DATA SHEET

THREATDOWN™

ThreatDown AI Detection & Response

AI visibility: Illuminate shadow AI

Overview

AI tools are everywhere. ChatGPT, Copilot, Gemini, and hundreds of other AI-powered tools are changing how employees get work done—but for IT and security teams, there's a basic problem: you can't manage what you can't see.

More than 80% of office workers already use AI at work, and only 22% exclusively use tools their organization has authorized. That gap creates a growing blind spot—and a risk that compliance, legal, and business leaders are starting to ask about.

80% **of office workers already use AI at work***

That's why ThreatDown is introducing AI visibility, the first wave of capabilities in ThreatDown AI Detection and Response (AIDR). AI visibility gives IT and security teams a centralized view of AI activity across managed endpoints—using signals already available in your environment, with no new agents or infrastructure required.

AI visibility Advantages

- **See every AI tool in use—authorized or not**: Get a centralized dashboard of AI tools detected across your environment, including tools with active usage that haven't yet been reviewed or categorized.
- **Build a living AI inventory**: See AI services detected across managed endpoints, organized by category—from general-purpose assistants to coding, writing, and other specialized tools along with where each was observed, first and last seen, and approval status.
- **Continuous AI activity trail**: The AI Activity view gives you an ongoing record of AI tool access across managed endpoints, so your team can investigate activity and maintain an audit trail of AI usage.

Challenges

- Shadow AI is outpacing oversight 80% of office workers use AI at work, but only 22% stick to tools their organization has authorized
- Blind spots create real exposure Employees using unsanctioned AI tools can expose sensitive company data without IT or security knowing
- Policy without visibility falls short 72% of organizations lack a comprehensive AI policy, leaving governance and detection gaps

Benefits

- See everything in one dashboard See every detected AI tool, including what's pending review and if it is authorized
- Understand your AI risk Get full usage details for every tool and tag by category or tool, down to policy-level overrides
- Be audit ready Know who's running which tools and how often, with per-endpoint activity you can sort, filter, and drill into

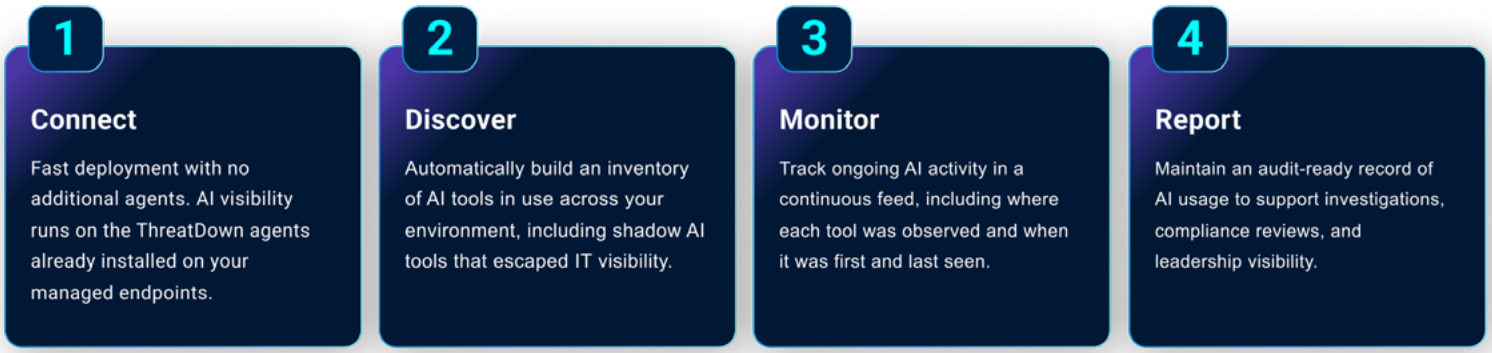
*IBM, Rising AI adoption is creating shadow risks, 2025

- **Works with what you already have**: AI visibility runs on the ThreatDown agents already deployed to your managed endpoints. There's nothing new to install and no new console to manage.
- **Included for every ThreatDown bundle customer**: AI visibility ships to all ThreatDown bundle customers at no additional cost—log in today to see which AI tools are active across your environment.

HOW IT WORKS

Illuminate shadow AI in minutes

AI visibility works through your existing ThreatDown deployment. Using signals already available across your environment, it identifies AI tool usage and gives IT and security teams a centralized view of AI activity across managed endpoints.



AI visibility is included for all ThreatDown customers. Log in today to see which AI tools are active across your environment. To learn more, visit threatdown.com/ai-detection-and-response

Copyright © 2026, ThreatDown. All rights reserved. ThreatDown and the ThreatDown logo are trademarks of ThreatDown. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind. 07/26