LayerX

STOP WEB DATA LEAKAGE AND INSIDER THREATS

LayerX is an all-in-one, agentless security platform that helps organizations prevent Web/SaaS data leakage, offering complete visibility into all user activity in the browser by monitoring all web and SaaS data transfer channels, for all users, across all browsers, on all devices **(managed / unmanaged)**, and enforces adaptive, risk-based protections to **completely** block sensitive data from being exposed.

Web channels are the #1 easiest channel for insider threats and inadvertent data leakage. Existing DLP solutions are file-centric and fail to protect data-in-motion, leaving organizations blind and exposed to sensitive data leakage. LayerX is the only solution that monitors all web and SaaS data transfer channels and enforces real-time, adaptive, risk-based protections.

Benefits of Choosing LayerX

Track All Web Data Transfer

Complete visibility into all websites and SaaS apps, tracking where your data is going and who is using it.

Prevent Sensitive File Leakage

Restrict copying files with sensitive data to external SaaS apps and unsanctioned file-sharing services

Protect File-less Data Activity

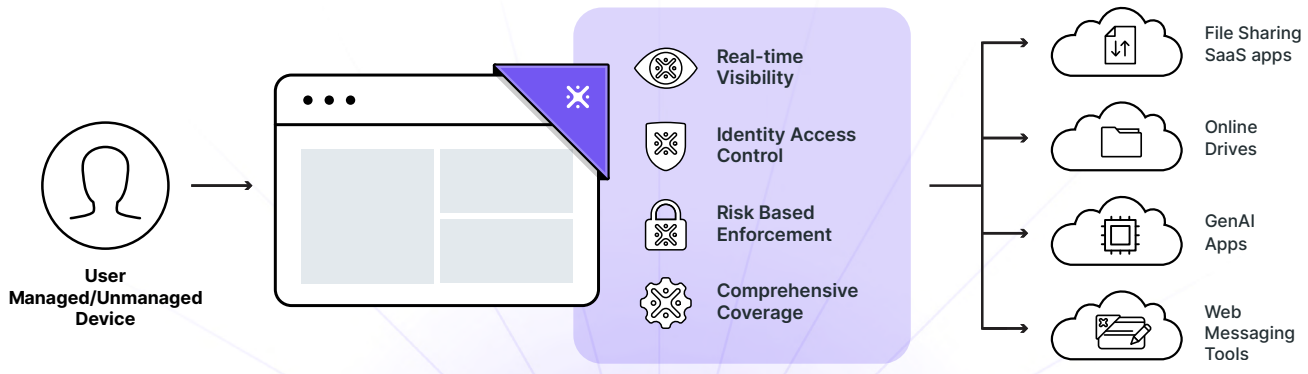
Enforce last-mile security guardrails to protect sensitive non-file data such as text input, copy/paste, etc.

Apply Identity Context

Add identity awareness to DLP logic to ensure sensitive data is accessed/shared only by verified corporate users

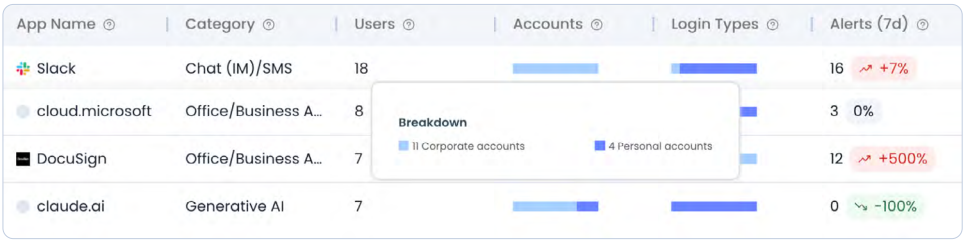
The Browser is the Main Point of Risk for Data Leakage

The browser has become the central enterprise workspace, meaning that most corporate data is created, stored, and transferred in the browser. This is why organizations need a dedicated browser-based security solution to enforce data security directly within the browser. LayerX, deployed as a browser extension, offers full visibility into all user activity and can fully enforce and govern user behavior to make sure that sensitive data doesn't leak out.



Complete Discovery of All Web/SaaS Data Transfer

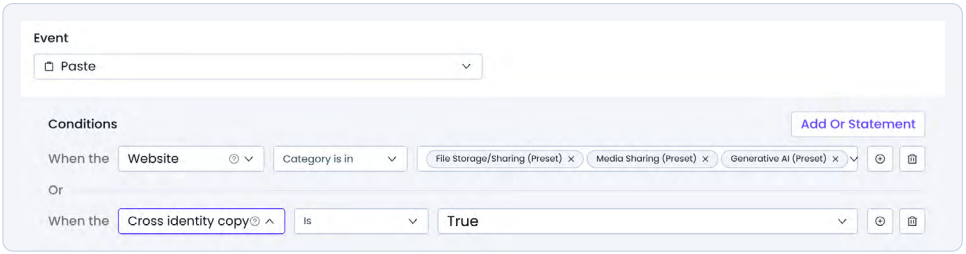
LayerX offers comprehensive visibility into Web and SaaS application usage by deploying directly as a browser extension. It monitors all user actions and activities, such as browsing, login attempts, data input, and file uploads, identifying which tools are accessed, by whom, and through which accounts (corporate or personal). This enables organizations to detect unauthorized data sharing and enforce policies to prevent data leakage to/from file-sharing SaaS applications.



Control File-based & File-less Data Transfer

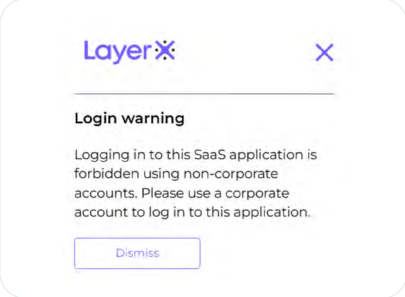
Traditional DLP and network-based solutions are file-centric and can't track data in motion. However, data on SaaS and AI apps is often not file based, using text input, copy/paste, etc., resulting in traditional DLP solutions not having any visibility into this data activity.

In contrast, LayerX monitors all user activities on all websites and SaaS applications in the browser and restricts both, file-based and file-less data transfer of sensitive corporate data. Organizations can define policies based on user identity, device status, website category, data sensitivity, etc., to create tailored security policies with a range of enforcement options, ranging from monitoring only, to warning users with customizable messages, to masking sensitive data, to completely blocking their actions.



Restrict Login and Activity on Multi-Tenant SaaS Apps

In a SaaS-first world, most organizations rely on applications that can be accessed by both non-corporate and corporate accounts. This is why restricting non-corporate account access to sensitive data is crucial. LayerX is the only solution that provides full browsing context with identity awareness and cross-identity controls, restricting login to web/SaaS file-sharing tools using non-corporate accounts, and ensuring sensitive corporate data can be accessed only by verified corporate users.



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
- Chrome / Chromium
- Edge
- Safari
- Firefox
- Windows / Mac / Linux
- Incognito mode
- And more...

Integration
- MDM
- IdP
- Access management
- Ticketing systems
- SIEM
- Data Labeling
- And more...