Secure AI Usage in Gaming Companies with LayerX

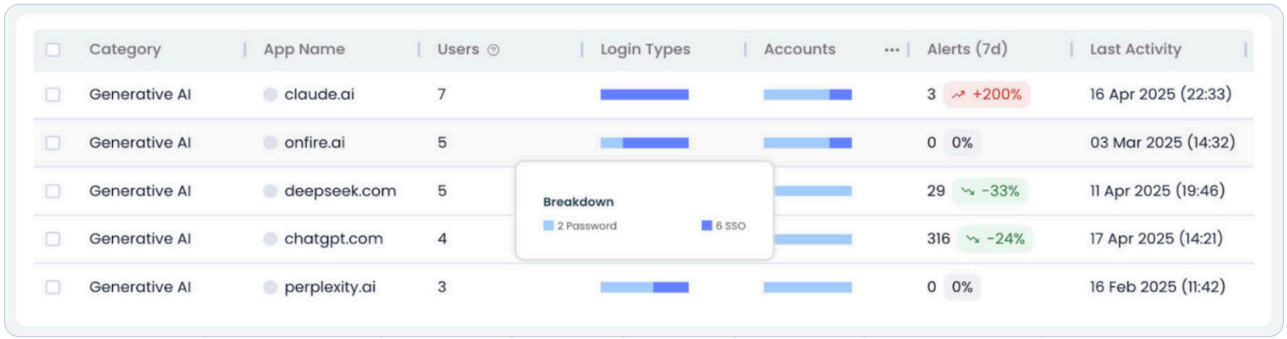
The LayerX interaction security platform protects gaming companies against the most critical AI, SaaS, web and data leakage risks across any browser, application, device, and identity, with no impact on user experience.

Gaming companies increasingly rely on AI across development, design, and live operations, exposing highly sensitive assets such as unreleased content, game logic, and monetization strategies. These workflows are fast-moving and browser-driven, with teams frequently using AI tools, plugins, and external platforms to accelerate production. Traditional DLP and SSE solutions lack visibility into real-time AI interactions and cannot control how sensitive game data is shared or processed within these environments. This creates new pathways for data leakage and intellectual property exposure that are difficult to track.

How LayerX Protects Gaming Companies

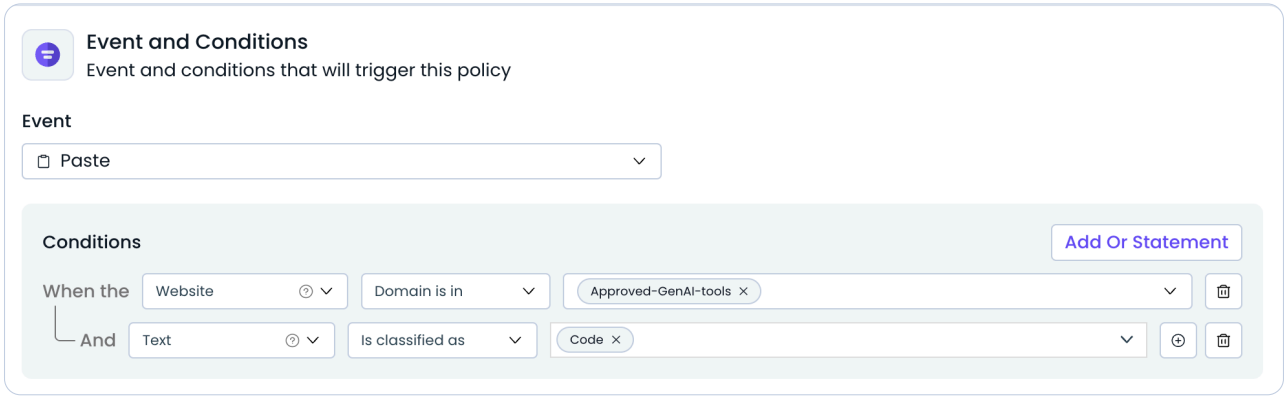
Comprehensive Visibility Across User AI Activity

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, applications, AI browsers, extensions, and devices, while monitoring real-time actions such as logins, text input, copy/paste activity, and file transfers. This enables gaming firms to understand how AI is being used across the organization while identifying and controlling shadow AI usage.



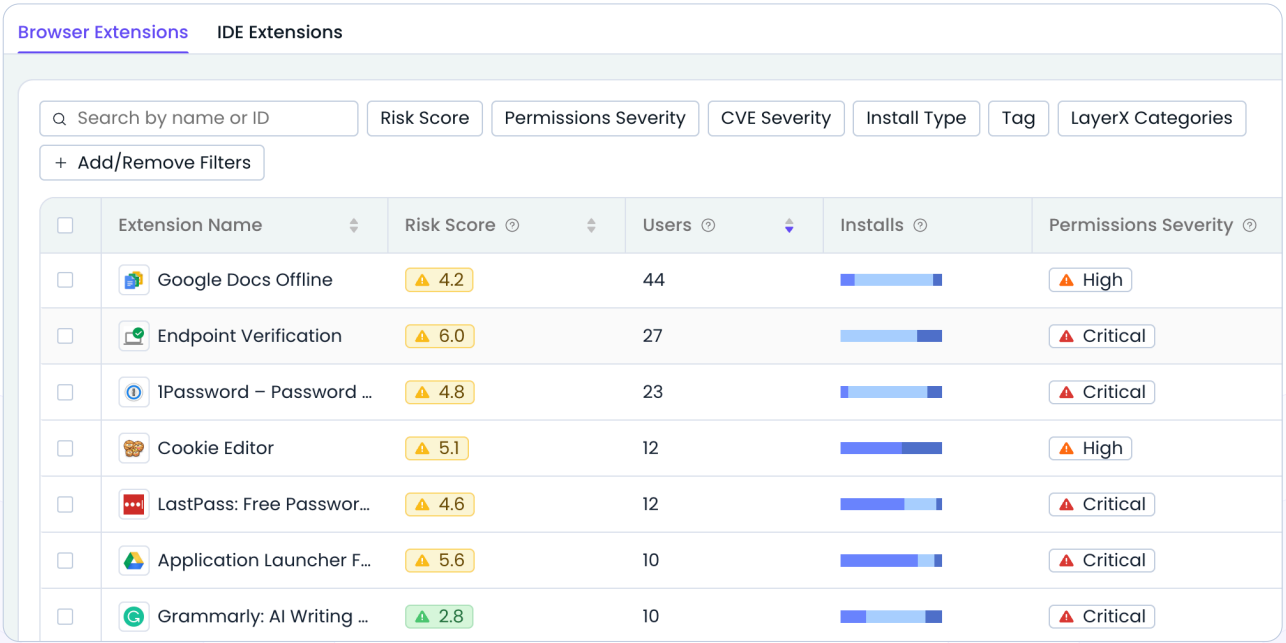
Classify and Protect Sensitive Gaming Assets Across AI Interactions

LayerX provides end-to-end visibility into AI conversations across major AI platforms, capturing both prompts and responses. It enforces real-time security guardrails that prevent employees from sharing source code, unreleased content, proprietary designs, or other confidential game assets with unauthorized AI tools, helping studios innovate safely while protecting their intellectual property.



Protection from Risky Extensions

Gaming companies rely heavily on browser and IDE extensions for development, design, AI-assisted workflows, productivity, and collaboration. However, these extensions often have broad access to source code, internal tools, unreleased content, player data, and other sensitive assets. LayerX continuously discovers, analyzes, and monitors browser extensions to identify risky or unauthorized extensions and prevent them from accessing sensitive information. This helps protect valuable intellectual property and reduce extension-based data leakage risks.



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...