

THREATLOCKER®
Zero Trust AI Control

Benefits

Define exactly how far AI can go
Set exact boundaries based on the task, application, data, and sensitivity of your environment.

Protect sensitive data
Control which files and folders an agent, and the processes it invokes, can read, modify, or delete.

Restrict connections
Limit agents to the internal resources and internet destinations required for the task.

Control execution and system changes
Define which applications, scripts, and administrative tools an agent can launch or interact with and restrict actions such as changes to protected registry locations.

Now you set the terms for how AI completes tasks.

You put your AI agents to work while staying in control of your environment with ThreatLocker® Zero Trust AI Control (ZTAIC). Give agents the access they need to complete tasks while keeping everything else out of reach, even as they invoke other applications and processes.

One request can trigger a chain of actions

Ask an AI agent to summarize project files, update a spreadsheet, and prepare a report. Behind the scenes, it may run a script, launch PowerShell, open Office applications, and connect to online services.

Approving the AI agent shouldn't mean approving everything that happens next.

ZTAIC carries Zero Trust controls through the workflow, applying guardrails as the agent invokes other applications and processes to complete its task.

Keep control through every step

Consider an AI agent preparing a quarterly analysis. It needs access to a designated folder, a script to process the data, and Office to format the report.

ZTAIC allows that workflow without extending those permissions to everything the underlying tools can reach.

If the agent invokes PowerShell, Office, or another approved application, its guardrails carry through the process. The workflow can use approved resources while access to unrelated files, systems, and internet destinations remains restricted.

The same principle applies to higher-risk actions. An agent could be permitted to draft a configuration change without being permitted to modify protected registry locations or launch unapproved tools.

AI permissions don’t override your strongest safeguards

Giving an AI agent permission to use a tool shouldn’t give it permission to bypass the controls already protecting that tool.

ZTAIC policy priorities keep higher-priority restrictions enforced throughout the workflow. An agent might be permitted to invoke PowerShell for an approved task, for example, while an existing policy continues to prevent PowerShell from accessing a protected location.

Security teams can enable useful AI workflows without weakening deliberate safeguards already in place.

Turn AI governance into enforceable controls

Written policies can define what AI should be allowed to do. ZTAIC helps enforce what it can do.

Translate AI governance into technical controls at the endpoint: which data agents can access, which tools they can use, where they can connect, and what actions they can take.

Those boundaries remain tied to the agent as it works across applications and processes. Now, approving Office, a browser, PowerShell, or another trusted tool doesn’t mean approving every action that tool can perform.

AI may be the immediate use case, but the principle is broader: delegated actions shouldn’t mean delegated control. Put AI to work and keep control of what happens next.



About ThreatLocker®

ThreatLocker Zero Trust Platform prevents breaches from both known and unknown threats by allowing only explicitly trusted software and activity across endpoints, networks, and cloud systems. Built to deploy quickly and scale across complex environments, the platform reduces operational overhead while keeping business running uninterrupted.

sales@threatlocker.com

threatlocker.com

©2026 ThreatLocker® Inc. All rights reserved.