LayerX

Complement Your Security Capabilities with Real-Time Protection Against Web-borne Threats and Browsing Risks

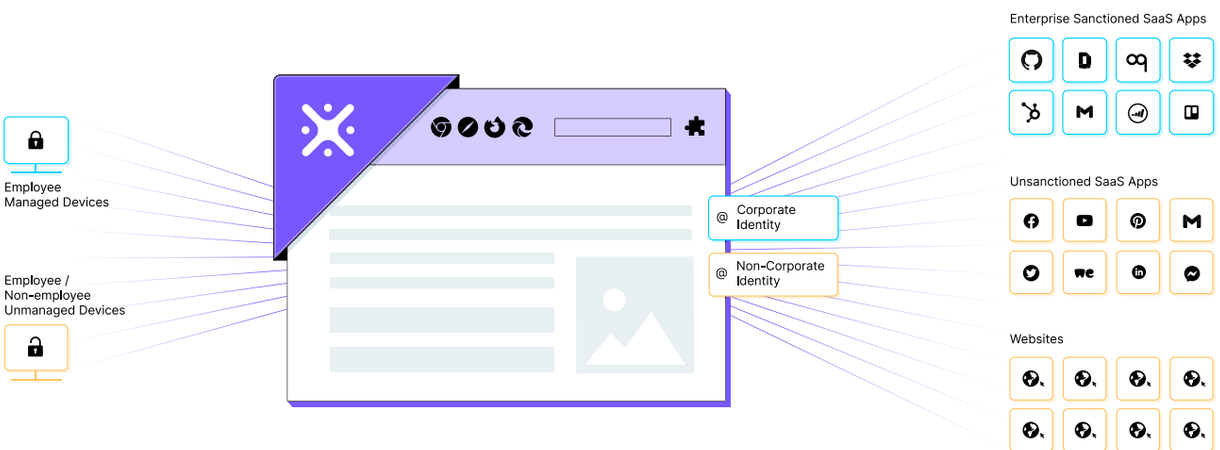
LayerX enterprise browser extension joins forces with Microsoft to deliver comprehensive protection against browser-related risks such as web data loss, malicious extensions, zero-hour phishing, and many more, that lead to account takeovers and data loss.

The Browser Is The Most Targeted Attack Surface, And The Main Source For Data Loss

The browser has become the core workspace in the modern enterprise, being the exclusive access interface to anything on the web, from managed SaaS applications to unsanctioned apps and websites. This subjects the browser to multiple web-borne attacks that aim to compromise enterprise applications, data, and devices, as well as making it a potential source of unintentional data leakage and other browsing risks.

Layerx: The Browser Security Platform

Leveraging a lightweight browser extension deployed in minutes on any browser, beyond the end-to-end encryption, LayerX 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.



Enhance your Microsoft tool portfolio with powerful integrations:

- **Azure AD**
  Set dynamic policies on your AD users and groups
- **Edge for Business**
  Add LayerX as an application level security tool on any device
- **Entra**
  Add LayerX as a conditional access factor on Entra to validate users logging into your SaaS application protected by Entra
- **AIP labels**
  Use LayerX to detect the movement of labeled documents via the browser to prevent data loss and guarantee compliance
- **Microsoft Sentinel**
  Stream logs and alerts from LayerX to Microsoft Sentinel and enjoy a single pane of glass

Layerx Use Cases

Web DLP

Prevent exposure of internal data in ungoverned websites and applications

- Prevention of insecure uploads
- Malicious insider protection
- Governance of data download to unmanaged devices

SaaS Discovery, DLP, and Protection

Eliminate shadow SaaS, prevent data leakage, and harden apps' security posture across all your sanctioned and unsanctioned SaaS and web apps

- Shadow SaaS discovery
- User account activity monitoring
- SaaS DLP
- User account security posture management

Risky Browser Extensions Protection

Block malicious or risky extensions to protect passwords, cookies, identities, and other browser-stored data from compromise

- Risky extensions detection
- Disabling the malicious extension downloading

GenAI Data Risks Protection

Mitigate any exposure risk to your sensitive data on ChatGPT and other GenAI tools

- Sensitive data paste prevention
- GenAI browser extension disablement

Zero-Hour Protection Against Browser-borne Threats

Gain real-time protection against all web-based attacked that couldn't be prevented before

- Browser patch management
- Phishing\social engineering pages detection
- Malicious web page activity disablement
- URL filtering
- User alerts when accessing risky web pages

Secure Browser-based Authentication to SaaS and Web Apps

Enforce secure access to your SaaS resources without requiring VPNs or other dedicated networking infrastructure for both managed and unmanaged devices

- VPN alternative
- SaaS IdP integration
- Seamless and rapid rollout
- Least-privileged authorization policie

Identity Security Posture Management

Identify and mitigate identity weaknesses and block account takeover activities

- Identity weaknesses detection
- Shadow identities discovery
- Compromised credentials discovery
- Authentication hardening

Secure 3rd Party Access

Provide your external contractors with seamless access to your resources without compromising security requirements

- Least-privilege access policies
- Seamless onboarding\offboarding
- Real-time malicious access blocking

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.