

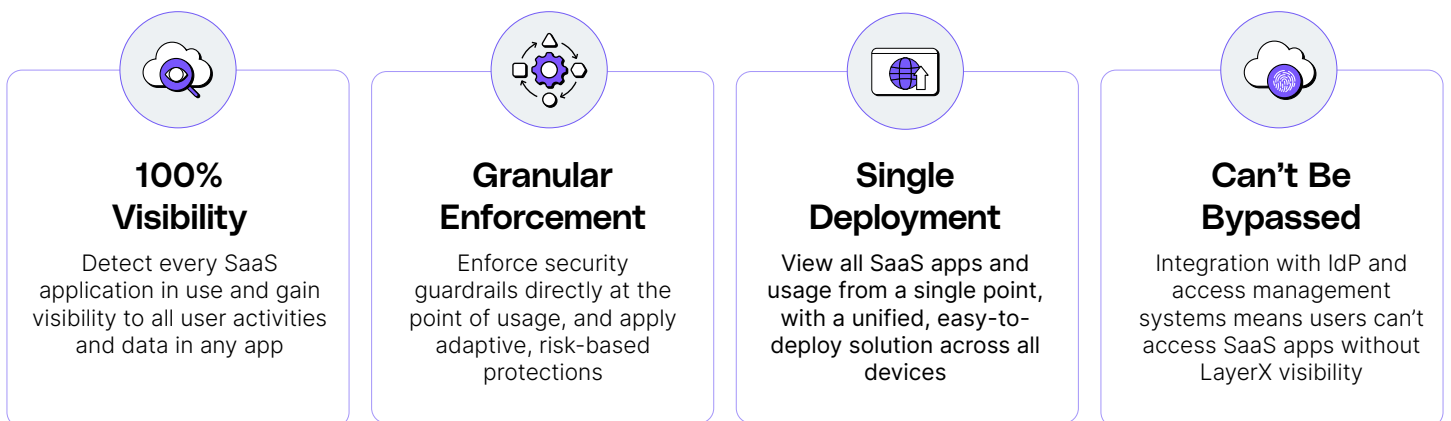


SECURE SAAS USAGE & ELIMINATE 'SHADOW' SAAS

LayerX is an all-in-one, Interaction 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.

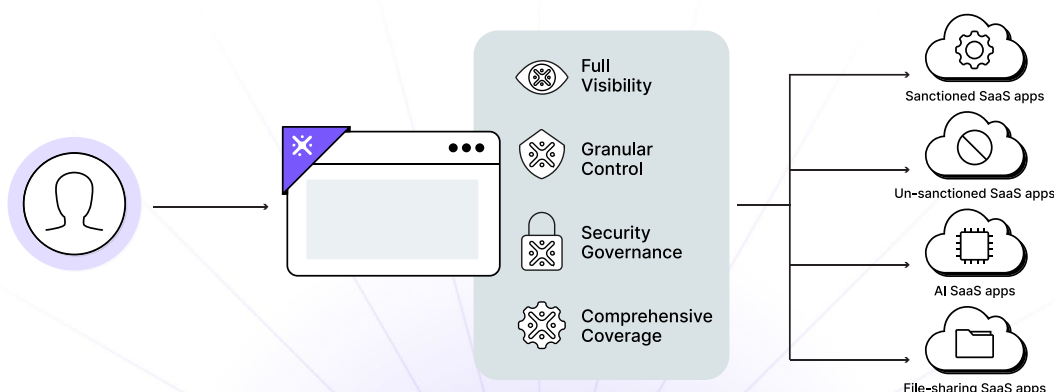
Most business applications today are deployed as SaaS solutions, meaning that SaaS security is increasingly synonymous with cyber security. However, existing solutions either lack detection and enforcement capabilities, or are incredibly complex to deploy (or both). LayerX is the only solution that detects 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



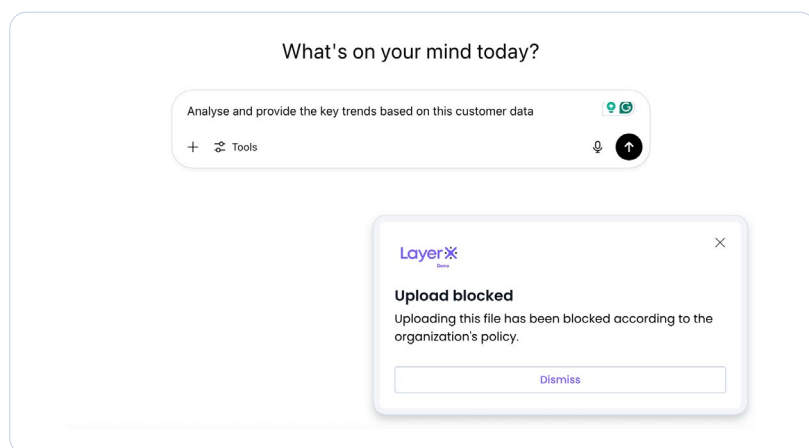
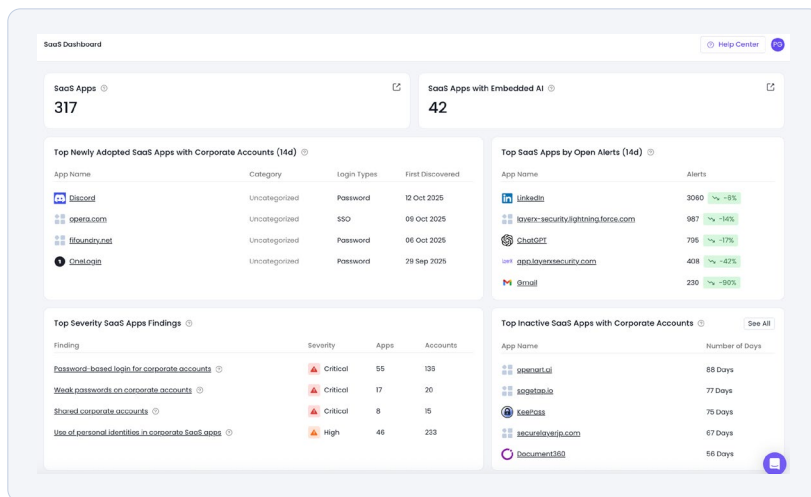
SaaS Security Requires Control at the Point of Use

Most business applications today are SaaS-based, accessed across web, desktop, and integrated environments. This makes user interaction with SaaS apps the primary control point for security and governance. Network-based solutions often lack the visibility and enforcement needed, leaving gaps that users can easily bypass. LayerX closes these gaps by delivering unified visibility and control over SaaS interactions, enforcing real-time policies to govern access, prevent misuse, and eliminate shadow SaaS exposure.



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. 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.

Conditions Add Or Statement

When the

And

And Add Condition

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 prevent sensitive files and data from being shared using personal accounts and/or unsanctioned apps.

Application Name	Users	Alerts (7d)	First Seen	Last Activity	Downloads (7d)	Uploads (7d)	Login Types	Accounts	Category
Google	21	296 (40%) ↑	02 May 2024 (14:36)	02 May 2024 (14:36)	117 (75%) ↑	190 (52%) ↑	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	
Okta	17	2 (-)	04 May 2024 (10:30)	04 May 2024 (10:30)	0 (-)	1 (0%)	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	SAAS
Imburse	17	133 (-24%) ↓	02 May 2024 (16:06)	02 May 2024 (16:06)	5 (67%) ↑	139 (8%) ↑	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div>	

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...