4 simple ways to fight cybercriminals

Complete cybersecurity solutions for small and mid-sized businesses

In 2019, 66% of small to mid-size businesses experienced a cyberattack. And what’s worse, 83% of companies impacted lacked the budget to deal with the repercussions, with 60% of those going out of business.

To protect your business from a potentially catastrophic cyberattack, you need to enforce a zero-trust mentality to guard against potential threats. That means taking a proactive approach to how you monitor the people, systems, or services already using your network.

Remember, threats can come from anywhere: an employee accessing a vulnerable app through the cloud, a mobile worker logging onto unsecure Wi-Fi or even a simple click on a phishing link—seemingly innocent behavior can bring everything crashing down.

Every device, connection and user poses a risk you need to manage. This is easier said than done when everyone from employees to contractors may require some level of access to your network to do their jobs.

83% of small to medium businesses lack the funds to deal with the repercussions of a cyberattack.
There are many ways for hackers to gain access to your network. Each avenue requires a specific cyber security solution to ensure your data is protected. As you review the cybersecurity needs of your business, you should evaluate options that provide these types of protection:

1. **Perimeter Protection**
   - A firewall that protects the company network, systems, and data from external threats (malware, viruses, and more).

2. **Private Network Access**
   - Provides secure access to specific company apps and data to those who need it without opening the entire network.

3. **Mobile Device Protection**
   - Allows company employees to be protected regardless of how or where they access the internet.

4. **Monitoring and Remediation**
   - Proactively searches PCs, tablets, servers for threats, quickly detecting issues and providing remediation.

At T-Mobile for Business, we offer a complete portfolio of cybersecurity options that help safeguard your business.

These solutions are specifically designed to protect your company by limiting unsafe user behavior, controlling access and by monitoring networks, apps, and data for malicious activity.

---

**Secure Threat Management**
Protects the company network, systems and data from external threats (malware, virus, etc) with a next generation firewall.

**Secure Web**
Protects mobile employees accessing the internet from any location and any device.

**Secure Private Access**
Managed and secure access to specified company apps and data.

**Secure AI**
Proactive device monitoring, threat detection and remediation.

All solutions mentioned can also be purchased separately.
Your Cybersecurity Portfolio, Unpacked

Part One: Protect

Our protection solutions act as your initial line of defense for your data, people and devices. And regardless of whether they’re on your payroll or not, all users must remain within the confines of these solutions.

Solution: Secure Threat Management

As new security threats and network vulnerabilities emerge, we understand how hard it can be to keep up, especially if you don’t know when, where, and how they’ll take shape.

With a united threat management solution (UTM), you can easily introduce security technology and expertise to your network, protecting it from new and ever-changing cyber threats—24/7.

This includes an on-premise UTM firewall, web filtering, proactive security event monitoring, and more.

It’s also easy to scale, so you can always add new security layers as needed—without hiring a costly in-house security expert—reducing the risk of revenue loss, reputation damage, and unexpected recovery costs.

Benefits of Secure Threat Management

Protector your operation
• Quickly identifies and resolves security threats to your network

Safeguards your revenue and reputation
• Reduces risk of revenue loss due to data breach, brand embarrassment and other costs to recover

Scales with your needs
• Enables you to layer on additional security services based on business needs

Simplifies security management
• Eliminates need for in-house experts
Solution: Secure Web

Mobility and the cloud have created a whole new threat landscape. When employees use web-based applications for work, you’re leaving your network vulnerable to hackers who can gain access through those apps. And when they connect remotely to the web using personal smartphones, tablets and laptops that may not be secure, that presents yet another avenue into your network.

With Secure Web, our as-a-Service security solution, you can help ensure that everyone stays protected from web-based threats, no matter where or how they access the internet. It moves security to the cloud to check all traffic instantly as it moves in and out of the internet. It also offers the ability to set policies from a single portal.

Secure Web offers a streamlined, centralized security model with minimal cost and complexity for multiple sites and user locations. Better still, because it’s a subscription-based “as-a-service,” model, you can add or change users and services as your needs change.

Benefits of Secure Web

**Streamlined security**
- Ensures faster threat detection with near-instant data filtering
- Responds and protects all clients when a threat is detected at any location

**Cost-effective**
- Scalable as your business needs change
- Eliminates hardware and maintenance costs

**User-friendly**
- Enables faster performance by eliminating the need to backhaul traffic to on-site security servers
- Provides consistent security regardless of location or device

**Administrative flexibility**
- Offers management from one console with near-real time analytics reporting
- Allows for simple user and service adds
Solution: Secure Private Access

Imagine for a moment that your accountant needs to do an inventory audit for your company, so you give them access to your network to do their job. But giving contractors, partners and employees access to your full network, when they only need access to certain apps, is a huge risk. That unfiltered access could give a hacker the opening they need to compromise your entire network.

Even if your business has cybersecurity solutions in place, when someone who doesn’t use those same security methods gains access, they give hackers a route to your network through their unprotected devices.

Secure Private Access delivers policy-based, secure access to private company applications without allowing access to your entire network. It’s an ideal solution for businesses that use contractors, partners and employees who don’t require full network access.

Benefits of Secure Private Access

**Controlled access to internal apps**
- Allows users access to specified company apps while limiting network access—ideal for contractors, partners or temporary employees
- Restricts access to only authorized apps and resources

**Cost-effective**
- Allows you to purchase only what you need and add or remove users
- Eliminates hardware costs and maintenance expenses

**User-friendly**
- Eliminates need to log into VPN if authorized
- Provides direct access to applications and eliminates latency

**Simple administration**
- Eliminates VPN hardware for rapid deployment
- Provides visibility to internal apps and allows for granular access rules
Part Two: Detect and Block

Even with the tightest lockdown and security measures, it’s inevitable that a threat will get past your first line of defense. When this happens, you’ll need a specific tool that proactively patrols the environment, identifying and eliminating any threats. This type of security is best delivered using artificial intelligence (AI).

Solution: Secure AI

Secure AI proactively hunts for and responds to threats and malicious behavior across your endpoints (such as PCs, servers, and laptops) by examining data and data behavior for abnormalities.

Designed to counter “alert fatigue”—when you become desensitized to threat alerts that don’t amount to anything—the solution will determine if a threat is real or a false alarm before alerting you and recommending a response.

And by analyzing historical data behavior, Secure AI can learn and adapt to detect and respond to new and unfamiliar threats.

Benefits of Secure AI

- Increases visibility
  • Enables full transparency across your devices and system data
- Simplifies management
  • Includes cyber protection capabilities on a single endpoint sensor, managed with a single UI
- Prevents alert fatigue
  • Provides contextual threat analysis to reduce false positives
- Blocks advanced threats
  • Secures your network with market-leading behavioral protection techniques
- Maximizes analyst abilities
  • Surfaces high-priority incidents, reduces noise in the environment, and decreases the number of alerts the team needs to handle with single-click threat response
- Shortens time between detection and response
  • Detects incidents more quickly using AI-based analysis

One provider for all your cyber security needs

The last thing you need to deal with is multiple invoices from multiple vendors. By choosing T-Mobile to handle all your cybersecurity needs, you’ll improve your security and simplify your work life all at once.
Why T-Mobile?

Your T-Mobile representative will work closely with you to identify the right solutions to help you minimize cyber-threats to your network systems, devices, and corporate data from any entry point.

Rest assured you’re in good hands with T-Mobile for Business. We have over 15 years of experience in data security and have developed a robust portfolio of innovative, industry-leading cybersecurity solutions to protect your company, users, and data from increasingly sophisticated security threats.

And with T-Mobile’s Magenta Glove experience you’ll get 24/7 access to our friendly, motivated team of security experts that will help you out every step of the way.

Let’s talk

To learn more about how T-Mobile Cybersecurity solutions can help keep your business secure, call your T-Mobile representative today at 1-877-924-9360 or see more details on our website.