CMIT Solutions® Technology Solutions for Your Business

VOL. 57

THE ADVISOR

IN THIS ISSUE

The new security minimum.

Antivirus	Endpoint Monitoring	Threat Detection And Response
⚠️ Block Known FIles	✅ Detect suspicious behavior	✅ Stop and contain attacks
❌ None	❌ None	✅ Continuous coverage
❌ Automated only	⚠️ Your internal team	✅ Dedicated security experts
❌ No One	❌ No One	✅ A live security analyst
⚠️ Weeks or Months	⚠️ Days if alerts are noticed	✅ Minutes to hours
⚠️ Often Insufficient	⚠️ High risk or conditional	✅ Meets baseline expectations
⚠️ High risk of downtime	⚠️ Recovery focused	✅ Business continuity focused
Security Level ★☆☆☆☆	Security Level ★★★☆☆	Security Level ★★★★★

2 THE PROBLEM

AI is powering both sides of cybersecurity

Artificial intelligence is transforming business operations at an incredible pace. It automates workflows, analyzes data instantly, and strengthens security tools beyond what was possible just a few years ago.

But there is another side to that story.

The same AI capabilities that make defensive software smarter are also being used by cybercriminals to make attacks faster, more convincing, and more scalable. Breaches are increasing not because organizations are careless, but because the tools attackers use have evolved.

The playing field has changed.

1. AI has removed the skill barrier for attackers.

In the past, launching a sophisticated cyberattack required deep technical expertise. Today, AI lowers that barrier.

Attackers can generate realistic phishing emails in seconds. They can mimic writing styles, eliminate spelling mistakes, and reference real company information pulled from public sources. AI tools can write malicious code, scan for vulnerabilities, and adjust tactics automatically.

More attackers now have access to more advanced capabilities.

The volume of threats increases.The speed increases. The sophistication increases.

2. Automation makes attacks relentless.

AI-driven systems scan networks continuously. They test weak passwords, identify unpatched systems, and exploit exposed services around the clock.

There is no downtime.

If a vulnerability exists, automated tools will find it. If credentials are leaked, bots test them across multiple platforms almost instantly. If one tactic fails, a new variation can be generated just as quickly.

This level of automation has quietly raised the minimum level of protection required to stay secure.

3. Why traditional defenses fall behind.

Signature-based antivirus was built to block known threats. It reacts after malware has already been identified somewhere else. That approach struggles when attacks are being rewritten in real time.

Even monitoring tools that generate alerts can fall short if no one is actively investigating them. Detection without rapid response gives AI-powered attacks time to spread, escalate privileges, and disrupt operations.

Technology alone cannot keep pace with automated threats. Human expertise alone cannot process millions of signals. Modern protection requires both.

4. The Human + AI advantage.

AI-driven security platforms analyze behavior patterns and detect anomalies at a scale no individual could manage. They identify subtle indicators of compromise before obvious damage occurs. But context matters.

A trained security expert evaluates those signals, determines intent, and takes action. Devices can be isolated. Credentials reset. Suspicious activity investigated immediately.

This partnership turns alerts into action.

It shifts security from reactive cleanup to proactive containment.

5. The cybersecurity minimum has increased.

As AI amplifies both offense and defense, relying on outdated tools creates a widening gap.

This is not advanced protection anymore. It is the new baseline. The question is no longer whether you have security software installed. It is whether your security strategy is built to compete in an AI-powered threat landscape.

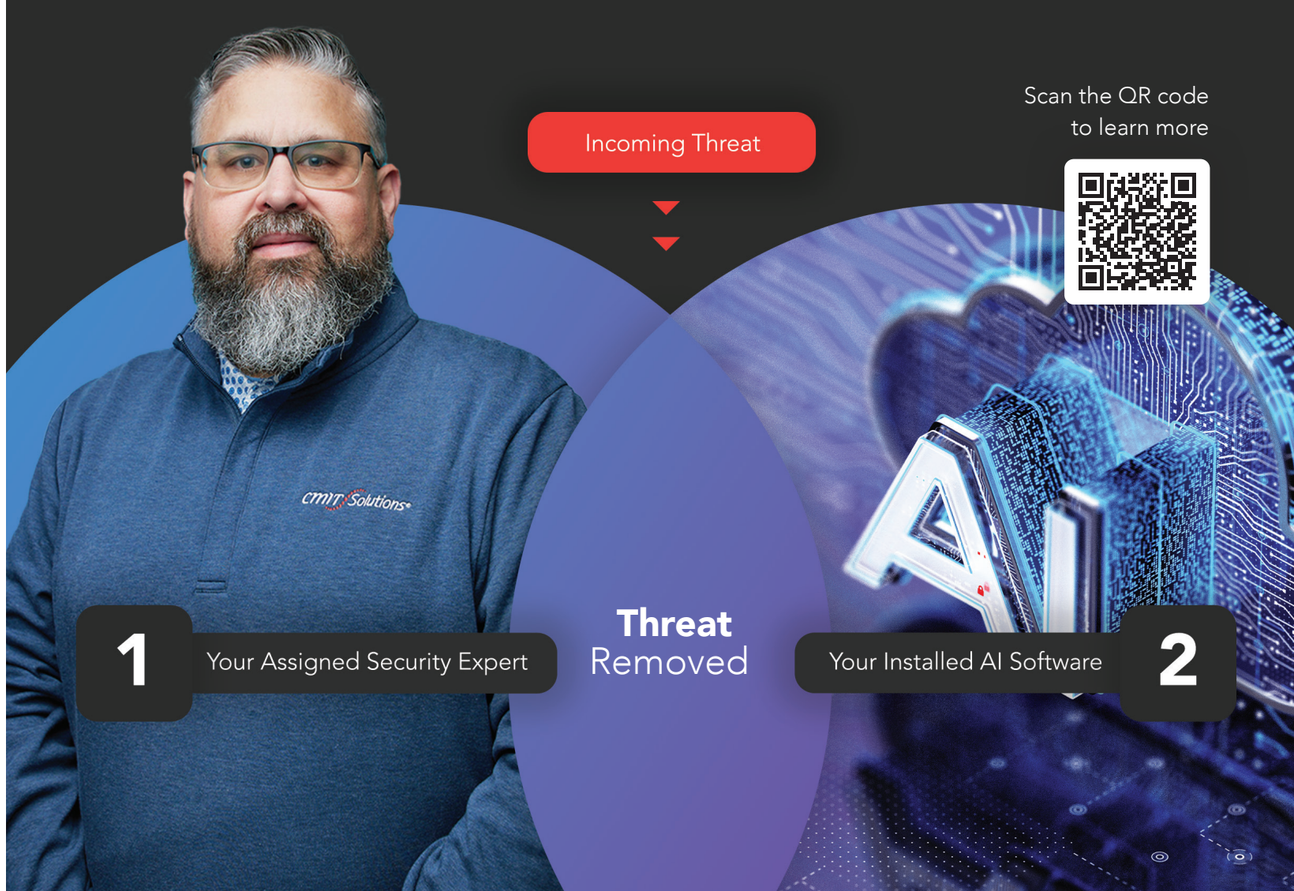
Visit www.cmitsolutions.com/blog for more tech tips.

CMIT Solutions®

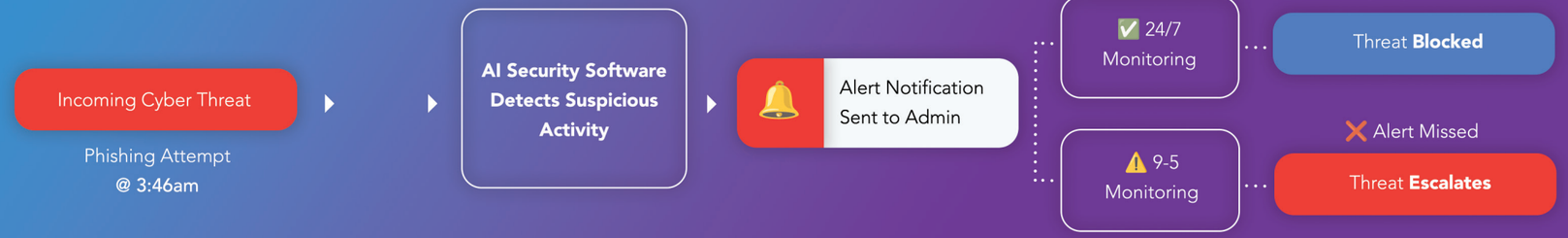
The new cyber**security minimum** includes the perfect **duo: Human + AI**

Combine AI-driven threat detection with real security experts who monitor your systems around the clock. Suspicious activity is identified, investigated, and responded to in real time—before it becomes a problem.

This is what the new cybersecurity minimum looks like.



The New Security Minimum



For years, installing antivirus software felt responsible. It checked the box. It satisfied basic requirements. It gave business owners confidence that they were protected. That standard no longer holds.

Modern cyber threats do not rely on obvious malicious files. They use automation, artificial intelligence, fileless attacks, and human behavior to bypass traditional defenses. As threats evolved, the minimum acceptable level of protection rose with them. Many businesses have not realized how much that baseline has shifted.

The conversation is no longer about whether you have security. It is about whether your security meets today's expectations.

1. Antivirus was built for yesterday's threats.

If your protection strategy stops at antivirus or simple monitoring, your business may be more exposed than you think.

Traditional antivirus software is designed to block known malicious files. It works by identifying signatures of threats that have already been discovered and cataloged.

That approach worked when attacks were slower and predictable.

Today's attackers create new variations instantly. Many threats never rely on a malicious file at all. Instead, they exploit legitimate tools, stolen credentials, or trusted applications already inside your system. Antivirus cannot detect behavior that does not match a known signature.

It does not continuously monitor activity. It does not investigate suspicious patterns. It does not stop an attacker already inside your network.

Antivirus still has a place. But by itself, it represents legacy protection, not modern security.

2. Monitoring improves visibility but not outcomes.

Advanced endpoint monitoring was the next step forward. Instead of only blocking known files, it watches devices for suspicious behavior. It can detect unusual activity, unauthorized access attempts, and patterns that suggest compromise. This is progress.

However, monitoring alone introduces a critical gap. Alerts must be reviewed. Suspicious activity must be investigated. Decisions must be made quickly. If no one is actively analyzing alerts in real time, detection does not prevent damage.

Many internal IT teams are already managing infrastructure, supporting users, handling projects, and responding to daily issues. Monitoring tools may generate alerts, but without dedicated oversight, response can be delayed.

When response is delayed, attackers gain time.

And in cybersecurity, time determines impact.

3. Threat detection and response changes the equation.

Threat detection and response combines advanced monitoring with continuous expert oversight. Instead of simply generating alerts, it actively investigates and contains threats before they spread.

This is the difference between observing a problem and stopping it.

With this approach, suspicious behavior is analyzed by security professionals. Compromised devices can be isolated. Malicious processes can be shut down. Incidents are escalated immediately. Response begins within minutes, not days.

Continuous coverage means someone is accountable at all times.

If an attack begins outside business hours, it is addressed. If ransomware attempts to move laterally across devices, it is contained. If unusual behavior appears across multiple systems, it is investigated in context.

The goal is not just detection.
The goal is protection of operations.

4. The building analogy makes it clear.

Imagine your business as a building.

Antivirus is a motion sensor. It detects movement and sends a signal, but it does not understand intent and cannot intervene.

Endpoint monitoring is a security camera. It records what is happening and may flag unusual activity, but someone must be watching and prepared to act.

Threat detection and response is a dedicated security team. They detect the intruder, assess the threat immediately, step in, and stop the incident before damage is done.

One tool observes.
One tool alerts.
One solution protects.

That is the progression. And that progression defines the new minimum.

5. Why the baseline has officially moved.

Several forces have pushed this shift.

Attack speed has increased. Automated tools allow attackers to scan networks, escalate privileges, and spread threats within minutes. Detection without immediate response often results in downtime, data loss, or ransomware impact.

Insurance expectations have changed. Carriers now evaluate security maturity, not just installed software. Continuous monitoring and rapid response are increasingly treated as baseline requirements, not premium upgrades.

Accountability matters more than ever. Alerts alone do not protect a business. Real security requires humans who are responsible for identifying, containing, and resolving threats.

When you look at the outcome, the difference is measurable. Antivirus often results in long threat dwell times and higher risk of downtime. Monitoring alone may reduce that window but still depends heavily on internal bandwidth. Threat detection and response reduces response time to minutes or hours and focuses on business continuity.

That level of protection is no longer considered advanced. It is expected.

6. Meeting the new security minimum.

The purpose of modern cybersecurity is not simply to install tools. It is to ensure that when something happens, your business remains operational.

The new minimum includes:

- Continuous monitoring
- Active investigation
- Dedicated security expertise
- Rapid containment
- A focus on minimizing business disruption
- Antivirus as legacy protection.

Monitoring alone is a tool

Threat detection and response delivers a real outcome.
The baseline has changed, whether businesses have adjusted or not.

The bottom line for business owners

You may have security software installed. You may receive alerts. But the real question is simple.

If an attack begins right now, who responds?

In today's environment, continuous monitoring with expert response is no longer an upgrade. It is the minimum acceptable standard for protecting your operations, your reputation, and your revenue.

Is your business truly protected, or just checking a box?■

Visit www.cmitsolutions.com/blog for more tech tips.

Will Your Cyber Insurance Actually Pay Out?

You might think cyber insurance guarantees recovery after an attack. In reality, coverage only pays out if your business can prove it met the security requirements in your policy when the incident occurred.

One dramatic example comes from Hamilton, a city in Ontario, Canada. In February 2024, a ransomware attack crippled much of the city's IT systems. Services like business license processing, transit scheduling, and finance operations were disrupted for weeks. The attackers encrypted key data and demanded a multimillion-dollar ransom.

The city believed its cyber insurance would cover the costs of response and recovery. Instead, the insurer denied the claim entirely. Why? Because the city had not fully implemented multi-factor authentication — a basic security control explicitly required by the policy. As a result, taxpayers now face the full financial burden of more than $18 million in recovery costs.

A preventable outcome.

Hamilton thought they were doing the responsible thing by purchasing cyber insurance. But certain security requirements in the policy were not fully implemented. When the breach happened, those gaps mattered.

And Hamilton is not alone. Industry analysis shows that many cyber insurance claims are rejected because organizations cannot prove they maintained required security measures at the time of the breach. One report found that more than 40% of cyber insurance claims were denied for reasons including non-compliance with policy conditions or inadequate documentation of security controls.

That trend reflects a fundamental shift in how insurers evaluate risk. Policies are no longer safety nets that pay out by default. They act as examinations of your security posture, and claims can be denied when controls fall short.

Detection without action widens the gap.

In many cases, breaches begin with subtle signs — unusual logins, access attempts from unexpected locations, or minor anomalies. Tools might generate alerts, but if no one is actively monitoring and responding to those alerts around the clock, threats can escalate unnoticed.

Insurers increasingly expect proof not just that a tool exists, but that it is actively managed and acted upon. Unreviewed alerts and undocumented incident response can be seen as unmanaged risk — a reason to limit or deny coverage.

This is the gap we aim to close. When suspicious behavior occurs, immediate investigation and containment can stop an attack long before it triggers an insurance claim — or before that claim is scrutinized and rejected.

The real cost of being unprepared.

When coverage is denied, the financial impact isn't the only consequence. Reputation, operations, and customer trust can all suffer.

In Hamilton's case, even though some services were restored and backups helped avoid paying the ransom, millions in recovery expenses went unreimbursed. The city had to revise its security posture and buy new insurance under stricter terms.

Many organizations face similar risks. If insurers find a security control missing or poorly documented, a claim can fall through. Failure to meet policy conditions like MFA, continuous monitoring, or documented incident response are among the top reasons cyber claims are rejected.

Coverage requires proof.

Cyber insurance is valuable, but it does not replace disciplined security practices. A policy only works when you can prove your organization met every required control before the incident occurred.

That proof must be documented. It must be consistent. And it must be defensible.

Continuous monitoring and expert threat response strengthen your position by helping you:

- Detect suspicious activity early
- Contain attacks before they escalate
- Document investigation and remediation steps
- Demonstrate to insurers that security controls were active and enforced

Protection is no longer just about having tools installed. It is about being able to show, with confidence, that those tools were actively monitored and managed.

Before your next renewal or before an incident forces the question, take time to review your policy requirements against your current security environment. Identify the gaps. Close them. Align your technology to the terms of your coverage. ■