DELL Technologies AMD

How to protect business and customer data from cybercriminals

8 cybersecurity strategies for small and medium businesses.

About this eGuide

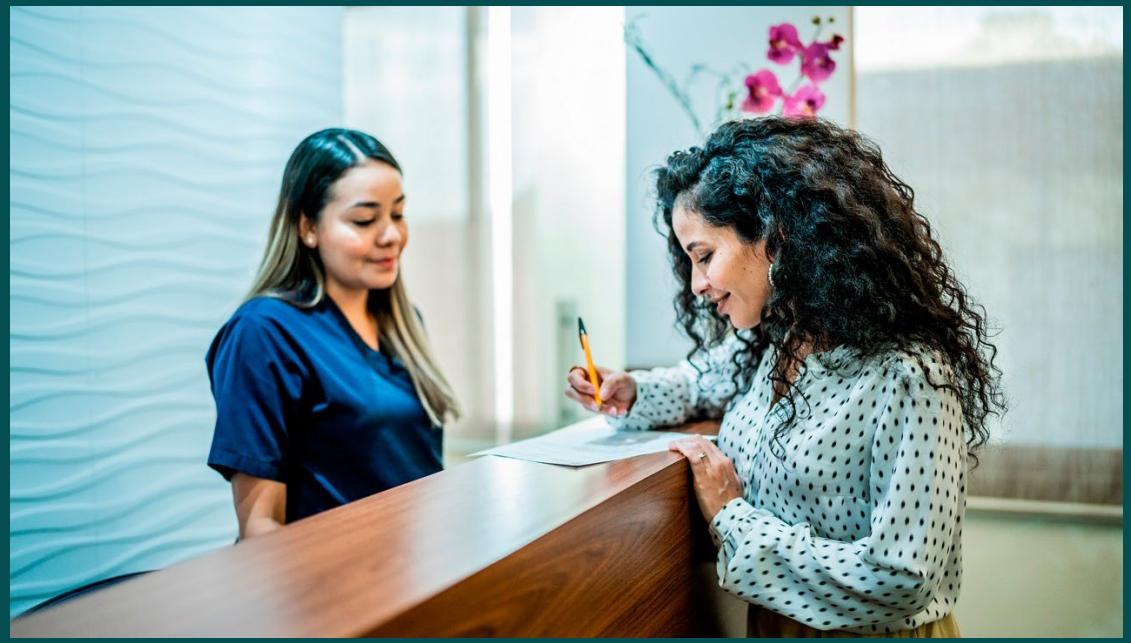
As a trusted IT and security partner to businesses of all sizes, Dell Technologies understands the everyday cybersecurity challenges small and medium businesses (SMBs) face. In this eGuide, we share eight smart strategies to help protect your business and customer data from cyber threats.

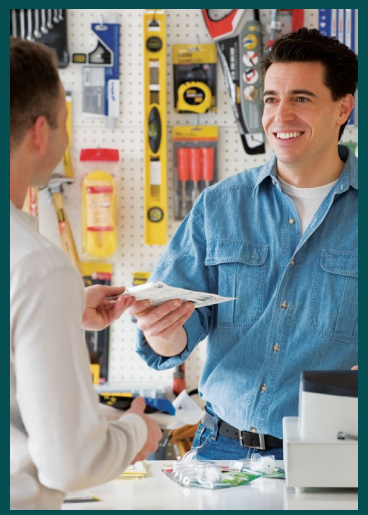
Table of Contents

Introduction

We've all seen the headlines—cyberattacks are happening more often and hitting businesses of every size. For SMBs, cybersecurity isn't just a "nice to have"—it's essential. Cyber criminals often target small and medium businesses, thinking they're easier to breach. While enterprises often have dedicated IT and security teams and resources, SMBs may not. In fact, research shows that 35% of small organizations worldwide believe their cyber resilience is inadequate. That's up seven times since 2022! All it takes is one misstep—a PC without the latest security patches, unprotected sensitive information, an unknown click on a phishing email—to open a business up to a whole host of problems, from financial setbacks to lost data to shaken customer trust.

The good news: A few proactive steps can go a long way. Protecting your business and customer data helps you stay confident, competitive, and ready for what's next. ►





Cyberattackers 101

Before we get into *how* you protect yourself, it's important to learn the mindset of the attackers themselves. Attackers are strategic—they look for easy entry points like unpatched PCs, weak passwords, and unsecured networks. They often study user behavior, target identities, and take advantage of overlooked vulnerabilities. By knowing their tactics, SMBs can better prioritize defenses, spot suspicious activity early, and build a security strategy that's proactive—not reactive. ►

Who are the attackers?

Attackers can range from common criminals (hackers with bad intent) to nation states. Some attackers can be easy to spot, using poorly written emails or texts. Some can have deep pockets and launch very sophisticated attacks.

Why do they attack?

Money is a key motivator. Global cybercrime continues to grow every year, with experts predicting annual costs reaching USD 10.5 trillion in 2025. Needless to say, the potential payout for one successful attack is too much to ignore.

How do attackers strike?

Cybercriminals are relentless—and they're getting smarter with AI at their fingertips. Here are a few methods they use:

- Attacks on "endpoints" such as PCs are a growing problem. In Endpoint Security Market Insights, Forrester Research, Inc., March 2025, the company explains, "Endpoints … are among the leading targets of external attacks for companies that have experienced a breach within the last 12 months."
- Identity attacks, too, are surging. Phishing remains a top threat. It's consistently one of the leading attacks, often used to steal credentials and deliver malware.
- Network attacks like ransomware continue to create havoc. Recent research shows small businesses were hit harder than enterprises, with 88% of their breaches involving ransomware.

In a nutshell, cyberattacks pay. The average successful ransomware attack nets cybercriminals $2 million. That's why persistence is part of their strategy—and why protection should be part of yours.

Major cybersecurity risks for SMBs

Device Compromise

Identity Compromise

Network Compromise

1 Know what you need to protect

Attackers go after sensitive customer and employee data – but you can't protect what you don't know. Take inventory of all your company's IT assets and data. Where is data stored? Who has access? What devices are on your network? With those insights in hand, take action. Ensure data is stored securely and restrict access to confidential information. Knowing your data is a key first step in protecting it. ►

2 Work with secure suppliers

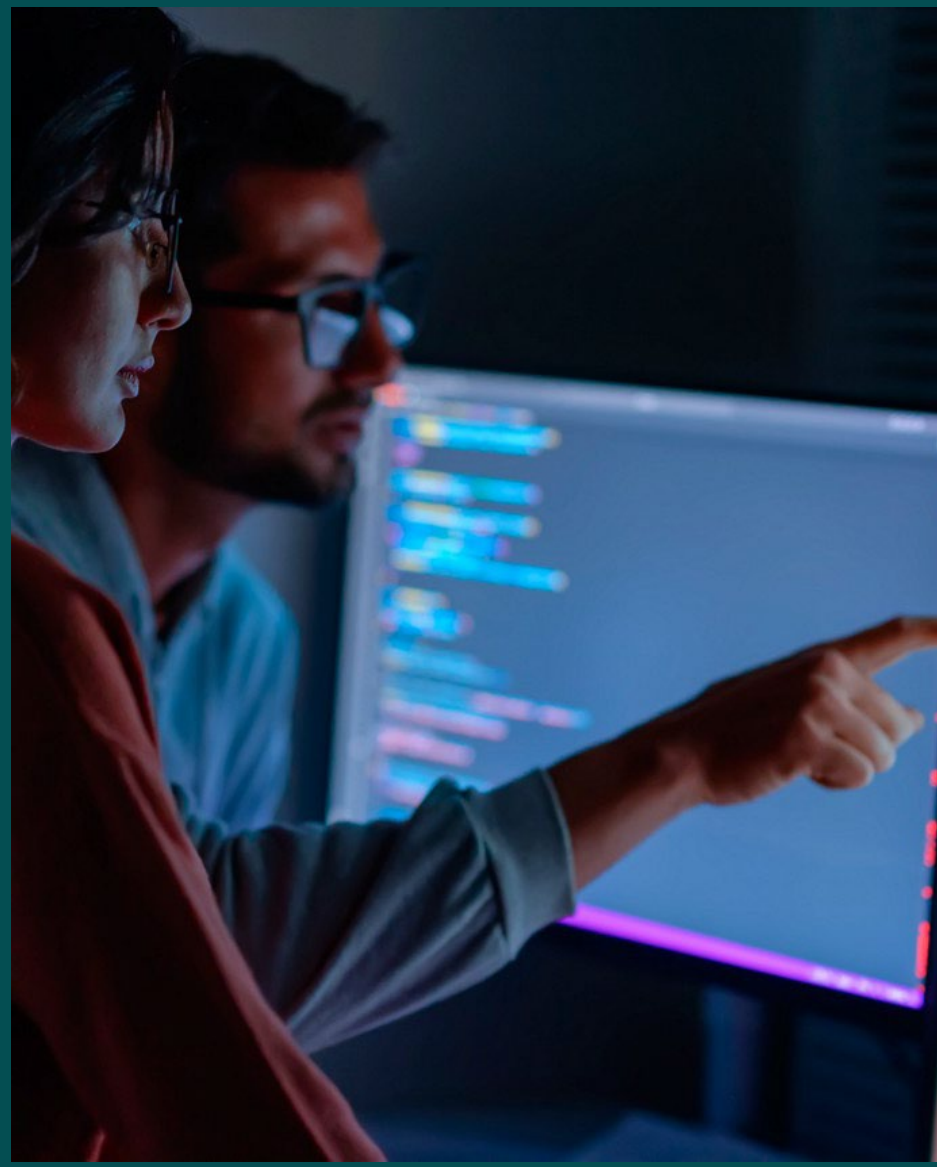
Think of the story of the Trojan Horse. The Greeks hid soldiers inside a seemingly harmless gift, which the Trojans brought inside their fortified city. Once inside, the attackers struck from within. Today's cybercriminals use similar tactics—sneaking in via trusted vendors, software updates, or hardware. SMBs often rely on many suppliers, making them vulnerable if one is compromised. That's why, e.g., vetting vendors, monitoring software integrity, and having visibility into shipment details, are essential to a strong cybersecurity strategy. ►

3 Get PCs with built-in security

Every PC is a potential entry point for cyberattackers. Built-in security features—like hardware protections, secure boot, and identity safeguards—help defend against threats right out of the box. Secure PCs simplify IT management and offer stronger defense against malware, phishing and unauthorized access. Also, keep in mind, attackers don't always strike from afar. An unattended PC in a public or shared space can be physically accessed and compromised by a fellow patron or someone posing as staff or maintenance. With limited resources and growing risks—both physical and digital—built-in security is a must today. ►

4 Keep PCs up to date

Cybercriminals often exploit known flaws in outdated systems, like sneaking through an unlocked door. Ignoring PC alerts and deferring updates can make you vulnerable. Software updates and patches are like locking that door; they fix bugs and security holes that attackers could use. Regular patches and updates fix those vulnerabilities, helping protect your business and customer data. For SMBs, it's a simple step that can prevent big problems. ►



5 Find problems and fix them quickly

Just because you have secure PCs and diligently keep them up to date doesn't mean a cyber criminal won't attack. Attackers can make an attempt on a single device dozens of times. They can send multiple phishes through email, through text. This increases their chance of breaking in and getting access to sensitive data. That's why it's important to have visibility across all business PCs, your network and any cloud environments that you work in. This is where a layer of software can help make sure you see everything and, importantly, so you can act quickly when you see suspicious activity. ►

6 Use strong passwords and enable MFA

Still using “123456” or “password”? You’re not alone—but it’s risky. Stolen credentials cause many breaches. Strong passwords are a must for a first line of defense. That said, persistent attackers find ways around them. That’s why Multi-Factor Authentication (MFA) matters—it adds a second layer, making it 99% less likely you’ll be hacked.

So, first, set strong passwords.

Then, combine that with a second way of verifying identity—like fingerprint readers, smart cards or NFC. For even stronger protection, store user credentials in secure hardware out of reach of malware that looks to steal them. ►

7 Train employees and test their skills

You are only as secure as your weakest link. Unfortunately, human error continues to be a major cause of breaches. This error can range from deferring critical PC updates to accidentally exposing sensitive data to re-using passwords. Cyberattackers are counting on human error and negligent behavior to get a toehold in your business. That's why cybersecurity training is critical. It helps employees recognize threats and follow secure practices. Issue training regularly and test their skills. Can they spot a phish? Do they respond appropriately? Why or why not? Reinforce learning and reveal gaps before it's too late. Empowering employees with knowledge turns them into a strong first line of defense. ►

8 Have a plan in place if there's a breach

Always plan for the worst-case scenario. There's too much at stake. Every second counts when you've been breached, and having an incident response plan in place gives your team a clear guide for what to do when something goes wrong. From detecting the breach to containing the damage and recovering safely, having a response strategy means less downtime and a faster return to business. Strong cybersecurity means being proactive and ready no matter what the issue. ►

Key takeaways

Modernizing the workplace is top-of-mind for many organizations as they look to Generative AI (GenAI) to boost productivity and enhance employee experience. And while recent research shows that 77% of SMBs say AI/GenAI is a key part of their business strategy, a majority say they are fearful that new innovations will increase their attack surface. It's a valid concern.

As AI PC adoption booms and Windows 10 support ends**, there has never been a better time to upgrade.** Unlock performance and security benefits with the latest AI PCs. ►

Summary of 8 best practices and how Dell can help

1 **Know what you need to protect.**
Dell Services can help take an inventory of your IT assets, networks and data.

2 **Work with secure suppliers.**
Dell's supply chain controls mitigate the risk of tampering. Secure PC design minimizes the risk of vulnerabilities.

3 **Get PCs with built-in security.**
Dell PCs come with embedded security at no additional cost.

4 **Keep PCs up to date.**
Dell keeps PCs secure with timely patches. Need help? Try a vulnerability assessment with Dell Security Services.

5 **Find problems and fix them quickly.**
Layer on Dell partner software to monitor for suspicious activity across PCs, networks and the cloud.

6 **Use strong passwords. Enable MFA.**
Take it a step further with Dell SafeID for hardware-based credential storage.

7 **Train employees and test their skills.**
Look to Dell Services for managed employee security awareness training.

8 **Have a plan in place if there's a breach.** *Dell's Incident Response & Recovery can help.*

Ready to refresh? See what PCs are right for your organization

Find AI PCs that meet your organization's security goals. Dell offers several options.

Fight device, identity and network attacks with secure AI PCs. Stay protected and focus on your day-to-day. ►

--

1 While a PC feature may be available within a product line, it does not guarantee that the feature is available on every platform.

2 "Most Secure Commercial AI PCs": Based on Dell internal analysis, March 2025. Applicable to PCs on AMD processors. Not all features available with all PCs. Additional purchase required for some features.

3 Authenticate via fingerprint reader with credentials securely stored in TPM.

4 Authenticate via fingerprint reader, smart card or NFC with credentials securely stored in Dell-unique ControlVault.

5 Some offers available by volume only and require a minimum number of licenses. FedRAMP authorized options are available.

			MOST SECURE[2]
Security that's available[1]	**Dell & Dell Plus**	**Dell Pro Essential**	**Dell Pro & Pro Max**
Supply chain assurance	•	•	•
Enhanced supply chain assurance			•
Anti-tamper solutions			•
PC security alerts			•
Privacy shutter	•	•	•
Lock slot	•	•	•
Fingerprint reader	•	•	•
TPM 2.0	•	•	•
Credential protection[3]			•
Enhanced credential protection[4]			•
Software updates & patches	•	•	•
PC management			•
Silicon optimized for AI	•	•	•
Silicon optimized for security			•
Next-gen antivirus (NGAV) software[5]	•	•	•
NGAV plus PC, network and cloud threat detection software[5]			•
PC self-healing, geolocation and resilience software			•
Advanced PC Support	•	•	•

Take the next step

Refresh your PCs.

Windows 10 support ends in October, leaving many SMBs exposed with outdated, unsupported PCs.

Upgrade to secure Dell AI PCs on AMD Ryzen AI PRO processors.

Layer on software.

Keep attackers out with multiple layers of defense.

Add software protection to new and existing PCs.

Need help managing security?

Security operations you need, from Dell cybersecurity experts.

Explore managed security services.

Upgrade to the latest Dell AI PCs on AMD Ryzen AI PRO processors.

To learn more:

Contact us: Global.Security.Sales@Dell.com

Visit us: Dell.com/Endpoint-Security

Follow us: LinkedIn @DellTechnologies | X @DellTech

About Dell Technologies

With limited resources, SMBs must be proactive in protecting business information and customer data. Investing in cybersecurity helps ensure business continuity, safeguards reputation, and builds customer confidence—making it a smart and necessary part of running a modern business.

From mitigating the risk of ransomware attacks, to detecting suspicious activity, and responding to real-time threats, Dell is here to help you create a security strategy and implement security solutions for your organization's needs today and tomorrow.