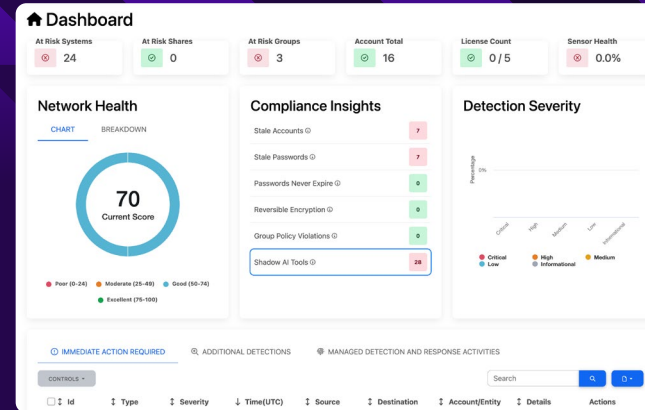


Adlumin Shadow AI Visibility

Know exactly what AI tools are running in your environment. Govern confidently. No new stack.



Employees use ChatGPT, Copilot, Gemini, Claude, Perplexity—and dozens of others—without IT’s knowledge, governance, or approval. Without visibility into which tools are in use, by whom, and on which machines, you cannot enforce data-handling policies, answer compliance questions, or produce the inventory auditors are now asking for. Adlumin Shadow AI Visibility closes this gap using network telemetry already deployed in your environment. No new agent. No new console. No new procurement motion.



Four-dimension attribution

Every AI tool active in your environment attributed to the specific tool, machine, user, and process—including browser extensions and background API calls.



Built on telemetry already deployed

No new agent, sensor, or proxy. Every AI tool interaction begins with a DNS query—Adlumin captures it using network monitoring infrastructure already in place.



Continuously updated coverage

ChatGPT, Copilot, Gemini, Claude, Perplexity, and a growing catalog of others. New AI services surfaced automatically—no configuration



Real-time policy enforcement

Policy violations surface as they happen—not at audit time. Identity attribution makes targeted enforcement practical at the user, team, and process level.



Audit-grade compliance evidence

Tool-, user-, machine-, and process-level records support SOC 2, HIPAA, PCI DSS, GDPR, ISO 27001, and CMMC—replacing self-reported surveys with continuous telemetry.



Baseline monitoring & anomaly awareness

Establishes normal AI usage patterns per user, machine, and process—so unusual changes stand out before they become incidents.

Adlumin Shadow AI Visibility

Feature highlights

Three capabilities that turn Shadow AI from an undocumented risk into a governed, auditable, and continuously monitored surface.

Complete AI visibility

A live inventory of every AI tool active in your environment—attributed to tool, machine, user, and process—using network telemetry already deployed, with nothing new to install.

- ✓ Live catalog of every AI service active across the managed environment, updated continuously as new tools emerge
- ✓ Process-level attribution captures browser extensions and background API calls that endpoint-only approaches miss
- ✓ Environment-wide coverage—no dependence on surveys, self-reporting, or procurement records

Governance & compliance control

Continuous, telemetry-driven AI governance that replaces self-reported surveys with a defensible evidence trail—and surfaces policy violations in real time, not at audit time.

- ✓ Tool-, user-, machine-, and process-level activity records—evidence that answers auditor and regulator questions directly
- ✓ Adlumin records which tools are in use by which users, machines, and processes—not the content or prompt data
- ✓ Identity attribution enables targeted enforcement—coaching, access controls, escalation—with facts, not assumptions

Threat awareness & anomaly detection

Baseline monitoring per user, machine, and process establishes what normal AI usage looks like—so deviations surface before they become incidents.

- ✓ Usage baselines per user, machine, and process enable teams to spot unusual changes in AI tool activity
- ✓ AI tool inventory feeds into Adlumin's broader detection and investigation workflow—no separate console or queue
- ✓ ATT&CK-aligned threat detection across Exfiltration, C2, Discovery, and Defense Evasion on active roadmap

Stop answering the AI question with surveys. **Start with data.**

[Learn more](#)

Available now. No extra cost.

Included in Adlumin—no new agents, licences, or procurement required.

<https://www.n-able.com/products/adlumin>



N-able protects businesses from evolving cyberthreats. Our AI-powered cybersecurity platform delivers business resilience to more than 500,000 organizations worldwide, leveraging advanced end-to-end capabilities, simplified workflows, market-leading integrations, and flexible deployment options to improve efficiency and drive critical security outcomes. Our partner-first approach pairs our technology with experts, training, and peer-led events that empower customers to be secure, resilient, and successful. n-able.com

This content may contain forward-looking statements regarding future product plans and development efforts. N-able considers various features and functionality prior to any final generally available release. Information regarding future features and functionality is not and should not be interpreted as a commitment from N-able that it will deliver any specific feature or functionality in the future or, if it delivers such feature or functionality, any time frame when that feature or functionality will be delivered. All information is based upon current product interests, and product plans and priorities can change at any time. N-able undertakes no obligation to update any forward-looking statements regarding future product plans and development efforts if product plans or priorities change.

This document is provided for informational purposes only. Information and views expressed in this document may change and/or may not be applicable to you. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained herein.

The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.

© 2026 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.