501CISO

501C CYBERSECURITY LEADERSHIP

Powered by ClearTone Consulting, LLC

# Reviewed Browser Extensions for Privacy - 2026

Prepared by

Brian Scott

# WHY BROWSER EXTENSIONS?

Using well-known, well-maintained extensions like uBlock Origin, Privacy Badger, and Decentraleyes helps strengthen browser security and privacy while keeping performance and reliability high. These tools reduce your exposure to malicious ads, invisible trackers, and unnecessary third-party requests, which lowers the risk of malware, profiling, and data leakage. Because they are open source, backed by reputable developers or organizations, and heavily scrutinized by large user communities, problems are more likely to be caught quickly and updates delivered promptly. Using widely trusted extensions also makes conversations with customers easier, since you can refer to tools that have strong reputations, independent reviews, and clear documentation rather than niche or opaque alternatives.

Researching browser extensions before installing or recommending them is important because extensions can see and modify a lot of what happens in a browser, which means they can either protect data or quietly steal it, depending on how they are built and maintained. A small set of high-quality, well-vetted tools usually gives better security, privacy, and performance than a large mix of unknown add-ons, and it also makes it easier to explain and defend choices to customers or stakeholders.

When evaluating a new extension, a concise set of questions to review includes:

- Who is the developer or organization behind it, and do they have a track record (site, code repository, prior projects, or a known nonprofit/company) that inspires trust?
- What permissions does the extension request, and do those permissions clearly match its stated purpose (for example, does a simple visual tweak really need access to all sites and data)?
- How many users, ratings, and recent reviews does it have, and do people report problems like data leaks, aggressive tracking, or sudden behavior changes after updates?
- Is the project open source or independently audited, and does it have recent updates that suggest active maintenance and security fixes rather than abandonment?
- Does it have a transparent privacy policy that clearly explains what data is collected, how it is used, and whether it is shared or monetized?

## Contents

## uBlock Origin

uBlock Origin is a free, open-source content blocker created and still actively maintained by independent developer Raymond Hill, and it is widely regarded as one of the most trustworthy and effective ad-blocking extensions available. It has strong user satisfaction scores, no known major security incidents, and a reputation for being lightweight, privacy-respecting, and uncompromised by ad industry influence.

### Creator and background

- uBlock Origin was created by developer **Raymond** Hill (often known by his handle "gorhill").
- Hill originally developed "uBlock" in 2014, then forked it into "uBlock Origin" in 2015, which he continues to lead and maintain with contributions from an open-source community.
- His GitHub profile shows sustained, high commit activity on uBlock Origin and related repositories through 2025, indicating ongoing active development and maintenance.

### Company and reputation

- uBlock Origin is not a product of a traditional commercial **company**; it is an open-source project led by Hill and supported by community contributors.
- Independent reviews describe it as having a "legendary reputation" for being powerful, lightweight, and strongly privacy-focused, with no "acceptable ads" program or paid whitelisting.
- Security and privacy reviewers consistently call the extension trustworthy, highlighting that it does not sell user data and that its open-source nature allows independent auditing of the code.

### User ratings and adoption

- On Trustpilot, ublockorigin.com has an overall score around 4.1 out of 5, with a small set of user reviews generally praising its effectiveness, despite a few complaints about aggressive blocking on some sites.

- Browser store stats show very high adoption: by late 2025 uBlock Origin had over 29 million active users on Chrome and over 10 million on Firefox, making it the most-installed extension on Firefox.
- Tech reviewers and ad-block testing sites routinely rank uBlock Origin among the top ad blockers for efficiency and protection, reinforcing a strong reputation in the privacy and security community.

## Known concerns and issues

- There are no major recorded security breaches or data-misuse incidents associated with uBlock Origin; security reviewers explicitly note the absence of such issues.
- Practical concerns tend to be functional rather than safety-related: some users report that it can block wanted content (like certain notifications, horoscopes, or emails) until they whitelist a site or adjust filters.
- A current strategic concern is Google's Manifest V3 extension platform for Chrome, which reduces what powerful blockers can do; this has forced the creation of a "uBlock Origin Lite" for Chrome with reduced capabilities and led to warnings in the Chrome Web Store about limited functionality under V3.

## Executive summary (what it does)

- uBlock Origin is a browser extension for Chromium-based browsers (Chrome, Edge, Brave, Opera) and Firefox that filters network requests to block ads, trackers, pop-ups, and many types of unwanted or malicious web content.
- It relies on community-maintained blocklists plus user-configurable rules to stop ads, tracking scripts, cryptocurrency miners, and some soft paywalls, while remaining resource-efficient so it uses less CPU and memory than many competing blockers.
- Advanced features include cosmetic filtering (removing visual ad elements), per-site rule controls, and options like temporarily disabling JavaScript on sites to reduce attack surface, aimed at more technical users who want fine-grained control over what runs in the browser.

## Privacy Badger

Privacy Badger is a free, open-source anti-tracking browser extension created by the Electronic Frontier Foundation (EFF) to reduce third-party tracking and enforce privacy signals like Global Privacy Control (GPC) and Do Not Track (DNT). It's best described as a tracker blocker (not a full ad blocker), and it's generally well-regarded because it's produced by a long-standing digital rights nonprofit rather than an ad-tech vendor.

### Creators and organization

- Privacy Badger is developed and published by the **Electronic Frontier Foundation (EFF)**, a nonprofit digital rights organization.
- The project is maintained openly on GitHub under the EFForg organization, with community contributions and public issue tracking.
- EFF positions the extension as a tool to stop online spying by blocking trackers that ignore privacy signals, rather than primarily targeting ads.

### Company reputation (EFF)

- EFF is widely known for digital privacy and civil liberties advocacy and is a prominent nonprofit in the web privacy space.
- Privacy Badger's credibility is strengthened by being open source and governed as an EFF public project, rather than being tied to monetization like "acceptable ads" programs.
- Major tech reviewers characterize Privacy Badger as a useful privacy tool, particularly for blocking trackers that list-based blockers may miss.

### User reviews and ratings

- Privacy Badger is distributed through major extension stores like the Chrome Web Store and Firefox Add-ons, where it is presented as an EFF-made tracker blocker.
- Published hands-on reviews and tests tend to rate it as "decent" at ad blocking but stronger as an anti-tracker, and often recommend pairing it with a dedicated ad blocker for maximum coverage.

- Some testing-based reviews publish numeric scores (example: one review reports 63/100 on AdBlock Tester and 2/3 on “Can You Block It”).

### Known concerns and limitations

- EFF previously changed Privacy Badger’s default behavior to rely on a “pre-trained” list (Badger Sett) rather than per-user local learning by default, citing risks that local learning could be abused for fingerprinting or limited history sniffing.
- Because it focuses on tracking behavior, it may not block all ads (for example, one review noted it did not block YouTube ads in their test).
- As with many privacy extensions, site breakage can happen when third-party resources are blocked, though Privacy Badger provides per-site controls to adjust blocking.

### Executive summary (what it does)

- Privacy Badger detects and restricts third-party domains that appear to track users across websites, reducing cross-site surveillance.
- It sends privacy signals (GPC and DNT) and escalates to blocking when trackers ignore those signals.
- It also includes features such as cookie/referrer restrictions for suspected trackers and click-to-activate placeholders for certain embedded widgets (like video players or comment tools).

## Decentraleyes

Decentraleyes is a free, open-source browser extension by developer Thomas Rientjes that locally emulates popular content delivery networks (CDNs) to improve privacy and sometimes speed. It is generally well-reviewed by users and privacy sites, with no major security incidents reported, though it has some functional limitations and occasional compatibility issues.

### Creator and background

- Decentraleyes was created and is maintained by **Thomas** Rientjes, an independent developer who distributes the project under the Mozilla Public License 2.0.

- Project information pages and extension listings explicitly credit him as the author and show ongoing maintenance and updates (for example, version 3.0.0 updated in November–December 2024).
- The project has an established history dating back to its first release in late 2015, initially for Firefox and later expanded to Chromium-based browsers and others.

## Reputation and trust

- Decentraleyes is positioned as a privacy-enhancing tool that complements, rather than replaces, traditional ad or tracker blockers.
- Security and privacy-focused write-ups describe it as a small, transparent extension with publicly available source code and a clear, narrow focus on replacing CDN requests, which contributes positively to its **reputation**.
- It has been recommended by tech and privacy outlets (for example, LinuxSecurity and others) as a way to reduce data exposure to large CDNs without breaking most websites.

## User ratings and adoption

- On the Chrome Web Store, Decentraleyes (version 3.0.0) shows a rating around 4.7 out of 5, based on roughly 240+ user ratings, with many reviews praising its “set-and-forget” design and privacy focus.
- Chrome usage statistics report on the order of 200,000+ daily users, with an average rating of about 4.78 from more than 1,500 reviews.
- It is also available on Firefox and other browsers, and is commonly listed in curated privacy-tool collections, which indicates a solid niche adoption among privacy-conscious users.

## Known concerns and limitations

- A practical limitation is coverage: Decentraleyes only bundles a finite set of common JavaScript libraries and CDNs, so it will not intercept every CDN request; when a library is not bundled, the request may still go out or rely on additional privacy tools.

- Some reports note that, in certain Firefox versions, Decentraleyes may fail to intercept specific CDN requests as expected, and that there is little visible logging or error feedback, which can make troubleshooting difficult.
- Community discussions have raised temporary availability issues (for example, the developer's self-hosted Git repository being briefly down), but these were resolved by the developer and were not tied to any extension compromise.

## Executive summary (what it does)

- Decentraleyes intercepts requests to major third-party CDNs (such as Google Hosted Libraries, Cloudflare's CDNJS, jsDelivr, and others) and serves matching libraries (like jQuery, AngularJS, and similar) directly from a locally bundled cache instead.
- By satisfying sites' library requests locally, it reduces the amount of information those CDNs receive about which sites a user visits, improving privacy and sometimes reducing latency.
- It is designed to run automatically out of the box with no configuration, and is explicitly intended to complement blockers like uBlock Origin or Privacy Badger rather than replace them.