PROTECT AGAINST WEB VULNERABILITIES WITHOUT DISRUPTING THE USER EXPERIENCE

LayerX is an all-in-one, agentless security platform that protects organizations against web vulnerabilities such as compromised websites, phishing, and malware, using real-time, AI-based protections to detect and block threats in real time, without breaking websites or impacting the user's browsing experience

The browser is the main point of work of modern enterprises, meaning it is also the main point of risk for web vulnerabilities. Traditional solutions like RBI address web security by executing web page code in remote containerized environments and streaming results to users. However, that leads to high latency, broken web pages, and poor user experience. LayerX is the only solution that protects against malicious sites and web vulnerabilities by enforcing last-mile, adaptive, risk-based protections without impacting the user experience or adding management overhead.

Benefits of Choosing LayerX

0-hour Web Protection

Secure all browsing activity with real-time, AI-based protection against all web-based attacks, including phishing, malware, adware, etc.

Last-Mile User Guardrails

Adaptive policy controls to enforce risk-based guardrails on any user activity or data in the browser

Works On Every Website

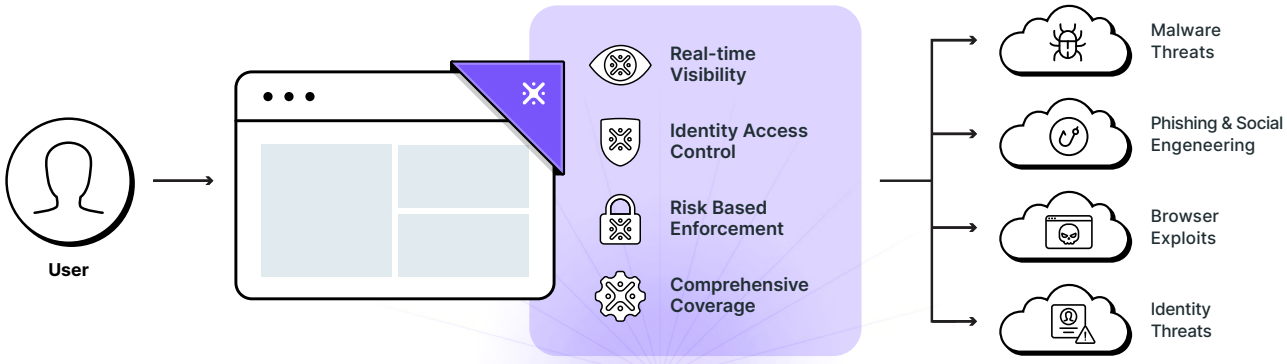
Protect all websites without breaking JS-rich webpages and maintaining the user browsing experience

0% User Friction

Protect users while browsing the web without adding latency or imposing frustrating browsing limitations

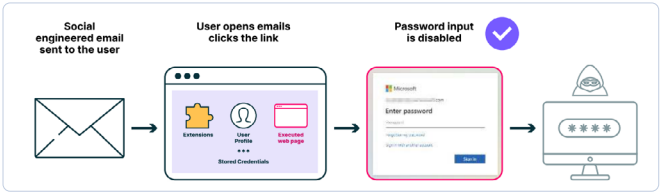
Secure Browsing is More Than Just Malware

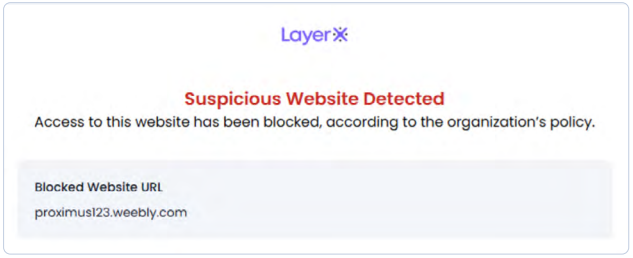
The browser is the primary gateway to the web and its prime point of risk. However, while traditional security tools focus primarily on malware and CVEs, modern web protection is more than just malware. RBI and SWG solutions help block malicious websites but don't address major use cases such as identity protection, phishing, and data leakage. Today's threat landscape needs a solution that addresses all web threats—from malware and phishing to identity theft and web exploits. LayerX is the only solution that provides that coverage across all security use-cases, users, browsers, and devices, with no additional latency or disruption to the browsing experience.



Prevent Against All Web Vulnerabilities, Exploits, and Phishing Attacks

LayerX delivers advanced phishing protection through full visibility into browsing activity, prevention of password reuse, and real-time blocking of malicious websites without disrupting the user experience. LayerX employs a dual-layer AI engine that inspects more than 250 parameters on every page, and combines local browser activity analysis with global web intelligence to enhance its phishing detection capabilities. This real-time risk analysis works together with advanced URL filtering and deep code inspection to block phishing sites and stop user interaction with malicious web pages.



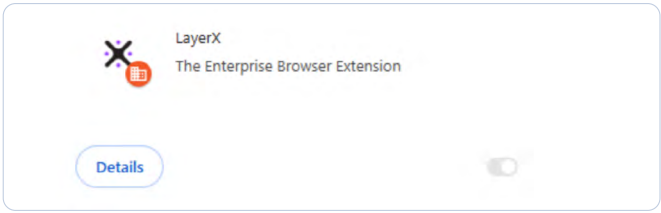


Protect Any Website without Disrupting the User Experience

Existing solutions like RBI can protect websites as they execute web page code in a containerized remote environment, but are very slow, disrupt user experience and break complex websites, leading to frustration amongst users. Since LayerX is deployed directly within the browser, it can protect against external web vulnerabilities in real-time, without making changes to page rendering or disrupting the native browsing experience. This enables users to continue browsing normally, even on JS-rich or multimedia-heavy websites, with no interruption or added latency.

Prevent User Bypass with Robust Anti-Tampering Capabilities

LayerX extension is resilient to malware-based tampering or user modification. It includes multiple layers of robust anti-tampering features to ensure that LayerX can't be disabled, uninstalled or bypassed by users, with coverage also of Incognito/Private mode, etc. This means that security teams can enforce policies consistently across all browsing environments, reduce the risk of human error or malicious intent, and ensure continuous protection and compliance without relying on end-user cooperation.



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...