seceon
SECURITY FOR EONS

Seceon aiTRiSM360

AI Activity Monitoring & Protection

An endpoint agent for generative AI activity browser tabs, extensions, and desktop AI apps (Window, Linux and MAC)

At a Glance

- An endpoint agent for generative AI activity browser tabs, extensions, and desktop AI apps (Window, Linux and MAC)
- Detects file uploads, clipboard paste, AI sessions, network access, and prompt security risks
- AI-only scope filters out non-AI destinations (Teams, Drive-only uploads, collaboration tools)
- Telemetry flows to Seceon aiXDR as AI Security events
- Privacy-first file names and metadata only; prompt hash/tags only, never plaintext payloads

Product Overview

aiTRiSM360 (AI Activity Monitoring & Protection) is a endpoint agent deployed with Seceon EDR (Windows, Linux and Mac). It gives security and IT teams visibility into how users interact with generative AI services ChatGPT, Copilot, Perplexity, Claude, Cursor, and dozens of others. aiTRiSM360 agent observes activity on the host and sends structured telemetry to the Seceon platform for detection, reporting, and policy workflows.

Highlights

PASSIVE OT VISIBILITY & ASSET DISCOVERY

Non-intrusive identification of every PLC, RTU, HMI, SCADA server, and IIoT device. Deep packet inspection across 60+ industrial protocols delivers a real-time, accurate asset inventory.

AI-POWERED THREAT DETECTION

Patented AI/ML and behavioral analytics detect zero-day attacks, ICS malware, unauthorized PLC programming, and lateral movement without requiring manual rule writing.

SAFE FOR PRODUCTION

One-way SPAN/TAP-based passive monitoring at the cell area zone. Zero impact on PLCs, RTUs, or process safety. Purdue Model-aligned architecture.

CONTINUOUS COMPLIANCE

Built-in mapping to IEC 62443, NIST 800-82, NERC CIP, NIS 2, NCIIPC, and CMMC 2.0 with automated audit reporting and continuous posture monitoring.

What Problem It Solves

Organizations need to know when employees:

- Upload files or paste sensitive data into AI services
- Use AI through browser tabs, browser extensions, or desktop agents
- Maintain long-running AI sessions that may involve data exfiltration or policy violations

aiTRiSM360 answers who, on which machine, used which AI service, how (upload, paste, session, network), and what type of content was involved without capturing AI prompt text or clipboard/file payloads by default.

Detection approach: OS-level signals (file dialogs, keyboard hooks, window titles, UI Automation) plus optional TCP flow observation to known AI API endpoints.

Core Capabilities

Capability	Trigger
File upload to AI	OS file picker (#32770) detected while an AI tab or application is active
Drag-and-drop upload	Files dropped onto an AI browser surface (enabled by default)
AI session tracking	AI tab or desktop agent opens, progresses, or ends a session
Clipboard paste to AI	Ctrl+V or Shift+Insert detected on an AI input surface
Prompt injection / jailbreak detection	Prompt submission via Enter key or suspicious paste activity (enabled by default)
Network-only AI usage detection	TCP connections to known AI API hosts, including extensions and background tabs
Browser extension awareness	Detection of extension pages, side panels, or installed AI browser extensions

How It Works

File Upload Detection

- Windows Open File dialog when the user attaches a file in an AI web app
- aiTRiSM360 hooks the dialog creation and identifies the owning browser or desktop AI process

- Resolves destination from address bar, title, or extension context
- Only AI-tagged destinations recorded; collaboration apps filtered out

Session, Paste, Network, and Prompt Security

- Session: polls visible AI tabs/apps; emits start, progress, and end events
- Paste: Ctrl+V / Shift+Insert on AI surfaces format, size, and security tags; never plaintext
- Prompt security: Enter submit and suspicious paste scanned for injection, jailbreak, extraction, exfiltration, coercion, obfuscation, and authority impersonation (on by default)
- Network: matches TCP destinations to the forward-DNS cache of AI API hostnames

Browser vs Extension vs Desktop App

Access Mode	How aiTRiSM360 Knows	Event Signal
Normal browser tab	URL bar or window title analysis	browser_extension omitted
Extension side panel or popup	Title hint detection or chrome-extension:// URL identification	browser_extension: true
Extension background traffic	AiNetworkWatcher combined with AI API hostname detection	browser_extension: true
Desktop AI application (e.g., Cursor, ChatGPT app)	Process name recognition and canonical hostname mapping	browser: null

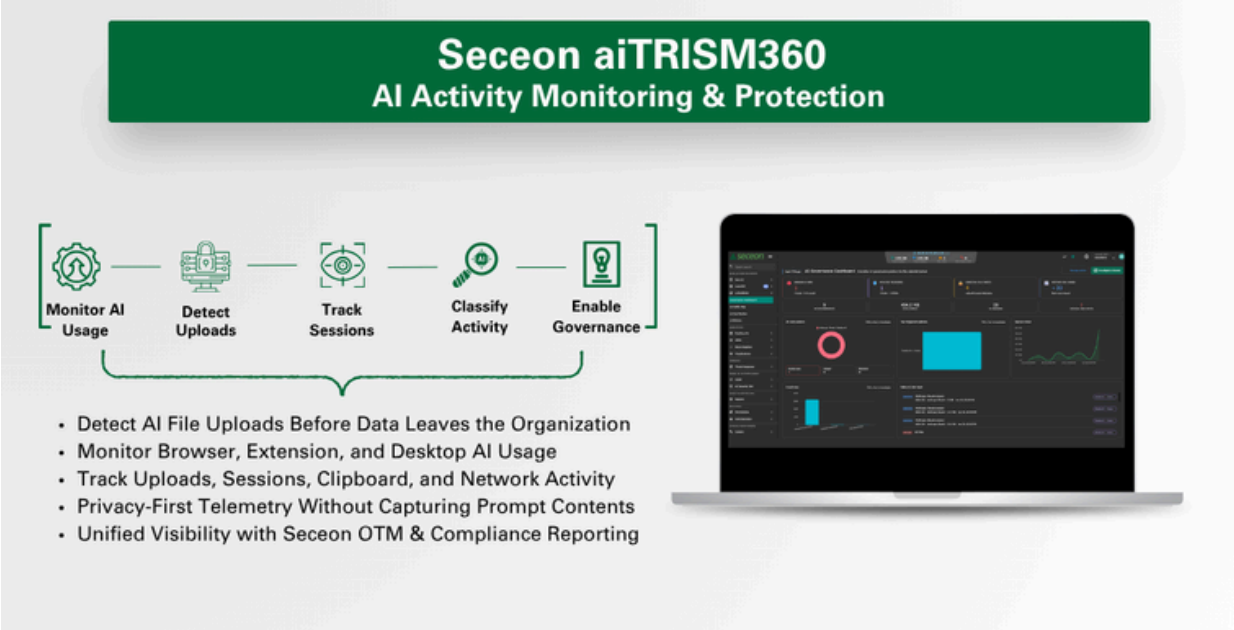
Supported AI Destinations (Examples)

Category	Services
Chat / Search AI	ChatGPT, Gemini, Claude, Perplexity, Copilot, Bing Chat, You.com, Poe, Phind, DeepSeek
Code AI	GitHub Copilot, Cursor, Windsurf, Codeium, Tabnine, Antigravity
Creative / Other	Midjourney, Stability AI, Runway, Jasper, Copy.ai, Writesonic, Notion AI
Local / Desktop	Ollama, LM Studio, Msty

Out of scope for AI ingestion: cloud storage-only uploads (Drive, OneDrive), code hosts, and collaboration tools (Teams, Slack, Zoom).

Platform Events (aiXDR)

Event Type	MITRE ATT&CK	When
File Upload to AI	T1567.002	Triggered when a file name is present in the event
Network Access via AI	T1071.001	Triggered during AI session or network activity without file interaction
Clipboard Paste to AI	T1115	Triggered during the paste phase or when the Clipboard subtag is present, without security tags
Prompt Injection Attempt	T1059	Triggered when content_tags includes prompt_injection
AI Jailbreak Attempt	T1059	Triggered when content_tags includes jailbreak
AI System Prompt Extraction Attempt	T1552	Triggered when content_tags includes system_extraction
AI Data Exfiltration Prompt	T1213	Triggered when content_tags includes data_exfiltration
AI Prompt Coercion Attempt	T1059	Triggered when content_tags includes coercion
AI Obfuscated Prompt Attempt	T1027	Triggered when content_tags includes obfuscation
AI Authority Impersonation Prompt	T1656	Triggered when content_tags includes authority_impersonation



Seceon aiTRiSM360 continuously monitors AI usage across users, applications, and endpoints to identify risks, enforce governance policies, and protect sensitive data using patented AI/ML-driven analytics.

Privacy and Data Minimization

Collected	Not Collected (by Default)
File name and file path	File contents
Clipboard format and size	Clipboard text or images
Content classification labels (e.g., PII, credentials)	Matched sensitive strings
Network 5-tuple and byte counts	TLS payloads or prompts
Prompt metadata (length and hash, enabled by default)	Prompt plaintext
Prompt security tags (prompt injection and jailbreak heuristics)	Prompt plaintext

About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 850 partners, Seceon supports more than 9,800 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/