

Secure Your Employee Endpoints

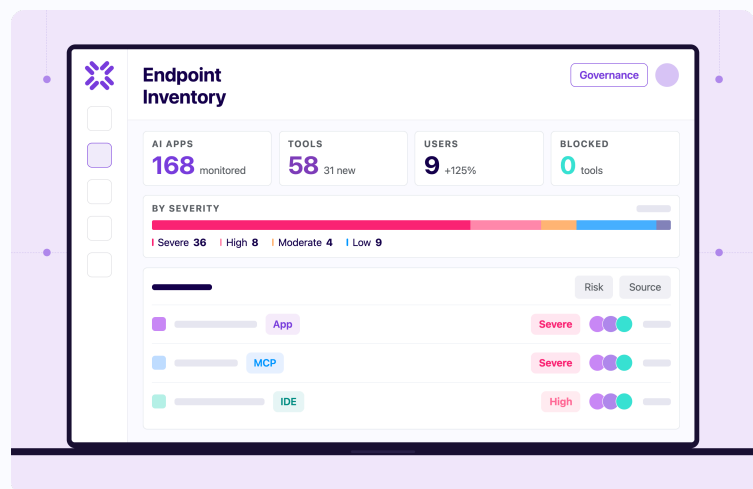
Control AI Tool Usage and Activity on Employee Devices

Employee Endpoints Are Part of the AI Attack Surface

Employee endpoints are part of the enterprise AI attack surface. Ovalix extends visibility and security controls to AI activity running directly on employee devices. Gain visibility into AI applications, AI agents, MCP servers, skills, and AI configuration files to identify AI-related risks and enforce appropriate access and security policies.

A Unified Platform for Securing Employee Endpoints

Ovalix secures AI tools running on employee endpoints by discovering and monitoring AI usage, enforcing policies, controlling AI access and actions, and preventing threats in real time. Security teams gain the visibility and control needed to reduce endpoint shadow AI, prevent unauthorized activity, and manage AI risk across employee devices.



Key Benefits



Full AI Inventory

Gain full visibility into AI tools running on employee devices.



Real-Time Visibility

Continuously monitor AI activity to identify endpoint risk.



Policy Enforcement

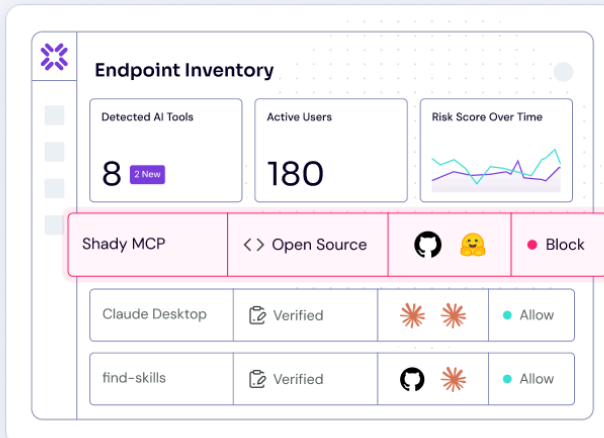
Apply policies across endpoints and prevent violations in real time



Threat Prevention

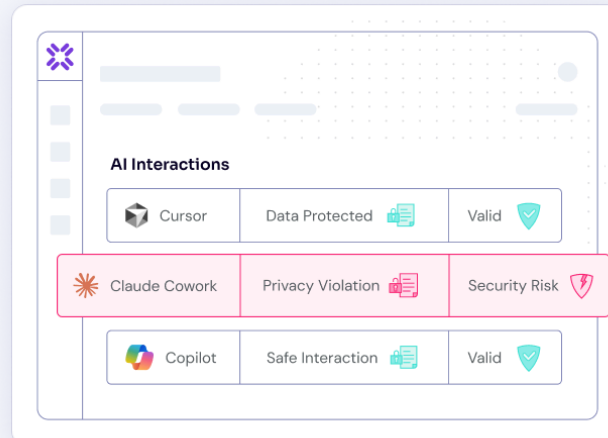
Proactively eliminate data leakage and unauthorized activity

Secure AI Activity Across Employee Endpoints



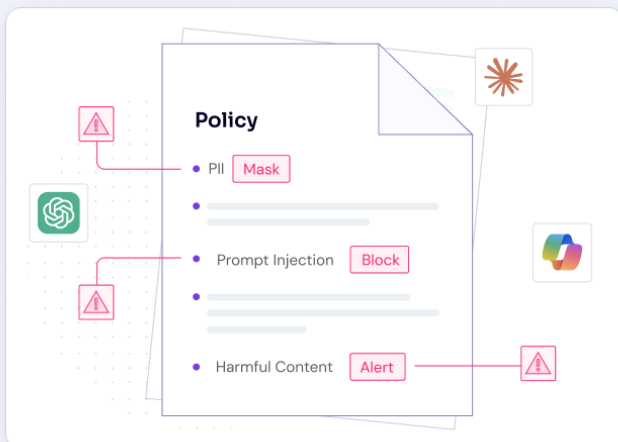
Discover AI Across Endpoints

Gain visibility into AI apps, coding agents, MCP servers, AI agent skills, and other AI tools on employee devices.



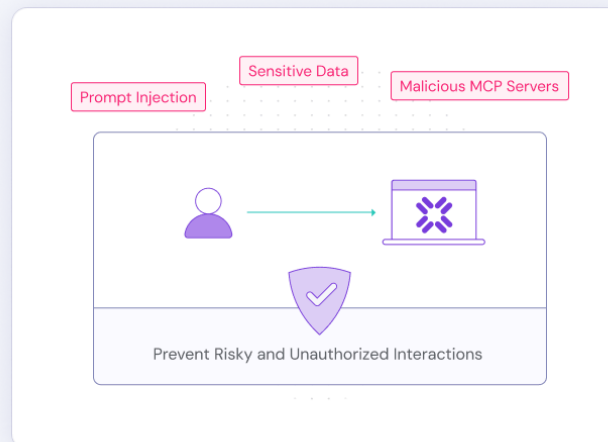
Monitor AI Activity

Track AI activity on employee devices to identify risky actions, threats, data leaks, and compliance gaps.



Enforce Policies and Controls

Apply security and governance policies and control what AI tools on employee endpoints access and do.



Prevent AI Threats

Proactively prevent prompt injection, data exposure, malicious MCP servers, and unauthorized activity.



Holistic AI Security



Seamless Integration



Operational Resilience



Business Enablement

About Us

Ovalix is on the mission of empowering organizations to harness the full potential of AI by providing a robust security platform that ensures the security and integrity of AI systems. Start your journey to secure AI adoption today!

