Secure AI Usage in Consulting Firms with LayerX

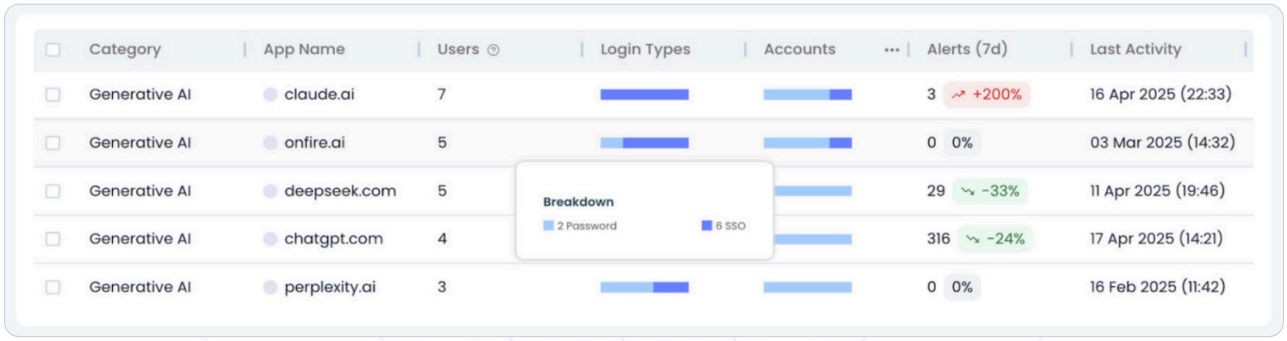
The LayerX interaction security platform protects consulting firms against the most critical AI, SaaS, web and data leakage risks across any browser, application, device, and identity, with no impact on user experience.

Consulting firms handle large volumes of sensitive client data across multiple engagements, increasingly using AI to generate insights, reports, and strategic recommendations. This introduces the risk of cross-client data leakage, where information from one engagement may be unintentionally exposed in another through AI prompts, conversations, or generated content. Consultants also work across devices, locations, and SaaS platforms, making centralized control difficult. Traditional DLP and SSE solutions cannot provide the granular, in-context visibility or enforcement needed to secure these dynamic AI-driven workflows.

How LayerX Protects Consulting Firms

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

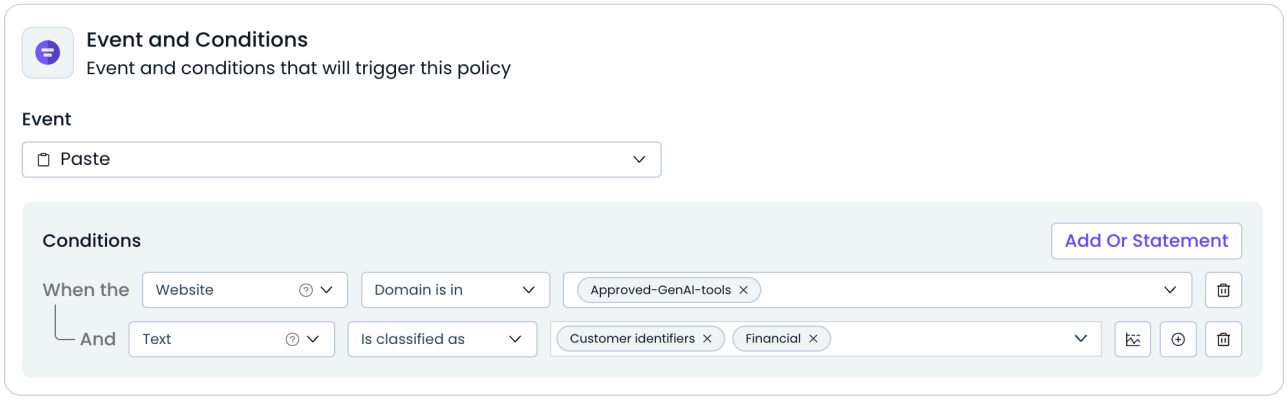


Visibility and Mapping of Consultant Activity

LayerX automatically maps every application, SaaS platform, AI tool, and web destination that consultants access, providing complete visibility into activity across client environments. It helps firms identify unauthorized or risky tools, validate time spent on client engagements for billing transparency, and maintain detailed audit trails to support client, compliance, and regulatory requirements.

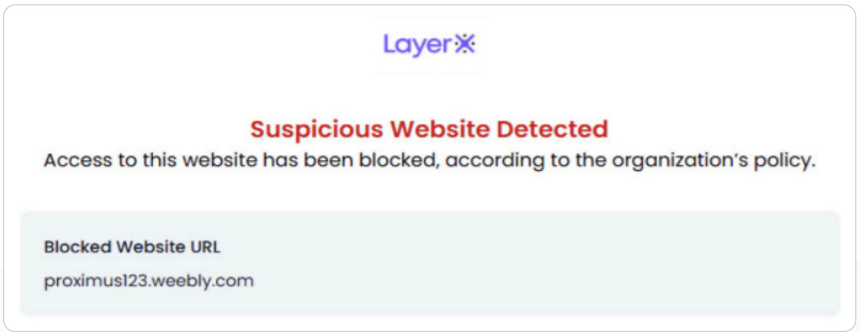
Classify and Protect Sensitive Client Data Across AI Interactions

LayerX automatically identifies and classifies sensitive consulting data, including client information, strategic initiatives, financial models, M&A activity, proprietary research, competitive intelligence, and confidential project deliverables. By understanding the context of client data within AI interactions, LayerX helps prevent cross-client data exposure and ensures sensitive information remains protected throughout the consulting lifecycle.



Protection from Advanced Phishing and Credential Theft

Consulting firms are frequent targets of phishing attacks due to the sensitive client data and privileged access their employees possess. LayerX protects consultants 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 they impact client engagements.



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...