

# PROTECT AGAINST MALICIOUS BROWSER EXTENSIONS

LayerX is an all-in-one, agentless AI and Browser security platform security platform that protects organizations against risky browser extensions, offering complete visibility to all extensions installed in the organization, detailed risk classification, real-time usage and behavior analysis of each extension, and adaptive risk-based enforcement options.

Malicious browser extensions are the biggest security threat that most security teams don't know about. Browser extensions are ubiquitous in modern web browsing. However, they are routinely granted extensive access permissions to sensitive data such as user identities, cookies, passwords, user input, and more, putting users and organizations at risk of data leakage or credential theft.

## Benefits of Choosing LayerX



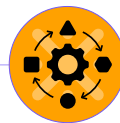
### Comprehensive Audit

Discover all extensions on all browsers for all users, with full visibility and control



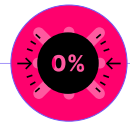
### Rich Risk Classification

Assess the risk profile of each extension using internal and external risk factors



### Adaptive Enforcement

Go beyond manual blocklists to automatically disable or block extensions based on their risk



### 0% User Friction

Easy deployment with no impact on the user browsing experience or existing workflows

## Comprehensive Risk Scoring

LayerX identifies risky browser extensions using a comprehensive risk-scoring approach that combines internal and external risk factors. LayerX examines the access permissions requested by each extension and whether it has access to sensitive information such as passwords, cookies, user input, and more. At the same time, LayerX analyzes the extension's reputation based on external factors such as user rating, number of downloads, age, and more. These parameters are combined to create a unified score reflecting each extension's risk.

### Permission Scope

- Network access
- Cookie access
- Web navigation
- Storage access
- Identity access
- and more...

### Risk Score

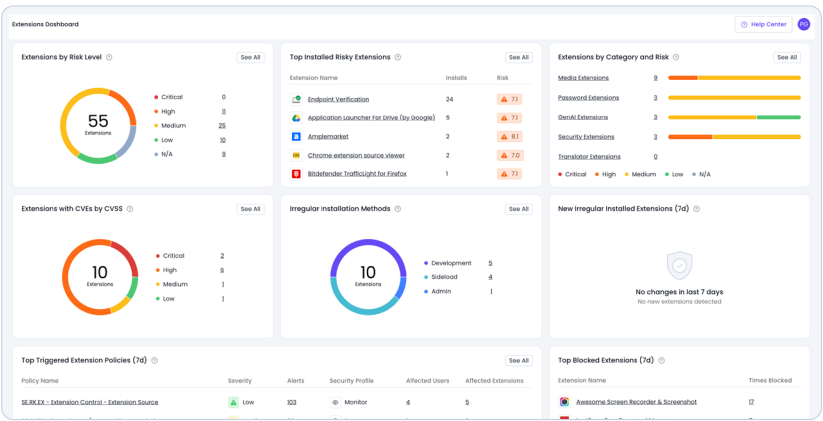
### Extension Reputation

- Total downloads
- Last updated
- Install type
- Publisher
- Rating
- and more...

# All Extension Risks in A Single View

LayerX offers a powerful Extension Security Dashboard that gives security teams centralized, real-time visibility into all browser extensions across the organization. The dashboard surfaces detailed inventory, risk scores, usage trends, and critical security alerts, enabling rapid detection of malicious or vulnerable extensions.

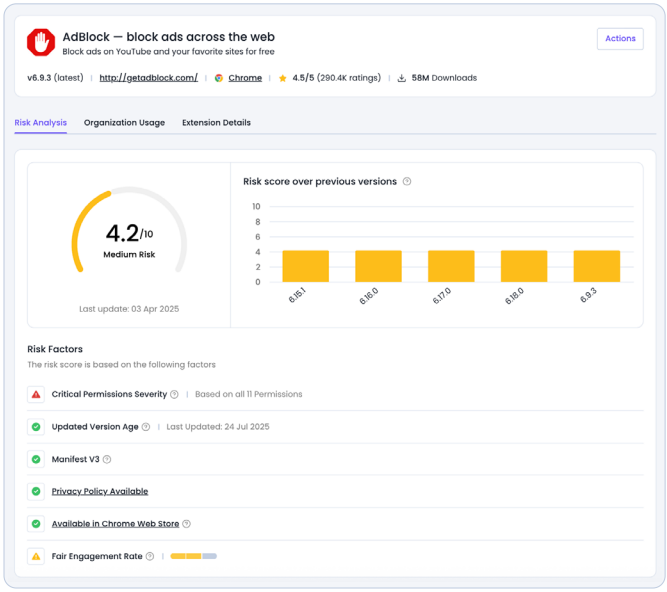
With built-in granular policy enforcement options available, security teams can block or allow extensions based on risk, ensuring streamlined control without disrupting productivity.



# Analyze the Risk of Any Extension with ExtensionPedia

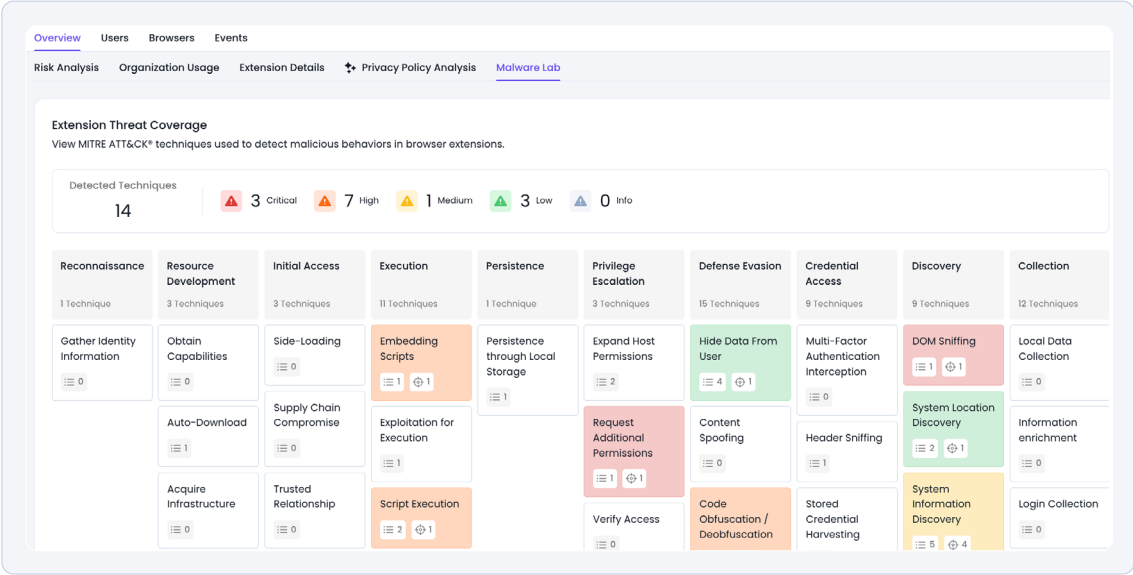
In the past, security teams had to install browser extensions in a controlled environment to evaluate their risk. With LayerX's ExtensionPedia, organizations can assess any extension, whether it's installed or not, using detailed risk profiles, permission analysis, developer reputation, and risk scoring.

This empowers security teams and enables proactive, effort-free evaluation of risky extensions before they ever reach the enterprise environment.



# Real-Time Extension Threat Analysis with MalwareLab

LayerX MalwareLab provides real-time analysis of browser extensions based on actual runtime behavior, not just static metadata or permissions. By executing extensions in a protected sandbox and analyzing real traffic, MalwareLab detects malicious actions as they occur, including behavior changes introduced in new versions. Detected activity is mapped to a dedicated MITRE-based framework for extension threats, giving security teams clear, actionable insight into extension risk that static analysis alone cannot uncover.



# Key Capabilities of LayerX

## Enforce Extension Security on Any Browser

LayerX is deployed a browser extension, allowing for seamless, unintrusive deployment that does not impact the user experience. LayerX supports all major commercial browsers, as well as any Chromium-based browser, thereby enabling LayerX to enforce browser and extension security on any browser, operating system, or device.



Cookies: Gives your extension access to the cookies API.

Critical

NativeMessaging: Gives your extension access to the native messaging API.

Medium

Storage: Gives your extension access to the storage API.

Medium

Enterprise.platformKeys: Gives your extension access to the enterprise.platformKeys API.

Low

Identity: Gives your extension access to the identity API.

Low

PlatformKeys: Gives your extension access to the platformkeys API.

Low

## Granular, Risk-Based Enforcement Options

Unlike other solutions that enforce extension security using manual blocklists based on the extension ID, LayerX offers an automated approach based on the risk classification of each extension.

These risk indicators are used in creating adaptive, risk-based enforcement policies, allowing organizations to create tailored security policies with a range of enforcement options ranging from monitoring only, to warning users with customizable messages, to outright disabling existing extensions or preventing the installation of new ones.

## Complete Visibility of Extension Installations and Usage

LayerX provides visibility to all extensions installed in the organization across all browsers, devices, and users. The LayerX management console displays key information about each extension, such as the extension's users, permission scope, category, installation type, source, and more. This allows security and IT managers to get a full view of all existing and new extensions and whether they need to address any extension security issues.

Extension Name	Tags	Users	Total Downloads	Permissions	Permissions Scope	Install Type	Status	Version Age	Store
Google Docs Offline		16	10M	4	High	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	Chrome
Endpoint Verification	ExtensionAllowList	14	4M	6	Critical	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	Chrome
Application Launcher Fo...		9	84M	1	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	Chrome
Salesforce	ExtensionAllowList	8	400k	4	Critical	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	Chrome
Amplemarket	Approved file sharing sites +1	7	6k	5	Critical	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	Chrome