AI-Powered Threats
Are Escalating. *Fast*.

LeapFrog®

AI-Powered Threats Are Escalating. Fast.

Cybercriminals have weaponized AI to launch faster, cheaper, and more evasive attacks. According to Capitol Technology University, nearly 40% of all cyberattacks in 2025 are now AI-driven, with machine-generated phishing, malware, and automation leading the charge.

The recent NX Build supply chain breach marked a chilling milestone: the first confirmed case of AI weaponization in a software development pipeline. But it's not an isolated incident. Anthropic's Claude model was hijacked by threat actors to automate ransomware creation, credential harvesting, and even generate psychologically targeted extortion demands, all without human oversight.

For years, artificial intelligence was seen as a powerful ally, a tool to streamline operations, enhance customer experiences, and strengthen cybersecurity. But in 2025, the narrative has shifted. AI is no longer just a tool. It's an attacker.

Impersonation Scams Are Exploding

AI isn't just attacking systems, it's mimicking people. In 2025, a study in TechRadar showed AI-driven impersonation scams surged by 148%, with deepfake voice, video, and text used to convincingly pose as executives, colleagues, or family members. These scams are no longer science fiction. They're boardroom reality.

In one case, highlighted by The Wall Street Journal, deepfake impersonations of CEOs led to over $200 million in fraudulent wire transfers in Q1 2024 alone. Employees were tricked during video calls with digitally fabricated executives, a tactic that's nearly impossible to detect with traditional security tools.

In-house Security Teams Are Struggling to Keep Up

Despite the growing threat, many organizations remain dangerously underprepared. Cisco's 2025 Cybersecurity Readiness Index reveals that 86% of security leaders experienced at least one AI-related incident in the past year, yet only 48% believe their staff truly understands the risks. That gap in awareness is a vulnerability in itself.

From Awareness to Action: What SMB Leaders Must Do Now

Small and mid-sized businesses (SMBs) are especially vulnerable. You don't need to be a Fortune 500 company to be targeted, and you don't need to be one to fight back.

Here's how to move from awareness to action:

- **Invest in AI-aware detection and governance:** Traditional tools won't catch AI-driven threats. You need systems that understand machine behavior and adapt in real time.
- **Partner with a Managed Security Services Provider (MSSP):** MSSPs – like Leapfrog Services – bring the expertise and operational capacity to immediately deploy defenses, without the overhead of building an internal security team.

The Bottom Line

Partnering with a managed IT provider helps trade partners reinforce plant-level cybersecurity without AI is no longer just a tool in your tech stack – it's a weapon in the hands of your adversaries. The question isn't whether your business will be targeted, but whether you'll be ready when it is.

At Leapfrog, we have over 25 years of experience helping SMBs leap ahead of threats, not just react to them. Our AI-aware frameworks are built to detect, disrupt, and defend against the new generation of cyberattacks. If you're ready to Leap Ahead, reach out today and inquire about our Ring of Security CyberRisk Assessment. Let's move from awareness to action.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you're ready to assess your threat level, Leapfrog is ready to help. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.

@leapfrogservices | 404.870.2122 | www.LeapfrogServices.com | 1190 W. Druid Hills Dr. Ste. 200, Atl, GA 30329