# LayerX Desktop Agent: Secure AI Interactions Beyond the Browser

AI usage no longer lives only in the browser. Today, users interact with AI and SaaS across multiple channels, including desktop applications, IDEs, and on-device AI agents, creating new ways for sensitive data exposure and risky behavior via channels such as:

**Native AI desktop applications**
(e.g., ChatGPT, Claude)

**Developer tools and IDE Plugins**
(e.g., Cursor, VS Code plugins)

**Local agents and background AI processes**

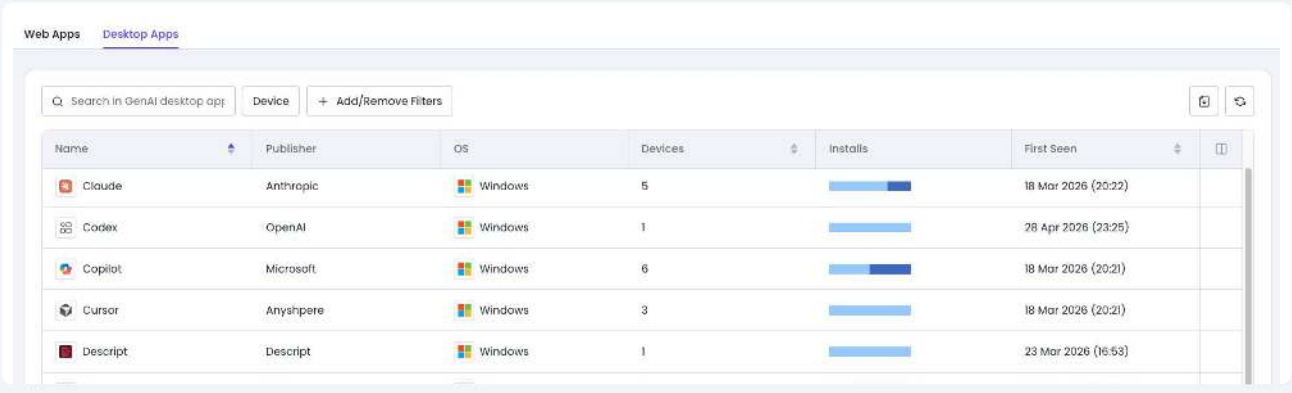
This creates a growing blind spot, especially as adoption of desktop AI apps and AI-powered IDEs accelerates.

The LayerX Endpoint Agent closes that gap. It is a lightweight desktop agent designed to bring AI governance and DLP to the desktop layer by providing a complete, unified view of all AI interactions across modern user workflows without disrupting performance or user experience. It connects the full user journey from browser to desktop and back so security teams can see, understand, and control every interaction.

## Key Capabilities

### AI Application Discovery and Usage Insights

Automatically identifies installed desktop AI apps (e.g., ChatGPT Desktop, Claude) and provides deep visibility into how they are used.



## Conversation-Level Visibility for AI Tools

LayerX captures and analyzes AI prompts and conversations across desktop AI platforms, enabling the detection of sensitive data exposure.

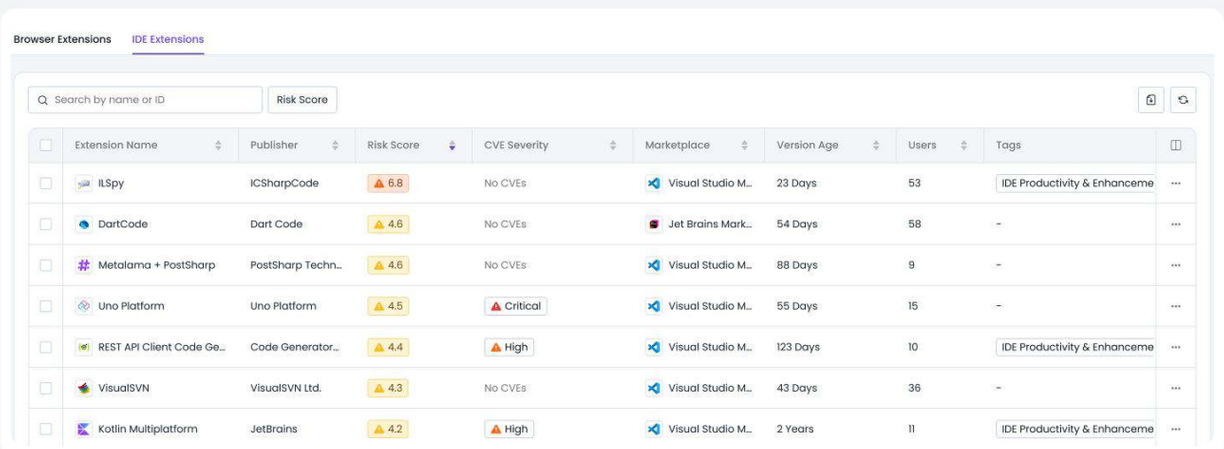
## IDE and Developer Environment Discovery

LayerX provides full inventory and monitoring of IDEs and developer workflows (e.g., VS Code, Cursor), a growing and often unmanaged risk surface across the organization.

## IDE Extension Discovery, Risk Assessment, and Control

LayerX provides deep governance over IDE extensions, including:

- Visibility into installed extensions and usage
- Risk assessment based on permissions, ownership, and code behavior
- Detection of extensions accessing sensitive data or file systems
- Enforcement actions: block, disable, or uninstall risky extensions




## Full Visibility and Control Across Browser and Desktop Activity

The LayerX agent works seamlessly with our extension to unify telemetry and policy enforcement across browser and desktop environments into a single, consolidated view, eliminating blind spots in user behavior and AI usage, and also ensuring no gaps in enforcement.

# Why It Matters

Without desktop visibility, AI usage remains partially invisible, and sensitive data can move freely between apps, turning developer tools into a major unmanaged attack surface.

The LayerX Endpoint Agent ensures:

**No blind spots across all AI usage channels with full user journey visibility (browser + desktop)**

**Consistent policy enforcement and stronger DLP across all AI interactions in desktop apps and developer environments**

**Complete visibility into desktop apps, IDEs, plugins, and data interactions**

**Secure adoption of AI tools without slowing users down**

# About LayerX

LayerX secures all user and agentic interactions in both AI and non-AI applications, across traditional and AI browsers, IDEs, and desktop apps. It is the only AI usage control & Browser Security platform that lets customers control every prompt and data exchange across any channel, without changing their network architecture or disrupting the user experience. Enterprises rely on LayerX's interaction security to secure their hybrid workforce in an AI-first world. For more information, visit https://layerxsecurity.com.