Secure AI Usage in Accounting Firms with LayerX

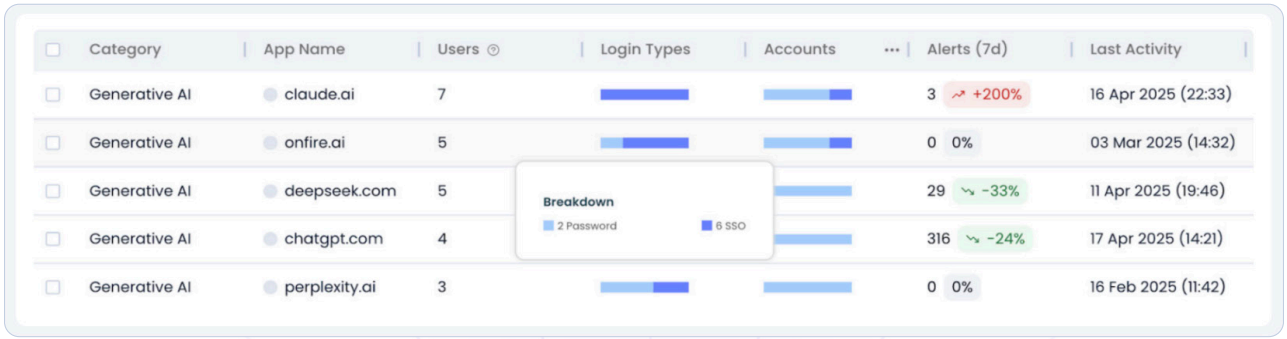
The LayerX interaction security platform protects accounting firms against the most critical AI, SaaS, web and data leakage risks across any browser, application, device, and identity, with no impact on user experience.

Accounting firms handle highly sensitive financial records, audit data, tax information, and client financial statements. As AI becomes embedded in accounting workflows, firms must balance productivity gains with the need to protect confidential financial data and business information. Traditional DLP and SSE solutions lack visibility into these real-time AI interactions, creating risks of data leakage, compliance violations, and loss of client trust.

How LayerX Protects Accounting Firms

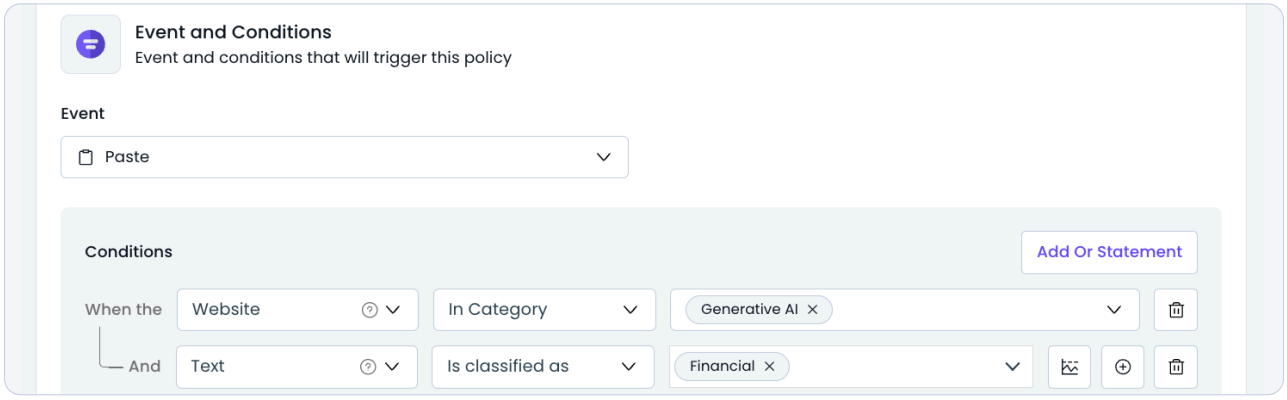
Complete Visibility and Mapping of User Activity

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. It helps firms identify unauthorized or risky applications, monitor access to financial systems, and maintain detailed audit trails that support compliance, governance, and regulatory requirements.



Classify and Protect Sensitive Financial Data Across AI Interactions

LayerX automatically identifies and classifies sensitive financial data, including tax records, audit documentation, financial statements, payroll information, PII, banking details, and client financial data. By understanding the context of financial information within AI interactions, LayerX helps prevent unauthorized exposure and ensures sensitive data remains protected.

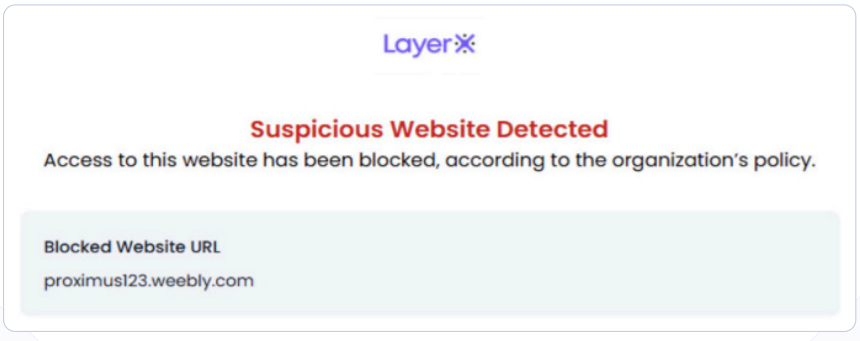


Prevent AI Data Leakage

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 confidential financial records, client data, tax information, or regulated data with unauthorized AI tools, helping firms maintain compliance and client confidentiality.

Protection from Advanced Phishing and Credential Theft

Accounting firms are frequent targets of phishing attacks due to the financial data and privileged system access their employees possess. LayerX protects users from sophisticated phishing attacks using AI-powered analysis that continuously inspects hundreds of web page signals to identify malicious sites, prevent credential theft, and stop account takeover attempts before sensitive financial information is compromised.



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...