LayerX

The All-In-One Platform for Securing AI Interactions

LayerX is the only AI usage control platform that lets you control every prompt, agent action, and data exchange, across any channel, without changing your network architecture

Solution Brief

The Modern Enterprise Challenge

Today, AI is breaking all the old security models. AI is dynamic, fileless, continuous. Users engage with it across a myriad of AI chatbots, websites, and applications, and often chase the next new model or killer AI app.

They use it on their desktop or on their phone, in the organizational network or on the go, and often use their own personal accounts for business activities. This makes the challenge of mapping and controlling all AI interactions impossible. AI is crucial for the business, but there is almost no governance of AI tools and agents, leaving enterprises exposed to data leakage, account takeover, compliance violations, and more.

Moreover, users are not the only ones generating these interactions, as new autonomous AI agents can now act on behalf of the user and perform actions on their own. As a result, the threat surface grows exponentially, since each one of these agent-driven interactions becomes a potential data risk.

And, as SaaS applications increasingly implement AI chatbots in existing services, every web and SaaS application becomes an AI app, and the threat surface grows even larger.

These trends are coalescing into each other with the advent of agentic AI browsers, such as ChatGPT Atlas, Perplexity Comet, and others, that combine an agent-driven AI-centric workspace inside the browser, within a single tool.

The problem, however, is that existing network security stacks offer little-to-no visibility or control over AI interactions. SASE/SSE are blind to real-time interactions that happen at the last-mile or are hidden behind encryption, offer coverage only to a limited number of applications through complex API integrations, and are complex to manage and deploy.

This means that activities by users or AI agents, such as accessing an unsanctioned AI application, pasting code to a personal ChatGPT account, or sharing sensitive data in an AI chatbot inside a SaaS app, cannot be stopped by existing security measures, leaving organizations exposed.

This is where LayerX comes in. It's an All-in-One AI security platform that helps organizations secure all user and agentic AI interactions and make sure that all data and identities stay safe. It provides deep visibility, real-time control, and AI-native security with zero user friction.

Since LayerX has direct visibility and control over data interactions, our protections can be applied to any web or SaaS application, not just AI.

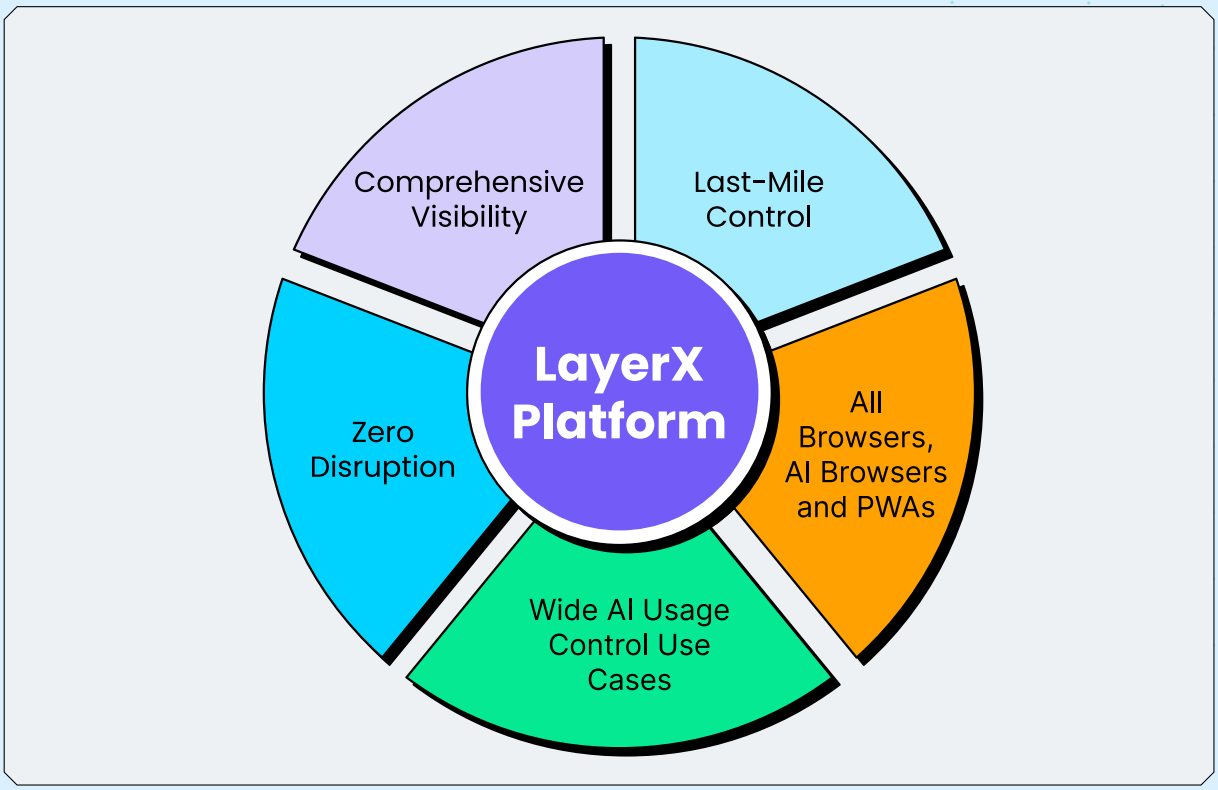
LayerX Solution Overview

The LayerX All-In-One Platform for securing AI interactions delivers the most comprehensive AI usage visibility & control over every prompt, agent action and data exchange, across any browser, channel, application, device, or identity, with no impact on user experience.

Delivered as an enterprise browser extension, LayerX gives enterprises the most extensive visibility and control over last-mile AI interactions in the organization: every prompt, every conversation, usage context, and data lineage going into or out of AI.

Since LayerX has direct visibility and control over data interactions, protections can also be applied to any web or SaaS application, not just AI. Enterprises can use LayerX to prevent shadow SaaS discovery, data leakage across web and SaaS channels, protection against malicious browser extensions, protection against zero-hour web attacks, identity governance over work and personal identities, and more.

Core LayerX Product Capabilities



Comprehensive Visibility Across All AI Interactions

LayerX provides enterprises with the most extensive visibility over last-mile AI interactions in the organization: every prompt, every conversation, usage context, and data lineage going into or out of AI. This includes a complete inventory of users, identities, applications, AI browsers, extensions, and devices, along with real-time monitoring of actions such as logins and authentications, text input, copy/paste, file uploads and downloads, and other data flows across structured and unstructured content. This depth of insight gives security teams the context needed to understand and govern all AI interactions, thereby helping the organization enable their users to use AI securely.

Real-Time, Last-Mile Control of User Activity from the Edge

LayerX enforces granular, risk-adaptive guardrails at the point of user interaction, allowing organizations to prevent risky behavior before it becomes an incident. Controls extend beyond simple allow/block decisions and can be configured to monitor, warn with customizable messages, block, redact sensitive information, or allow controlled bypass options. This real-time enforcement ensures that policy is consistently applied at the last-mile, where users interact with data, SaaS and AI systems.

Broad Support for All Browsers and PWA-Enabled Desktop Applications

LayerX integrates natively across all major commercial, enterprise, and AI browsers, as well as PWA-enabled desktop applications commonly used for SaaS and AI workloads. This ensures organizations can apply consistent protection and policy enforcement regardless of which browser or application users adopt.

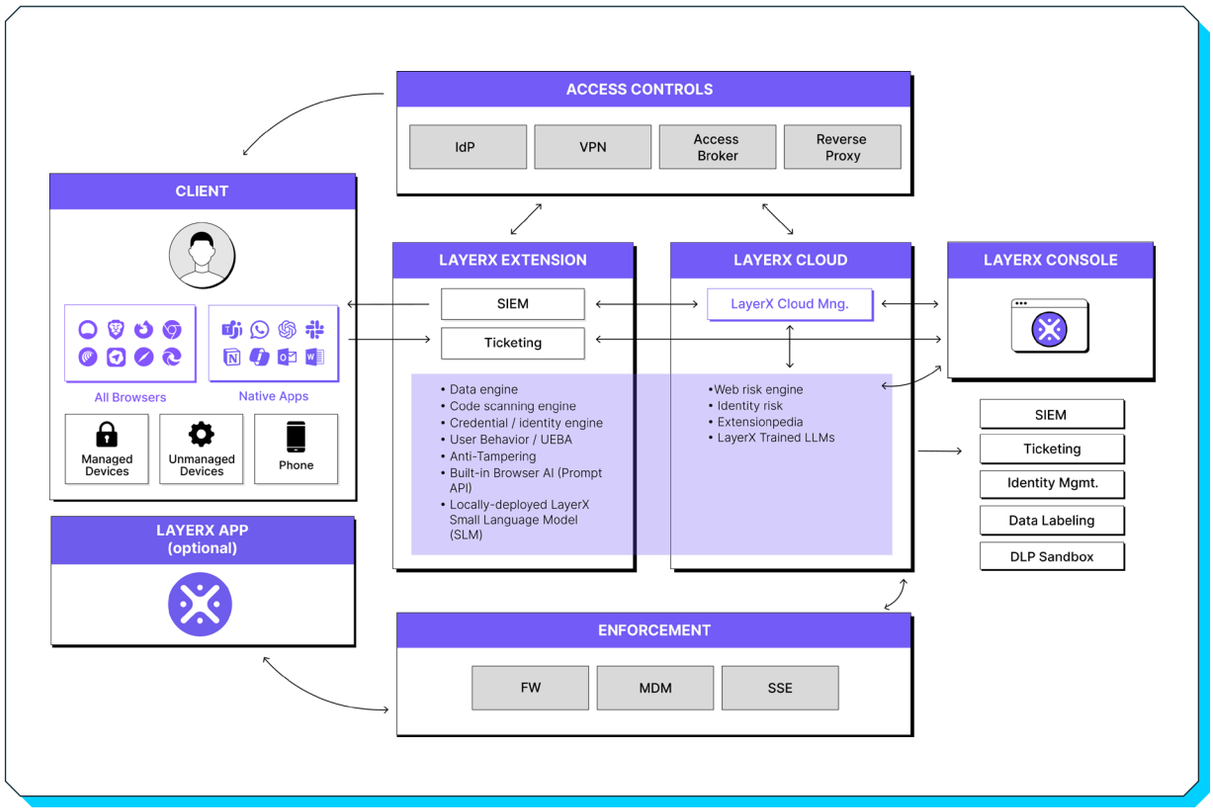
Support for a Broad Range of AI and Browser Security Use Cases

LayerX is not a point tool that is designed to solve only AI challenges but is built to address the full spectrum of risks that emerge from user interactions on AI and SaaS channels. The platform provides end-to-end protection against AI and web data leakage, shadow AI and shadow SaaS usage, malicious browser extensions, web-based vulnerabilities, phishing, identity misuse, and other browser-driven threats. This breadth of coverage ensures organizations can consolidate multiple controls into one platform while securing every user and agent interaction across AI, SaaS, and Web channels.

Zero Disruption to User Experience

LayerX preserves the native experience of the user's preferred browser without requiring new software, hardware, or changes to established workflows. Deployment is seamless, and security enforcement occurs without adding friction, latency, or altering how users interact with their tools, ensuring both strong protection and high end-user satisfaction.

LayerX Architecture



The LayerX solution is composed of the following key components:

The Extension

The LayerX extension turns any browser into a secure, policy-enforced workspace by monitoring, analyzing, and controlling user activity in real-time. Acting as both Sensor and Enforcer, it applies protections directly in the browser without disrupting the user experience.

AI Risk Analysis Engine

This is the core of the LayerX platform and is responsible for analyzing the risk of an asset or transaction

Cloud Infrastructure

It aggregates sensor data, collects logging and alerting information, adds additional layers of threat intelligence and integrates with enterprise IdP, access management, SIEM, and other systems.

Technical Specifications

Cross-Browser Support

LayerX supports all common (or uncommon) modern browsers, including Google Chrome, Microsoft Edge, Mozilla Firefox, Safari, and any independent Chromium or Mozilla-based browser. It also works seamlessly on Incognito / Private mode, ensuring full visibility and enforcement at all times. The browsers include:

- Chrome
- Edge / Edge Copilot Mode
- Safari
- Firefox
- Brave
- Comet
- ChatGPT Atlas
- Dia
- Genspark

Integration with IdP

LayerX seamlessly integrates with leading Identity Providers, ensuring unified user identity management and consistent policy enforcement across all browser activity. This includes:

- Okta
- Entra
- Azure AD
- Google Authentication

SIEM System Integration

LayerX offers built-in integrations with major SIEM systems that deliver real-time, high-fidelity browser telemetry directly into existing security operations. Teams gain deeper context, faster investigation paths, and improved threat detection without additional configuration complexity. These integrations include:

- Splunk
- Datadog
- Sentinel
- CrowdStrike Falcon
- Sumo Logic
- Coralogix
- Elastic SIEM
- Google SecOps
- QRadar
- Stellar Cyber

OS Support

LayerX supports all major operating systems, ensuring consistent protection and policy enforcement across every device your workforce uses. This includes:

- Windows
- Mac
- Linux
- iOS
- Android
- ChromeOS

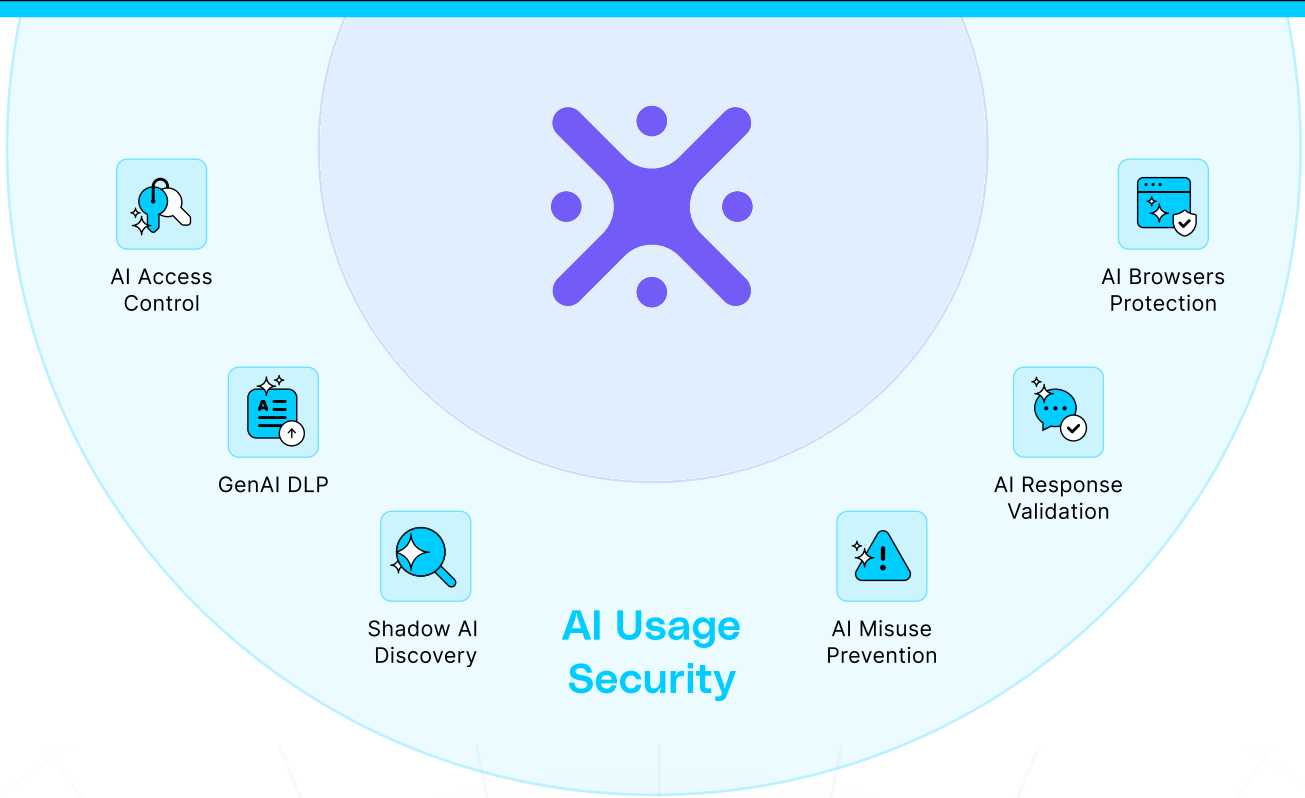
Support for Local, Native Desktop Applications

LayerX provides visibility and enforcement of security rules not just inside the browser, but also on native desktop applications, through Progressive Web Apps (PWA). This means that any application running in PWA mode is fully supported by LayerX, just like any browser-based AI or SaaS application. Some examples of the applications LayerX supports include:

- Microsoft Office 365
- ChatGPT
- Claude
- Copilot
- Perplexity
- Outlook
- Telegram
- WhatsApp
- LinkedIn
- Signal
- Facebook Messenger
- Zoom
- Slack
- Teams
- Notion
- Trello
- VSCode

Use Cases

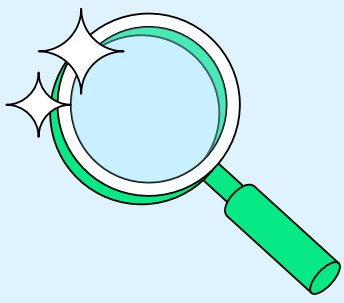
The LayerX solution covers key customer use-cases across AI usage securtiy.



AI Usage Security Use Cases

USE CASE #1

Shadow AI Discovery



The Challenge & Risks

As AI usage rapidly accelerates across the enterprise, employees increasingly turn to unapproved GenAI tools such as plug-ins, browser-based LLMs, AI assistants inside SaaS apps, and embedded AI features in productivity suites. This "shadow AI" activity is invisible to traditional security controls. The risk is significant: employees may input proprietary data, customer information, source code, or regulated content into unmanaged AI systems that store or train on that data, creating silent compliance and IP-loss risk.

Why It's a Problem

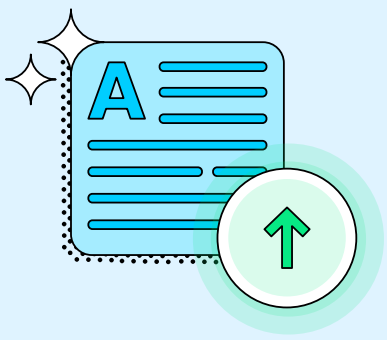
Security teams often have no reliable inventory of which AI tools users access, from which devices, or what data they are feeding into prompts. Without visibility, organizations cannot enforce purpose-built AI governance, cannot distinguish harmless experimentation from high-risk behavior, and cannot prevent data from landing in external AI systems. This blind spot introduces data exposure and undermines governance frameworks that CISOs are now expected to enforce.

How LayerX Helps

LayerX performs continuous, real-time discovery of every AI interaction, including web-based tools, embedded AI widgets, SaaS-native AI features, and LLM plug-ins. It identifies the users, identities, devices, accounts, and data involved and classifies the risk of each interaction. With this visibility, security can finally govern AI usage with contextual, last-mile enforcement by monitoring low-risk experiments, applying guardrails for uncontrolled tools, or blocking unsafe interactions entirely.

USE CASE #2

AI Data Leakage Protection



The Challenge & Risks

GenAI tools have become one of the easiest places for users to accidentally leak sensitive data. Employees frequently paste code snippets, contracts, customer records, or internal documents directly into prompts. Traditional DLP cannot see this activity in real-time because it occurs in the browser before data touches the network, endpoint, or API channel.

Why It's a Problem

This "copy/paste exfiltration" channel is now one of the fastest-growing vectors for unintentional data loss. Data submitted to LLMs may persist, be logged, or be used for model training, thereby violating corporate confidentiality, regulatory standards (HIPAA, PCI, GDPR), and contractual obligations. Organizations lack a reliable, scalable way to ensure safe AI usage while still enabling productivity.

How LayerX Helps

LayerX provides GenAI-specific DLP with granular, real-time controls at the moment of user interaction. It inspects text inputs, attachments, file uploads, and copy/paste operations into AI tools. If sensitive information is detected, LayerX can warn the user, block the action, redact fields, or allow a managed bypass with justification. Customers use LayerX to prevent IP loss, customer data exposure, and leakage of confidential documents into GenAI models without slowing down AI adoption.

USE CASE #3

AI Access Control

The Challenge & Risks

Enterprises must differentiate between allowed, high-trust AI systems and untrusted or high-risk AI tools. Without granular access control, users may access external models that don't meet governance, privacy, or contractual requirements. Blanket blocking is impractical and harms productivity, while open access creates risk.

Why It's a Problem

Network or identity controls cannot distinguish between safe and unsafe AI interactions inside the browser. Moreover, businesses need dynamic control. This means not all users, devices, or data types should be treated equally. Without contextual enforcement, organizations cannot implement risk-based AI governance.

How LayerX Helps

LayerX enables policy-driven, granular AI access controls based on user identity, device posture, AI tool risk rating, and the type of data being handled. It can allow access to approved AI systems, restrict high-risk LLMs, or redirect users to approved AI tools. It can also apply restrictions on access using personal or non-SSO accounts and apply data controls based on the user identity used to access the AI tool. LayerX uniquely applies these guardrails directly in the browser where the user interacts with AI tools to deliver precise, last-mile governance without breaking workflows.

USE CASE #4

Shadow AI Misuse Prevention

The Challenge & Risks

Even when using sanctioned AI platforms, employees can still perform unsafe or non-compliant actions, such as generating harmful content, offloading confidential work, or circumventing policy. AI misuse may be accidental (e.g., uploading regulated data) or intentional (e.g., using AI to generate malicious code or bypass controls).

Why It's a Growing Concern

As AI tools integrate deeper into daily workflows, the enterprise has limited ability to monitor whether outputs, prompts, or actions violate policy. Misuse exposes organizations to regulatory, reputational, and security risks, and it often bypasses traditional detection technologies that cannot see browser-level interactions.

How LayerX Helps

LayerX enforces AI-misuse prevention policies by detecting and intervening when a user attempts risky AI actions. It can block sensitive data uploads, prevent prompt injection attempts, ensure outputs comply with policy, and enforce acceptable-use rules. LayerX's risk-adaptive guardrails give CISOs a scalable way to ensure safe, compliant AI usage without restricting innovation.

USE CASE #5

AI Response Validation

The Challenge & Risks

AI responses can be incorrect, hallucinated, biased, or misleading. This leads to business errors, compliance failures, or the propagation of inaccurate information. In security-critical industries such as finance, healthcare, legal, etc., relying on unvalidated AI output can create severe downstream risks.

Why Existing Tools Can't Solve It

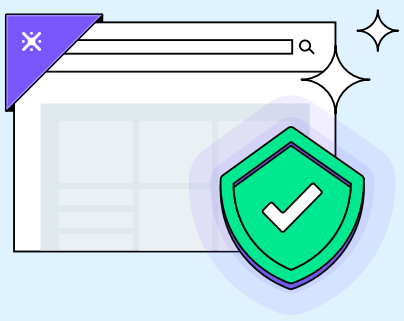
Traditional DLP and SSE solutions inspect data flowing out of an enterprise, but not data being generated by an AI engine. They cannot validate whether AI output violates policy, introduces risk, or contains sensitive information synthesized from user input.

How LayerX Helps

LayerX analyzes AI outputs in real-time, validating responses against enterprise policies and identifying risks such as hallucinated data, leakage of sensitive information, or outputs that violate compliance standards. It can alert, block, or enforce safer alternatives. This provides CISOs with a governance layer that doesn't just secure what users send to the AI model, but also what they receive back.

USE CASE #6

AI Browser and Extension Protection



The Challenge & Risks

With the rise of agentic AI browsers such as Atlas, Comet, Dia, or Edge Copilot Mode, users are increasingly interacting with AI-based agents directly embedded into their browser environment. These next-gen browsers open a new class of risk: data input, uploads, and commands that are routed through autonomous AI agents, not human users. Without proper controls, sensitive corporate data could be submitted to or extracted by these agents, while malicious websites or phishing attacks can target the side-loaded AI context, abusing trusted agent functionality.

At the same time, AI-powered browser extensions are often granted extensive permissions to identities, cookies, credentials, SaaS sessions, and user input. A single extension can read keystrokes, access enterprise apps, or exfiltrate data - yet most organizations lack visibility into which extensions are installed, how they behave, or the risk they introduce.

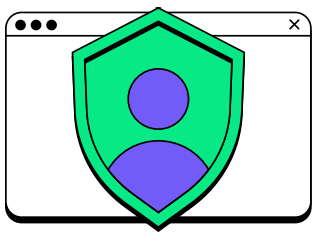
Why It's Particularly Dangerous

Unlike traditional browsers, AI browsers blur the line between user intent and agent intent. A compromised AI agent or a malicious prompt injection can exfiltrate data or perform unintended actions. Attackers can also exploit zero-day web threats through agent-driven browsing, since embedded AI components may not be well protected by legacy security. When combined with powerful, often ungoverned AI extensions that have broad access to identities, sessions, and user input, organizations are left with limited visibility and control over who is using these AI browsers or extensions, how they operate, and what data they can access or share.

How LayerX Helps

LayerX delivers deep visibility and control across both AI browsers and extensions. It automatically detects agentic AI browsers in use, maps users and installed extensions, and monitors real activity, not just static attributes. Security teams can enforce risk-based policies to control what data can be typed, uploaded, or shared based on identity, device posture, and data sensitivity.

LayerX also provides full extension inventory, permission analysis, risk scoring, and real-time threat analysis, including behavioral monitoring as extensions operate. High-risk extensions can be blocked automatically, approved extensions allowed, and malicious web content or phishing attacks stopped in real-time. By applying last-mile guardrails, LayerX keeps both human and AI-agent activity secure without disrupting productivity.



Maintain Security Without Disrupting The User Experience

#1

Unlock Visibility No Other Tool Can Provide

LayerX delivers real-time, holistic visibility across all users, identities, AI tools, SaaS applications, browsers, and data flows. It discovers every AI and SaaS service in use, maps the identities associated with each, and monitors all file-based and file-less transactions occurring within them. This gives security teams an unparalleled view into last-mile user activity, something that traditional SSE, CASB, EDR, and DLP solutions simply cannot access.

#2

Enforce Last-Mile Security with Smart, Adaptive Guardrails

Instead of the binary “allow or block” controls offered by conventional tools, LayerX applies intelligent, context-aware enforcement. Security teams can set adaptive guardrails that automatically adjust based on user behavior, application risk, data sensitivity, and real-time context. These controls monitor, warn, block, redact, or offer guided bypass options to enable safe AI and SaaS usage without shutting down productivity.

#3

Achieve Full Deployment with Zero Infrastructure Change

LayerX deploys as a lightweight, enterprise-grade browser extension that requires no network routing, hardware, proxies, or browser replacements. It supports all major and emerging AI browsers, all mainstream web browsers, and any PWA-enabled desktop app. Organizations can achieve complete coverage instantly, with no user friction, no IT burden, and no architectural changes.

#4

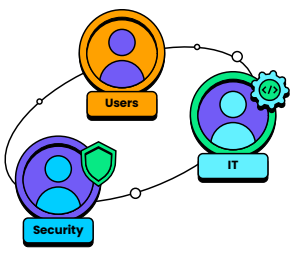
Ensure Zero Friction for End Users

LayerX works silently in the browser that the user already knows. There are no new workflows, no training requirements, no performance overhead, and no need to switch to an enterprise browser. This ensures adoption remains 100% while security remains airtight.

#5

Enable AI Productivity Without Compromising Security

LayerX empowers organizations to safely embrace AI assistants, AI browsers, and high-velocity SaaS workflows. By protecting sensitive data, guiding users toward safe practices, and illuminating risky behaviors, LayerX helps accelerate AI adoption while reducing the risk of data leaks, misconfigurations, unsanctioned tools, and user-driven mistakes. The result is both higher productivity and stronger security for the AI-enabled workforce operating within secure, well-governed boundaries.



Achieve Happy Users, Happy Security, and Happy IT All At the Same Time

#1

Broadest Coverage Across All AI, SaaS, and Browser Security Use Cases

LayerX is not a point tool that is designed to solve only AI challenges but is built to address the full spectrum of threats that emerge from user interactions on AI, SaaS and Web channels, including data leakage, shadow AI and SaaS adoption, malicious extensions, phishing, identity misuse, and browser-based vulnerabilities. This breadth allows customers to consolidate multiple tools while ensuring comprehensive protection across all user-driven channels.

#2

Powerful Last-Mile Enforcement Where Other Tools Cannot Operate

Unlike traditional SSE, CASB, EDR, or DLP solutions that lack visibility into the last-mile of the user session, LayerX provides real-time, actionable visibility and enforcement at the exact moment users interact with data, AI, and SaaS applications. It prevents sensitive information exposure by governing text inputs, copy/paste actions, file uploads, downloads, and authentication flows, all in real-time and at the point of interaction in the browser.

#3

Granular, Context-Aware Policy Controls

LayerX offers the industry's most precise and adaptable policy engine. Policies can be defined based on attributes such as user identity, web domain, activity type, endpoint posture, session context, location, data sensitivity, and more. Enforcement ranges from passive monitoring to warnings, redaction, guided bypass, or full blocking. This allows security teams to design highly tailored guardrails that match risk, user roles, and business needs without over-blocking or restricting productivity.

#4

Unified Protection Across All Browsers and Local Desktop Applications

In addition to securing all browsers and every AI and web application, LayerX extends its protection to native desktop applications through Progressive Web Application (PWA) technology. Today, the most commonly used tools, like Office 365, Outlook, ChatGPT, Microsoft Copilot, Slack, Telegram, and even developer tools like VS Code, can be wrapped as PWAs. LayerX secures them with the same visibility and last-mile enforcement as any browser-based workflow. With this approach, LayerX uniquely unifies security across AI, web, and desktop applications, ensuring consistent protection across the entire user workspace.

#5

Zero Impact on the User's Native Browsing Experience

Alternative solutions often require network rerouting, proxies, or the adoption of custom enterprise browsers that typically introduce latency, complexity, and user disruption. In contrast, LayerX preserves the user's natural browsing experience without adding any friction. It requires no architectural changes, introduces no performance degradation, and keeps workflows exactly as users expect. Protection is applied invisibly, ensuring high user satisfaction and eliminating adoption barriers.

#6

Deep Integration with All Browsers for Maximum Security

LayerX offers unmatched compatibility and deep technical integration with all major browsers, strengthened through strategic partnerships with browser vendors. This enables advanced capabilities, including anti-tampering and enhanced event capture that standard extensions or security tools can't replicate.

#7

Easy Deployment Across Devices with Zero Architecture Changes

LayerX can be deployed instantly across managed and unmanaged devices without installing agents, hardware appliances, or reconfiguring the network. Organizations gain complete coverage in minutes, even in distributed or BYOD environments, dramatically reducing IT overhead and accelerating time to value.

#8

Tamper-Proof and Bypass-Resistant by Design

Unlike typical extension-based tools that users can disable or evade, LayerX incorporates multi-layer anti-tampering controls at the browser, page, and file-system level. It also preserves visibility and enforcement in Incognito/Private Mode. These capabilities ensure that users cannot disable protections or operate outside of governance, giving security teams confidence that policies remain intact across all scenarios.

Return on Investment: Unlock Savings and Value Like No Other Tool

LayerX delivers measurable security, productivity, and architectural savings from the very first day of deployment while continuing to expand value over time. Unlike traditional tools that require complex rollout cycles or infrastructure changes, LayerX provides immediate visibility and control from day 1, and ultimately allows organizations to simplify architecture and retire legacy tools over the long term.

On Day 1: LayerX Closes Visibility & Security Gaps Instantly

Within minutes of deployment, LayerX provides full, real-time visibility into all last-mile user interactions across any browser, AI tool, or SaaS application. It includes:

- AI & SaaS DLP that protects sensitive information during text input, file upload, copy/paste, and prompt submissions
- Discovery of shadow AI and SaaS usage including embedded SaaS-native AI features
- Protection against web-borne threats such as phishing, malicious pages, etc.

This instant visibility and protection begins generating savings from the first day of rollout by dramatically reducing unmanaged risk, data exposure, and incident response burden.

Within 1 Week: Securely Enable AI & SaaS Productivity

Within just one week, organizations can securely enable AI and SaaS-driven productivity across the enterprise. LayerX provides the governance and guardrails needed to use GenAI assistants, LLMs, AI-embedded SaaS apps, AI-native features, AI agents, and AI-driven browsing environments safely. It ensures compliant usage and prevents data leakage or misuse. This quick rollout speeds up safe AI adoption and boosts productivity, while reducing compliance and data-exposure risks.

Over Time: Simplify Architecture and Reduce Legacy Spend

As LayerX becomes the central control point for browser, AI, and SaaS interactions, organizations can consolidate tools, streamline their security architecture and cut legacy spend on costly technologies like RBI, VDI for SaaS workflows, SWG/CASB, VPN/SSE for BYOD, and TLS interception. LayerX's deep browser-level visibility and last-mile enforcement allow organizations to streamline their security stack, reduce costs, and retire tools that no longer fit the modern, browser-native, AI-driven enterprise.

Secure your AI Interactions where they happen without slowing anyone down.

→ Contact us to experience how LayerX delivers the most comprehensive AI usage visibility & control.