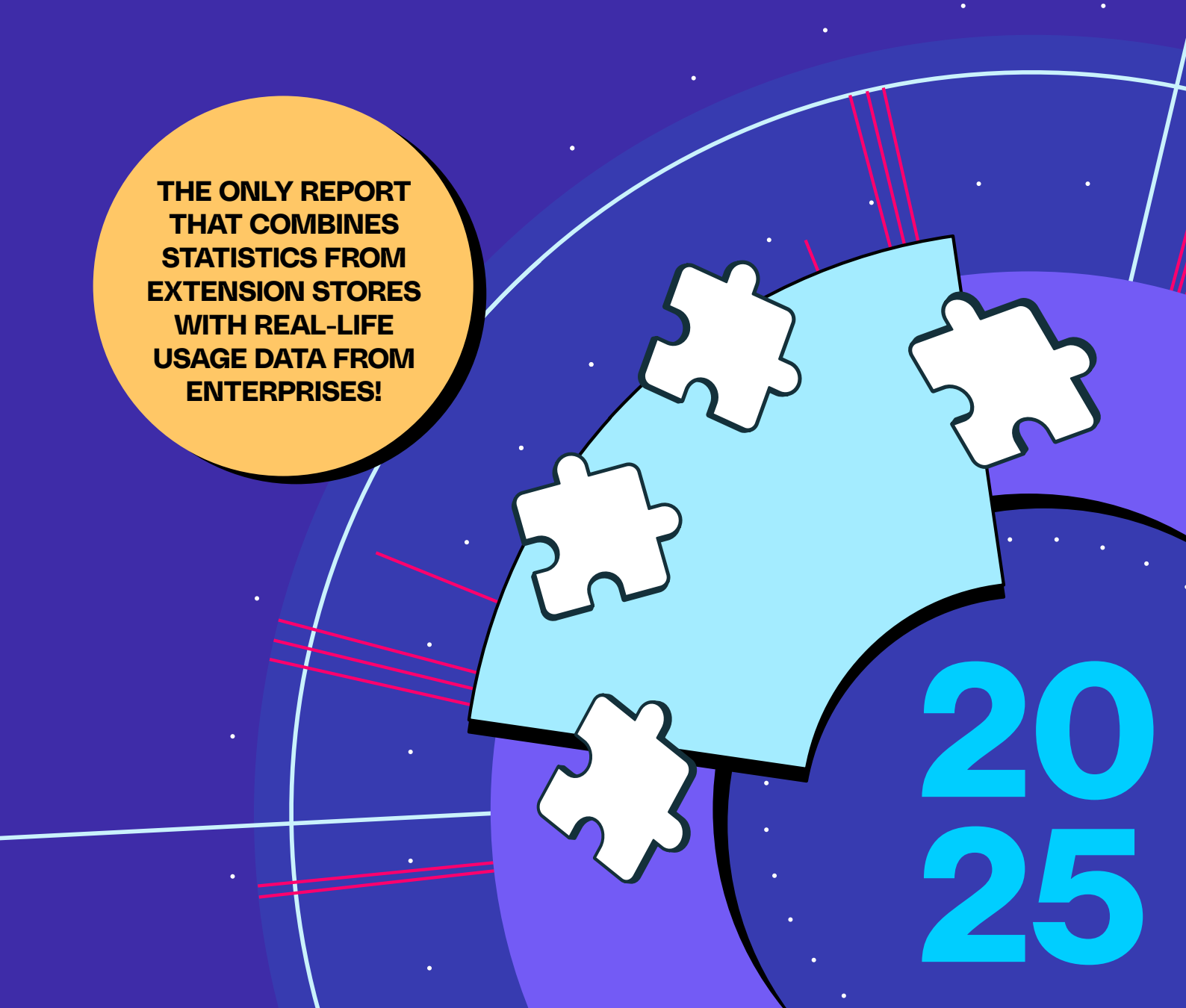
LayerX

Enterprise Browser Extension Security Report 2025

Real-life data on browser extensions, their risks and impact, usage in enterprises, and their key security blind spots

THE ONLY REPORT THAT COMBINES STATISTICS FROM EXTENSION STORES WITH REAL-LIFE USAGE DATA FROM ENTERPRISES!



2025

Introduction

Browser extensions have become a ubiquitous part of the browsing experience, and many users often use such extensions to fix their spelling, find discount coupons, or other productivity uses. However, most users don't realize that browser extensions are routinely granted extensive access permissions that can lead to severe data exposure should those permissions fall into the wrong hands.

This is particularly a risk to organizations since many organizations do not control what browser extensions users install on their endpoints, and a compromised browser extension of an individual user can lead to exposure and breach of the organization as a whole.

However, there is lack in tangible industry-level data about browser extension security that can quantify the extent and level of risk.

This research does exactly that:

it provides hard data on browser extensions, their permissions, the publishers behind them, and enterprise usage based on data and telemetry taken from both public extension stores, as well as real-life data collected from LayerX Security's enterprise customer base.

What's In This Report

This report covers several areas relevant to browser extension risks and threats, including:

- How many enterprise users use browser extensions
- How many enterprise extensions have risky permissions
- How common are key permissions that can access users' cookies, passwords, and browsing information
- Who are the developers behind browser extensions, and how much can we trust them
- And more...

The findings are a combination of public data from extension stores, overlayed with telemetry collected from LayerX's unique data set.

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.

The LayerX Security solution is deployed directly within users' web browsers, meaning that LayerX has full visibility to all user activity and data that passes through the browser. This allows us comprehensive insights on the usage of browser extensions and their access permissions.

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

How can you protect against what you don't know about?

#1

Browser Extensions Are Everywhere, Even in Enterprise Environments

99% of enterprise users have a browser extension installed in their browsers, and more than half (52%) of employees have more than 10 extensions installed. This means that browser extensions are a threat surface that touches almost every single enterprise employee.

#2

Most Browser Extensions Have Access to Sensitive Data

53% of enterprise users have installed a browser extension with 'high' or 'critical' risk scope, meaning that such extensions have access to sensitive data such as cookies, passwords, web page contents, browsing information, and more, putting users at risk of credential theft or data exposure. The implication is that the compromise of an extension at the individual user level can lead to a breach at the organizational level.

#3

Extension Publisher Reputation is a Black Hole

54% of extension publishers are identified solely by a free webmail (Gmail) account, meaning that anyone can upload an extension to public stores while hiding their identity. The overwhelming majority (79%) of extension publishers published only a single extension, 58% of extensions do not publish a privacy policy, and 22% of extensions are new (younger than 180 days), meaning for most extensions, there is little track record that users or organizations can rely on to establish an extension's trustworthiness.

CISO Recommendations

- **Audit all browser extensions:**
  The ubiquity of browser extensions across enterprise users means that almost every employee can be potentially impacted. Therefore, conducting a full audit of all extensions, across all browsers, on all devices, is the only way to fully understand your browser extension threat surface.
- **Assess extension risk:**
  Once you have a full picture of your threat surface, you need to assess the risk posed by each extension. This should analyze both the potential impact (i.e., what data the extension is exposed to, as defined its access permissions), as well as its reputation (as defined by the trustworthiness of the extension publisher). A holistic risk-scoring approach should factor in both the permission scope and trustworthiness of the extension.
- **Actively enforce security rules to block/disable risky extensions:**
  Once you have a full picture of your extension threat surface, and the risk associated with each extension, the next step is to apply risk-adaptive security rules that block or disable risky browser extensions.

Key Findings

#1

Even Though Browser Extensions Have Become a Staple, the Extent of the Threat Surface is Surprising: 99% of users have at least one extension installed in their browsers, and 52% have more than 10 browser extensions, making browser extensions a threat surface that touches nearly every single enterprise user. While the majority of extensions come from official stores, 17% of extensions originate from non-official stores, and 26% of extensions are sideloaded by external applications, making extensions not just a browser risk but a malware risk, as well.

#2

Despite Growing Concerns over Browser Extension Security, Extensions in Corporate Environments had Higher Permissions than Average: 53% of enterprise users installed extensions with 'high' or 'critical' permission scope. Whereas approximately 4.8% of all extensions request access to user cookies, in practice, 11% of extensions installed in enterprise users' browsers had cookie access. Similarly, while only 3.5% of all extensions require access to user identity data, more than 7.5% of extensions installed in corporate environments have access to identities, meaning that enterprise users are at a higher risk of exposure.

#3

While AI Web Tools Make the Headlines, GenAI Browser Extensions are a Hidden Risk: AI-enabled browser extensions are a 'side door' for AI usage in the organization that can often bypass network-layer GenAI access controls. More than 20% of enterprise users have a GenAI extension installed on them, and 45% of those users have more than GenAI extension. Moreover, GenAI extensions can typically access sensitive data such as identities, cookies, scripting permissions, and control over browser tabs at twice the average rates of other extensions, and 58% of GenAI extensions have 'high' or 'critical' level permissions (vs. an average of 53%), making GenAI extensions an outsized risk should they become compromised.

#4

Although Most Focus is On Browser Extension Permissions, Publisher Reputation is Just as Big of a Problem: When discussing browser extension security, extension permissions rightly take up a substantial part of the conversation in an effort to understand what data the extension can access. The second part of the question is how well can I trust it. However, while analyzing permission is pretty straightforward, establishing the trustworthiness of extensions is virtually impossible: 89% of extensions have fewer than 1,000 users, 54% of extension publishers are identified solely by a free webmail account, 79% of publishers have published just a single extension, and 22% of extensions have been in the store for less than 6 months (41% for GenAI extensions), meaning there is little-to-no information to go by to establish credibility.

#5

For All the Talk of New Extensions, Unmaintained Browser Extensions are a Growing Concern: More than half (51%) of extensions haven't received an update in more than 12 months. Not only does this open extensions up to software vulnerabilities and supply-chain risks, but it also raises the risk of abandoned extensions that no one is maintaining: 25% of extensions haven't received an update in a year, and are published by publishers identified only by a Gmail account, raising the possibly that these are 'hobbyist' extensions that have been abandoned.

With Great Power Comes Great Responsibility: The Extensive Permissions of Browser Extensions

99%

Of enterprise users have at least one extension installed in their browsers

53%

Of enterprise users have 10+ browser extensions installed

53%

Of corporate users installed extensions with ‘high’ or ‘critical’ permissions

20%

Of enterprise users have a GenAI extension installed

45%

Of users who have a GenAI browser extension, have more than one such extensions

58%

Of GenAI extensions have ‘high’ or ‘critical’ permissions scope

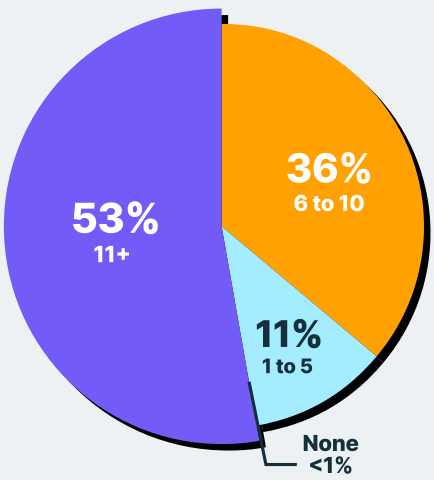
The Finding

Browser extensions have become ubiquitous in enterprise environments: 99% of enterprise users have at least one extension installed in their browsers, and 52% of enterprise users have more than 10 browser extensions installed.

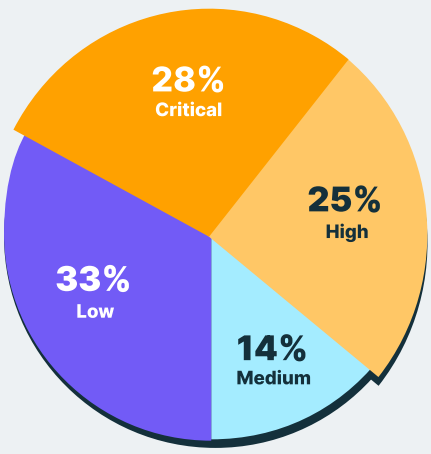
While most users treat browser extensions as harmless, they are often granted extensive permissions to user data. Browser extension permissions are governed by the APIs they use, which are declared in the extension’s manifest file.

An analysis of browser extension deployments on across LayerX’s customer base shows that 53% of enterprise users installed an extension with ‘high’ or ‘critical’ permission scope.

Enterprise Users by Number of Extensions Installed



Extension Permissions by Enterprise Users



We also examined a number of specific permissions that can be used to access sensitive data, and investigated how common they are:

Identity API:

Provides access to user account information when interacting with Google services, including OAuth authentication and access to user profile data.

Cookies API:

Allows extensions to read, modify, and delete cookies. A malicious extension could steal or delete session cookies, effectively hijacking or terminating the user's session, and/or create fake cookies to impersonate legitimate users.

Scripting API:

Allows the injection of JavaScript code into web pages, which can be used for a variety of activities such as capturing login forms, keystrokes, or scraping credentials from fields on the page, or manipulating web pages to exfiltrate stored credentials, interacting with password fields or modifying content on the page.

Tabs API:

Allows extensions to manage browser tabs, including creating, updating, and removing them. It could be used to force the user to navigate to malicious websites or phishing pages, or close legitimate session-related tabs to disrupt the user's workflow or session continuity.

webRequest API:

Allows extensions to observe and intercept network requests. Malicious extensions could intercept session cookies or modify request headers to impersonate users or disrupt active sessions.

webNavigation API:

Could be used to intercept HTTPS requests to gather sensitive data such as certificate information if users are tricked into using insecure connections (e.g., MITM attacks). It could also tamper with headers to inject malicious certificates into communication.

We examined the prevalence of these permissions across the entire population of browser extensions in the Chrome Web Store, as well as across a selection of specific categories that LayerX identifies as particularly noteworthy: GenAI extensions, VPN extensions, and Password Management extensions.

We looked specifically at GenAI extensions because of their popularity: over 20% of enterprise users have installed a GenAI browser extension, and 45% of users who have a GenAI extensions installed on their computer, have more than one such extension. VPN and Password Management extensions are not quite as popular, but we examined them because of the degree of control they often have, and the sensitivity of the data they touch.

The findings indicate that overall, two of the most popular permissions for browser extensions are the tabs and scripting APIs, used by 23.92% and 14.34% of all extensions, respectively. However, when we compared to other categories, we saw that GenAI extensions invoked the scripting API at nearly twice that rate, of 26.97% (vs. 14.34% for all extensions).

Another noteworthy difference was with the cookies API, which grants extensions access to user's cookies. Whereas only 4.87% of all extensions invoked this permission, GenAI extensions used it at nearly twice the rate (8.66%), as did VPN extensions (8.16%).

Likewise, whereas only 3.51% of all extensions required access to the identity API, GenAI extensions requested that permission at more than double the rate (7.74%).

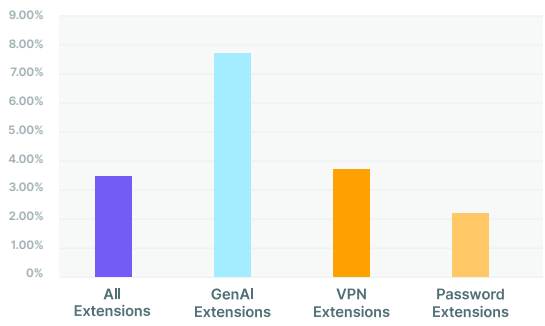
It is no surprise, therefore, that 58% of GenAI extensions had 'high' or 'critical' -level permissions (vs. an average of 53% across all enterprise users). This means that GenAI and VPN extensions were much more likely to have access to user cookies and identity data than the general population of extensions, without an obvious explanation of why they would need that access.

Comparing the data across all extensions to telemetry collected from LayerX's customer base, we saw that in real life, 7.5% of enterprise users had extensions that provided access to identity data (vs. an average of 3.5%), and 11% of users installed extensions that allowed access to cookies (vs. an average of 4.8%).

Examining permissions that can view or modify page data, we saw big differences in the prevalence of the webRequest and webNavigation APIs between categories: while those permissions were used only by 4.67% and 3.18% of all extensions, respectively, a whopping 63.95% of VPN extensions invoked the webRequest API, and approximately 7% of VPN and password management extensions invoked the webNavigation API.

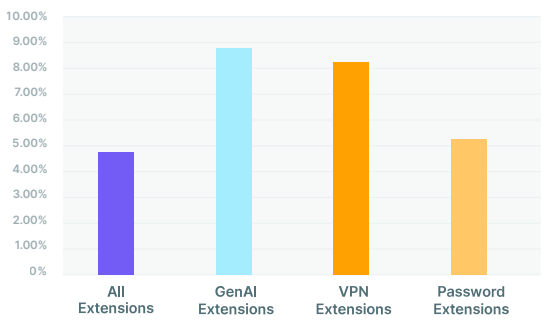
While this makes sense to a certain degree, given that VPN extensions probably use these permissions to redirect traffic via secure proxies, it also opens up the possibility of exploitation by these extensions for a host of other uses, such as disrupting active sessions, redirecting traffic to unsecure destinations, and otherwise interfering with web traffic.

Extensions with Access to User Identity



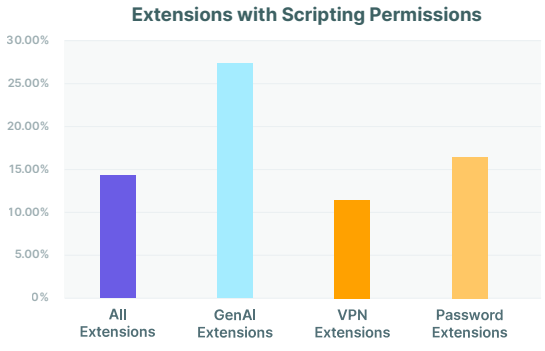
Provides access to user account information when interacting with Google services, including OAuth authentication and access to user profile data.

Extensions with Access to Cookies



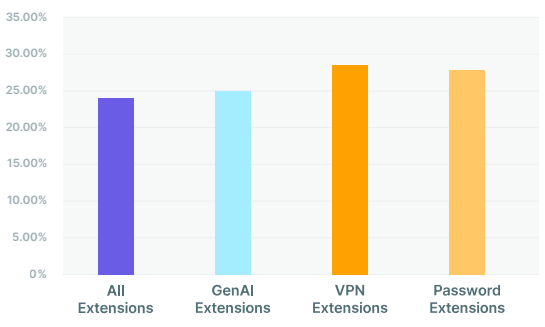
Allows extensions to read, modify, and delete cookies. A malicious extension could steal or delete session cookies, effectively hijacking or terminating the user's session, and/or create fake cookies to impersonate legitimate users.

Extensions with Scripting Permissions



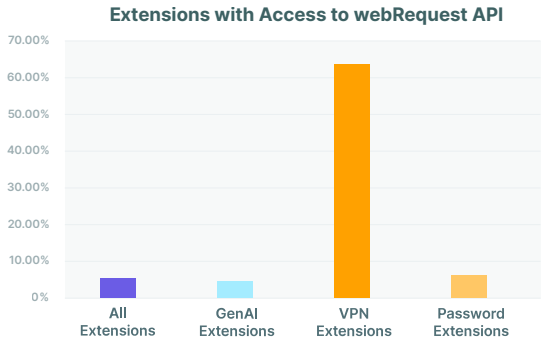
Allows the injection of JavaScript code into web pages, which can be used for a variety of activities such as capturing login forms, keystrokes, or scraping credentials from fields on the page, or manipulating web pages to exfiltrate stored credentials, interacting with password fields or modifying content on the page.

Extensions with Access to Browser Tabs



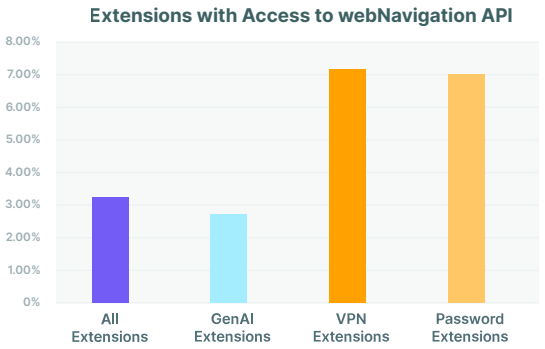
Allows extensions to read, modify, and delete cookies. A malicious extension could steal or delete session cookies, effectively hijacking or terminating the user's session, and/or create fake cookies to impersonate legitimate users.

Extensions with Access to webRequest API



Allows extensions to observe and intercept network requests. Malicious extensions could intercept session cookies or modify request headers to impersonate users or disrupt active sessions.

Extensions with Access to webNavigation API



Could be used to intercept HTTPS requests to gather sensitive data such as certificate information if users are tricked into using insecure connections (e.g., MITM attacks). It could also tamper with headers to inject malicious certificates into communication.

Analysis

The risk and impact of browser extension compromise are largely determined by the permissions granted to them.

Through these permissions, extensions can access a broad range of sensitive user data including cookies, passwords, identity information, browsing information, page contents, and much more. Therefore, an analysis a browser extension's permissions is important in order to address the question of what is the impact of compromise of that extension.

The findings show the extent to which enterprise users are exposed to such permissions, and in particular to those who can access cookies (via the cookies API), identity information (via the identity API), page information (via the tabs API), or invoke custom scripts within the browser (via the scripting API).

GenAI extensions stand-out in particular both due to their popularity, and the broad extent of permissions that such extensions tend to have.

Therefore, the first step to assessing the risk posed by browser extensions is to enumerate all browser extensions in the organizations, assess their permissions in order to define their potential impact, and enforce permission-based access controls at the browser level.

Chrome is King, but The Extension Threat Surface is Broader Than You Think

145K+

Extensions in the Chrome Web Store

17%

Of extensions in enterprise environments are from non-official stores

26%

Of extensions installed in enterprise users' browsers are sideloaded

The Finding

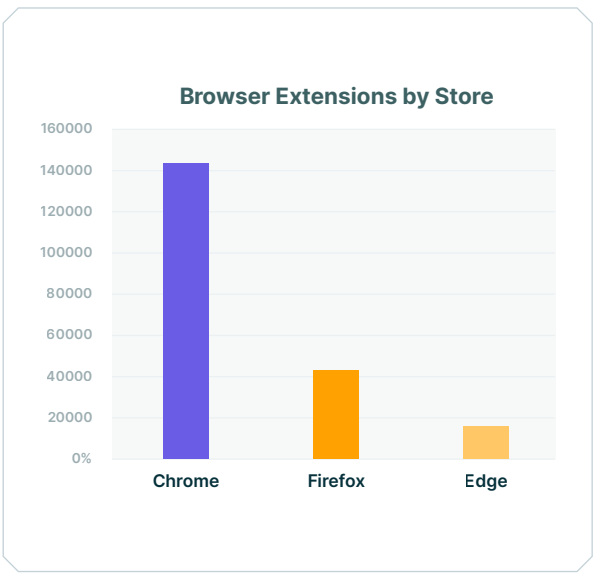
Where do extensions come from? We'll give you a hint: it's not with a stork.

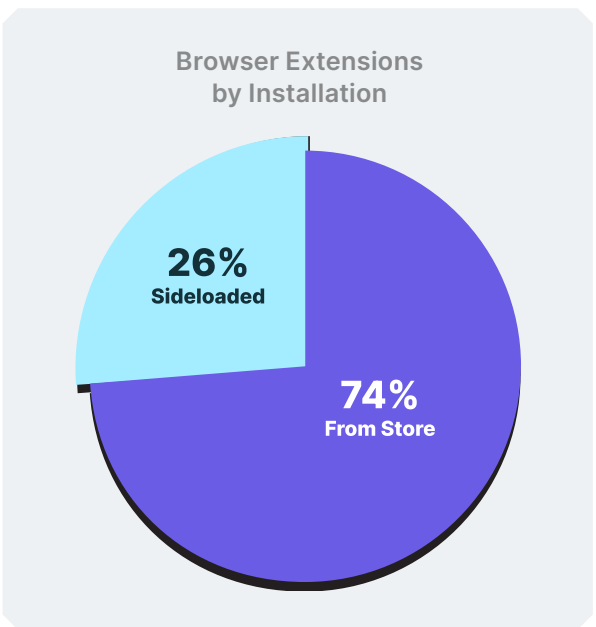
While the official extension stores by Chrome, Edge and Firefox are the most common sources for extensions, research shows that the browser extension threat surface is much wider than most users realize.

The Chrome Web Store is far-and-away the largest source of browser extensions, with approximately 145,000 extensions in its store. This should come as no surprise, given that Chrome has 67% of the market share for desktop browsers worldwide[1].

Following Chrome is the Mozilla add-on store, with approximately 43,000 add-ons. This is a somewhat surprising finding, given that Mozilla Firefox has only 5.75% share among desktop users worldwide.

Finally, the Edge add-on store comes in third, with about 13,000 extensions, bout one-sixth of the number of Chrome extensions and less than a half of Mozilla addons, a somewhat disappointing figure given that Edge has nearly three times the market share of Firefox (15.69%) and is prevalent in many enterprises.





However, an examination of the sources of these browser extensions shows that the official browser stores are just one avenue to installing browser extensions: according to LayerX telemetry from its user base, 17% of extensions deployed on enterprise endpoints are from non-official stores, and 26% of extensions were side-loaded, meaning that they were deployed directly into the browser by another process or application. Note that in all likelihood, these figures largely overlap, as side-loaded extensions can be taken from non-official stores (in fact, they are probably more likely to be from non-official stores), but it demonstrates the variety in sources and install methods of browser extensions.

[1] *"Top Desktop Browsers Market Share in February 2025." Similarweb, https://www.similarweb.com/browsers/worldwide/desktop/.*

Analysis

The data show that it's a Chrome-first world, and that's where most of your security efforts should go. Most users – even among enterprise users – use Chrome, and therefore, securing Chrome browsers should be an organizational security team's #1 priority.

That said, the outsized number of Firefox extensions in comparison to its market share suggests that this is also a potential hidden threat surface that should be addressed.

Finally, while Edge has a significantly lower market share than Chrome, and a relatively small number of add-ons in comparison to the other stores, it comes pre-packaged with every Windows PC, and is prevalent in many organizations – particularly those that are Microsoft shops and rely on Office365 and other Microsoft SaaS solutions. Therefore, a holistic approach to browser extension security should cover all major browsers and official sources of extensions.

Special note should be taken of the installation method and source of extensions installed in enterprise environments. As the findings show, a significant number of browser extensions are sourced from non-official stores. Extensions from such sources do not go through the verification process of the official extension stores (which is not very rigorous, of itself), and post a risk of introducing compromised or malicious extensions.

Moreover, about one in four extensions are sideloaded, meaning that they are installed directly by external applications. While many commercial applications or SaaS solutions offer a browser extension, it also creates a risk for malware to push browser extensions into unsuspecting users' browsers, as we've seen in a number of recent attacks.

It’s Lonely at the Top: Most Extensions Barely Have Any Installs

89%

Of Chrome extensions have fewer than 1,000 users

95%

Of Chrome extensions have fewer than 10,000 installs

0.2%

Of Chrome extensions have more than one million users

33%

The median number of installations among all Chrome extensions

23,362

Average number of installs among all Chrome extensions

10.53%

Percentage of extensions deployed in enterprise environments have fewer than 10,000 installs

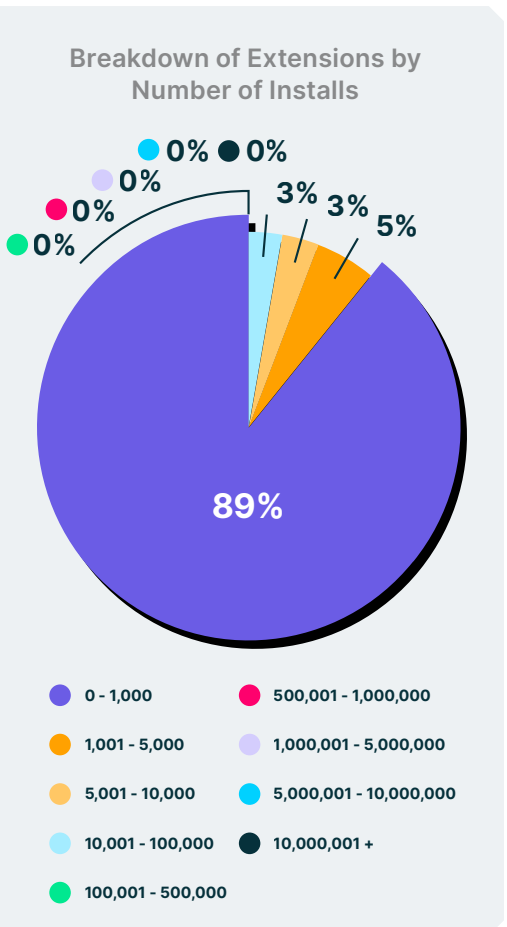
The Finding

If a browser extension falls down in a forest, and no one is using it, does it still make a sound?

While we often think of high-profile extensions such as Grammarly (46 million users), LastPass (9 million users), or Loom (8 million users), the overwhelming majority of browser extensions have few, if any, users.

A whopping 88.5% of Chrome extensions have fewer than 1,000 users. Over 95% of extensions have fewer than 10,000 users, and achieving 100,000 installs will land you in the top 1% of browser extensions (meaning that over 99% of extensions have fewer than 100,000 users).

High-profile extensions with millions of users are few and far between: only 0.43% of all browser extensions have more than one million installations, and the most popular extensions, with over ten million users, account only for 0.02% of all extensions.



The heavy skew of a small number of very popular extensions is evident in comparison of the average and median figures for browser extension installations: whereas the average number of installs per extension was approximately 23,000, and median number was a mere 23. This is a classic case of a left-tail distribution with a (very) large number of extensions with little-to-no installs, and a small number of hugely popular extensions.

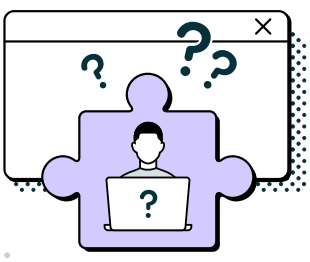
Analyzing extensions installed in enterprise environments reveals that 10.53% of all extensions installed in corporate employees’ browsers have less than 10,000 installs, and 7.89% have fewer than 5,000 installations.

Analysis

When most users think of browser extensions, they tend to think of well-known, commonly used and reputable extensions such as Grammarly. However, hidden beneath that thin layer of high-profile extensions is a hidden threat surface of unknown and barely-used extensions, on which there is virtually no information (also see the analysis in the subsequent pages).

While a low number of installs is not, in itself, a condemnation of an extension’s trustworthiness, it can be an indicator of an abandoned extension or an extension by an unknown or bad actor.

As organizations map out and audit their browser extension threat surface, including the number of installs as a risk factor can be a useful practice in extension risk analysis. Moreover, organizations should consider actively blocking extensions with a low number of installs to prevent unknown extensions from being deployed within the organization.



Who Can You Trust: Most Extension Developers are Unknown

54%

Of extensions are identified by a free Gmail account

64%

of GenAI extensions are identified by a free Gmail account

79%

Of extension developers published just a single extension

The Finding

Anyone can create and upload a web extension to public extension stores – and, as the research shows – many people do.

The findings reveal that the majority of extension publishers are private individuals, identified by free Gmail accounts. Over 54% of extensions on the Chrome Web Stores are published by publishers who are identified via Gmail accounts.

On the one hand – this should not be a surprise: Gmail is the world's most popular webmail service, and the Chrome Store is operated by Google, which requires – at minimum – a Gmail account to identify developers by. So it is a small wonder that most developers do, in fact, use Gmail.

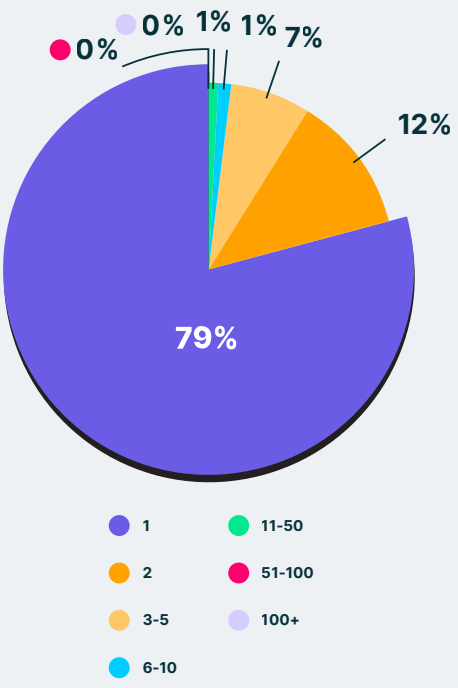
However, at the time, it creates an opening for unknown – and potentially malicious – actors to create and upload extensions to public stores, which could then be downloaded and used by unsuspecting users.

This share is even higher among GenAI extensions, where nearly two-thirds (64%) of extensions are created by publishers identified by Gmail accounts.

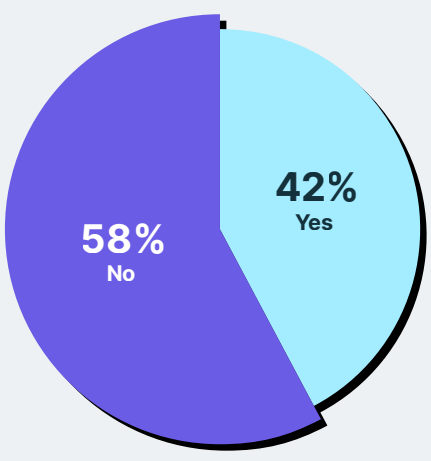
Finally, 79% of extension developers have published just a single extension, and only about 2% of developers published more than five. This indicates that extension development is a 'one-off' or a 'hobbyist' activity, and most publishers do not persist with it.

Another parameter we examined is whether an extension has a privacy policy. Only 42% of all extensions provided a privacy policy (meaning that 58% did not). GenAI and VPN extensions provided a pleasant surprise, with 66% of GenAI and 87% of VPN extensions offering a privacy policy (not perfect, but much better than average). However, password managers matched the poor overall trend, with 58% not providing a privacy policy.

Number of Extensions per Publisher



Extensions by Privacy Policy



Analysis

Any analysis of browser extension security should focus not just on the risk posed of each extension, in terms of the data it can access (as defined by its access permissions), but also its trustworthiness, in terms of to what extent you can trust its publisher.

Using a free webmail account, of itself, is not necessarily an indicator that a developer or an extension are malicious or should not be trusted. However, this low entry bar makes it easy for bad actors to create fake identities and publish malicious extensions to unsuspecting users.

The number of extensions published by each developer is also an indicator of its 'enterprise' trustworthiness. While a developer doesn't need to publish many extensions to become trustworthy (moreover, the overwhelming number of publishers who publish even just one extension are trustworthy), the overwhelming percentage of developers who publish just a single extension suggests that for many of them, this is a hobby, not an ongoing commercial effort.

The analysis of privacy policies published (or rather, not published) by many extensions also leads to the same conclusion: while a privacy policy is not a prerequisite for publishing an extension, and not having one is not necessarily an indicator of foul play, it is another parameter by which to assess the seriousness and enterprise readiness of an extension, and whether a user (or an organization) can trust their data with it.

Something Old, Something New: Most Extensions are Either New or Unmaintained

22%
Of extensions are younger than 6 months

41%
Of GenAI extensions are younger than 6 months

51%
Of extensions haven't been updated in a year

25%
Are potentially abandoned

The Finding

Analysis of the age of extensions on the Chrome store shows a sharp contrast between old and new extensions: whereas 22% of extensions are younger than 6 months (180 days), more than half (51%) of all extensions haven't been updated in over a year.

This contrast is even more pronounced in specific categories of rapidly emerging technologies, such as GenAI extensions, where 41% of extensions are new.

A cross-cut of extensions that haven't been updated in over a year against extensions where the developer was identified only by a free Gmail account (discussed in the previous section) reveals that nearly 25% of extensions in the browser store meet these two criteria, and are potential candidates for abandoned extensions (even excluding all other factors).

The implication of these findings is that just over a quarter of extensions (27%) in the Chrome Store have established histories (extension age of more than 6 months) and receive regular updates.

Analysis

Extension age is an indicator of its trustworthiness.

New extensions that have only been added to the store do not offer a long-enough history on which to gauge its reputation. On the other hand, long periods during which an extension has not been updated can indicate the extension has been abandoned.

Abandoned or outdated extensions can expose users to vulnerabilities, exploits, or takeover of the extension by malicious parties.

Combined with other indicators (such as whether the publisher is an individual using a free webmail account or an established company or the number of extensions the developer has published), these are valuable indicators of whether the extension is undergoing continuous development and its level of trustworthiness.

Key Recommendations

While many users and organizations are not aware of the potential risks associated with browser extensions, there are a number of key actions they can take to protect themselves:

#1

Audit all extensions

Many organizations don't have a full picture of all extensions that are installed in their environment. Many organizations allow their users to use whichever browsers (or browsers) they wish to use and install whatever extensions they want. However, without a full picture of all extensions on all browsers of all users, it is impossible to understand your organization's threat surface. This is why a full audit of all browser extensions is a foundational requirement for protecting against malicious extensions. While Chrome is the most popular browser by market share (and also with the most available extensions), the availability of high numbers of Firefox and Edge extensions should lead to organizations enforcing extension controls on those browsers, as well.

#2

Categorize extensions

As the data on GenAI extensions showed, some categories of browser extensions are more susceptible to exploitation than others. Part of this is the popularity of certain types of extensions that makes them appealing to attack because of their broad user base (such as GenAI extensions), and part of it is because of the permissions granted to such extensions, that hackers may wish to exploit (such as access to network and browsing data given to VPN extensions, for example). This is why categorizing extensions is a useful practice in assessing the browser extension security posture.

#3

Enumerate extension permissions

While understanding which extensions are installed in corporate environments is one side of the coin, the other side of the coin is understanding what those extensions can do. This is done by enumerating their precise access permissions and listing all the information they can potentially access.

#4

Assess extension risk

Once they understand what permissions they have installed on corporate endpoints and the information that these extensions can touch (via their permissions), organizations need to assess the risk posed by each individual extension. A holistic risk assessment should encompass both the permission scope of the extension (i.e., what it can do), as well as external parameters such as its reputation, popularity, publisher, installation method, and more (i.e., how much we trust it). These parameters should be combined into a unified risk score to help organizations assess the risk posed by each extension, and whether it is safe for that extension to be installed.

#5

Apply adaptive, risk-based enforcement

Finally, taking into consideration all the information they have at hand, organizations should apply adaptive, risk-based enforcement policies tailored to their uses, needs and risk profile. They can define policies to block extensions that have certain permissions (e.g., access to cookies), block extension based on external parameters (e.g., extensions which haven't been updated in more than a year), or define more complex rules tailored to their specific use case (e.g., block GenAI and VPN extensions with a 'High' risk score).

While browser extensions offer many productivity benefits, they also expand organizations' threat surface and their risk of exposure. Recent attack campaigns targeting browser extensions with malicious code should be a wakeup call for organizations to define how they protect against malicious and compromised browser extensions.

About LayerX
One Browser Extension to Rule Them All

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

LayerX browser security platform provides full protection against malicious browser extensions. LayerX's secure browser extension can integrate with any browser, and as such has full visibility into all other installed extensions.

LayerX's extension continuously monitors the existing and newly installed extensions, evaluating permissions, installation method, web store parameters, and external risk parameters.

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.

With its granular policy engine, LayerX enables its users to trigger notifications, alerts, or even complete disablement of an extension, when any risk indicator or combination of these are detected. LayerX extension runs at a higher permission level than ordinary extensions, and cannot be tampered with or uninstalled by users.

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!