LayerX

PREVENT GENAI DATA LEAKAGE & ELIMINATE SHADOW AI

LayerX is an all-in-one, agentless security platform that helps organizations prevent AI data leakage, offering complete visibility and control over any sanctioned and unsanctioned AI apps and blocks sensitive data from being exposed in real-time with no impact on the user experience.

AI is a critical part of day-to-day work. Embracing AI is no longer optional; it's essential for staying competitive. But while AI has huge productivity benefits, it also exposes organizations to a variety of security risks such as data leakage, compliance violations, and inadvertent disclosure. Existing security solutions fail to protect the last mile of user activity, leaving organizations blind and exposed to AI data leakage. LayerX is the only solution that provides both visibility and risk-based enforcement on all user AI interactions.

Benefits of Choosing LayerX

100% Visibility

Detect all GenAI apps in use and gain full visibility into all user activity in any GenAI application

Control Access to GenAI

Restrict usage of shadow AI apps and secure access to sanctioned AI apps using corporate accounts

Prevent AI Data Leakage

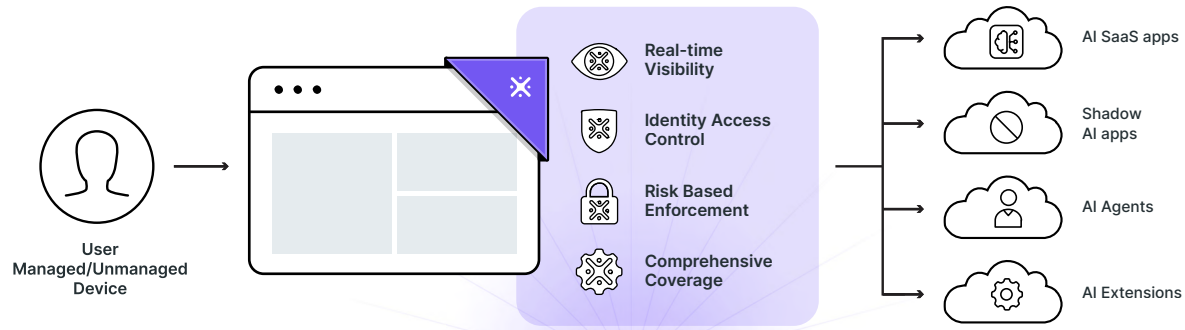
Enforce last-mile AI security guardrails to stop users from sharing sensitive data with GenAI tools

Protect from AI Extensions

Identify and block risky AI browser extensions that expose sensitive user data to external AI engines

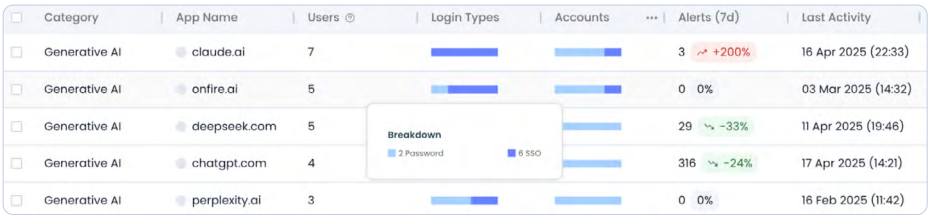
The Browser is the New Point of Control for AI

Most users consume GenAI tools via the browser, making the web browser the main point of control for AI security. Traditional DLP and network-based solutions are complex to deploy, don't provide real-time visibility, and lack control over most GenAI apps, allowing users to bypass them. Only LayerX, deployed directly as a browser extension, offers comprehensive visibility and control over all AI applications and extensions, effectively addressing GenAI data security and 'shadow' AI challenges. Enforce last-mile AI security guardrails to stop users from sharing sensitive data with GenAI tools.



Complete Discovery of GenAI Apps

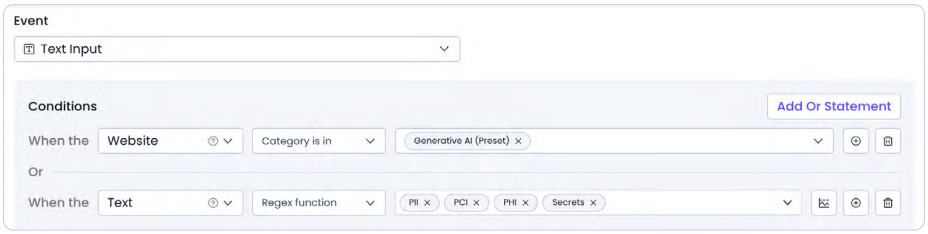
LayerX offers comprehensive visibility into GenAI application usage by deploying directly as a browser extension. It monitors user actions such as browsing activity, login attempts, data input, and file uploads, identifying which tools are accessed, by whom, and through which accounts (corporate or SSO or personal). This enables organizations to detect unauthorized data sharing and enforce policies to prevent data leakage from GenAI and other 'shadow' AI applications.



Enforce Granular Last-Mile Security Guardrails

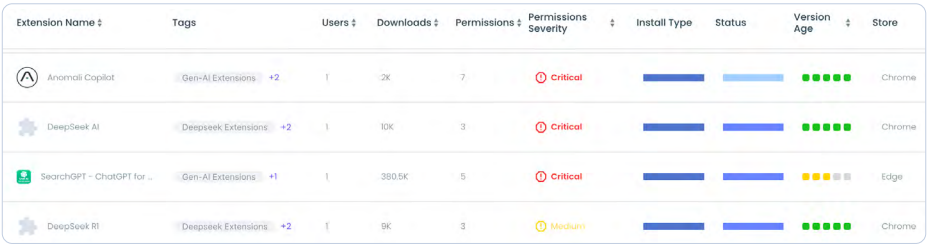
Traditional DLP and network-based solutions typically follow a binary enforcement approach of either fully allowing or fully blocking access to GenAI apps, and require complex API integrations for more granular controls (assuming that the application even offers them, in the first place).

In contrast, LayerX permits organizations to directly detect and enforce policies on these apps in the last mile, direclty within the browser. Organizations can define policies based on user identity, device status, website category, data sensitivity, etc., to create tailored security policies with a range of enforcement options ranging from monitoring only, to warning users with customizable messages, to masking sensitive data, to completely blocking their actions.



Identify and Restrict GenAI Browser Extensions

AI-enabled browser extensions are a 'side door' for AI usage in the organization that can often bypass network-layer GenAI access controls. LayerX's automatically categorizes GenAI extensions and provides visibility to all AI extensions installed within the organization, including users, permission scope, category, installation type, source, etc. This allows security and IT managers to get a full view of all GenAI extensions and whether they need to disable or prevent the download of any malicious or risky extension.



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...