Vertilocity™
An HBK Company



2026 CYBERSECURITY THREAT REPORT

What Every Small and Mid-Sized Business Needs to Know

vertilocity.com

Powered by the ConnectWise Cyber Research Unit ™ (CRU)

TABLE OF CONTENTS

Cyber Risk Has Changed 2

Remote Access & VPN 3

Stolen Logins & Identity 4

Ransomware Speed 5

Supply Chain Risk 6

AI-Driven Attacks 7

The Real Business Impact 8

Smart IT Partnerships 8

Cyber Risk Has Changed. Here's What It Means for Your Business.

Cyberattacks are no longer just a big business problem. Small and mid-sized businesses are now a primary target. The threat landscape has shifted in ways that make traditional defenses fundamentally insufficient.

> "78% of SMBs fear a serious cyberattack could put them out of business."
>
> ConnectWise State of SMB Cybersecurity Report, 2025

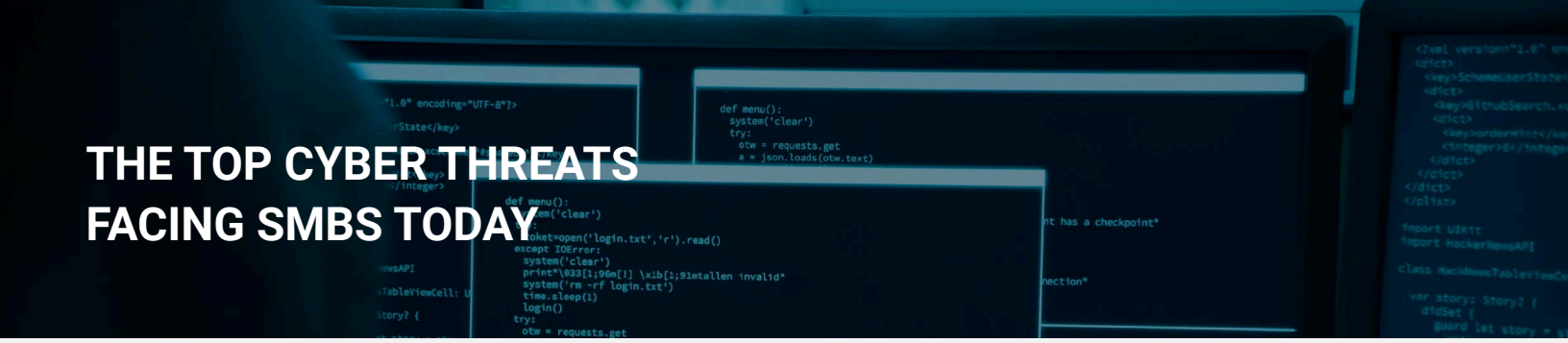
The biggest shift is how attacks happen. Cybercriminals are no longer "breaking in." According to ConnectWise's 2026 MSP Threat Report, compiled from real-world incident response investigations and customer telemetry, attackers are logging in. They use stolen credentials, trusted tools, and everyday access points to operate undetected inside business networks.

As Patrick Beggs, Chief Information Security Officer at ConnectWise, put it: "The defining theme of 2025 was the abuse of trust."

Most successful attacks follow a recognizable pattern:

- Gain access using stolen or weak credentials.
- Move through systems using legitimate tools.
- Disable backups and security controls.
- Steal data and/or deploy ransomware, often within hours.

The common thread is trust. Attackers exploit normal business activity to avoid detection. This means traditional perimeter defenses are no longer enough. Businesses need to focus on preventing the misuse of access, not just blocking threats at the door.



THE TOP CYBER THREATS FACING SMBS TODAY

1 Remote Access and VPN Vulnerabilities

The tools that enable remote work have become one of the most exploited entry points in modern cyberattacks. Weak or improperly configured remote access infrastructure gives attackers an initial foothold, which they can use to escalate privileges and move laterally through your network.

Cybercriminals are actively targeting:

- Exposed VPN systems
- Misconfigured remote access tools
- Weak or missing authentication methods

> In documented incidents, attackers achieved full system compromise within hours of gaining initial remote access.
>
> ConnectWise 2026 MSP Threat Report

Groups like Akira have demonstrated rapid “scan, steal, encrypt” lifecycles that prioritize speed and early backup disruption. In some cases, they bypassed MFA entirely by exploiting inherited VPN configuration artifacts or retained appliance secrets. This is a reminder that enabling MFA alone is not sufficient if configurations aren’t regularly reviewed and hardened.

What This Means for Your Business

If remote access is not properly secured, it becomes a direct and fast path into your network, and one that may not trigger any alarms until significant damage is already done.

What You Can Do

- Secure all remote access tools with properly configured MFA
- Apply the principle of least privilege: restrict access to only what each user needs
- Regularly audit and update configurations for all remote access systems



2 Stolen Logins and Identity Abuse

Identity abuse has become the defining attack vector of this era. Rather than hacking systems directly, attackers increasingly gain access using valid usernames and passwords, allowing them to appear as legitimate users from the moment they enter your environment.

This can happen through:

- Phishing emails designed to harvest credentials
- Weak or reused passwords across systems
- Compromised employee accounts purchased on the dark web

> "Phishing accounted for 83% of all email threats. BEC attacks surged 48% in May 2025 alone."
>
> Acronis Cyberthreats Report H1 2025; FBI Internet Crime Report 2024

> "The FBI received 193,407 phishing and spoofing complaints in 2024, resulting in over $70 million in losses. BEC scams alone cost businesses $2.77 billion that year."
>
> FBI Internet Crime Report, 2024

When attackers assume a trusted identity, they can bypass many traditional security controls and move through systems without raising immediate suspicion. The ConnectWise 2026 MSP Threat Report notes that identity, access, and trust relationships have become the primary battleground in modern cyberattacks.

What This Means for Your Business

A single compromised employee credential can give an attacker the same access rights as that employee, often without triggering any security alert.

What You Can Do

- Require multi-factor authentication (MFA) for all critical systems and remote access
- Enforce strong, unique passwords and consider a password manager across your organization
- Limit access based on roles and regularly review user permissions



3 Ransomware That Moves Faster Than Ever

Ransomware attacks are no longer defined by technical sophistication; they are defined by speed. Rather than developing complex new tools, today's ransomware operators have refined their access methods to maximize efficiency and minimize exposure time.

In documented 2025 attacks, threat groups:

- Gained initial access quickly through compromised credentials or remote access vulnerabilities
- Exfiltrated sensitive data before triggering encryption
- Targeted backup infrastructure first to prevent recovery
- Encrypted systems, often within hours of first entry

47%
of small businesses hit by ransomware in past year.

500%
Surge in average ransom payment ($2M).

70%
Surge in ransomware victims globally.

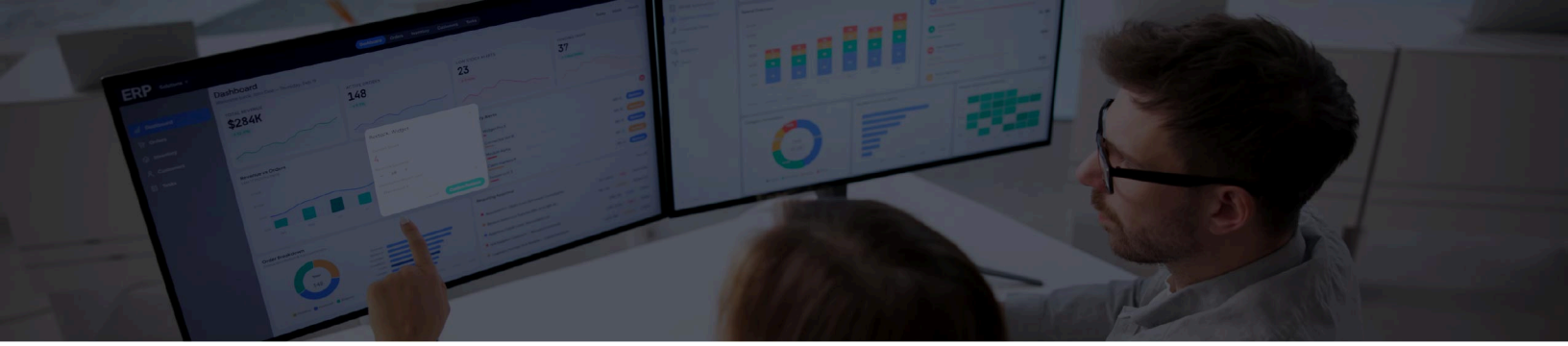
For many SMBs, the window between first compromise and operational shutdown is far shorter than expected, and far shorter than traditional detection and response timelines allow.

What This Means for Your Business

Downtime, lost revenue, and recovery challenges can materialize faster than most organizations anticipate. If backup systems are compromised first, recovery becomes significantly more difficult and expensive.

What You Can Do

- Maintain secure, isolated, immutable backups that cannot be altered or deleted by ransomware
- Test your ability to restore systems and data on a regular schedule
- Monitor your environment continuously for unusual activity to catch threats earlier in the attack lifecycle



4 Software and Supply Chain Risk

Businesses depend on third-party software every day: for productivity, operations, and infrastructure. Attackers have recognized this dependency and are increasingly targeting the vendors and tools you already trust, rather than attacking you directly.

The ConnectWise 2026 MSP Threat Report specifically flags software supply chains as one of the most significant and growing threat vectors for MSP-managed environments. European manufacturing and supply chain ecosystems saw a notable increase in argeting through credential and remote access abuse throughout 2025.

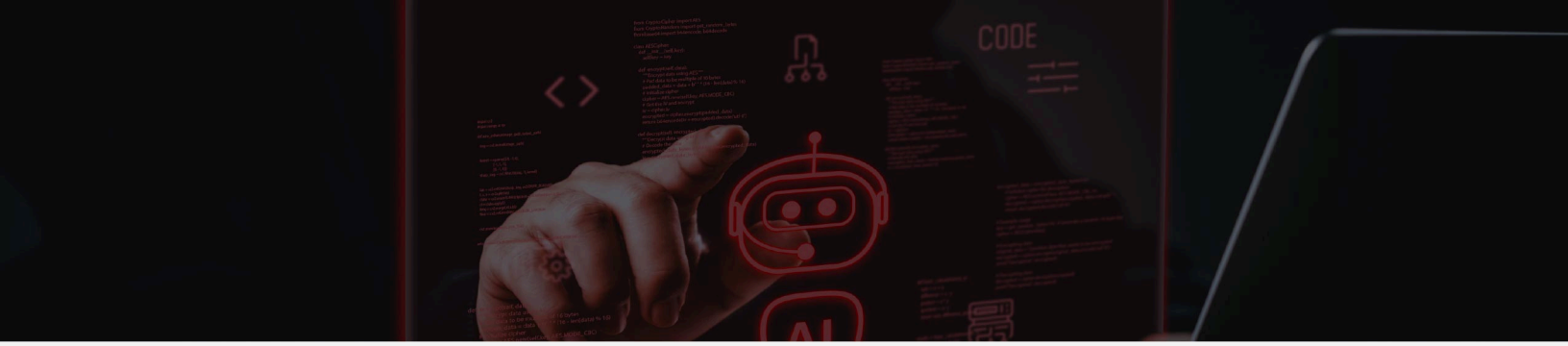
> Supply chain attacks are among the fastest-growing threat categories for SMBs, with attackers compromising trusted software updates and vendor tools to gain access at scale.
>
> ConnectWise 2026 MSP Threat Report

What This Means for Your Business

Even routine software updates or widely trusted applications can introduce risk if the vendor has been compromised. You may be doing everything right internally and still be exposed through a third party.

What You Can Do

- Keep all software and systems up to date with the latest security patches
- Work with vendors who have transparent security practices and monitor their advisories
- Limit the access and permissions granted to third-party applications



5

AI-Driven Attacks

Artificial intelligence is fundamentally changing the economics and scale of cybercrime. Tasks that once required skilled attackers, from crafting convincing phishing emails to impersonating executives and developing malware, can now be automated at a fraction of the cost and at a scale that was previously impossible.

AI is enabling attackers to deploy:

- Hyper-realistic phishing emails tailored to individual targets
- Deepfake audio and video for business email compromise (BEC) scams
- Faster malware development and iteration

83%
of SMBs say AI and generative AI have increased the cybersecurity threat.

48%
increased in attacks for May 2025 alone compared to the prior.

16%
increase in email attacks per organization year-over-year in 2025.

Only 51% of SMBs have implemented any AI security policies, despite the near-universal recognition of the threat it represents. This gap between awareness and action is one of the most significant vulnerabilities in the SMB landscape today.

What This Means for Your Business

It is becoming harder for employees to recognize threats. AI-powered attacks are more convincing, more personalized, and more frequent, which dramatically increases the risk of human error.

What You Can Do

- Train employees regularly on evolving phishing and social engineering tactics
- Establish verification protocols for unusual or urgent requests, especially those involving financial transactions or credential access
- Implement email security and endpoint protection tools capable of detecting advanced, AI-assisted threats

The Real Business Impact

Cyber incidents are not IT problems. They are business crises. The downstream effects of a single successful attack can touch every part of your organization and linger long after systems are restored.

60%
of small businesses that suffer a cyberattack shut down within six months.

58%
af SMBs spent more on cybersecurity in 2024 than originally planned; most of it reactive, not preventive.

Potential impacts include:

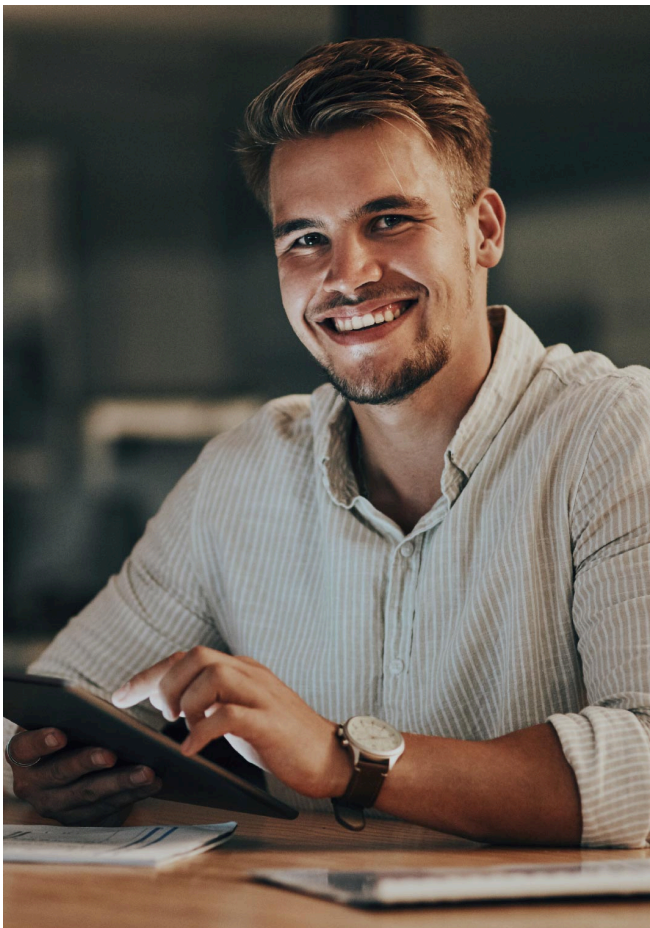
- Operational downtime and lost productivity
- Direct revenue loss during and after the incident
- Damage to customer trust and long-term brand reputation
- Regulatory and compliance exposure
- Recovery costs that often far exceed the initial ransom or incident response fees

For many SMBs, even a short disruption has consequences that extend well beyond the incident itself. The financial math is stark: prevention consistently costs a fraction of recovery.

Why the Smartest SMBs Work with an IT Partner

Cybersecurity has grown more complex than most internal teams can manage alone, not because of a lack of effort, but because the threat landscape now demands round-the-clock monitoring, specialized expertise, and integrated tooling that most businesses simply cannot maintain independently.

> "Only 14% of SMBs consider their cybersecurity posture to be highly effective. Yet 73% of SMBs aren't fully confident their IT provider can adequately defend them."
>
> Cybersecurity Magazine; ConnectWise / Vanson Bourne, 2025



An experienced IT partner, operating on a unified platform built specifically for this environment, can close that gap. ConnectWise-powered partners bring together the tools, intelligence, and 24/7 coverage that reactive, piecemeal approaches cannot match.

The right IT partner can help you:

- Identify risks and vulnerabilities before attackers do
- Monitor systems continuously, not just during business hours
- Respond to threats faster and earlier in the attack lifecycle
- Build a long-term security strategy aligned to how your business actually operates

In a threat environment defined by speed and trust abuse, reactive security is no longer an option. The question is not whether your business will face a threat; it is whether you will be ready when it arrives.

Sources

The following sources were used to support the data, statistics, and findings cited throughout this report. All third-party sources are either government agencies or confirmed ConnectWise ecosystem partners.

ConnectWise (Primary Sources)

1. ConnectWise Cyber Research Unit™ (CRU). 2026 MSP Threat Report: How Identity Abuse is Redefining MSP Risk. ConnectWise, March 2026. connectwise.com/resources/msp-threat-report
2. ConnectWise and Vanson Bourne. The State of SMB Cybersecurity 2025. ConnectWise, 2025. connectwise.com/resources/state-of-smb-cybersecurity
3. ConnectWise. SMB Cybersecurity Statistics and Trends. ConnectWise Blog, July 2025. connectwise.com/blog/smb-cybersecurity-statistics-and-trends

Acronis (ConnectWise Marketplace Integration Partner)

4. Acronis Threat Research Unit (TRU). Acronis Cyberthreats Report H1 2025. Acronis, August 2025. acronis.com/en/resource-center/resource/acronis-cyberthreats-report-h1-2025
5. Acronis Threat Research Unit (TRU). Acronis Cyberthreats Report H2 2025: From Exploits to Malicious AI. Acronis, February 2026. acronis.com/en/resource-center/resource/acronis-cyberthreats-report-h2-2025

Government and Regulatory Sources

6. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). 2024 Internet Crime Report. FBI, 2025. ic3.gov/AnnualReport

This report was prepared on behalf of ConnectWise. Statistics and data are drawn exclusively from ConnectWise proprietary research, ConnectWise Marketplace integration partners, and U.S. government agencies.