cyberhaven

Protecting the New Frontier: Agentic AI Security

Eliminate the next enterprise security blind spot with the unified AI & Data Security Platform from Cyberhaven.

As organizations adopt agentic AI solutions like Claude Cowork, Claude Code, Codex, and OpenClaw, a dangerous security blind spot is emerging on employee endpoint devices. These locally installed agents gain access to enterprise data and system privileges to automate workflows, yet they often operate with limited security visibility. Traditional tools fail to monitor autonomous actions taken by these agents, leading to risks like goal hijacking, privilege abuse, stolen data, and exposed instances that turn experimental AI into major security liabilities.

How Cyberhaven Can Help

Cyberhaven's unified AI & Data Security Platform reimagines security by combining data lineage with AI-powered content inspection and a best-in-class security endpoint agent to provide comprehensive visibility into how locally-run AI agents interact with sensitive information in your organization. This innovative platform is able to understand the full context of AI activity, ensuring secure AI adoption without disrupting innovation.

The Benefits:

Holistic Agent Visibility:

Automatically inventory AI agents across endpoints, SaaS, and developer environments to identify shadow AI agents.

Context-Aware Guardrails:

Enforce precise policies that govern agent access to data and permitted actions in real time.

AI Observability:

Reconstruct agent behavior with data lineage to understand exactly what files were accessed and which APIs were called during an automated workflow.

Stop Autonomous Data Leaks:

Detect abnormal agent behavior and block risky autonomous actions before sensitive data leaves the endpoint.

Accelerated Incident Response:

Investigate AI-related alerts up to 5x faster with AI-generated incident summaries and comprehensive forensic evidence.

Non-Disruptive Protection:

Deploy a lightweight endpoint agent that provides high-fidelity visibility into AI activity without impacting device performance or user productivity.

Ready to secure your AI journey?

Don't let autonomous agents become your biggest data risk. Learn how Cyberhaven gives you the visibility, observability, and control to securely adopt agentic AI.