Secure AI Usage in Legal Firms with LayerX

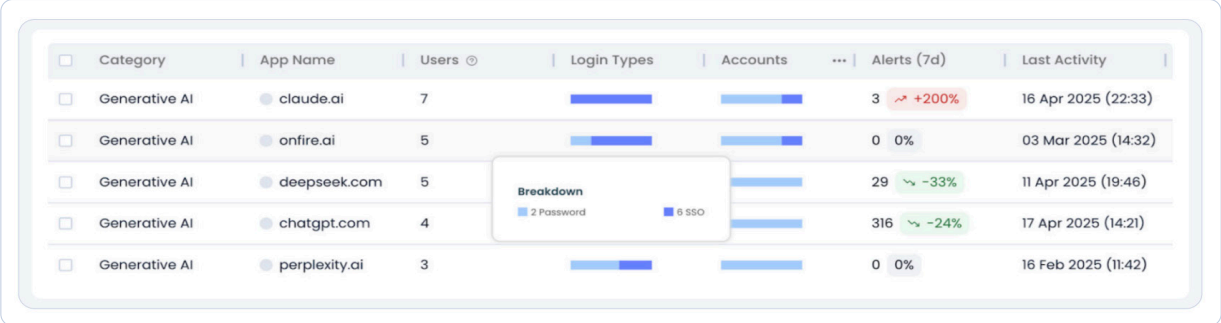
The LayerX interaction security platform protects legal organizations against the most critical AI, SaaS, web, and data leakage risks across any browser, application, device, and identity, with no impact on user experience.

Legal firms are integrating AI into core workflows such as case research, contract drafting, and document analysis, where privileged and highly confidential client data is constantly in use. This creates a significant risk of sensitive information being exposed through AI prompts or third-party tools. Much of this activity happens outside traditional control points of standard DLP and network security solutions, leaving critical gaps in compliance and data protection.

How LayerX Protects Legal Organizations

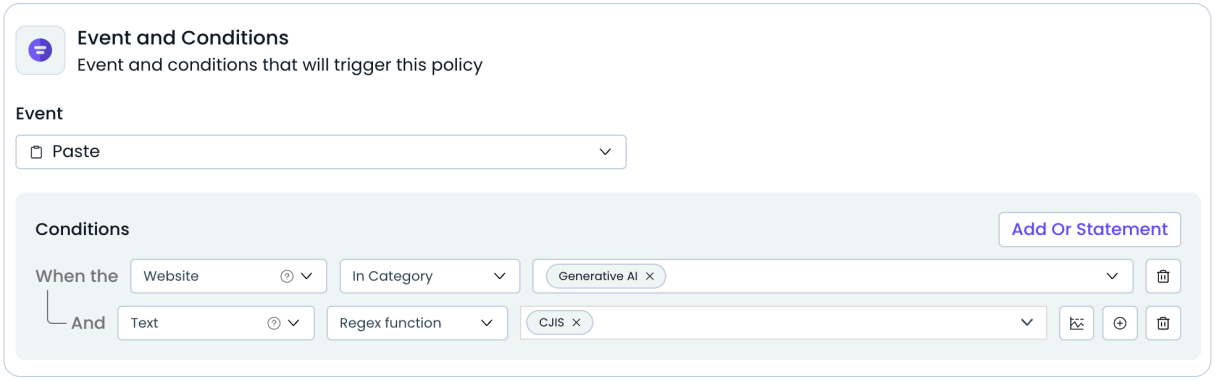
Comprehensive Visibility Across All AI Interactions

LayerX delivers full visibility into last-mile AI interactions: every prompt, conversation, usage context, and data flow in and out of AI. It provides a complete inventory of users, identities, apps, AI browsers, extensions, and devices, while monitoring real-time actions like logins and authentications, text input, copy/paste, and file transfers. This context enables security teams to understand, govern, and securely enable AI usage across the organization while restricting the usage of shadow AI apps.



Data Classification for Sensitive Legal Data Across AI Interactions

LayerX classifies privileged CJIS and legal data, including client information, case details, contracts, and sensitive communications, ensuring strict confidentiality across AI usage. It provides deep visibility and control over how legal data is used within AI workflows, including support for legal-specific LLMs like Harvey, enabling firms to securely leverage AI without compromising client trust or privilege.

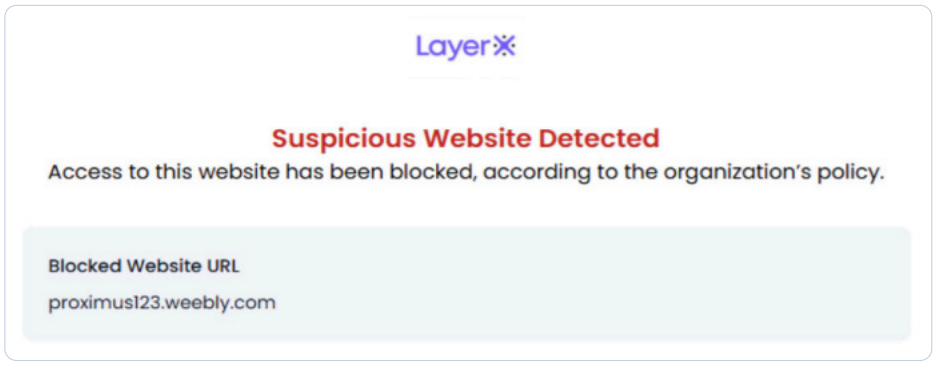


Prevent AI Data Leakage

LayerX provides end-to-end visibility into GenAI conversations across all major AI platforms, capturing both prompts and responses. Based on that, it enforces last-mile adaptive security guardrails to stop users from sharing sensitive data with GenAI tools and gives security teams the context needed to detect exposure, accelerate investigations, and ensure regulatory compliance.

Protection from 0-Day Phishing Attacks

Legal firms are frequent targets of phishing attacks due to the sensitive client data and privileged access their employees possess. LayerX protects organizations against sophisticated phishing attacks with its AI-powered analysis engine that continuously inspects over 250 web page parameters to identify malicious phishing attempts and stop credential theft and account takeover attacks.



LayerX Interaction Security Platform

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.

LayerX Usecases

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

Key Capabilities

Visibility

Users
Identities
AI Apps
AI Prompts
AI Browsers
AI Agents
Extensions
And more...

Control

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

Deployment

Traditional Browsers (Chrome / Edge / Safari / Firefox / etc.)
Agentic AI browsers (Atlas, Comet, Dia, etc.)
Windows / Mac / Linux
Incognito mode
And more...

Integration

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