scanning and improve your security continuously, regularly updating your strategies and tools to stay ahead of emerging threats.

Want to learn more about how TEM can help your company? Contact us today for help staying safe in the digital world.

"TEM uses special software to scan your entire network. It finds places hackers could attack and helps you fix these weak spots."

Contact Information

Tech Experts Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Securing Remote Access Technology: What Every Small Business Owner Needs to Know

Remote access technology has become essential for modern businesses. Whether your employees work from home, connect to the office while traveling, or access critical systems after hours, secure remote access can greatly enhance productivity and flexibility.

However, without proper security measures, it can also open the door to significant risks, including data breaches, ransomware attacks, and unauthorized access to sensitive information.

Here's what small business owners need to know about securing their remote access technology.

Why secure remote access matters

Remote access allows users to connect to your business's network or systems from anywhere. While this connectivity is convenient, it also presents a larger attack surface for cybercriminals.

Hackers often target remote access solutions because they can be a weak link in your cybersecurity strategy if not properly secured.

The consequences of a breach can be devastating: financial losses, reputational damage, and even legal penalties for failing to protect customer or employee data.

The good news is that implementing secure remote access methods doesn't have to be complicated. With the right tools and practices, you can greatly reduce your risk while enabling your team to work efficiently from anywhere.

Key strategies for securing remote access

Use strong authentication methods
Passwords alone are no longer enough to protect remote access. Instead, implement multi-factor authentication (MFA). MFA requires users to verify their identity using two or more factors, such as a password, a smartphone app, or a fingerprint.

This adds an extra layer of security, making it much harder for attackers to gain access, even if a password is compromised.

Deploy a virtual private network (VPN)
A VPN creates a secure, encrypted connection between a remote user and your business network. This ensures that sensitive data, such as login credentials or customer information, cannot be intercepted by hackers.

Ensure your VPN is configured properly and use strong encryption protocols to maximize its effectiveness.

Limit access privileges
Not all employees need full access to all systems. Use the principle of least privilege to limit access based on each user's specific role. By restricting what employees can see or do within your network, you reduce the potential damage if their credentials are ever compromised.

Keep software up to date
Outdated software can contain vulnerabilities that hackers exploit to gain unauthorized access. Regularly update remote access tools, operating systems, and any third-party applications your business relies on.

Enable automatic updates whenever possible to ensure you don't miss critical security patches.

Educate employees on cybersecurity
Even the most secure systems can be compromised by human error. Train your employees on best practices for cybersecurity, including recognizing phishing attempts, creating strong passwords, and avoiding suspicious links or downloads. An informed workforce is one of your strongest defenses against cyber threats.

Monitor and audit remote access activity
Use monitoring tools to track who is accessing your network and when. Unusual activity, such as login attempts from unfamiliar locations, can be an early warning sign of a potential breach. Regular audits can help you identify and address vulnerabilities before they are exploited.

The cost of neglecting security

Some small business owners hesitate to invest in secure remote access solutions, viewing them as unnecessary expenses. However, the cost of a data breach or cyberattack often far exceeds the cost of preventive measures. Beyond financial losses, you could face downtime, lost trust from customers, and even regulatory fines.

By prioritizing secure remote access, you're not only protecting your business but also demonstrating to clients and partners that you take cybersecurity seriously. This can enhance your reputation and give you a competitive edge in an increasingly digital world.

Take action today

If your remote access technology isn't as secure as it should be, now is the time to act. Consult with IT professionals to evaluate your current setup, identify vulnerabilities, and implement a security plan tailored to your needs.

With the right measures in place, you can enjoy the benefits of remote access without compromising your business's security.