Secure All AI User and Agent Interactions

LayerX is the only interaction security platform that secures all user and agentic interactions across any application, browser, and IDE. It provides customers control over every prompt and data exchange across any channel, without changing their network architecture or disrupting user experience.

Employees now interact with AI and non-AI tools across a growing number of channels, including web and desktop applications, browsers, chatbots, and embedded AI assistants, creating new pathways for cyberattacks and sensitive data exposure. However, legacy network and endpoint security solutions can't see or control most real-time AI prompts, conversations, or agent-driven actions. Only a dedicated AI usage control platform can provide visibility and protection over these last-mile interactions in the AI-powered workplace.

The LayerX Security Platform

LayerX offers the most comprehensive visibility and enforcement capabilities over AI and Browsing risks, including:

AI Usage Control

Shadow AI Discovery
Discover and enforce security guardrails on all AI apps

AI Data Security
Prevent leakage of sensitive data on AI tools

AI Access Control
Restrict user access to unsanctioned AI tools or accounts

AI Threat Prevention
Protect against prompt injection, compliance violations, and more

AI IDEs and Plugins
Discover and secure all AI IDEs and IDE plugins

AI Browsers & Extensions
Protect AI browsers and extensions against attacks and exploitation

Enterprise Browser Security

Web/SaaS DLP & Insider Threat
Prevent data leakage across all web channels

Browser Extension Management
Detect and block risky browser extensions on any browser

Shadow SaaS & SaaS Security
Discover 'shadow' SaaS and enforce SaaS security controls

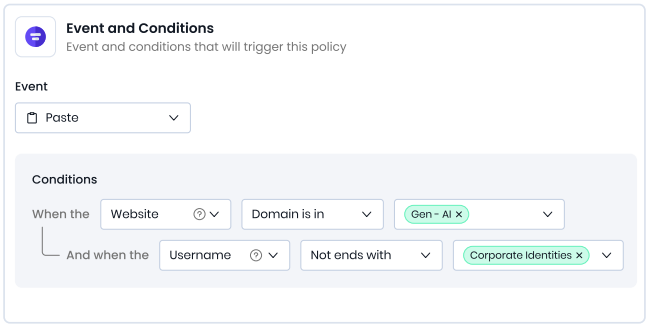
Safe Browsing
Protect all browsing activity against web exploits

SaaS Identity Protection
Discover and secure corporate and personal SaaS identities

BYOD & Secure Access
Secure SaaS remote access by contractors and BYOD

Unlock Visibility You Can't Get From Any Other Tool

LayerX provides real-time visibility to all users, applications, and data across all AI, SaaS, and web transactions. LayerXoffers full discovery of all AI and SaaS applications, identitiesassociated with them, user activity, and all file-based andfile-less data transactions in them. This gives customersunmatched visibility into the last mile of user activity.

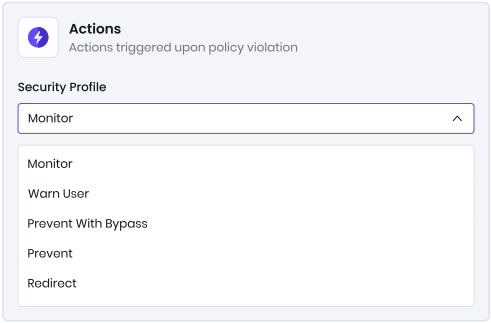


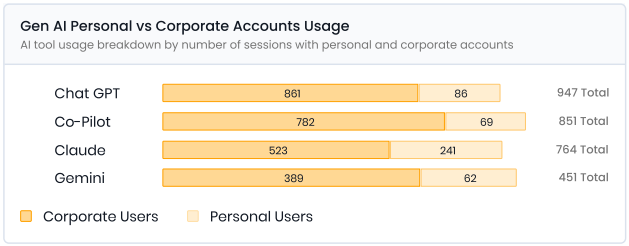
Enforce Last-Mile Security Guardrails

Traditional security tools often force organizations tochoose between allowing everything or blocking it all.LayerX, on the other hand, provides smart, risk-basedadaptive enforcement options, enabling security teams todefine the level of enforcement they desire based on therisk profile of the application or user.

Full Deployment Without Infrastructure Changes

LayerX can be easily deployed with no disruption to the user experience and no changes to existing network architecture. LayerX supports all common (and uncommon) web and AI browsers, as well as any native desktop application, so organizations can achieve full deployment without user pushback or IT headaches.





Enable Responsible Usage of AI and SaaS

In today's world, adopting AI and SaaS technologies is no longer an option. LayerX helps organizations unlock the productivity benefits of these technologies, helping drive adoption, usage education, and responsible usage, without compromising data security or risking data loss.

Key Capabilities

Visibility

- Users
- Identities
- SaaS Apps
- Cookies
- Passwords
- Extensions
- And more...

Control

- Browsing activity
- Text input
- Copy/paste
- File upload/download
- Login events
- OAuth / SAML
- And more...

Deployment

- Chrome / Chromium
- Edge
- Safari
- Firefox
- Windows / Mac / Linux
- Incognito mode
- And more...

Integration

- MDM
- IdP
- Access management
- Ticketing systems
- SIEM
- Data Labeling
- And more...