MORPHISEC

Solution Brief

AI Usage Control (AIUC)

Endpoint-native Governance for the Autonomous Enterprise

Challenge

As organizations adopt AI – from coding assistants to autonomous agents – a new and largely invisible attack surface has opened on every endpoint. **The risk has two faces:**

- Shadow AI – Unmanaged AI, outside IT view. Staff paste confidential data into AI assistants and run AI desktop apps outside oversight – touching files and workflows directly on the device.
- Compromised AI – Trusted AI, then hijacked. Enterprise AI agents run with broad permissions; a poisoned prompt or supply-chain attack inherits that trust, and malicious commands look completely legitimate.

Three structural failures keep defenders blind:

1. Visibility gap – No reliable way to identify every AI tool or agent on endpoints, or tell authorized from unauthorized use.
2. Control gap – Even when AI is identified, there is no runtime enforcement to define acceptable behavior or terminate a risky process.
3. Prevention gap – Detection is reactive; AI acts at machine speed, completing its objective before alerts ever fire.

Firewalls, identity, and EDR watch people and devices. Network, CASB, and browser tools see only routed traffic or the browser tab. None of them govern what AI can reach, execute, or weaponize where it actually runs – locally, on the endpoint.

The Solution

Morphisec AI Usage Control (AIUC) is endpoint-native AI governance embedded in the Morphisec Protector – with no new agent. It shifts AI security from detection to prevention at the point of execution through four moves: Discover, Govern, Guardrails, and React. AIUC extends **the Anti-Ransomware Assurance Suite,** powered by Automated Moving Target Defense (AMTD).

Governs AI Including:

- General assistants, code AI, and local LLM platforms
- MCP connectors, browser extensions, and IDE-embedded AI
- Shadow AI, compromised agents, and adversarial AI tooling

Core capabilities

- **AI Visibility (Discover)** – Auto-identifies and inventories every AI tool, account, agent, extension, LLM service, and MCP connector – including shadow AI.
- **Identity-Aware Enforcement (Govern)** – Maps each AI action to user identity, service account, and device; enforce which AI may operate, by role or department.
- **Least-Privilege Guardrails (Control)** – Default-deny policies block access to credentials and PII, writes to backup/recovery locations, and risky process spawns.
- **Local Anomaly Detection (React)** – Each AI tool gets a local behavioral baseline that flags exfiltration, file-operation spikes, and abnormal connector usage in real time.
- **Endpoint-Native, No New Agent** – Embedded in the Protector across Windows, Linux, and macOS – covering offline and air-gapped endpoints with audit-ready compliance evidence built in.

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.
- **Compliance Evidence** – Audit events and inventory exports ready for EU AI Act, NIST AI RMF, ISO 42001, and SOC 2.
- **Safe AI Enablement** – Developers keep Copilot, Claude, and Cursor; guardrails prevent harm without blocking productivity.
- **Prevention-First, No New Agent** – The engine that already stops ransomware now governs AI – riding the Protector you run.

The Morphisec Difference

Endpoint-native by design. Prevention-first by nature.

Network and browser tools detect AI risk after traffic leaves the device. AIUC governs AI where it runs – on the endpoint – and blocks risky actions before exfiltration or encryption. It is the only AI control plane that rides an agent you already deploy and is tied directly to anti-ransomware prevention.

Capability	Benefit
Discover	Full inventory of every AI tool, account, agent, extension, LLM service, and MCP connector – including shadow AI.
Govern	Maps every AI action to identity, service account, and device – enforce policy by role or department.
Guardrails	Default-deny blocks credential/PII access, backup writes, and risky spawns before damage.
React	Per-tool local baseline flags exfiltration, file-op spikes, and abnormal connector usage in real time.
Audit-Ready Compliance	One-click evidence for EU AI Act, NIST AI RMF, ISO 42001, and SOC 2.

AIUC vs. Network & Browser AI Control

Capability	Network / CASB / Browser AI Tools	Morphisec AIUC
Visibility	Routed traffic or browser tab only	Endpoint-native: local LLMs, CLI agents, IDE & desktop AI, MCP
Enforcement Point	After traffic leaves, or in the browser	At execution, on the endpoint
Action on Risk	Detect, classify, log	Default-deny prevention – stops the action
New Agent Required	Often a proxy, gateway, or browser	None – rides the Protector you already run
Offline / Air-Gapped	Blind	Fully covered
Anti-Ransomware Tie-In	None	Same engine that already stops ransomware

Proven Against Real Threats

The Threat	How Morphisec AIUC Stops It
PromptLock – polymorphic AI ransomware	Local Ollama auto-flagged; file-write spike + child-process spawn → Critical alert; local LLM blocked by policy.
QUIETVAULT – AI-weaponized supply-chain theft	SSH-key and credential-directory access blocked by Day-1 guardrails – no ML baseline required.
GTG-2002 – autonomous extortion campaign	Claude Code identified instantly; data-volume + sensitive-dir anomaly → High alert; egress policy blocks unapproved LLMs.
Unconstrained Deletion – runaway AI agent	Detects MCP DELETE access, blocks AI from backups, flags mass deletion as critical – before it completes.

Ransomware-Free Guarantee

Peace of Mind, Proven in Practice

Morphisec offers an industry-first Ransomware-Free Guarantee:

- **100% Money-Back Assurance:** Full reimbursement of subscription fees if a ransomware breach occurs on a protected endpoint.
- **Expert Incident Support:** Dedicated Morphisec Incident Response team for rapid containment, forensic investigation, and remediation.

Stop AI-Driven Threats Before They Start.

See Adaptive AI Defense in action today.

Get a demo

About Morphisec

Morphisec is the global leader in **prevention-first cyber defense** and **anti-ransomware protection,** delivering preemptive security that stops attacks **before execution.** Powered by **Automated Moving Target Defense (AMTD),** Morphisec protects millions of endpoints across **finance, healthcare, manufacturing,** and **technology industries worldwide.** By integrating **Adaptive AI Defense** into its multi-layer Anti-Ransomware Assurance Suite, Morphisec empowers organizations to achieve ransomware-free resilience with **minimal overhead** and **few false positives.**

At Morphisec, we don't just respond - we prevent.

Because when AI accelerates the threat, preemption is peace of mind.

 | morphisec.com