DATA SHEET

Menlo Security Browser Posture Manager

Reduce Your Organization's Attack Surface with Browser Extension Control and Benchmarked Policies

Control browser extensions

Automate standards compliance

Customize policies for different users and groups

The browser is the most used application in the enterprise. It's also the one most likely to be treated like a utility — managed loosely, reviewed infrequently, and assumed to be someone else's problem.

That assumption has a cost. Browser management typically falls between security and IT teams, with neither owning it fully. The tools to manage browsers and extensions exist — Chrome and Edge both expose extensive policy controls — but parsing through thousands of options against a security benchmark is tedious work, and it rarely rises to the top of anyone's list. The result is a browser environment that drifts: policies unenforced, extensions unreviewed, and a growing layer of risk that most security tools weren't built to see.

Menlo Browser Posture Manager was built to close that gap — making it straightforward to define a secure browser baseline, benchmark your policies against recognized standards, review extensions, and push consistent configurations to your managed fleet.

> " Web browsers are the primary access method for most modern corporate applications and provide an endpoint-agnostic enterprise security control point. " [1]

KEY BENEFITS

Safeguard users against browser extensions that are outdated, insecure or malicious, while pushing those that you want

Stay in compliance even as browsers themselves change.

Differentiate policies by users and group.

The Extension Problem Is Growing Faster Than Most Teams Realize

Browser extensions have become a serious and underappreciated attack vector. Because extensions sit inside the browser — with privileged access to sessions, credentials, and sensitive data — attackers can use them for surveillance, session hijacking, and credential theft without deploying a single piece of malware. In many cases, users never see a warning.

The scale of the problem is significant. As recently as February 2026, researchers uncovered a network of malicious Chrome extensions with more than 37 million combined users.[2] AI-themed extensions are now the fastest-growing category of malicious extension: the first appeared in early 2023, promising quick access to ChatGPT. This extension, and others to follow, evaded notice because they delivered what they promised — and quietly hijacked Facebook accounts and stole session cookies in the background.

With more than 100,000 extensions in the Chrome Web Store alone, no review process catches everything. And your users are likely to be installing extensions you haven't approved, on devices you manage, with access to data you're responsible for, all in service of getting their work done.

Browser Policy Compliance Is Harder Than It Should Be

Between Chrome and Edge, there are thousands of configurable policies — and most organizations enforce only a fraction of them. The benchmarks that define secure configurations — CIS, DISA, and others — are long, technical, and not easy to parse. Mapping your current configuration against them manually is the kind of work that gets scheduled and then postponed.

Compounding the challenge: compliance rules don't change often, but browsers do. A configuration that was benchmark-aligned last quarter may not be this quarter, because the browser vendor updated their product. Staying current requires ongoing attention that most teams can't consistently apply.

The result is a compliance posture that drifts quietly, often invisibly, until an audit or an incident makes the gap visible.

Browser Posture Manager Closes Both Gaps

Menlo Browser Posture Manager gives your security and EUC teams a practical way to take control of browser extensions and policy compliance — without turning browser management into a dedicated workstream.

Define and Enforce a Safe Extension Baseline

The process starts by exporting your browser configuration as a .JSON file — a step that takes less than a minute. That file becomes the baseline Browser Posture Manager works from: think of it as a golden image for your managed devices. BPM reads the extensions associated with that configuration and gives your team a clear view of what's there, so you can decide what stays, what gets blocked, and what gets replaced.

For extensions where you're uncertain, BPM integrates with spin.ai to provide a third-party risk score, giving you an objective basis for the decision. If a flagged extension provides functionality your users depend on, it's straightforward to identify an approved alternative with an acceptable risk score.

Extensions you want your users to have can be delivered via force-install — your team selects them and pushes them to the relevant devices when you're ready to deploy. Extensions that shouldn't be there are blocked. Your managed fleet runs the set of extensions your team has reviewed and approved, not whatever users have installed on their own.

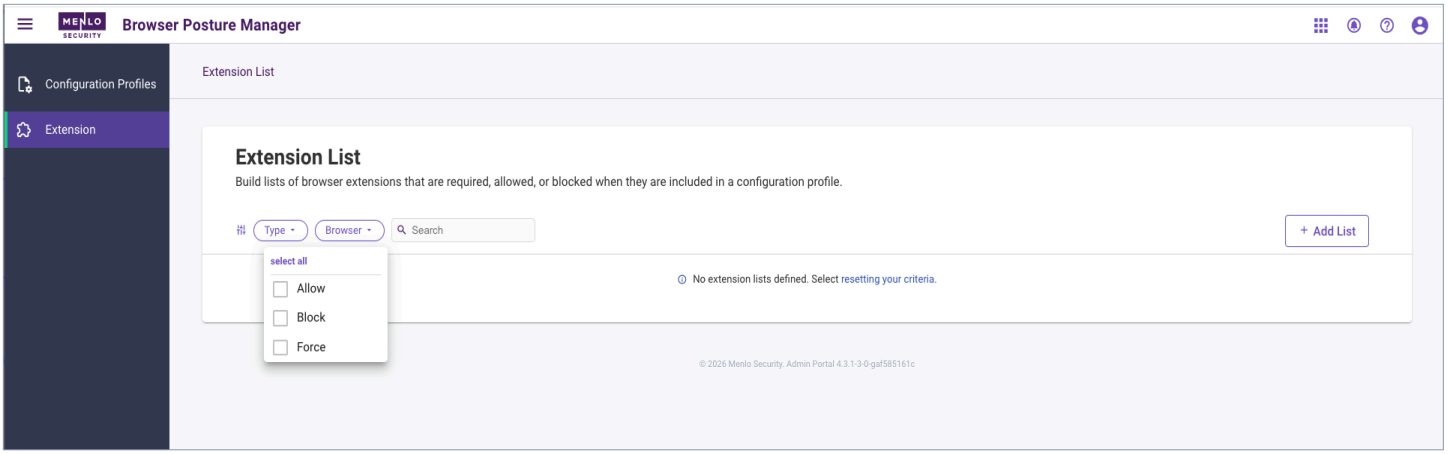


Figure 1-Select to Allow, Block or Force-Install Extension

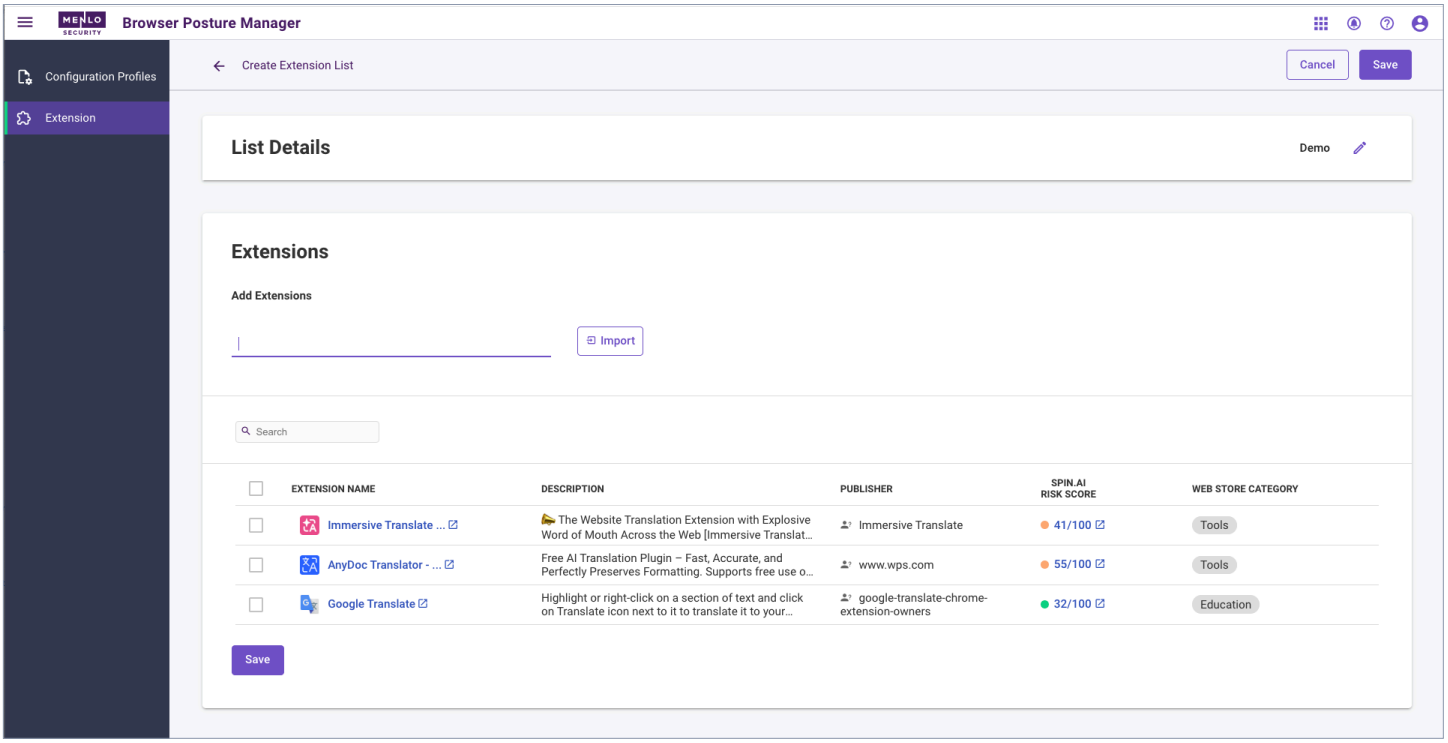


Figure 2 - View Extension Risk Score

Benchmark Your Policies and Close the Gaps

Upload your .JSON configuration to Browser Posture Manager and select the benchmark you need to comply with — CIS, DISA, or others — along with the appropriate security level. BPM immediately compares your current configuration against the benchmark specifications and returns a prioritized list of gaps. Menlo has even created its own set of benchmarks that you can use to stay secure between benchmark updaes.

Suggested changes are presented in order of importance: first, policies that directly conflict with the benchmark; then, settings where the default is insecure. Each recommendation includes a plain-language explanation of the policy itself — including implications you may not have considered — so your team can make an informed decision rather than applying changes without context.

Once you've selected or adapted the policies that fit your environment, you can export the profile, using configuration management infrastructure you already have. Your policies stay current until the browser vendor changes their product — at which point the same straightforward process brings you back into alignment.

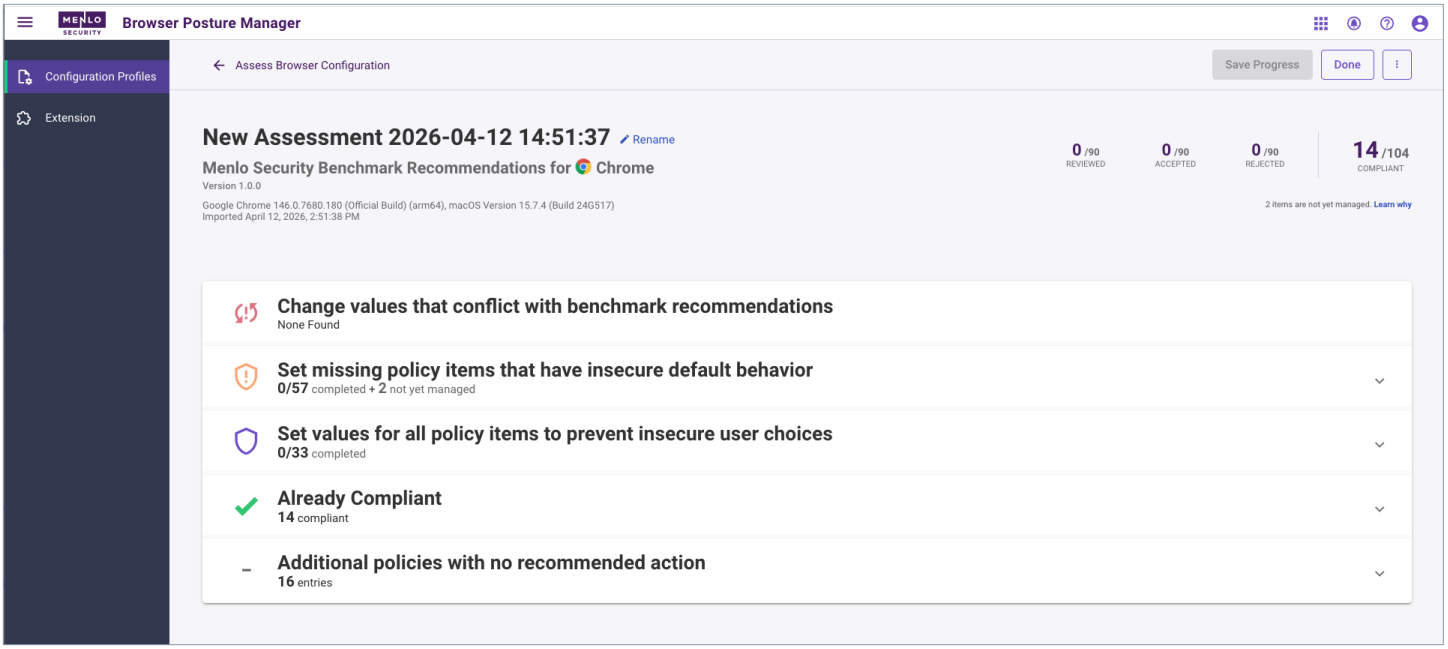
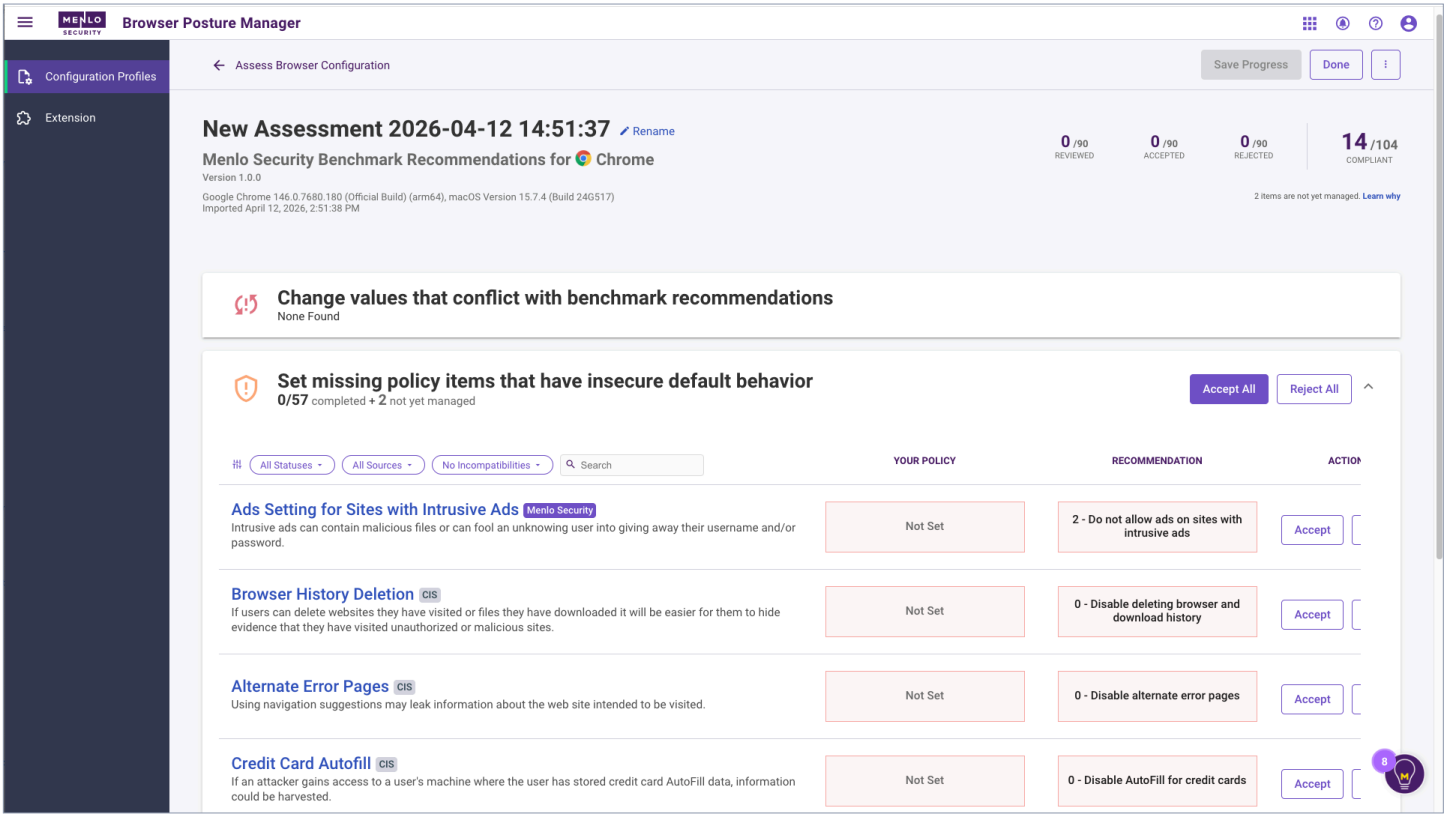


Figure 3 - Get an Overview of Suggested Browser Policy Changes to Meet Benchmarks



4 - Get Detailed Suggestions; You Decide Best Fit

What Changes with Browser Posture Manager

Your managed fleet runs a defined, reviewed set of extensions. Your browser policies are aligned to a recognized benchmark, with a clear record of where they stand. The browser— which has historically been managed by exception, if at all — is governed with the same consistency you apply to the rest of your security stack.

Your security team has an auditable record of your browser posture. Your EUC team has a repeatable process for keeping it current. And your users keep working without interruption, because the extensions they need are still there — reviewed, approved, and consistently deployed.

Manage the Browser with Menlo Security

Highly evasive and advanced threats (HEAT attacks) increasingly target the browser precisely because it's been treated as a utility rather than a critical control point. Browser Posture Manager changes that. Your attack surface shrinks. Your policies hold. Your team has a repeatable, low-overhead process for keeping the browser environment consistent — and the browser finally gets the governance it's always deserved.

[1] Gartner. April, 2025

[2] https://www.securityweek.com/over-300-malicious-chrome-extensions-caught-leaking-or-stealing-user-data/

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Cloud. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Cloud prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Learn more: https://www.menlosecurity.com
Contact us: ask@menlosecurity.com