LayerX

The All-in-One AI & Browser Security Platform

LayerX agentless AI & browser security platform protects enterprises against the most critical AI, SaaS, web and data leakage risks across any browser, application, device and identity, with no impact on user experience

The browser is the main interface for user interactions with AI, SaaS and web applications, making it the main point of risk for data leakage and cyberattacks. However, legacy network and endpoint security solutions can't see or control most in-browser user activity. Only a dedicated browser-based security platform can provide visibility and protection over the last-mile of user activity in the AI-powered workplace.

The LayerX Security Platform

Delivered as an Enterprise Browser Extension, LayerX offers the most comprehensive visibility and enforcement capabilities over AI and Browsing risks, including:

AI Usage Security

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

GenAI DLP
Prevent leakage of sensitive data on AI tools

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

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

AI Response Validation
Ensure AI response validity and data security

AI Browsers Protection
Protect AI browsers against attack and exploitation

Enterprise Browser Security

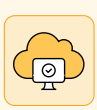
Web/SaaS DLP & Insider Threat
Prevent data leakage across all web channels

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

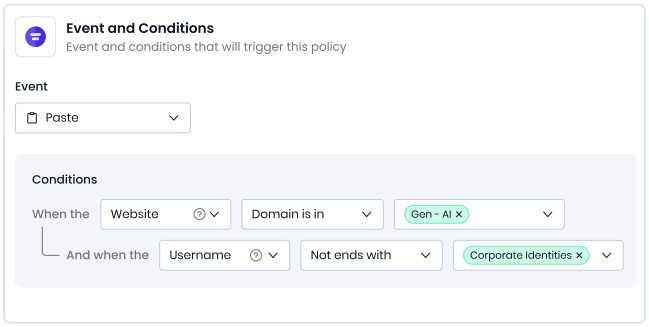
SaaS Identity Protection
Discover and secure corporate and personal SaaS identities



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. LayerX offers full discovery of all AI and SaaS applications, identities associated with them, user activity, and all file-based and file-less data transactions in them. This gives customers unmatched visibility into the last mile of user activity.

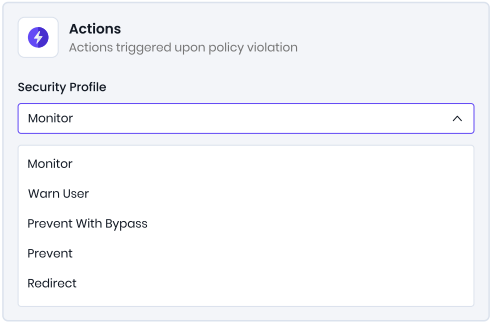


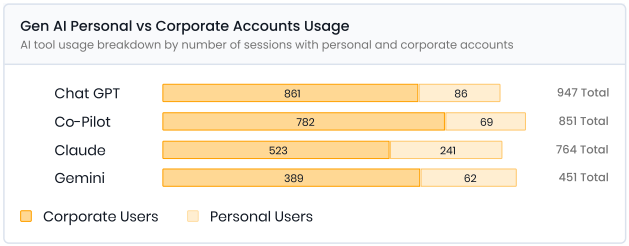
Enforce Last-Mile Security Guardrails

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

Full Deployment Without Infrastructure Changes

LayerX is deployed as a lightweight browser extension, meaning LayerX can be easily deployed with no disruption to the user experience and no changes to existing software installations or network architecture. LayerX supports all common (and uncommon) web and AI browsers, as well as any PWA-based native 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...