LayerX

Secure SaaS Identities and Detect Hidden Identity Threats

LayerX is an all-in-one, agentless security platform that helps organizations secure all web-based corporate and non-corporate identities across browsers and SaaS applications with real-time identity threat protection, identity security governance, and last-mile guardrails based on identity security parameters to prevent web vulnerabilities such as phishing, credential theft, etc.

In the world of hybrid work, the corporate identity is the new security perimeter of modern organizations. However, SaaS applications are rife with non-corporate and non-federated identities that are hidden from organizational IAM services, leaving organizations blind to identity risks and compromise. LayerX is the only solution that monitors all web-based identities and enforces real-time, adaptive, risk-based protections to secure identities against threats and misuse.

Benefits of Choosing LayerX

Discover All Identities

Complete discovery of both corporate and non-corporate identities used in web and SaaS apps

Enforce Identity Governance

Enforce security guardrails based on identity parameters such as password strength, user risk, SSO status, etc.

Prevent Identity Threats

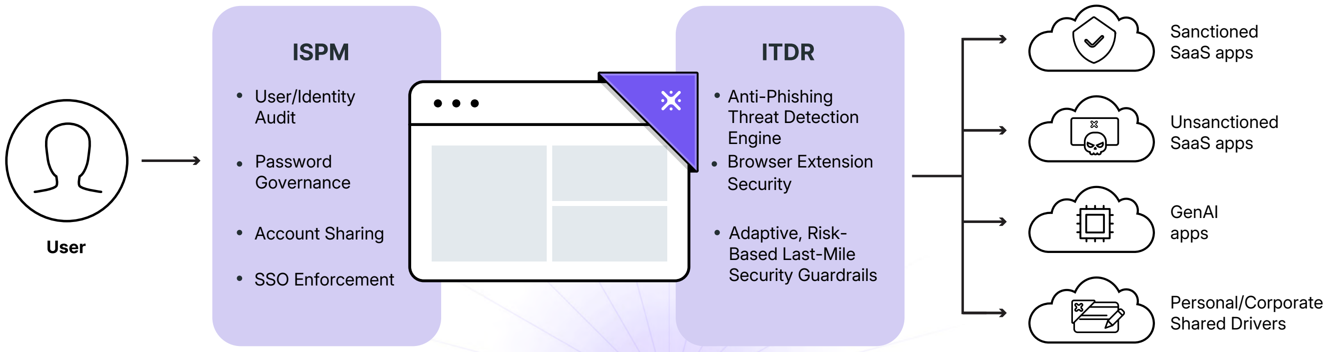
Built-in, real-time AI protection engine to stop 0-day web and phishing attacks

Protect Against Malicious Extensions

Identify and block risky browser extensions that can access user identity data

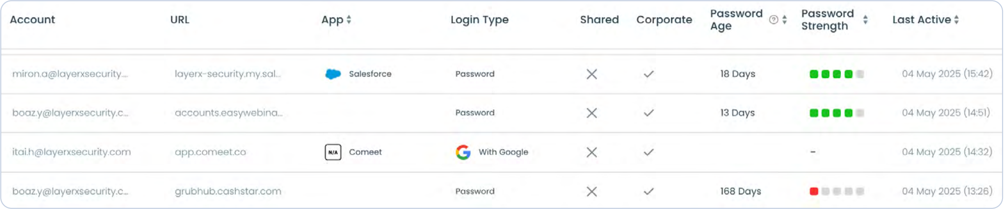
The Browser is the New Point of Risk for Hidden Identity Threats

In a SaaS-first world, shadow identities—non-corporate or non-SSO accounts—bypass IAM and IdP controls, leaving organizations exposed at a governance and threat level to risky behavior. This is why organizations need a dedicated browser-based security solution to cover Identity Security Posture Management (ISPM) and Identity Threat Detection & Response (ITDR) directly within the browser. Only LayerX, deployed directly as a browser extension, provides the visibility and control needed to manage identity posture, enforce identity governance and prevent identity threats like phishing and data exposure.


User
ISPM
User/Identity Audit
Password Governance
Account Sharing
SSO Enforcement
ITDR
Anti-Phishing Threat Detection Engine
Browser Extension Security
Adaptive, Risk-Based Last-Mile Security Guardrails
Sanctioned SaaS apps
Unsanctioned SaaS apps
GenAI apps
Personal/Corporate Shared Drivers

Complete Discovery of All Web/SaaS Identities

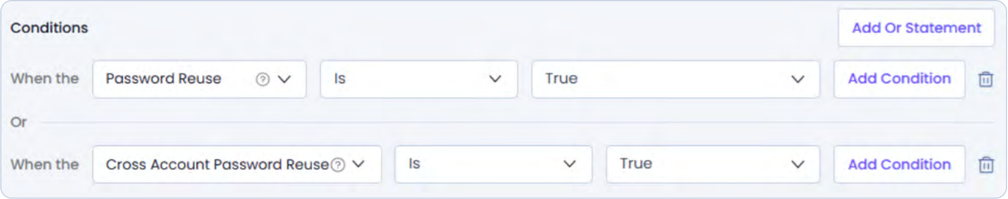
LayerX offers comprehensive visibility into Web and SaaS identities, including corporate and personal identities, as well as corporate identities not connected via SSO and not visible to organizational IdP systems. This enables organizations to detect all shadow identities within the organization and enforce risk-based restrictions on their usage.



Account	URL	App	Login Type	Shared	Corporate	Password Age	Password Strength	Last Active
miron.a@layerxsecurity...	layerx-security.my.sal...	Salesforce	Password	✕	✓	18 Days	🟩🟩🟩🟩⬜	04 May 2025 (15:42)
boaz.y@layerxsecurity.c...	accounts.easywebina...		Password	✕	✓	13 Days	🟩🟩🟩🟩⬜	04 May 2025 (14:51)
itai.h@layerxsecurity.com	app.comeet.co	Comeet	With Google	✕	✓		-	04 May 2025 (14:32)
boaz.y@layerxsecurity.c...	grubhub.cashstar.com		Password	✕	✓	168 Days	🟥⬜⬜⬜⬜	04 May 2025 (13:26)

Enforce Last-Mile User Guardrails Based on Identity Security Parameters

With LayerX, organizations can apply identity governance controls over all identities – both corporate and non-corporate - and enforce password strength rules, identify and restrict cross-account password re-use, detect and prevent account sharing, enforce SSO usage on all corporate identities, audit and control OAuth permissions, and more. Organizations can define policies based on user identity, device status, 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 completely blocking their actions.



Conditions

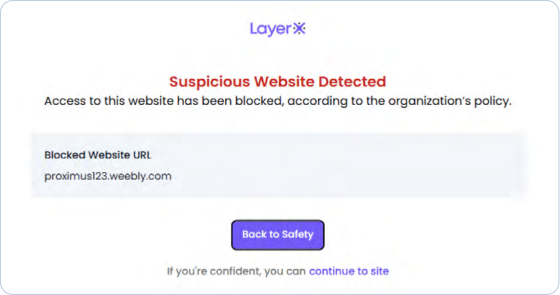
When the Password Reuse Is True

Or

When the Cross Account Password Reuse Is True

Block External Identity Threats: Zero-day Phishing and Risky Extensions

Phishing and malicious browser extensions are prime drivers for identity attacks and credential theft. Existing solutions cannot enforce security controls directly in the browser, leaving organisations exposed to browser-based identity vulnerabilities. LayerX provides multiple layers of real-time protection to protect against external identity threats. LayerX protects against external web vulnerabilities with a built-in AI-based analysis engine that scans every code element on every web page and SaaS application in real-time to block risky websites. In addition, LayerX protects against malicious browser extensions that can steal user identity data with comprehensive audit and discovery of all extensions, automatic risk assessment of extensions, and adaptive security policies to block risky extensions.



LayerX

Suspicious Website Detected

Access to this website has been blocked, according to the organization's policy.

Blocked Website URL

proximus123.weebly.com

If you're confident, you can continue to site

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...