MORPHISEC

Data Sheet

AI Usage Control (AIUC)

Endpoint-native AI Governance: Discover, Govern, Implement Guardrails, React

AI has opened blind spots on every endpoint. Employees, enterprise AI agents, and AI-wielding attackers all converge on the device – and **none of them are governed by legacy controls.** Firewalls, identity, and EDR were built to watch people and devices; none govern what AI can reach, execute, or weaponize on the endpoint.

Morphisec AI Usage Control (AIUC) closes that gap. Embedded in the Morphisec Protector – with no new agent – AIUC **discovers every AI tool and agent, governs who can use what, enforces least-privilege guardrails,** and reacts to anomalous AI behavior in real time, before exfiltration or encryption. AIUC extends **the Anti-Ransomware Assurance Suite,** powered by **Automated Moving Target Defense (AMTD).**

Key Benefits

Full AI Inventory

- Know every tool, user, and MCP connector – including everything IT never approved.

Ransomware Resilience

- Block pre-encryption AI recon, backup deletion, LoLBin abuse, and credential theft before damage occurs.

Compliance Evidence

- Audit events, enforcement records, and inventory exports ready for EU AI Act, NIST AI RMF, ISO 42001, and SOC 2.

Safe AI Enablement

- Let engineering use Copilot, Claude, and Cursor. Enforce guardrails that prevent harm without blocking productivity.

No New Agent

- Rides the Protector already deployed – no proxy, cloud relay, or separate rollout to manage.

Prevention-first

- The same engine that stops ransomware stops risky AI actions – it stops the action, not just logs it.

How It Works

AI runs on the endpoint with trusted permissions and at machine speed. Network, CASB, and browser tools only see routed traffic or a single browser tab; they are structurally blind to local execution. AIUC rides the Protector you already run, so it sees and governs AI exactly where it acts: on the device.

- **Discover** – Build a live inventory of every AI tool, agent, extension, LLM service, and MCP connector.
- **Govern** – Map each AI action to user identity, service account, and device, and enforces policy by role.
- **Apply Guardrails** – Apply least-privilege at the point of execution, blocking risky actions before they complete.
- **React** – Baseline each tool locally and stops anomalous behavior before exfiltration or encryption.

Example Use Cases

Polymorphic AI Ransomware (PromptLock)

✚ Ollama is auto-flagged as an AI agent; a file-write spike plus child-process spawn rate triggers a Critical alert, and the local LLM is blocked by policy.

AI-Weaponized Supply-Chain Theft (QUIETVAULT)

✚ SSH-key and credential-directory access is blocked by Day-1 guardrails – no ML baseline required.

Autonomous Extortion (GTG-2002)

✚ Claude Code is identified instantly; a data-volume and sensitive-directory anomaly raises a High alert, and egress policy blocks unapproved LLM services.

Runaway AI Agent (Unconstrained Deletion)

✚ Detects the MCP connector's DELETE access pre-emptively, blocks AI from backup locations, and flags mass deletion as critical – stopping the action before it completes.

Shadow AI Discovery & Governance

✚ Auto-inventories unapproved AI assistants and local LLMs and enforces role-based policy – without banning the tools employees rely on.

AI Coverage at a Glance

AIUC discovers and governs AI across the categories employees and attackers actually use:

- **General Assistants** – Microsoft Copilot, ChatGPT, Claude, Gemini, Grok, DeepSeek.
- **Code AI** – GitHub Copilot, Cursor, Codex, Amazon Q, Cody, Windsurf, Cline, Aider, Tabnine, Replit.
- **Local LLM Platforms** – Ollama, LM Studio, AnythingLLM, GPT4All, Jan.ai, OpenCode.
- **Enterprise & Workspace** – Teams/Office, Notion AI, Glean, Salesforce Einstein, Databricks AI.
- **Malicious AI** – WormGPT, FraudGPT, GhostGPT, LameHug, PROMPTFLUX, Evil-GPT and other adversarial tooling.

AI Adoption Demands AI Usage Control

AI adoption is accelerating faster than most organizations can secure it. As AI agents become embedded across enterprise applications, they introduce new pathways for cyber risk, data exposure, and ransomware attacks. **Morphisec AI Usage Control (AIUC)** gives organizations the ability to discover, govern, and secure AI usage at the endpoint–helping security teams safely embrace AI while reducing risk. Available as a standalone solution or as part of **Morphisec's Anti-Ransomware Assurance Suite,** AIUC extends Morphisec's prevention-first approach to the next generation of enterprise threats.

About Morphisec

Morphisec is the trusted global leader in prevention-first Anti-Ransomware protection, redefining cybersecurity with our industry-leading Automated Moving Target Defense (AMTD) technology. Our solutions are trusted by over 7,000 organizations to protect more than 9 million endpoints worldwide, stopping 100% of ransomware attacks at the endpoint and safeguarding businesses against the most advanced and dangerous threats, including zero-day exploits and ransomware.

At Morphisec, we don't just fortify defenses – we proactively prevent attacks before they happen, delivering unmatched protection and peace of mind to our customers. With our Ransomware-Free Guarantee and commitment to Preemptive Cyber Defense, we set the standard for accountability and innovation in the fight against modern cybercrime.

As a rapidly growing company, we are dedicated to empowering security professionals and organizations to adapt, protect, and defend against ever-evolving threats. Join us in shaping the future of cybersecurity with prevention-first strategies and unparalleled expertise.

To learn more, visit morphisec.com