keep aware

Cheat sheet

Browser Extension Risk

A defender's quick reference for managing the real risks browser extensions bring to your organization.

Why extensions are an unmanaged attack vector

Browser extensions run as third-party code with broad access to web content, credentials, and clipboard data — making them a high-value attack surface most security teams can't see.

Declared permissions, background scripts, and content injection give add-ons the ability to silently read and manipulate browsing activity. Even trusted extensions become backdoors when their developers are compromised.

Sensitive data loss & credential theft

Read and exfiltrate clipboard data, login fields, file uploads, and page content — leading to unauthorized access and regulatory exposure.

Reconnaissance for future attacks

Monitor browsing activity, internal app URLs, and SaaS usage to craft targeted phishing and tooling-aware attacks.

Vulnerabilities & shadow IT

Outdated, unwanted, or unapproved extensions create blind spots security teams cannot audit, leaving avoidable exposure.

User manipulation

Redirect to phishing pages, inject deceptive ads, and spoof notifications to steal credentials or push PUPs and malware.

Residual effects of third-party compromise

Even trusted extensions can be hijacked, turning a trusted tool into a silent backdoor in your environment.

Indicators of a risky extension

A. Context of installation – How did it get there?

- Installed without the user's knowledge, or via popup or notification prompt
- Logged as "admin" install type but not deployed by IT or Security
- Logged as "sideloaded" or "developer" install type on a non-developer's machine
- Installed while the user was searching for something else or clicked an ad

B. Characteristics & behaviors – What can it do?

- Unknown publisher, poor reputation, or removed from the browser's official web store
- High install count paired with either few reviews or reviews flagging malware or "can't remove"
- Communicates with young, parked, expired, or low-reputation IPs and domains
- Homepage or update URL is neither the browser web store nor the vendor's domain
- Requests permissions beyond what its advertised function requires

C. Changes – What just shifted?

- Publisher changed (your data is now under a new entity)
- New domain or IP appears in the latest version (possible compromise, requires investigation)
- New permissions added without a clear justification

Most intrusive permissions to watch for

Ask: does this extension need these permissions to do what it advertises?
If not, treat the extension as a high risk application.

Permissions	Why it's intrusive
`alarm`	Schedule code to run at specific times
`all_urls`	Observe, analyze, and modify web traffic
`cookies`	Read everything the user copies, including credentials and sensitive data
`tabs`	Read browser history; create, modify, and rearrange tabs; alter page content
`webRequest`	Observe, analyze, and modify web traffic
`clipboardRead`	Read everything the user copies, including credentials and sensitive data
`management`	Access and manage other installed extensions, such as disabling security-focused add-ons
`searchProvider`	Change the default search engine to intercept user search activity and manipulate results

OWASP cross-reference: Builder risks, defender actions

OWASP's Browser Extension Vulnerabilities Cheat Sheet tells extension developers what flaws to avoid. Here is how those same flaws appear on the defender's side of the fence — and how Keep Aware can help when they show up.

OWASP vulnerability	What it looks like in your environment	How Keep Aware can help
Permissions overreach	Extension requests broad permissions (all_urls, tabs, webRequest) that don't fit its stated function.	Flag extensions with uncommon or intruvsive permissions via policies.
Data leakage	Extension posts page contents, URLs, or form data to unexpected external endpoints.	Log domains and IPs the extension communicates with; alert on unexpected destinations or domains of poor reputation; readily review destinations added to code updates.
Insecure communication	Background or content scripts call plain HTTP endpoints or update URLs.	Alert on extensions containing HTTP endpoints or update URLs.
Code injection	Extension loads remote scripts dynamically or uses eval() on fetched code.	Easily inspect background and content scripts; block extensions that fetch and execute remote code or contains otherwise suspicious code.
Malicious updates	A new version starts communicating with a newly registered domain or unfamiliar IP.	Track every version observed in your environment; alert on publisher change, communications to new destination, unexpected update sources, or significant code changes.

Quick-start checklist

- Inventory every extension across your environment
- Build a list for known-good and trusted business extensions
- Review and uninstall unapproved VPN extensions or unsanctioned password vaults
- Alert and review when a new extension is installed
- Use policies to subscribe to threat intel that flag and disable malicious extension IDs
- Identify and review every extension that requests any permission from the intrusive list above
- Flag any extension whose publisher or update domain changed
- Set up alerting on any new domain or IP introduced in an updated extension version

About Keep Aware

Keep Aware is an enterprise browser security layer that delivers deep visibility and browser detection and response across every work and AI browser. The platform prevents modern browser-native attacks, protects GenAI usage, enforces fine-grained controls over browser activity, and stops identity threats and malicious extensions — all while deploying without disrupting productivity. Request a demo to learn more.