The Logical Advantage

TeamLogicIT®
Your Technology Advisor

JULY 2026

Adopt 24/7 Endpoint + Identity Monitoring

Research reveals that the average time for hackers to work from breaching a network to committing some form of cyber fraud has dropped below 30 minutes.

How? Cybercrooks increasingly apply accelerating technologies like agentic **artificial intelligence (AI)**. These tools are capable of independently planning, automating and executing complex multistep campaigns like phishing – and generative AI – apps that create images, text, videos and other media for social engineering using techniques like deepfakes.

That's why the U.S. government and major technology companies are formally shifting their cybersecurity policies and programs to what they describe as "active defense," an approach that emphasizes not only early detection but also rapidly disrupting incursions to prevent or minimize damage.

As advocates for **cyber resilience**, we recommend clients practice **24/7 endpoint and identity monitoring**:

- **Endpoint Monitoring** – Our Security Operations Center (SOC) watches network endpoints (e.g., desktops, laptops, smartphones, tablets, etc.) for suspicious activity. A confirmed threat launches a chain of response actions that may include isolating the suspected device and escalating the issue to your team for rapid remediation.
- **Identity Monitoring** – Our SOC team examines sign-ins and other authentication processes across applications and cloud services to detect unusual behaviors and patterns that signal account misuse. Countermeasures may include isolating an identity, forcing sign-out or freezing an account for further investigation.

Call us today to discuss how TeamLogic IT can enhance your cybersecurity program.

The Logical Advantage

Viewpoint

How AI Adoption Spurs SMB Growth

How well employers train workers with the understanding, skills and ethics to navigate **artificial intelligence (AI)** tools determines the level of "productivity and return on investment" generated by the apps, according to prominent analysts from Forrester Research. We agree – especially when applied to small- to medium-sized businesses (SMB) operations. Why are we convinced? Three reasons:

1. Business studies indicate a 10-percentage point increase in workforce exposure to AI apps predicts increases in revenues for SMBs.
2. Other research estimates SMB AI usage is already greater than half of all employees.
3. Further analysis shows just training employees to recognize AI-aided phishing techniques could save millions by preventing data breaches.

What type of AI could generate this kind of growth? Today's most common applications are:

- **Generative AI** tools that generate images, text, videos and other media
- **Agentic AI** systems capable of independently planning and executing complex, multistep tasks, acting autonomously, communicating with other agents and adapting to new information

How can leaders take advantage of this growth opportunity? Work with TeamLogic IT to enable AI:

- **Readiness Assessments**
- **Business Discovery Workshops**
- **Security and Data Governance Planning**
- **End-User Training** (e.g., Copilot, ChatGPT, Gemini, Claude)
- **AI Assistant Enablement** (i.e., helping create custom AI agents)

IT Strategy

Fight Phishing with Continuous Monitoring

Studies show cybercriminals increasingly impersonate legitimate users to breach networks. And phishing is among their favorite ways to swipe those credentials.

Per the certification organization CompTIA, in a phishing attack, scammers send deceptive messages to trick individuals into sharing sensitive information like user IDs and passwords. The fraudster typically claims to represent a trusted entity or individual – e.g., a bank or company executive.

Techniques vary by communication channels and targets. Most common are:

- **Classic Phishing** – delivered by email, urging recipients to click a link or open an attachment
- **Smishing and Vishing** – former perpetrated via texts, latter by voice calls or messages
- **Spear Phishing and Whaling** – campaigns targeting specific individuals rather than large groups; called whaling when targets are executives

Analysis regularly confirms that financial damage from cybercrime like phishing can run into millions of dollars, a cost that can threaten the livelihood of a small- to medium-sized business (SMB.)

That's why as a premier managed services provider (MSP) we recommend **24/7 endpoint and identity monitoring** to blunt its impact. Here are the core benefits of this managed IT service's benefits:

1. **Exhaustive vigilance** increases early detection of cyber incursions
2. **Rapid response** reduces the operational risks of lengthy systems downtime
3. **Proof of protection** facilitates compliance with regulators and cyber insurance providers

Want more details? Call us for a consultation.

Visit our blog for more trending technology articles at TeamLogicIT.com/blog.

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor