LayerX Enterprise Browser Extension

LayerX integrates with any browser to secure your identities, data, and SaaS apps and devices against web-borne threats and browsing risks that legacy network and endpoint solutions are blind to, while maintaining the user experience

The Browser is the Most Attacked Attack Surface and the Main Source for Data Loss

The browser is the modern point of risk for most cyberattacks. However, legacy security solutions such as CASB, SWGs, and endpoint solutions are blind to user activity and data that goes through it. As a result, organizations are exposed to browsing risks and vulnerabilities such as account takeover, GenAI data exposure, shadow SaaS, and more. LayerX is an enterprise browser extension that turns any commercial browser into the most secure environment, protecting organizations against web-borne threats and browsing risks while maintaining the user browsing experience.

What You Get When You Choose LayerX:

ZERO-HOUR WEB PROTECTION

AI-based analysis engine detects malicious web content in real-time and blocks account takeover, phishing, and more

WEB/SAAS/GENAI DLP

Detect data leakage across all web channels and prevent activity such as copy/paste of sensitive data, file uploads, etc.

SHADOW SAAS DISCOVERY & BLOCKING

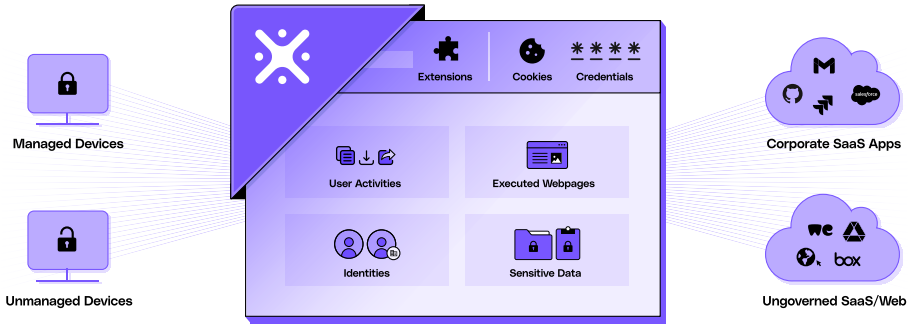
Discover 'shadow' SaaS apps missed by your CASB, and block sensitive data from leaking through them

BROWSER EXTENSION PROTECTION

Identify and block risky browser extensions that steal cookies, compromise credentials, and track users

Eliminate The Blind Spots in Existing Security Tools

Legacy endpoint and network security solutions such as CASB, SWG, RBI and endpoint security provide limited visibility into data and user activity in the browser. LayerX, on the other hand, provides 360° granular visibility across all browsing accounts, events and data. As a result, LayerX can protect both managed and unmanaged devices and provide visibility and enforcement for all SaaS apps, including 'shadow' SaaS applications.



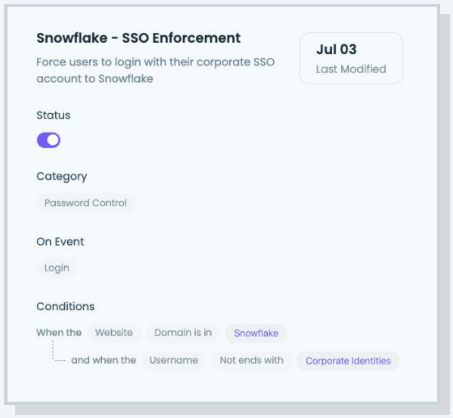
Deploy Easily on Any Browser

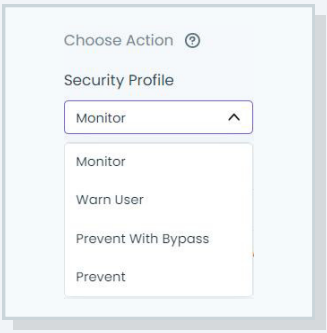
LayerX supports all major commercial browsers (Chrome, Edge, Firefox, Safari), as well as any Chromium-based browser (Brave, Arc, Tor, etc.). LayerX also integrates with common IdP solutions such as Okta and Entra, MDM solutions and SIEM systems, so it can be deployed effortlessly and doesn't require users to change their browsers or workflows.

Don't Just Know About It. Fix It

While many security tools only tell you about a problem but do not help you fix it, LayerX offers granular enforcement capabilities with a graphical rules wizard that enables security managers to easily define detailed security rules. Policies can be determined according to user identity, activity (copy/paste, file upload/download, etc.), URL, and more and applied to a single user or a group of users.

This allows security teams to define granular policies for their specific needs, such as preventing R&D teams from pasting code to GenAI tools or ensuring users connect to corporate SaaS apps only with corporate accounts backed by SSO.





Enforce Security Without Breaking the User Experience

Traditional security tools often force organizations to choose between allowing everything or blocking everything. LayerX, on the other hand, provides multiple enforcement options, from monitoring only, to prompting users, restricting access with overrule options, or fully blocking. This enables security teams to choose the level of enforcement they desire based on the risk profile without sacrificing productivity.

Discover Shadow SaaS, Personal Accounts, Weak Passwords, and More

LayerX provides visibility into all user data and activity that passes through the browser on both managed and unmanaged devices. This means you can see exactly where users are going, discover unsanctioned 'shadow' SaaS applications, detect SaaS usage on personal accounts not backed by SSO/MFA, identify weak or re-used passwords and shared accounts, and more.