## Abadata Computer Corp. Helps Businesses Harness AI Without Exposing Sensitive Data

**Leading MTSP Explains New Secure AI Platform for SMBs**




MICHIGAN – June 2026 – Abadata Computer Corp., a leading managed technology services provider (MTSP), announced today, that the company has is providing small to mid-sized business and non-profits artificial intelligence tools without exposing their organizations to the common security risks posed by the most popular platforms. As organizations have adopted AI tools like ChatGPT, Claude, Grok, Claude, and Copilot, their employees are unknowingly creating a major security risk: exposing sensitive information to public AI technologies. Abadata now provides an all-encompassing AI solution that combines all of the popular tools with the highest level of security.

In January 2026, BlackFog found that 86% of workers use AI at least weekly for work tasks and 49% of workers admit using AI tools at work without employer approval. Whether workers are using these tools to conduct searches, create documents or enter organization information they are doing it in a risky manner because none of the tools are secure. Most organizations have invested in cybersecurity. They have implemented firewalls, endpoint protection, Multi-Factor Authentication (MFA), email security, backup systems, and network monitoring. However, most are now unknowingly bypassing all of those protections the moment workers begin interacting with an unsecured public AI tool.

In other words, organizations may spend years fortifying the front door of their IT network, only to have workers unintentionally "hand the keys" to sensitive information directly to public AI platforms, exposing the organization to liability, security issues and hackers.

"Organizations have worked incredibly hard to secure their networks and protect their data like financial, employee, and customer information," said Dave Wineman, President of Abadata. "The challenge now is that workers are using AI tools independently, often without realizing the potential consequences of where that data is going."

"The majority of your staff are already utilizing AI in some form, whether employers officially approve it or not. That means that even if they're using AI to summarize documents, write emails, analyze spreadsheets, generate reports, troubleshoot problems, and automate workflows, they need to be aware of the liabilities they can inadvertently expose the business to," added Mr. Wineman.

The reality is simple: employees are already getting AI assistance from somewhere. Which means businesses need to become actively involved in how AI is being used inside their organizations. Sensitive customer information, financial records, legal documents, internal communications, proprietary processes, source code, pricing models, and confidential business strategies can all unintentionally become exposed when entered into unsecured public AI systems.

"Most businesses know they need to start leveraging AI to stay competitive," Wineman commented. "But they also need guardrails. Companies want the productivity benefits of AI, but we step in and lock down these tools, so they are safe and secure."

Abadata secures AI tools helping organizations establish guardrails around how AI is used, allowing workers to benefit from automation and intelligence while maintaining oversight, compliance, and human review. "AI has quickly become the most powerful productivity tool ever created," Wineman said. "But the organizations that win long-term won't necessarily be the ones using the most AI. They'll be the ones using it securely, responsibly, and strategically."

Call Abadata 989 883 3411