LayerX

EXTEND PARTNER PROGRAM BY LAYERX

LayerX – The All-in-One AI & Browser Security Platform (delivered as a browser extension) Secures your customers Identities, SaaS apps, Data & Devices from All Web-Borne Threats and Browsing Risks.
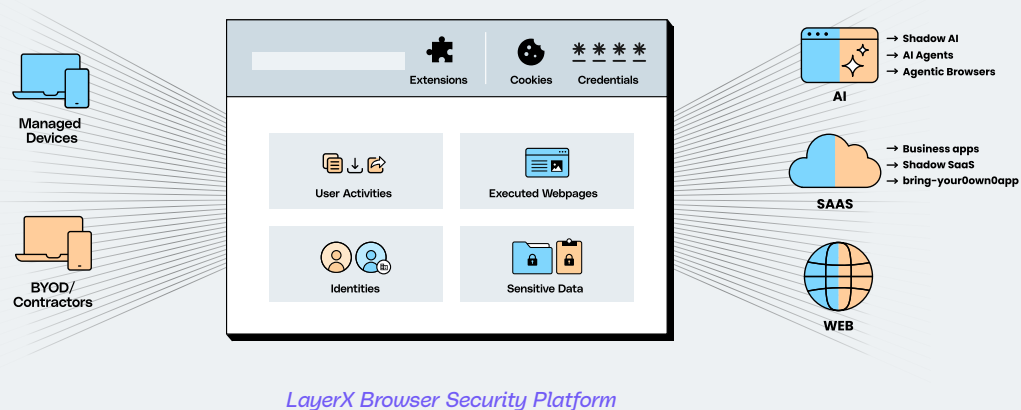
Partner ONLY organization ✕ Dedicated channel manager ✕ Tailored, collaborative partnership experience

The browser is your customer's #1 security blind spot

The most prominent cyber threats your customers face either target or involve their employees' browsers; phishing pages that lure them to log in, malicious extensions that steal critical data from their browsers, shadow SaaS where corporate passwords are reused, GenAI tools like ChatGPT that expose sensitive data, and data leakage over the web and SaaS apps. These and other threats have one thing in common: they are beyond the protection scope of the solutions your customers have in their security stack.

LayerX: Protection against all web-borne threats with a single, seamless solution

Leveraging a lightweight extension deployed in minutes on any browser, beyond the end-to-end encryption, LayerX AI and browser security platform was purpose-built to monitor, analyze, and govern the workforce's interactions on the web. It eliminates the browser blind spots and security gaps, prevents otherwise undetected zero-hour attacks, and addresses data security risks when using unsanctioned SaaS applications and unmanaged devices.

LayerX Browser Security Platform

Unmatched visibility and control across any browser with near-zero impact on the user experience

LayerX monitors and analyzes browsing events at the highest resolution, using deep session analysis. An AI-powered engine detects early indications of potential risks and enforces adaptive activities and access policies to prevent them. High-level granularity ensures that only risky activities are blocked, without violating users' privacy or disrupting their overall browsing experience.

Seamless deployment with zero infrastructure required

The LayerX extension integrates with the existing browsers your customers' employees already have on their computers. Deployment takes place instantly via a group policy, with the option of individual sign-in for unmanaged devices. This translates to effortless, rapid deployment that enables your customers to drive immediate value from the product within minutes.

Complement your security offering by solving the most critical security gaps

From preventing the simplest-to-execute, yet hardest-to-detect web-borne attacks, through providing monitoring and governance on users' activities on the browser, and up to reducing the browsers' attack surface - whatever your challenges are – LayerX has got you covered.

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

AI Browsers Protection
Protect AI browsers against attack and exploitation

AI Usage Security

GenAI DLP
Prevent leakage of sensitive data on AI tools

AI Browsers Protection
Protect AI browsers against attack and exploitation

Shadow AI Discovery
Discover and enforce security guardrails on all AI apps

AI Access Control
Restrict user access to unsanctioned AI tools or accounts

AI Misuse Prevention
Protect against prompt injection, compliance violations, and more

AI Response Validation
Ensure AI response validity and data security

Key Benefits

Eliminate critical blind spots

Gain the most granular visibility into unsanctioned apps, shadow identities, DNS over HTTPS, SaaS apps and dynamic websites.

Real-time protection

Enforce access & activity policies to restrict browsing activities that expose your apps, devices, and data to compromise.

High-precision risk detection

Multilayered AI analysis of every user activity and web session flags anomalies that can indicate risk in the browser session.

Unified browser management

Manage and configure your workforce's browsers from a single, centralized interface.

Bring your own browser

Enable your users to keep on using their browser of choice for both work and personal use.

Rapid deployment

Deploy across your entire environment and integrate with browser management tools and identity providers in a single click.

Extend Partner Program by LayerX

Dear partner,

We are delighted to welcome you to the Extend Partnership Program by LayerX, with this partnership we can create a safe, secure and efficient workspace for businesses.

At LayerX we strongly believe in the power of collaboration and innovation, with a partnership program designed to fulfill our mission of being a partner led company, and a solution designed to address the ever-evolving threats and risks of the browser being the modern workspace and a critical organizational asset.

The Extend Partner Program is crafted to provide you with the tools, resources, and support you need to succeed, and is constantly evolving with more. From attractive financial incentives to comprehensive training and dedicated support, we are here to empower your business and drive mutual growth.

By joining our program, you become a part of a select group of partners who are at the forefront of cybersecurity innovation. We value your expertise and look forward to building a strong, collaborative relationship that delivers exceptional value to our customers.

Thank you for choosing to partner with LayerX. Together, we can achieve remarkable success and make a significant impact in the cybersecurity industry.

Welcome aboard, looking forward to a successful partnership.

The LayerX Partnerships Team

Partner ONLY organization ✖ Dedicated channel manager ✖ Tailored, collaborative partnership experience

Financial incentives
- Simple margin structure and volume discounts
- Partner promotions and competitive pricing
- Additional services revenue opportunities

Technical
- Technical training and Lab POC and Demo license
- PS and Consultancy training
- Flexible training options: Online and In-Person

Non-financial incentives
- Lead sharing and co-prospecting
- Early access to new features
- Joint study cases and partnership PR

Marketing
- Co-marketing activities and campaigns
- Marketing plans, co-branding and MDF
- Industry webinars and events

Sales
- AEs and SEs to support you win business deals
- Short sales cycles, focused on ease of sale
- Deal registration and protection

Enablement
- Sales Kits: Brochures, presentations, and demo tools
- Planning: Account mapping, Business planning
- Enablement: Sales training, workshops and periodic meetings

About LayerX

LayerX agentless AI & Browser Security Platform protects organizations against AI, SaaS, web & data leakage risks across any browser, application, device, and identity, with no impact on user experience. Delivered as an Enterprise Browser Extension, LayerX secures all last-mile user interactions with AI, SaaS & web applications and offers the most comprehensive visibility and enforcement capabilities for AI and browsing risks, including: shadows AI and SaaS discovery, data leakage prevention across GenAI, web and SaaS channels, protection against malicious browser extensions, protection against zero-hour web attacks, identity governance over work and personal identities, and more.

LayerX

The All-in-One AI & Browser Security Platform

LayerX agentless AI & browser security platform protects enterprises against the most critical AI, SaaS, web and data leakage risks across any browser, application, device and identity, with no impact on user experience
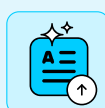
Integrates with All Commercial, AI and Enterprise Browsers

The LayerX Security Platform

Delivered as an Enterprise Browser Extension, LayerX offers the most comprehensive visibility and enforcement capabilities over AI and Browsing risks, including:

AI Usage Security

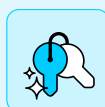**GenAI DLP**
Prevent leakage of sensitive data on AI tools

AI Browsers Protection
Protect AI browsers against attack and exploitation

Shadow AI Discovery
Discover and enforce security guardrails on all AI apps

AI Access Control
Restrict user access to unsanctioned AI tools or accounts

AI Misuse Prevention
Protect against prompt injection, compliance violations, and more
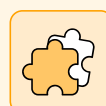
AI Response Validation
Ensure AI response validity and data security

Enterprise Browser Security

Web/SaaS DLP & Insider Threat
Prevent data leakage across all web channels

Browser Extension Management
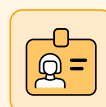Detect and block risky browser extensions on any browser

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 and Secure Access
Secure SaaS remote access by contractors and BYOD