LayerX

Report

UNVEILING THE THREAT OF MALICIOUS BROWSER EXTENSIONS

November 2023

Table of Contents

Introduction

Web browsing has ushered in unprecedented convenience and connectivity. But in doing so, it has exposed users to an array of online threats. Among these threats, one has notably surged in recent years: **malicious browser extensions**. These deceptively benign add-ons harbor hidden malicious intentions. They possess the capacity to surreptitiously gather sensitive data, monitor online activities, inject unwanted advertisements, divert traffic to malicious sites, and even take control of a user's browser. This jeopardizes users' privacy, security, and overall online experience.

Due to their placement within the legitimate browser, malicious extensions are able to evade the detection and prevention capabilities of the endpoint and network security stack. This allows them to perform their malicious activities. It has also made them a popular choice for malicious attackers looking to infiltrate the organization's network.

In this report, we will discuss the domain of malicious extensions, unveiling their tactics for infiltration, explaining the potential repercussions, and exploring the intricate challenges that confront companies looking to fortify their networks. At the end, you will be able to better identify potential malicious extensions and safeguard your organization against them.

The Growing Threat Landscape

The increasing growth in SaaS usage means that an equally increasing part of interaction with organizational data is carried out through the browser. From an adversary standpoint this means that compromising the browser has a high return on investment, potentially even higher than compromising the endpoint itself.

A browser extension, often simply referred to as an "extension," is a small software module that adds specific features or functionalities to a web browser, enhancing the user's browsing experience. These extensions are designed to customize and extend the browser's capabilities beyond its default settings. They can perform a wide range of tasks, from blocking advertisements and improving security to integrating with third-party services or providing productivity tools.

Browser extensions are typically available through official extension stores specific to each browser, such as the Chrome Web Store for Google Chrome or the Firefox Add-ons site for Mozilla Firefox. Users can select and install extensions that align with their preferences and needs, tailoring their browsing environment to suit their requirements.

However, a browser extension can become malicious through various means and actions taken by its developers, or by attackers who compromise legitimate extensions.

Installing a malicious extension provides an attacker with full visibility and control over all the data that flows or resides within the browser. This is the logic that stands behind the massive growth of attacks that use **malicious extensions; they are simply the ultimate browser compromise vector.**

Recent years have seen a surge in extension-based attacks. One notable example is the **DataSpii incident**. This incident shed light on the extent to which malicious browser extensions could compromise user privacy and corporate data security.

DataSpii involved a network of browser extensions, primarily for Chrome, that had been downloaded by millions of users. These seemingly innocent extensions, claiming to offer features like productivity enhancements or security tools, were, in reality, harvesting user data with alarming efficiency. The attack flow of DataSpii was particularly deceptive. After installation, these extensions would request extensive permissions under the pretense of their supposed functionalities. These permissions enabled them to scrape user data, which was then routed through a complex network of third-party services. This data, which included sensitive corporate URLs, PII (Personal Identifiable Information), and private browsing histories, was subsequently monetized through a commercialization scheme.

The Nigelthorn malware attack in 2018 was another notable instance of attackers using browser extensions for illicit purposes. In this case, the attackers distributed malware through malicious Chrome extensions that were disguised as legitimate software. The attackers first spread these malicious extensions through social engineering tactics, convincing users to download and install them. Once installed, the extensions injected malicious code into the victim's browser, enabling the mining of cryptocurrency, specifically Monero, using the victim's computing resources. The malware also had the ability to steal sensitive information, such as login credentials and personal data, posing significant risks to user privacy and security.

The Nigelthorn malware managed to infect thousands of users before Google took action to remove the malicious extensions from the Chrome Web Store. Users who unwittingly installed these extensions experienced reduced system performance, increased energy consumption, and potential exposure to data theft.

In all the above-mentioned cases, the attack flow followed a similar path: the user innocently installed an extension, the extension silently collected data or granted unauthorized access, and the attacker capitalized on this foothold to carry out further attacks.

The underlying reason these malicious extensions are able to carry out these attacks is the permissions that extensions require. Users often grant broad permissions to extensions, inadvertently giving them access to sensitive data or even control over the entire browser. This lack of granularity in permission management contributes to the ease with which attackers can exploit extensions.

The Internals of Malicious Extensions

In this section we'll break down the anatomy of browser extensions and show the components and capabilities that can be used by a malicious actor.

Our analysis focuses on the following aspects:

1. Types of malicious extensions
2. Installation process of the extension
3. Risk indicators derived from usage and maintenance
4. Permissions the extension uses
5. Built-in security weaknesses

1 Types of Malicious Extensions

This section maps the various types of extensions that can introduce either an active or potential risk when installed on a workforce browser.

Initially malicious extension

An extension that was created by an adversary from scratch to serve a malicious purpose. It will be either:

- Uploaded by the attacker to the web store
- Hosted on the attacker’s infrastructure

Compromised extension

An initially legitimate extension that is owned by an adversary after either:

- Directly purchasing the extension
- Compromising the extension’s developer account

Risky extension

A legitimate extension that have excessive permissions that can result in either:

- Compromise by adversaries
- Data exposure and leakage

2 Installation

This section details the different methods in which a malicious extension gains residence on a victim's browser.

Admin

Extensions distributed centrally by network administrators within the company. These are extensions with explicit organizational approval. Many times, a network admin will want to install the same extensions throughout their organization.

The security question to ask: What is the necessity and security of such extensions within the corporate network?

Normal

Extensions downloaded from official browser stores. Users install extensions by visiting an extension's listing in the browser Web Store. Analyzing these extensions shows which extensions are most popular among the workforce.

The security question to ask: What are the potential risks associated with allowing employees to make these choices independently?

Developer

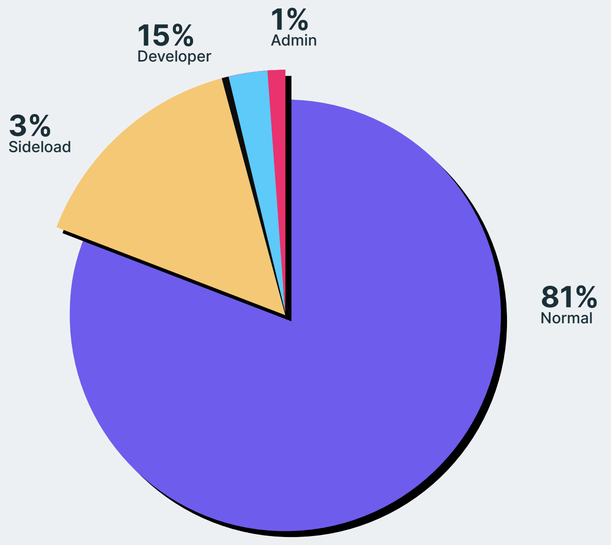
Extensions loaded from employees' local computers present an intriguing set of data for analysis. It's a potential risk since such extensions, originating from employees' workstations, are not subject to the usual vetting process on installed software. It prompts a critical examination of the security implications of allowing employees to load unpacked extension files directly from their machines.

Sideload

Extensions installed by third-party applications, such as Adobe or other software providers. This is the least secure option since it can be easily abused by adversaries to install a malicious extension without the user ever being aware of it.

The security question to ask: How do these applications interact with browsers and what kind of access and permissions do they grant extensions?

The following figure shows the distribution of installation types as within LayerX install base:



The distribution of extension installation types

Software Update

The four methods above relate to the initial installation of a malicious extension on the victim's browser. There's also a scenario in which an adversary purchased an initially legitimate extension with the purpose of abusing this extension for malicious needs. In such a case, the adversary will embed malicious code in the extension's periodic software update package, which is typically downloaded automatically. Following the download and execution of the update, the extension can serve as a tool for the adversary's purpose.

3 Usage and Maintenance: Indicators of Potential Risk

In this section we provide what can indicate that an extension is potentially a malicious one.

Web Store Indicators

The information that is available in the web store about an extension can provide insights into its security posture. As a rule of thumb, the more an extension is widely used in a standardized manner, the safer it is to download. Counter to that, the following list shows which extension attributes should raise caution:

- **Address and Email:** If the developer's contact address or email is missing from the Chrome Web Store listing, this could indicate potential obscurity and a lack of accountability,
- **Last Updated:** How long ago the extension was last updated, reflecting the potential security and compatibility risks associated with outdated extensions.
- **Privacy Policy:** If an extension lacks a privacy policy in its Web Store listing, this could indicate potential concerns about data handling and user privacy.
- **Rating:** The extension's user ratings, assessing the extension's overall quality and user satisfaction.
- **Rating Users:** The overall number of user ratings at the time of assessment. The more ratings, the smaller the risk.
- **Support Site:** No support site associated with the extension on the Web Store, could suggest potential challenges in receiving assistance or troubleshooting issues.
- **Users:** The overall number of users. A low number of users may impact support and indicate lower reliability.
- **Website:** No website associated with the extension, potentially signifies a lack of additional information or resources.

External Indicators

These indicators are warn signs you should be watchful for:

- The extension doesn't appear in any official store.
- The extension features an uncommon install type, such as side-loading or developer mode.
- The extension is promoted either for free, or in any other way that doesn't make economic sense, for example free extensions pushed by paid ads

4 Permissions

Browser extension permissions are a crucial aspect of how these add-ons interact with your web browser and the data they can access. They are essentially a set of rules that dictate what actions an extension is allowed to perform within your browser. Permissions are requested and granted when you install an extension, and they can vary widely depending on the extension's intended functionality.

The table below summarizes some of the notable permissions that can easily become a vehicle to malicious operations.

Note that:

- These permissions span a full attack lifecycle as they provide both the ability of the malicious action itself (credential compromise, capturing session and system data, altering host configuration etc.), as well as setting an outbound network connection with the adversary's remote infrastructure.
- These permissions are used by many common extensions. From an adversary's perspective they are the ultimate 'Living-off-the-Land' tools.

Permission	Rating	Details	Examples of legitimate extensions using this permission	Potential risks
cookies	● Critical	Use the chrome.cookies API to query and modify cookies, and get notified when they change.	Okta, Grammarly, Loom	Malicious extensions can steal or manipulate cookies to access sensitive data or perform unauthorized actions on websites.
debugger	● Critical	Instrument network interaction, debug JavaScript, mutate the DOM and CSS, etc., enabling reading and changing all data on all websites.	Full Screenshot, Microsoft Power Automate, Selenium IDE	Malicious extensions can use the debugger permission to access and manipulate the JavaScript code of web pages, potentially injecting malicious scripts.
webRequest	● Critical	Use the chrome. webRequest API to observe and analyze traffic and to intercept, block, or modify requests in-flight.	Okta, Grammarly, adblock, adobe, FreeVPN, NordVPN	This permission can be exploited to intercept and modify network requests, allowing malicious extensions to manipulate web traffic, inject ads, or steal data.
<all_urls>	● Critical	Grants access to all hosts, enabling reading and changing all data on all websites.	Loom, adblock, adobe, FreeVPN, Dark Reader	Malicious extensions with this permission can access and interact with all web pages, posing a significant security and privacy risk.
clipboard	● High	Read data you copy and paste.	Office - Enable Copy and Paste, Chrome Remote Desktop, Tampermonkey	Malicious extensions can abuse clipboard access to intercept and steal sensitive data copied by users.
contentSettings	● High	Change settings that control websites' access to features, such as cookies, JavaScript, plugins, geolocation, microphone, camera, etc.	Adblock, FreeVPN	This permission allows extensions to control website content settings, which can be abused to alter security settings or block access to legitimate sites.
desktopCapture\ pageCapture	● High	Capture the content of a screen, individual windows, or tabs.	Loom	These permissions enable extensions to capture the content of the user's desktop or web pages, potentially invading privacy or exposing sensitive information.
history	● High	Use the chrome.history API to interact with the browser's record of visited pages. Add, remove, and query URLs in the browser's history.	Adobe, Click&Clean	Malicious extensions can access a user's browsing history, compromising their privacy and potentially exposing sensitive information.
privacy	● High	Change your privacy-related settings.	ExpressVPN	Extensions with this permission can manipulate privacy settings or track user behavior, leading to privacy violations and data collection without consent.
proxy	● High	Get and set the browser's proxy configuration.	FreeVPN, NordVPN	Malicious extensions can route internet traffic through a proxy server controlled by attackers, potentially exposing sensitive data or redirecting users to malicious websites.
tabCapture	● High	Access a MediaStream containing video and audio of the current tab.	Screencastify, Loom	This permission can be abused to capture the content of user's browser tabs, potentially invading privacy or exposing sensitive information.
https://*/*	● High	Grants access to all hosts.	Okta, Grammarly, Click&Clean	Extensions with this permission can access all HTTPS websites, making it possible to intercept secure communications and steal sensitive data.

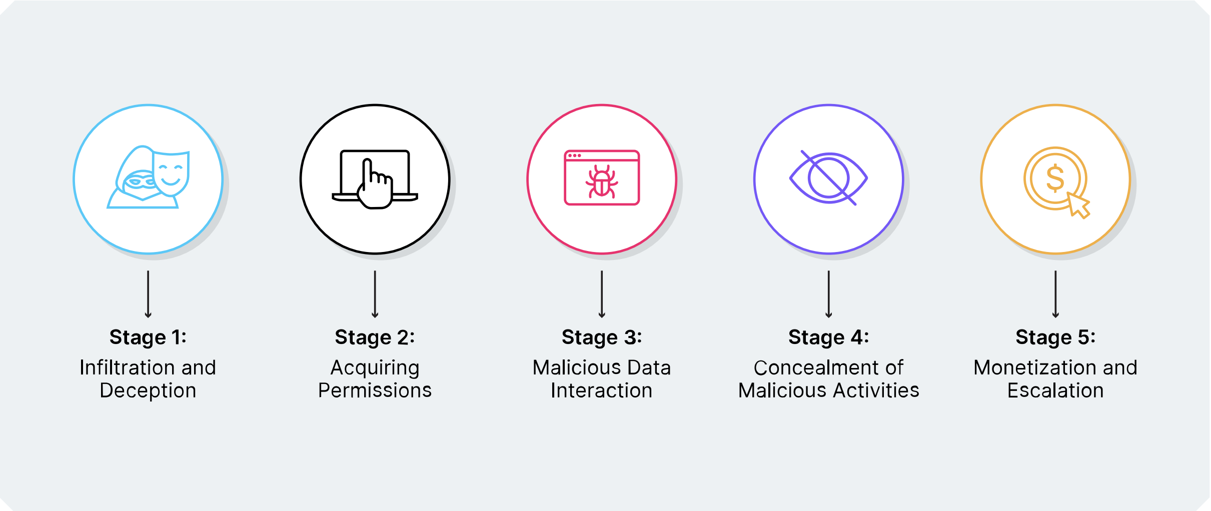
5 Built-in Weaknesses

Chrome doesn't automatically uninstall extensions that were unpublished by their developers or that were taken down from the store. Moreover, it would not do so even if the extension was marked as malware by threat intelligence engines. As of August 16, Chrome had started to pop up a warning message upon detection of an extension that meets the above criteria. But it's still the users' responsibility to remove the extension.

This means that whenever a user has installed a malicious browser extension, it stays on the user's browser for good. This is a major security weakness that enables adversaries to easily gain persistence on victims' browsers.

Browser Extension Attack Vector

The attack vector of a malicious browser extension is a complex web of devious tactics, often involving multiple stages that aim to exploit the trust of users and the vulnerabilities within browser ecosystems. Understanding this attack flow is crucial for comprehending how seemingly harmless extensions can morph into formidable threats.



Stage 1: Infiltration and Deception

Stage 2: Acquiring Permissions

Stage 3: Malicious Data Interaction

Stage 4: Concealment of Malicious Activities

Stage 5: Monetization and Escalation

Stage 1
Infiltration and Deception

MITRE mapping: Reconnaissance, Resource Development, and Initial Access

TA0043 Reconnaissance: The adversary maps out the victim's web activity to determine what type of extension would best lure them.

TA0042 Resource Development:

- The adversary writes an extension from scratch and either uploads it to a web store or hosts it on their server.
- If the adversary purchases an existing extension, they will write an updated package that contains malicious code.

TA0001 Initial Access:

- Installation of new extension by either:
  - Luring the victim with social engineering, or
  - Sideloading the extension in the background.

The journey typically begins with the attacker creating or manipulating an innocent-looking browser extension. To enhance its appeal, these extensions may promise enticing features, productivity enhancements, or security benefits. They often employ social engineering techniques, persuasive language, fake incentives, or even convincing marketing campaigns to lure users into installing them. These initial stages rely heavily on exploiting users' trust, convincing them that the extension is both safe and beneficial.

Stage 2
Acquiring Permissions

MITRE mapping: Privilege Escalation

The core of using a browser extension as a malicious tool is its ability to gain excessive permissions that can be easily leveraged for malicious purposes.

TA004 Privilege Escalation: Once installed, the extension often requests a range of permissions , such as access to the browsing history, personal data, and more (see detailed list above). Accomplishing this equips the malicious extension with all it needs to launch its malicious activities.

Stage 3
Malicious Data Interaction

MITRE mapping: Credential Access and Collection

With permissions granted, the extension can begin executing its nefarious activities. These can vary widely but often include:

TA0006 Credential Access: Adversaries may access passwords, cookies, and certificates that are stored in the browser, rendering them access to any SaaS\web resources these credentials apply to.

TA0009 Collection:

- Extracting data from the browser app, like credentials.
- Capturing data from the browsing session itself: video, audio, and anything that's copied\pasted\filled\typed on the web page.
- Spying on and monitoring the user's typical web activities to facilitate future attacks.

Stage 4
Concealment of Malicious Activities

MITRE Mapping: Persistence and Command and Control

Many malicious extensions are designed to operate stealthily, evading endpoint and network detection methods. This helps ensure continuous activity.

TA0003 Persistence:

- The malicious extension, when installed on the browser, is not subject to any scrutiny by EDR solutions.
- Adversaries might manipulate the extension's update URL to silently mount additional malicious capabilities.

TA0011 Command and Control

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Stage 5
Monetization and Escalation

MITRE mapping: Impact and Exfiltration

As the attack progresses, the harvested data and the adversaries' foothold on the browser can be monetized through various means.

TA0010: Exfiltration

Adversaries may exfiltrate the data that's captured or extracted by the extension by various channels. They often prefer using standard web protocols due to the common lack of outbound traffic inspection by firewalls\proxies.

TA0040: Impact:

There are numerous ways a malicious extension-based attack can cause harm, depending on the intentions of its initiating threat actor.

- Malicious access to organizational resources using the harvested credentials.
- Increasing organizations' exposure to attacks by selling compromised data on the dark web.
- Targeted phishing attacks based on the users' harvested data.
- Consuming computer power for crypto mining.
- Injecting adware and malvertising to redirect users to malicious websites.

Mitigation

The fight against malicious extensions is no easy feat, and the arsenal of defenses is both complex and nuanced. Browser vendors strive to screen extensions before listing them in official stores. However, the sheer volume of extensions makes thorough vetting challenging, leading to the inadvertent inclusion of malicious ones.

User education is a proactive approach. Yet, attackers constantly adapt their tactics, making even vigilant users susceptible. Behavior-based detection, powered by advanced algorithms, seeks to identify malicious extensions. Despite its potential, false positives and negatives hinder its reliability.

Regular audits of installed extensions offer a way to uncover and remove suspicious ones. However, this approach relies heavily on user compliance and vigilance, posing limitations. Implementing a zero-trust architecture, though effective, can inadvertently impede legitimate extensions and user productivity.

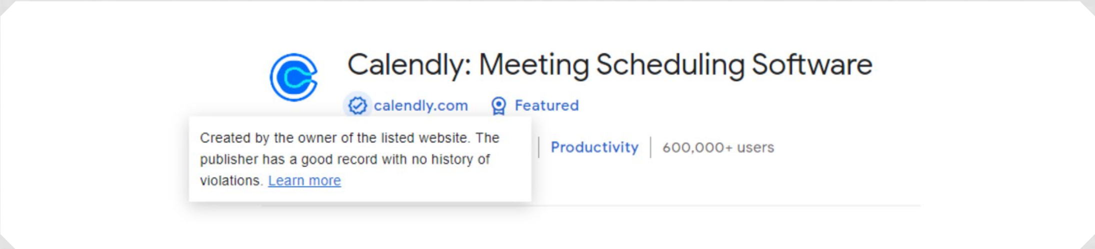
So what can we do?

1. **Download from Trusted Sources:** Only install extensions from official browser extension stores, such as the Chrome Web Store for Google Chrome or the Firefox Add-ons site for Mozilla Firefox.

2. **See When the Extension Was Last Updated:** Checking the last update of an extension is crucial, because it reflects the developer's commitment to maintaining the extension's security and functionality. Regular updates are often an indicator of a responsible developer who addresses vulnerabilities and ensures compatibility with the latest browser versions. Conversely, outdated extensions may lack critical security patches and may pose a greater risk of exploitation.

3. **Review the Privacy Practices Section and the Extension's Website:** These provide insights into the developer's transparency and data handling practices. Legitimate extensions typically provide clear and concise privacy policies detailing how user data is collected, used, and protected. Any lack of such information or vague policies can be red flags, suggesting potential misuse of user data.

4. **Research the Extension:** Track total downloads, reviews and ratings. Assessing the popularity and user feedback of an extension is an effective way to gauge its trustworthiness. Extensions with a high number of total downloads, positive reviews, and high ratings are more likely to be legitimate and safe to use. Be cautious of extensions with minimal user engagement, few reviews, or low ratings, as they may not have undergone thorough scrutiny, and their reliability could be questionable. An example of a reliable extension can be seen in the following picture:



Calendly: Meeting Scheduling Software

calendly.com | Featured

Created by the owner of the listed website. The publisher has a good record with no history of violations. Learn more

Productivity | 600,000+ users

5. **Check Permissions:** Review the permissions and extension requests. Be wary if an extension requests unnecessary or excessive permissions that seem unrelated to its functionality.

6. **Use Security Software:** Install reputable antivirus and anti-malware software that can help detect and prevent malicious extensions.

7. **Be Skeptical:** If an extension promises something that seems too good to be true or claims to offer illegal content for free, it's likely malicious.

8. **Regularly Review Extensions:** Review the extensions you've installed and remove any that you no longer use or that you suspect might be malicious.

Conclusion: In Search for a Solution that can Mitigate the Threat of Malicious Extensions

Malicious browser extensions are an active threat that is rapidly increasing. Organizations must acknowledge this risk and take action accordingly. The first step is to educate users to overcome their implicit trust in web stores and pay close attention to the permissions their downloaded extensions request.

However, similar to any other cyber threat, user awareness is not enough. The way to combat an emerging threat that targets a certain attack surface is with a dedicated technology that's purpose-built to mitigate it. One of the gravest challenges malicious extensions introduce to security teams is that beyond the scope of the existing endpoint, network, and other tools in today's security stack. Clearly there is a need for a dedicated security solution that is purpose built to mitigate these threats.

What are the core capabilities such a solution should possess? In light of the above analysis, these following capabilities are imperative:

- Scan all the extensions that were downloaded to the workforce's browser.
- Analyze of each extension based on its permissions, web store indicators, install methods and any other parameter that indicate a potential risk.
- Disable extensions that the above analysis proves to be malicious.
- Enable IT and security teams to either whitelist or blacklist extensions to proactively prevent future downloads of malicious extensions.

A solution that's capable of providing these capabilities is the most critical need for security teams today.

About LayerX

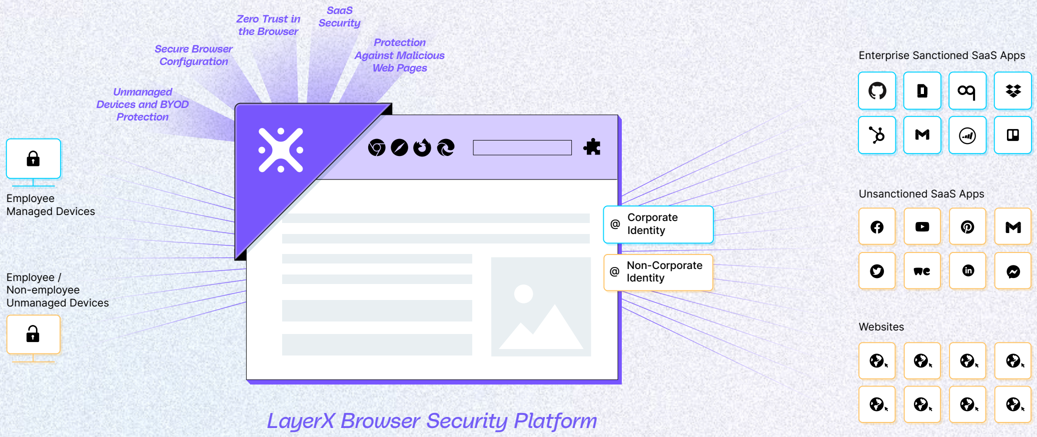
LayerX provides a secure Browser Security Platform that's purpose built to monitor, analyze and protect against any web-borne threats and data risks. Delivered as a browser extension, LayerX natively integrates with any commercial browser, transforming it into the most secure and manageable workspace.

Using LayerX, customers gain comprehensive protection against all browser extensions that either target the browser directly or attempt to utilize it as a bridge to the organization's devices, apps, and data.

The LayerX extension continuously scans all browsers in the environment to detect and analyze installed extensions. Upon discovery of extension, LayerX analyzes it and assigns it a risk score. When LayerX identifies extensions that introduce a potential risk, it disables it and enables the user to add it to a block list to prevent future downloads.

LayerX achieves this with near-zero disruption to the user's browsing experience.
With LayerX your workforce can securely browse anywhere.

Request Demo


Zero Trust in the Browser
SaaS Security
Secure Browser Configuration
Protection Against Malicious Web Pages
Unmanaged Devices and BYOD Protection
Employee Managed Devices
Employee / Non-employee Unmanaged Devices
Corporate Identity
Non-Corporate Identity
Enterprise Sanctioned SaaS Apps
Unsanctioned SaaS Apps
Websites

LayerX Browser Security Platform

KEY BENEFITS

Eliminate critical blind spots

Gain the most granular visibility into unsanctioned apps, shadow identities, DNS over HTTPS, SaaS apps, and dynamic websites.

Real-time protection

Enforce access & activity policies to restrict browsing activities that expose your apps, devices, and data to compromise.

High-precision risk detection

Multilayered AI analysis of every user activity and web session flags anomalies that can indicate risk in the browser session.

Unified browser management

Manage and configure your workforce's browsers from a single, centralized interface.

Bring your own browser

Enable your users to keep on using their browser of choice for both work and personal use.

Rapid deployment

Deploy across your entire environment and integrate with browser management tools and identity providers in a single click.