LayerX

Enterprise Browser Extension Security Report 2026

Real-world data on extension usage in enterprise environments and the rising risk of AI browser extensions

Introduction

Browser extensions are everywhere. Even within enterprise environments, extension usage is ubiquitous across organizations of every size. Moreover, the explosion in AI usage in enterprises has led to the emergence of a new class of AI extensions, some even with agentic capabilities that can take action on behalf of the user. This creates a new class of security concerns, both from an extension security perspective and an AI perspective.

The problem, however, is that most enterprises have no idea who's using extensions in their environment, what extensions they have, or what capabilities these extensions can access.

This research fills this gap: it provides hard data on browser extensions in the enterprise, based on real-life telemetry collected from LayerX's customer base. In particular, this research focuses specifically on AI extensions to help organizations manage their browser extension risk as part of managing their AI governance and usage controls.

What Makes LayerX's Data Unique

LayerX's data set is unique because of where we collect our data and who we collect it from. LayerX is deployed on over 1 million devices in enterprise environments, meaning that LayerX has unparalleled visibility to user activity and behavior. This allows us to gain comprehensive insights into the usage of browser extensions and AI extensions. Moreover, LayerX's customer base is comprised entirely of enterprises, meaning that the insights we collect are specific to enterprise users and organizations.

Executive Summary

#1

Even Though Extensions Usage Flies Under the Radar, Nearly Every Employee Uses Them, Creating an Enterprise-Wide Attack Surface

99% of enterprise users run at least one extension, with more than one-in-four enterprise users having even 10+ installed extensions. This means that the extension risk surface is practically everyone.

#2

AI Extensions Have Become The AI Consumption Channel Nobody Talks About

AI extensions are rapidly emerging as a primary way employees interact with AI tools. Adoption is already widespread, with 1-in-6 enterprise users already using at least one AI extension. These extensions create a new and largely ungoverned channel for AI usage, where sensitive data can be accessed, processed, or transmitted without visibility or control.

#3

AI Extensions Are Disproportionately More Risky Than Most Extensions

AI extensions are now among the fastest-growing categories, with 17% of enterprise users already adopting them. However, they also show a significantly more dangerous risk profile: AI extensions are 60% more likely to have a CVE than average, 3x more likely to have access to cookies, 2.5x more likely to have scripting permissions, and 2x more likely to be able to manipulate browser tabs. This combination of fast adoption, elevated access, and weak governance makes AI extensions an urgent emerging threat vector.

CISO's Recommendations

Continuous audit of all browser extensions across every browser, device, and user

With 99% of enterprise users running at least one extension, a full inventory is a mandatory first step toward risk reduction. CISOs should require an organization-wide extension audit covering all browsers, managed and unmanaged endpoints, across all users. Without comprehensive visibility, organizations cannot accurately assess their extension threat surface nor detect high-risk or unauthorized installations.

Implement strict, risk-adaptive policies focused on AI extensions

AI extensions represent an outsized risk due to their elevated permissions that can expose SaaS sessions, identities, and sensitive in-browser data. CISOs should enforce targeted guardrails and continuous monitoring of AI-related extensions before these tools can interact with enterprise environments.

Don't stop with static parameter assessment; actively analyze extension behavior

Browser extensions aren't static. They change hands, get updated, and sometimes stop being maintained altogether. That makes their trustworthiness a moving target. CISOs should keep a close, ongoing eye on who's behind each extension, how often it's updated, and whether it has clear signals of transparency like a privacy policy or stable ownership. When an extension starts showing unclear origins, inconsistent maintenance, or sudden changes, it should be flagged and automatically restricted or removed before it becomes a pathway for malicious updates or supply-chain attacks.

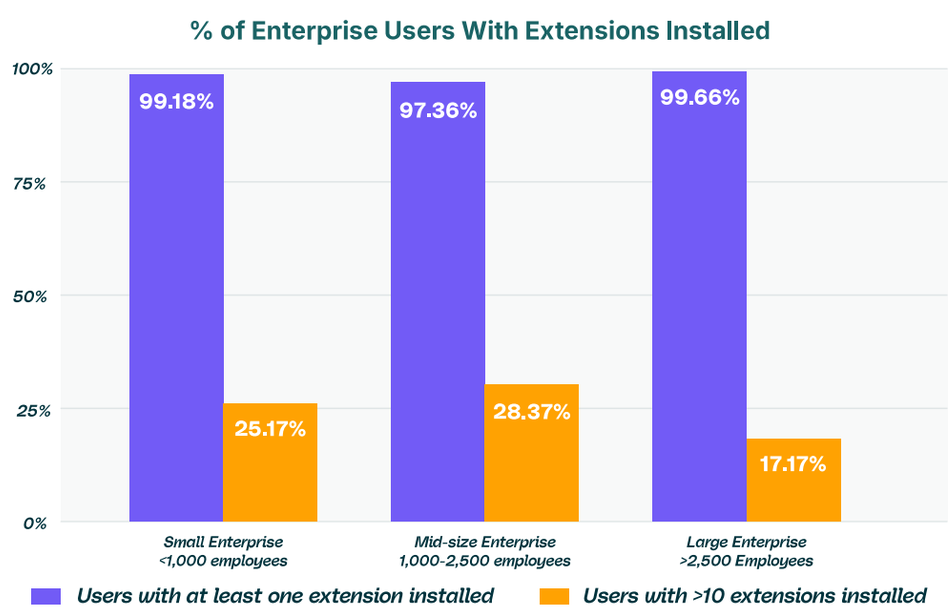
Extensions Are Everywhere

> The overwhelming majority of users in enterprise environments have extensions installed on their endpoints. Do you have a full picture of your extension threat surface?

99% of enterprise users have extensions installed. These figures are almost identical across organizations of different sizes: 99% of users in small-to-medium (SME) organizations, 97% in mid-sized enterprises, and 99.66% in larger enterprises.

Moreover, many enterprise users have a large number of browser extensions installed. In small and medium-sized organizations, more than 1-in-4 users have over 10 extensions installed, while even in large enterprises, about 1-in-6 users exceed that number.

While the rates of overall installation of extensions across organizations are fairly similar, users at large enterprises are less likely to have large numbers of extensions. This is probably due to stricter organizational policies that limit the installation of extensions on corporate devices.

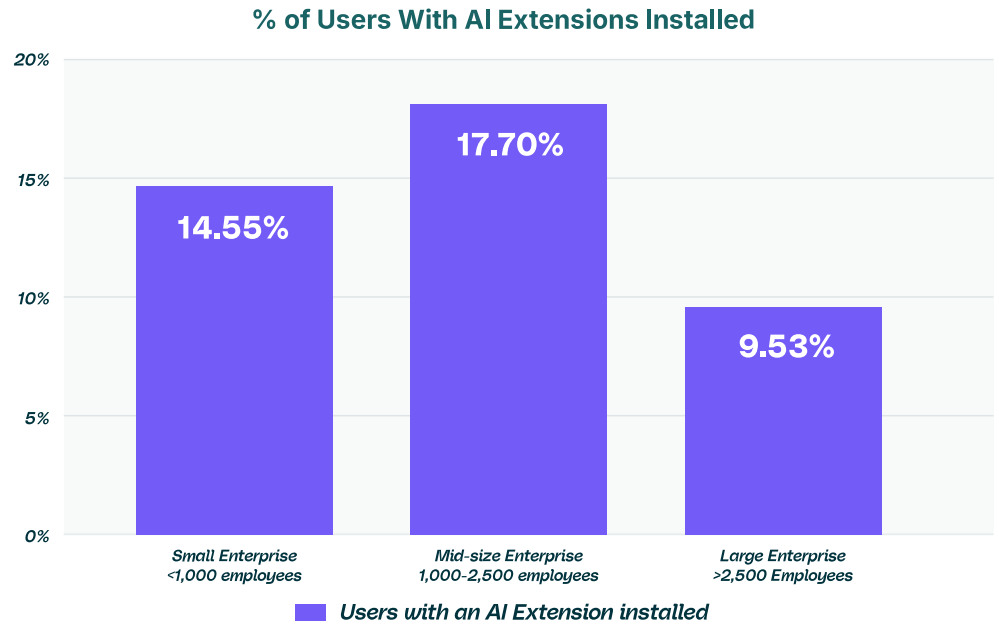


Why it matters: Extensions are everywhere, in every organization of every size. This means that extension security isn't a niche IT concern anymore; it is a significant security threat surface for enterprises.

AI Extensions Are Becoming a New Channel for AI Usage

AI extensions adoption is accelerating across enterprises, becoming a key access point for interacting with AI services.

AI extension usage is emerging across enterprises, with small and mid-size organizations showing the highest adoption, about 1-in-6 users run at least one AI extension. Similar to overall extension usage, we see lower rates of AI extension deployments in larger enterprises, again probably due to stricter security policies.

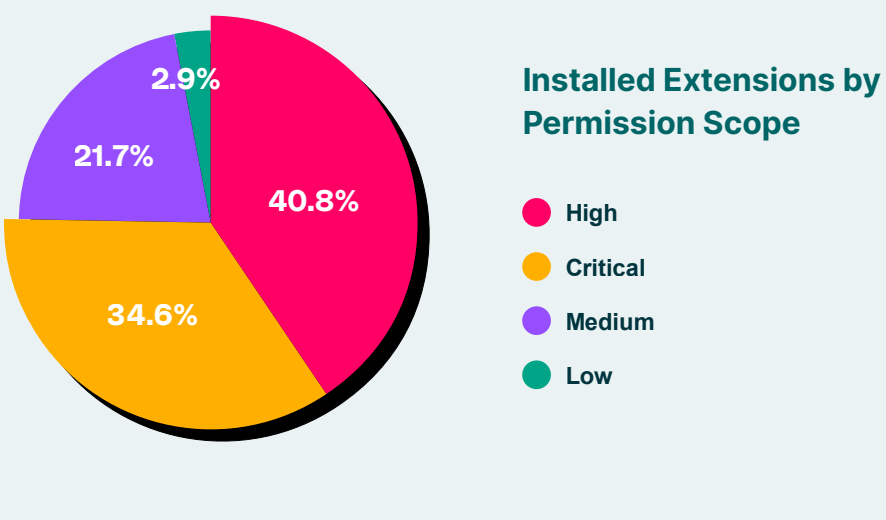


Why it matters: AI extensions are now one of the fastest-growing extension categories that can access sensitive data, capture user inputs, or transmit information to unknown LLM providers, introducing both data leakage and extension supply chain risks.

Most Extensions Have Extensive Access to Sensitive Data

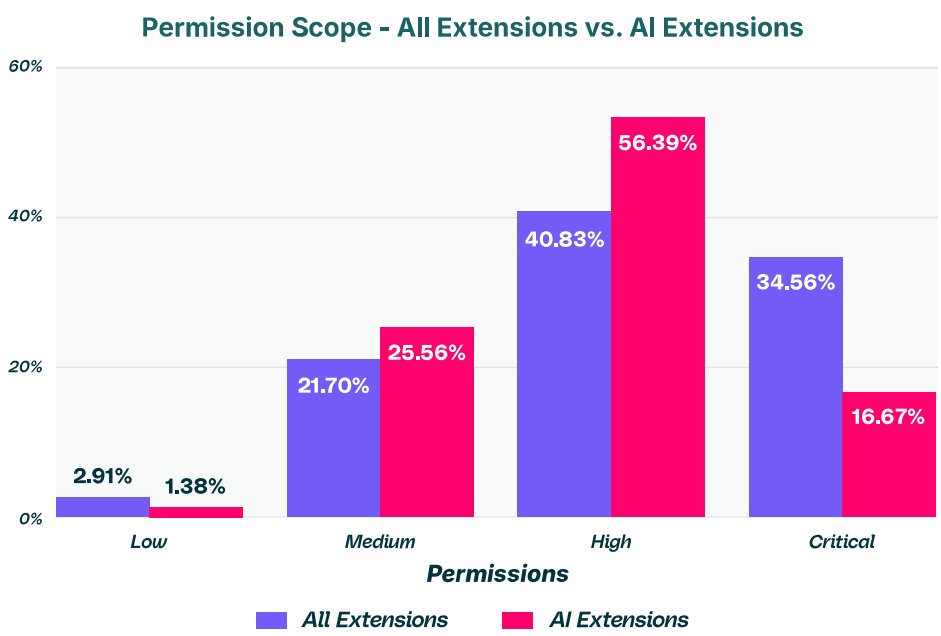
> Most extensions request elevated permissions, and AI extensions request them even more frequently, expanding the potential attack surface inside the browser.

Nearly 75% of browser extensions request high or critical permission levels (40.83% high, 34.56% critical), while only 2.9% operate with low permissions.



Over one-third of all browser extensions have critical permissions, and another 40% of all extensions have ‘high’ permission scope. When comparing AI extensions to all extensions, AI extensions have higher rates of ‘high’ permission scope compared to average (56% vs. 40%), but a lower proportions of ‘critical’ permissions (16% vs. 34%). Altogether, over 75% of extensions have high or critical permissions scope, while AI extensions have a slightly lower rate, at approximately 73% having High or Critical permission scope.

Only 21% of all extensions have medium-level permissions scope, and less than 3% of all extensions can operate with ‘low’ permissions.

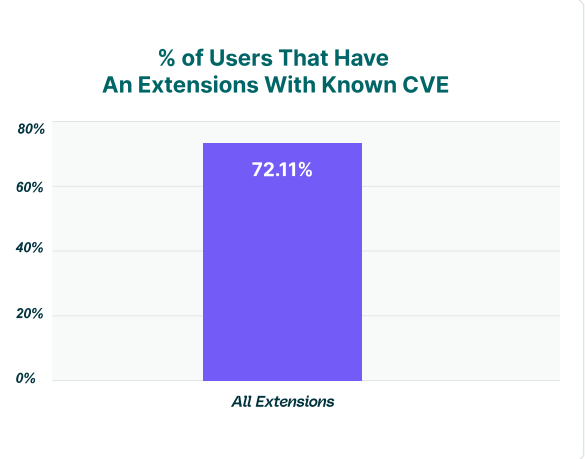


Why it matters: Extensions with elevated permissions can access sensitive browser data and user activity, which means a malicious or compromised extension could easily expose sensitive information or take over user sessions.

AI Extensions Are More Risky

> AI extensions carry a significantly higher risk profile with greater exposure to vulnerabilities and elevated permissions, increasing the risk of data exposure and misuse.

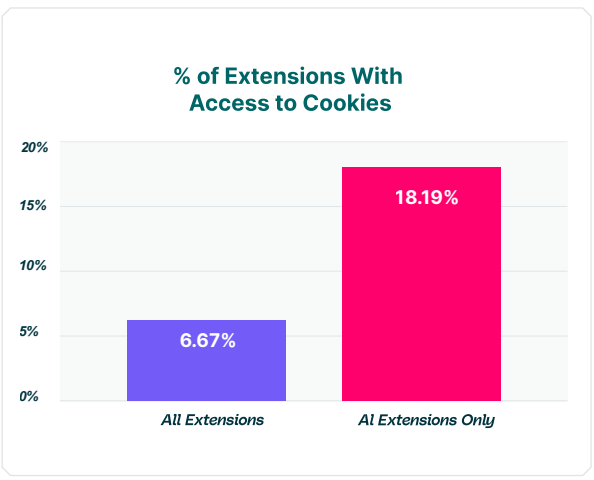
AI extensions show a higher security risk profile. 16.31% of AI extensions have known CVEs, compared to 10.8% across all extensions. Looking at it from a user perspective, 72% of all enterprise users have at least one browser extension with a known CVE.

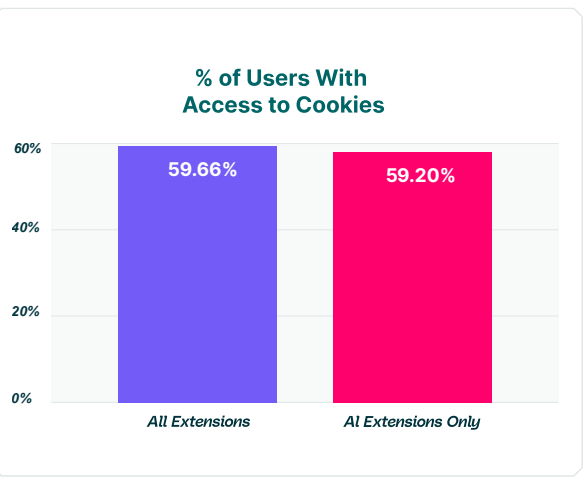


Why it matters: The higher CVE rate in AI extensions means that they require stricter vetting, monitoring, and management before being deployed in enterprise environments. While overall user CVE exposure remains widespread across all extensions, the low user count for AI extensions could be driven by maintenance trends, where older, less frequently updated extensions accumulate more CVEs, while newer AI extensions are typically updated more actively.

AI extensions consistently request far more powerful and sensitive permissions than the average extension. This means that they introduce higher privacy, security, and data-access risks and require stricter governance, review, and ongoing monitoring in enterprise environments.

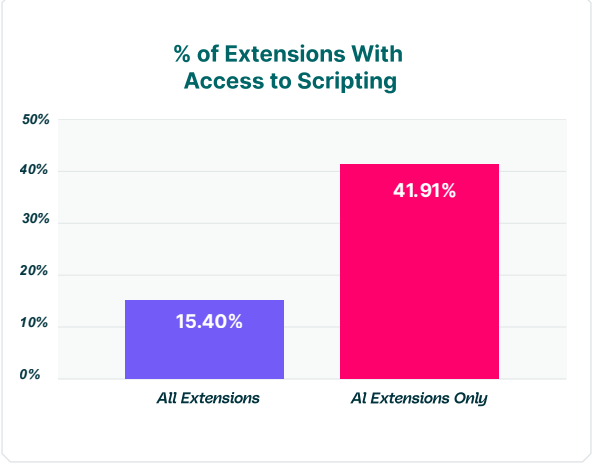
AI extensions are nearly 3x more likely to request cookie access than the average browser extension. However, overall exposure remains high, with around 60% of users having at least one extension with cookie access across both AI and non-AI extensions.

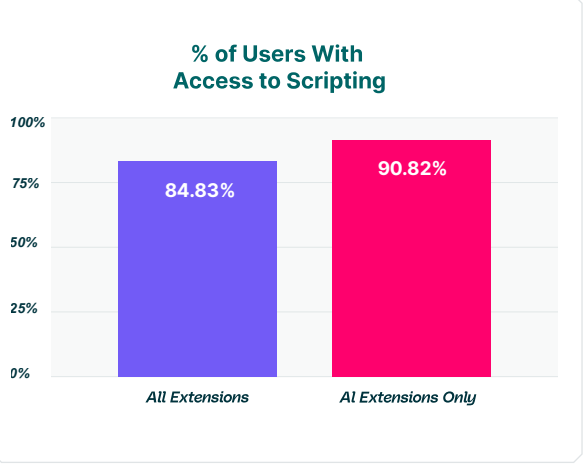




Why it matters: Cookie access can expose session tokens and authentication data, increasing the risk of account takeover or unauthorized access especially given how widespread this exposure is across users.

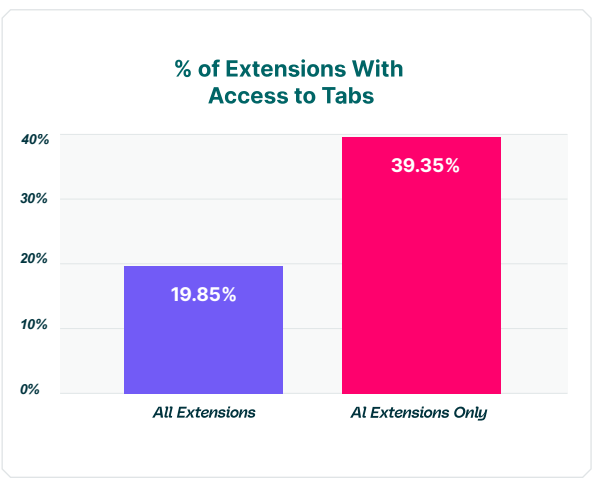
41.91% of AI extensions request scripting access, compared to 15.4% of all extensions. This means that AI extensions are 2.5x more likely than average to have the ability to execute scripts. At the same time, over 84% of users have at least one extension with scripting access,with this figure rising up to over 90% of users of AI extensions highlighting broad, organization-wide exposure.

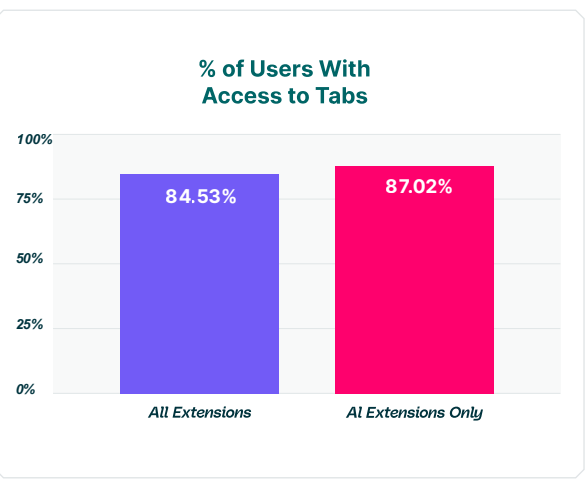




Why it matters: Scripting permissions allow extensions to inject code into web pages, enabling activities like capturing inputs, manipulating content, or extracting sensitive data by manipulating web pages, making this near-universal exposure a significant and high-impact risk.

AI extensions are nearly 2x more likely to request tab access than the average browser extension. At the same time, over 84% of users have at least one extension with tabs access, rising to over 87% for AI extensions.





Why it matters: Tab access allows extensions to manage browser tabs, including creating, updating, and removing them. With more than 84% of users exposed, tab access becomes a high-impact risk enabling malicious extensions to monitor sensitive browsing activity, track behavior or redirect users to malicious or phishing sites without their awareness.

Browsers Extensions Are Evolving Entities; They Don't Stay Static

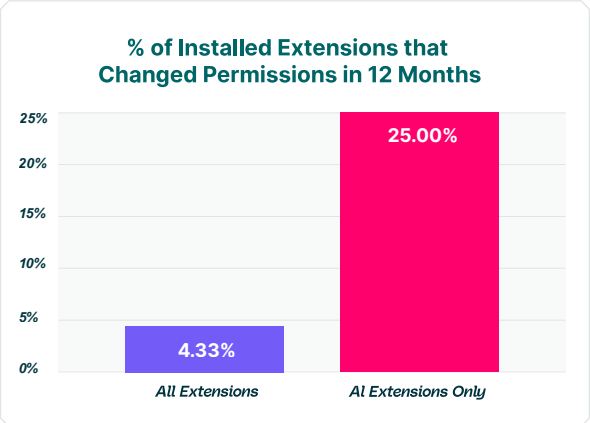
> AI extensions are far more likely to change permissions over time, significantly increasing their risk profile post-installation

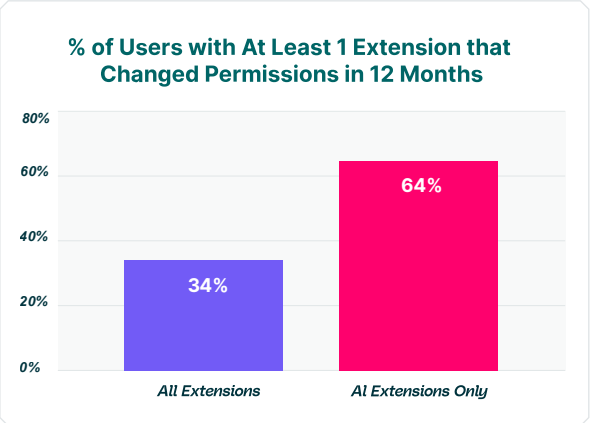
One of the common misconceptions regarding browser extensions is that their deployment is one-and-done; that once you installed them, they stay the same for their entire lifecycle.

In practice, extensions, even in enterprise environments, change and evolve over time, often without users being aware of it.

According to the data, 4.33% of extensions installed in enterprise environments changed their permissions over the last 12 months. However, when it comes to AI extensions, this figure jumps to 25%.

64% of users have at least one AI extension installed that changed its permissions in the past 12 months, compared to 34% of users across all extensions.





Why it matters: Permission changes can introduce new capabilities after installation, meaning an extension that initially seemed safe may later gain access to sensitive data without users realizing it. AI extensions are nearly 6x more likely to change or expand their permissions, and almost twice as many users have at least one AI extension that has done so, making them a significantly higher and constantly evolving risk.

The Extension Ecosystem Is Built On Weak Trust Signals

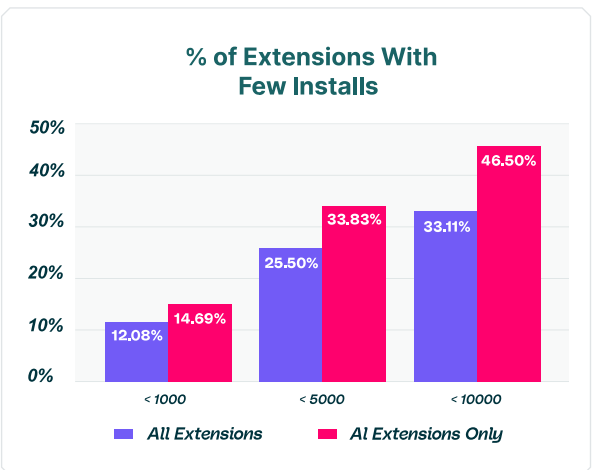
> Low number of users, missing privacy policies, and outdated code lead to widespread trust and transparency gaps in the browser extension ecosystem.

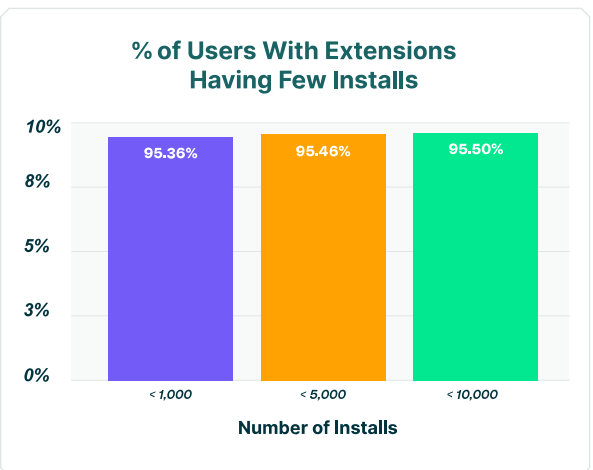
When it comes to extension security, there are various parameters that, of themselves, do not indicate malicious intent, but can be indicators of trustworthiness or reputation. Most extensions, even in enterprise environments, fail on these parameters.

Even in enterprise environments, more than 10% of all extensions have fewer than 1,000 users, a quarter have fewer than 5,000 users, and a third have fewer than 10,000 installations.

When it comes to AI extensions, the situation is even more dire, with almost 15% having fewer than 1,000 installations, a third having less than 5,000 deployments, and nearly half (46.5%) having fewer than 10,000 users.

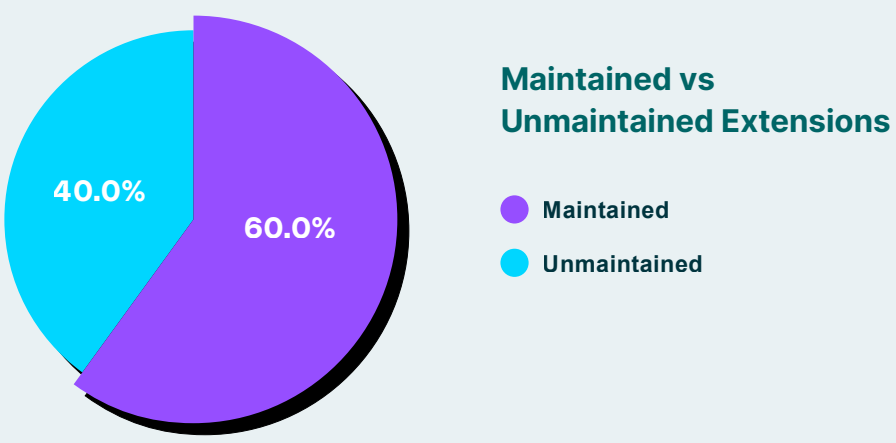
A whopping 95% of enterprise users have installed a browser extensions with less than 1,000 users.

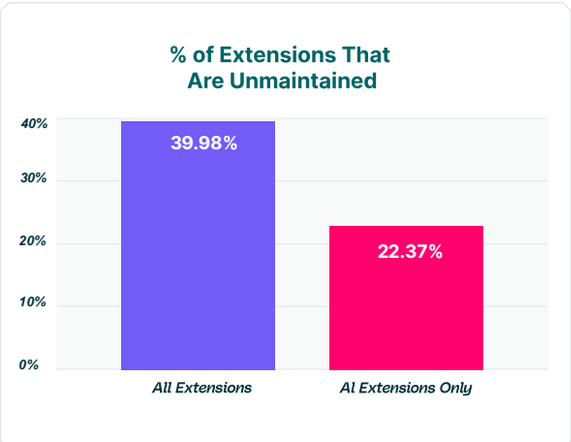


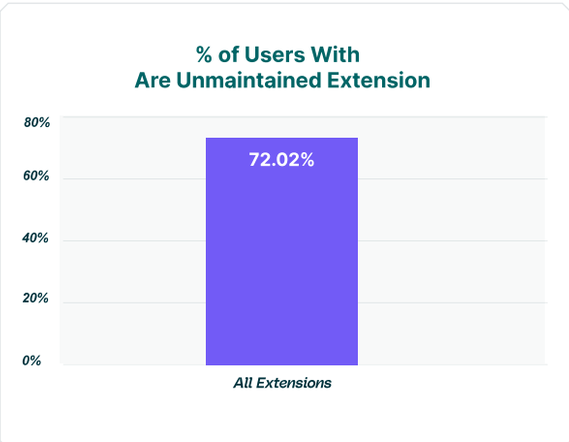


Why it matters: Since reputation is often a by-product of user base, a low install base means that for a significant number of extensions it is difficult to establish reputation with any meaningful certainty. While a low install count doesn't automatically make an extension untrustworthy, it can signal that the extension is abandoned, unvetted, or created by an unknown or potentially malicious publisher.

Extension age is another indicator of its trustworthiness. Ideally, from a reputation standpoint, we want extensions that are not completely new (and we have information on them), but also those that receive regular updates (so they are not left unmaintained). Unmaintained extensions are those that haven't been updated in over a year. Around 40% of all extensions are unmaintained, while only about 22% of AI extensions fall into this category. Moreover, 72% of all users have at least one extension that is not maintained. However, only 2.7% of users have an AI extension that is not maintained. The lower rate of unmaintained AI extensions is somewhat expected, since such extensions tend to be newer (and with a higher hype factor) and therefore tend to still be under active development. The lower rate of unmaintained AI extensions is somewhat expected, since such extensions tend to be newer (and with a higher hype factor) and therefore tend to still be under active development.

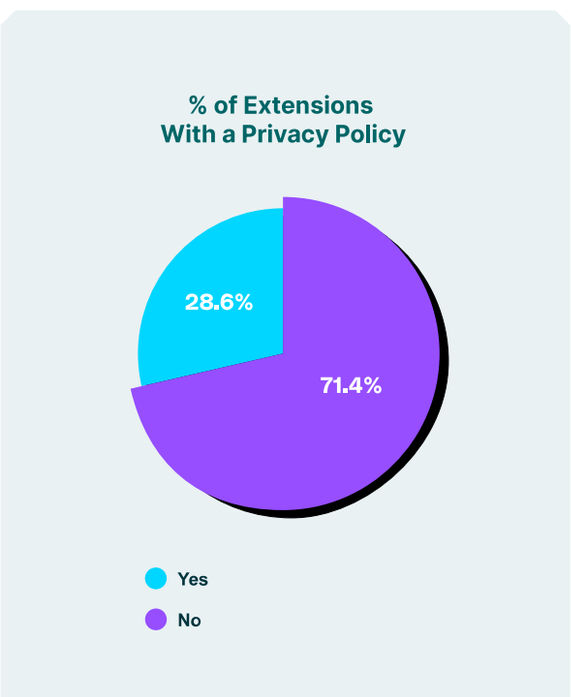


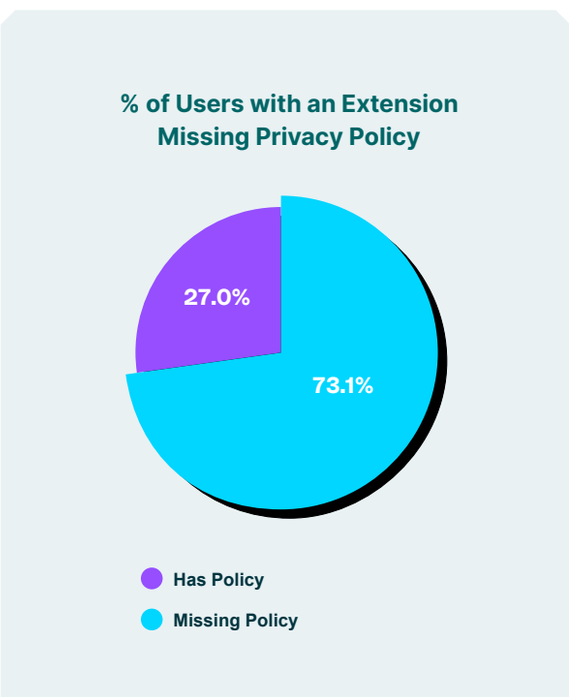




Why it matters: Extensions that are not regularly updated may contain unresolved vulnerabilities or outdated code that attackers exploit.

Over 71% of all extensions do not provide a privacy policy, and as a result, more than 73% of users have at least one extension installed that lacks a privacy policy.





Why it matters: This indicates that the vast majority of users lack transparency into how their data is being collected and used, creating significant privacy risks and potential regulatory compliance violations.

Key Recommendations

The data in this report highlights that browser extensions represent a widespread and largely unmanaged security risk across enterprise environments. To reduce exposure, organizations should adopt a structured approach to extension governance that combines visibility, risk assessment, and continuous monitoring.

#1

Continuously Audit Your Extension Threat Surface

Security teams must maintain a complete inventory of all browser extensions across users, devices, and browsers. Without centralized visibility, high-risk or unauthorized extensions can remain active and undetected.

#2

Implement Risk-Based Guardrails for High-Permission Extensions

Since most extensions request high or critical permissions, organizations should enforce policies that restrict extensions from having unnecessary access to cookies, scripting, tabs, or network requests.

#3

Apply Targeted Security Controls to AI Extensions

AI extensions often request elevated permissions and interact with sensitive enterprise data. Organizations should apply stricter approval processes and governance policies to control how these extensions access and transmit data.

#4

Continuously Monitor Extension Changes and Supply-Chain Risk

Extensions can change ownership, permissions, or functionality over time. Security teams should continuously monitor for these changes and automatically flag or restrict extensions that introduce new risks.

#5

Enforce Trust and Transparency Requirements

Extensions that have very low install counts, lack privacy policies, or show poor maintenance history should be treated as higher risk. Establishing minimum trust criteria helps reduce exposure to unverified or abandoned extensions.

How LayerX Can Help

Comprehensive Audit

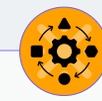
Discover all extensions on all browsers for all users, with full visibility and control

Rich Risk Classification

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

Analyze Extension Behavior

Go beyond static analysis of extension risk factors with runtime behavioral analysis of extensions as they change



Adaptive Enforcement

Risk-based enforcement to block suspicious extensions based on their risk profile

LayerX provides a comprehensive extension security platform to manage the entire lifecycle of browser extensions, giving organizations full control over browser extensions and AI usage without disrupting user productivity.

It delivers real-time visibility into all browser extensions across every user, device, and browser, continuously assessing risk based on permissions, real-time behavior, publisher trust signals, and known vulnerabilities. With a granular policy engine, LayerX enables security teams to trigger alerts, enforce controls, or automatically disable extensions when risk indicators are detected.

Moreover, LayerX goes beyond one-time, static analysis of extension parameters, and continuously monitors extension behavior as it changes, across its entire lifecycle. Suspicious changes are automatically flagged, enabling security teams to respond immediately to emerging threats such as malicious updates or extension takeovers.

Enterprises use LayerX to secure their extension risk surface and allow usage of legitimate browser extensions while restricting the use of suspicious or malicious extensions.

To learn more about how LayerX can help you manage and secure your browser extensions, go to www.layerxsecurity.com and schedule a demo today!