LayerX

SECURE SAAS USAGE & ELIMINATE 'SHADOW' SAAS

LayerX is an all-in-one, agentless AI and Browser security platform that secures organizations' SaaS applications, detects and enforces controls over 'shadow' SaaS apps, and fortifies the organization's SaaS security posture, directly from within the browser, with no impact on the user experience.

Most business applications today are deployed as SaaS solutions, meaning that SaaS security is increasingly synonymous with cyber security. However, existing solutions either lack detection and enforcement capabilities, or are incredibly complex to deploy (or both). LayerX is the only solution that detects all SaaS usage in the organization and applies granular enforcement without disrupting the user experience or existing network architecture.

How LayerX Helps You Enforce SaaS Security and Eliminate 'Shadow' SaaS

100% Visibility

Detect every SaaS application in use and gain visibility to all user activities and data in any app

Granular Enforcement

Enforce security guardrails directly at the point of usage, and apply adaptive, risk-based protections

Single Deployment

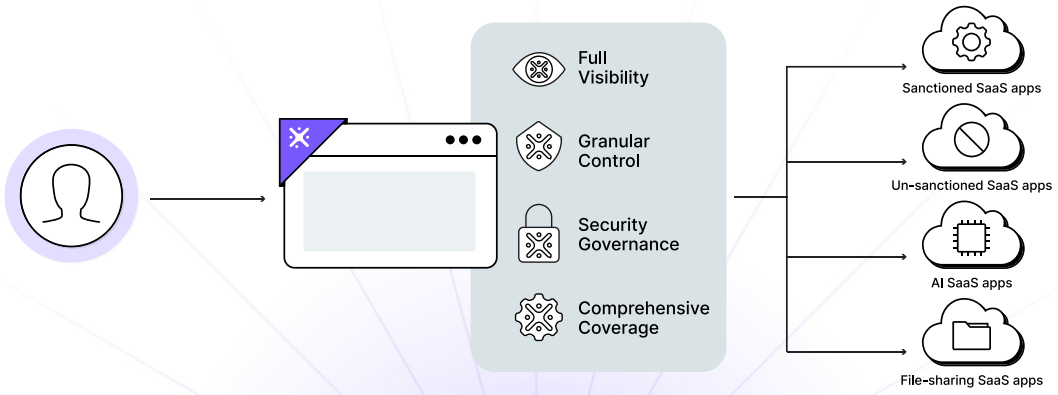
View all SaaS apps and usage from a single point, with a unified, easy-to-deploy solution across all devices

Can't Be Bypassed

Integration with IdP and access management systems means users can't access SaaS apps without LayerX visibility

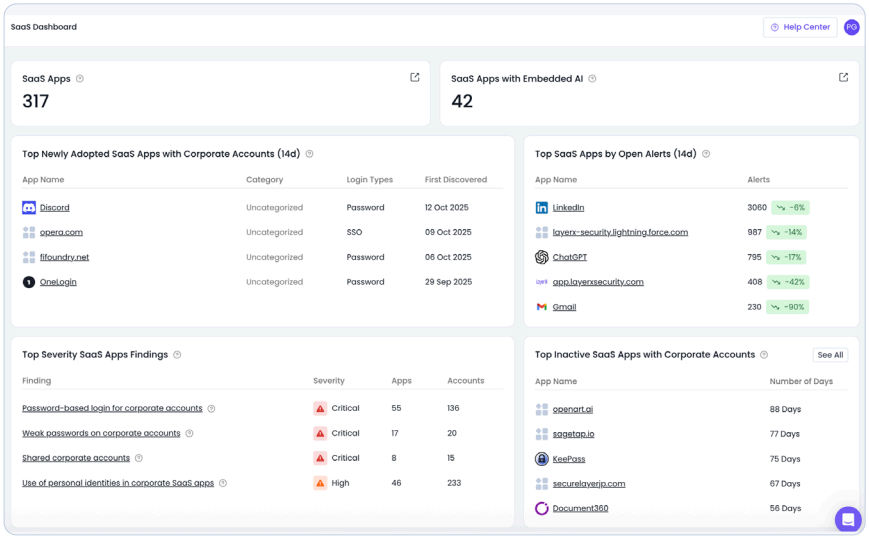
SaaS Security is a Browser Security Problem

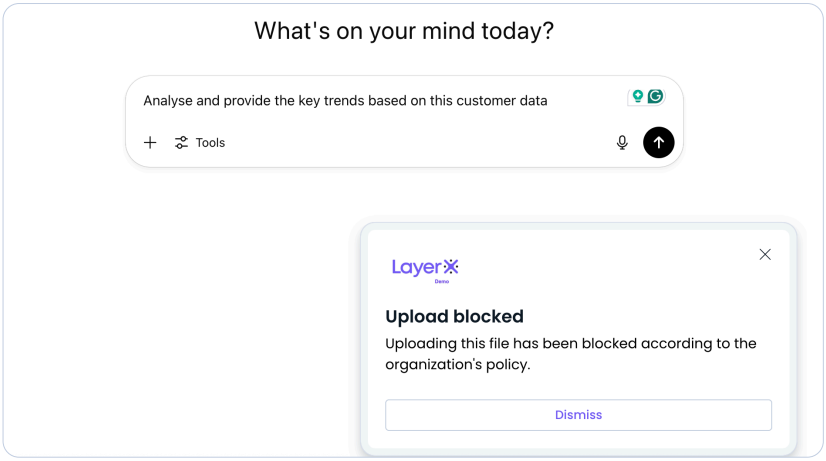
Most business applications in organizations today are SaaS solutions accessed via the web browser, making it the main point of control for SaaS security and management. Network-based solutions typically lack comprehensive visibility and/or enforcement capabilities, and leave open too many interfaces that users can bypass. Therefore, only a solution deployed directly in the browser can fully solve SaaS security and 'shadow' SaaS challenges. LayerX is deployed as a browser extension directly within users' browsers, giving it full visibility and granular control over all SaaS applications.



See All SaaS Data Risks in One Unified View

Gain complete visibility into all SaaS activity across the organization in one view. The LayerX SaaS Security dashboard surfaces newly adopted apps, usage trends, high-risk security findings such as weak passwords or shared accounts, and flags inactive apps that may create vulnerabilities. With one dashboard, IT regains control over SaaS security while keeping legitimate usage seamless.





Prevent Sensitive Data Exposure In The Browser and On Native Desktop SaaS Applications

LayerX provides visibility and enforcement over desktop SaaS applications via Progressive Web Application (PWA) technology. This means that LayerX can be deployed on nearly any native application, and it offers full control over all data transfer, just like any browser-based AI or SaaS application.

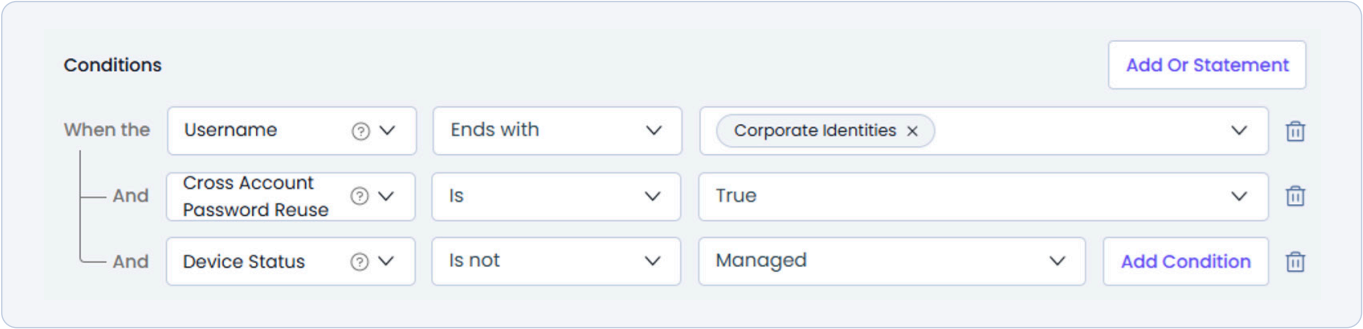
Conditional Access to Organizational SaaS Apps

LayerX integrates with organizational IdP and access management systems, meaning it can prevent access to enterprise SaaS applications by any user or device that don't have LayerX installed. This ensures that only authorized users can access sensitive applications and that all SaaS access is monitored and controlled.

Enforce Granular Last-Mile SaaS Guardrails

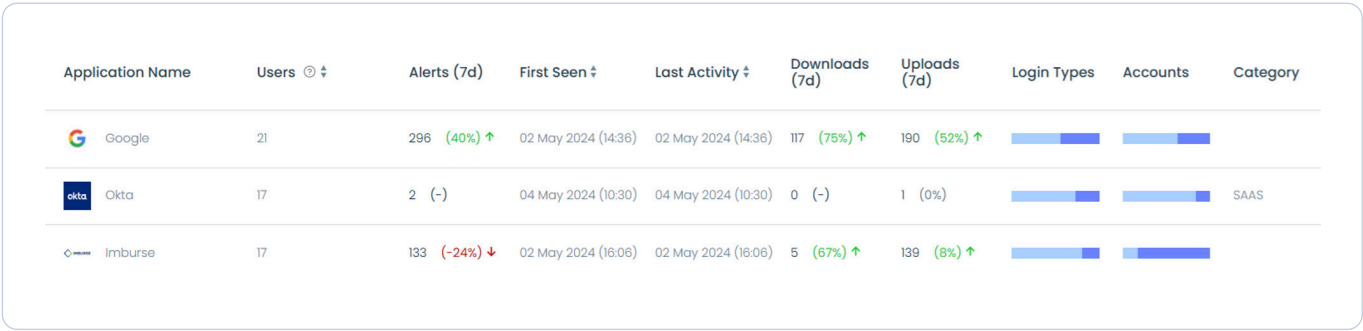
Traditional SaaS controls such as CASB or SSPM typically follow a binary enforcement approach of either fully allowing or fully blocking access to SaaS applications, and require complex API integrations for more granular controls (assuming that the application even offers them, in the first place).

LayerX, on the other hand, allows organizations to cut through connectors, interfaces, APIs, etc. and to detect and enforce directly where SaaS apps are used. Organizations can define policies based on user identity, device status, password strength, website category, and more, to create tailored policies to audit all SaaS identities, restrict personal SaaS account usage, enforce controls on unmanaged devices, and more.



Detect & Secure 'Shadow' SaaS Applications

LayerX allows organizations to map all SaaS sites and applications in your organization – and who's using them. This helps to sensitive files and data from being shared using personal accounts and/or unsanctioned apps.



Key Capabilities

Visibility

- Users
- Identities
- SaaS Apps
- Cookies
- Passwords
- 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...