OVALIX

AI ENDPOINT SECURITY

The CISO's Guide to Securing AI on Employee Endpoints

How to discover, monitor, govern, and secure AI activity on employee devices.

Every Endpoint Is Becoming an AI Endpoint

AI is no longer limited to employees using GenAI tools in a browser.

AI apps, coding agents, MCP servers, AI agent skills, and other AI technologies are now running directly on employee devices. They can access local files, interact with development environments, connect to enterprise systems, and perform actions autonomously.

> **For security teams, this expands the endpoint attack surface.**

Traditional endpoint security solutions such as EDR and XDR weren't designed to provide visibility into AI activity, interactions, and risks.

Security teams now need to understand which AI tools are running on which devices, what they can access, what actions they can take, and whether their activity complies with organizational policies.

The AI Endpoint Visibility Gap

AI activity on an employee device can extend into sensitive enterprise resources.

A coding agent may access proprietary source code. An AI agent may retrieve customer records, interact with CRM platforms, or trigger business workflows. An MCP server may provide access to enterprise knowledge bases, internal databases, or third-party SaaS platforms.

Questions security teams need to address:

- **Which AI tools are installed across employee devices?**
- **Which coding agents have access to source code?**
- **Which AI tools are interacting with private data?**
- **Which MCP servers are employees connecting to?**

> **Without proper visibility, AI activity can become endpoint shadow AI, operating without IT oversight.**

Securing AI on Employee Endpoints

Discover AI Tools on Endpoints

Build a complete inventory of AI tools running on employee devices to understand what AI is being used and where.

Monitor Endpoint AI Activity

Track AI activity across employee devices in real time to identify threats, risky actions, data leaks, and compliance gaps.

Enforce Policies in Real Time

Apply policies to block unauthorized activity, restrict risky actions, and prevent violations in real time.

Control AI Actions

Control what AI tools can access and the actions they can perform on employee devices.

Prevent AI Threats

Prevent prompt injection, malicious MCP servers, sensitive data exposure, and unauthorized AI activity.

AI Endpoint Security Checklist

Can your security team:

- [ ] Identify AI tools installed across employee devices?
- [ ] Monitor AI activity across employee endpoints?
- [ ] See which AI tools access sensitive data?
- [ ] Control the actions the AI tools can perform?
- [ ] Enforce policies in real time?
- [ ] Prevent AI-specific threats?

> **If the answer to any of these questions is no, AI activity may be operating outside existing governance processes.**

Safe AI Adoption Starts at the Endpoint

Employees will continue using AI because it helps them do their jobs more effectively. The security requirement is to manage and control the AI operating on employee devices.

ABOUT OVALIX

Ovalix provides a holistic platform for organizations to safely adopt AI technology. The platform eliminates critical risks including data leakage, shadow AI, malicious prompts, and compliance failures across a wide range of AI applications — from basic GenAI tools and homegrown apps to employee endpoints and advanced agentic AI systems.