MENLO SECURITY

Data Sheet

Menlo Security Browser Posture Manager

Reduce your organization's attack surface with proven, benchmarked policies

The need to secure enterprise browsers has never been higher, as bad actors are increasingly targeting vulnerable browsers with Highly Evasive and Adaptive Threat (HEAT) attacks. Despite the fact that the browser is understood to be the most widely used application in business, most enterprises struggle to manage it well.

A big part of the problem is what "managing the browser" actually entails. Google Chrome has thousands of policies, of which a tiny fraction are typically enforced. The stats on Microsoft Edge are similar; out of thousands of policies, just a few dozen are enforced on average. With that amount of policies to consider, it is impossible for oversubscribed security teams to know exactly which are important. The result is that about 45% of browser configurations return errors, while over 60% have explicit extension policies.

Things to know:

By 2027, the enterprise browser will be a central component of most enterprise superapp strategies.[1]

Chrome releases a full OS update about every 4 weeks. Minor updates, such as security fixes and software updates, happen every 2-3 weeks.[2]

Between November 2022 and November 2023, 175 CVEs classified as high or critical were issued.

133 new features were added to Chromium in 2023.

1 https://resources.menlosecurity.com/all-content/state-of-browser-security-defending-browsers-against-zero-hour-phishing-attacks, Emerging Tech: Security — The Future of Enterprise Browsers — Gartner, April 23

2 https://support.google.com/chrome/a/answer/3168106?hl=en#:~:text=Chrome%20releases%20as%20full%20OS,happen%20every%202%E2%80%933%20weeks

Not only is the array of available policies overwhelming, but the browsers themselves are constantly changing. Google Chrome issues a full OS release about once a month, with minor updates, including security fixes and software updates, every two to three weeks. Microsoft Edge is now scheduled to release major updates every four weeks, following the Chromium schedule. Whether updates are based on security or bug fixes or on new feature additions, the task of staying up to date with supporting policies becomes more difficult with every release. A few of the new settings introduced by Chrome in 2023 included:

- **HttpsUpgradesEnabled** – This setting ensures that most of your traffic ends up using HTTPS rather than HTTP.
- **SafeBrowsingDeepScanningEnabled** – This setting has implications in terms of how well file scanning will work as well as privacy/DLP concerns around files being shared with Google.
- **PasswordSharingEnabled** – This option, enabled in Google Canary, is designed to let users share passwords with others, such as family members. Regardless of the intent, the setting is likely to be inappropriate for enterprise use.
- **HelpMeWriteSettings** – This feature, which is already available in Gmail and Google Docs, uses generative AI to compose text. Like any other use of generative AI, it is important to weigh benefits against possible privacy and DLP issues that could arise.
- **DomainReliabilityAllowed** – This feature, designed to help verify that users can request and reach Google domains, has privacy implications.
- **WindowManagementAllowedForUrls** – This setting, along with the companion blocking option, may have been introduced to reduce attack surface. That said, it may also conflict with other methods chosen by the security team.

Each of these policy options require analysis to understand the deeper implications and make a decision on how to enforce, and each update has many such choices. The browser update schedule is slated to become even more frequent, at least partly because Chromium, which powers Chrome and many other browsers, is an open source project. As most security practitioners will agree, open source software provides a level of testing, transparency, and accountability that closed or proprietary systems do not. If there is a downside, however, it is the very visibility that open source projects provide. Malicious entities can view comments and changes and craft exploits for users that haven't yet received the security fix — a tactic known as "n-day exploitation."[2]

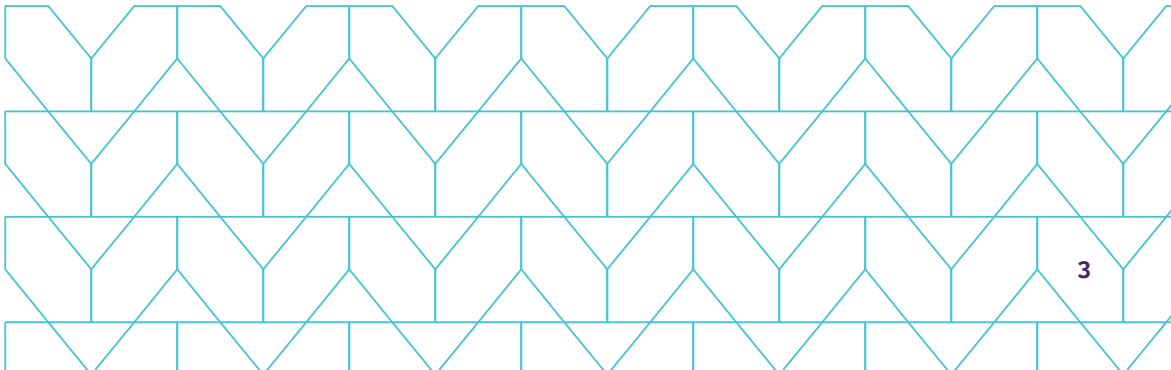
One of the worst aspects of handling your own selection of policies in a browser is determining which changes will make meaningful changes in enterprise security. The best way to handle this question, if you do it yourself, is also the most costly and difficult: continuous, data-driven benchmarking. The process is not only time-consuming, but it requires security personnel that most organizations simply don't have.

Browsers provide the initial foothold for cyber adversaries. With the rising frequency and complexity of threats targeting the browser, particularly those classified as HEAT attacks, the need to secure the browser attack surface has become increasingly critical. Menlo Security Researchers observed a 206% increase in attacks classified as evasive.[3]

How can you possibly keep up?

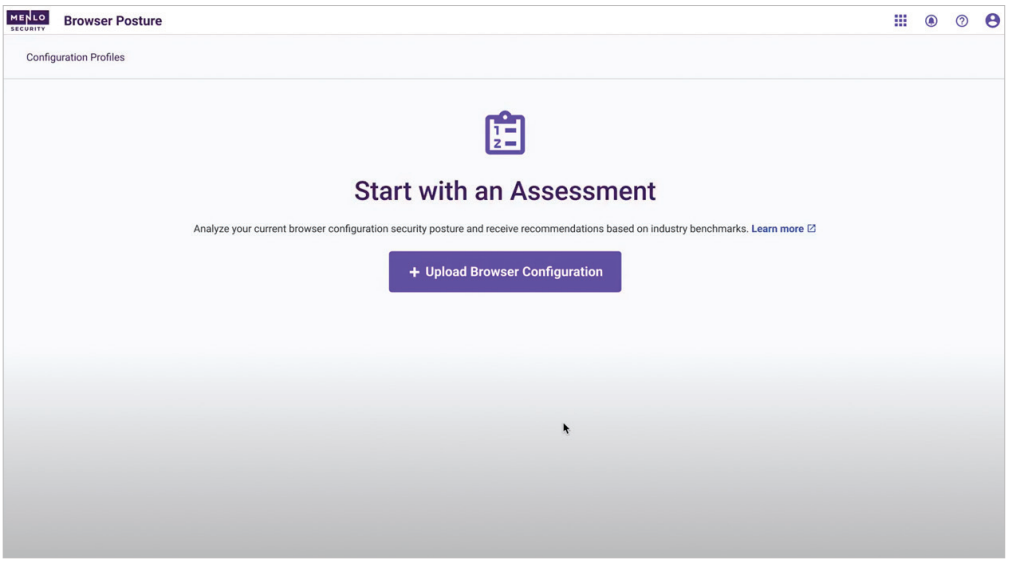
With so many changes continuously occurring within browsers, it is extremely difficult to keep up. The good news is that with Menlo Browser Posture Manager, you don't have to. Menlo is constantly monitoring changes to browsers, and it enables you to compare how you stand against updated benchmarks anytime.

3 https://resources.menlosecurity.com/all-content/state-of-browser-security-defending-browsers-against-zero-hour-phishing-attacks



Get real-world browser policy benchmarks from the experts

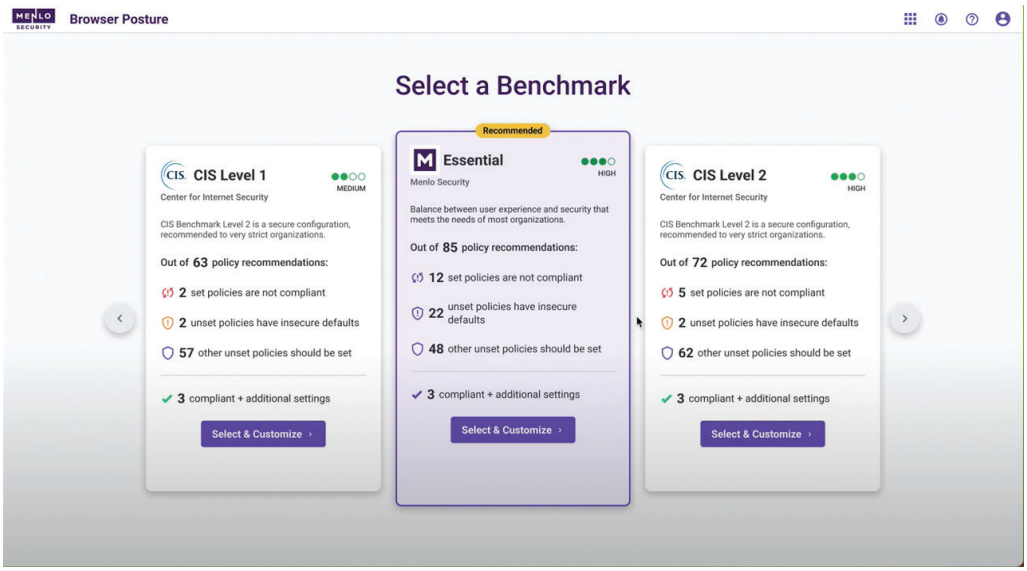
Menlo Security, the leader in enterprise browser security, makes the process easy and automatic with our new Brower Posture Manager. With a few clicks, you can see exactly how your browser security policies compare with a variety of policy benchmarks. Security teams only need to upload a configuration file, and Menlo Security will compare what you have in place with known best-in-class configurations.



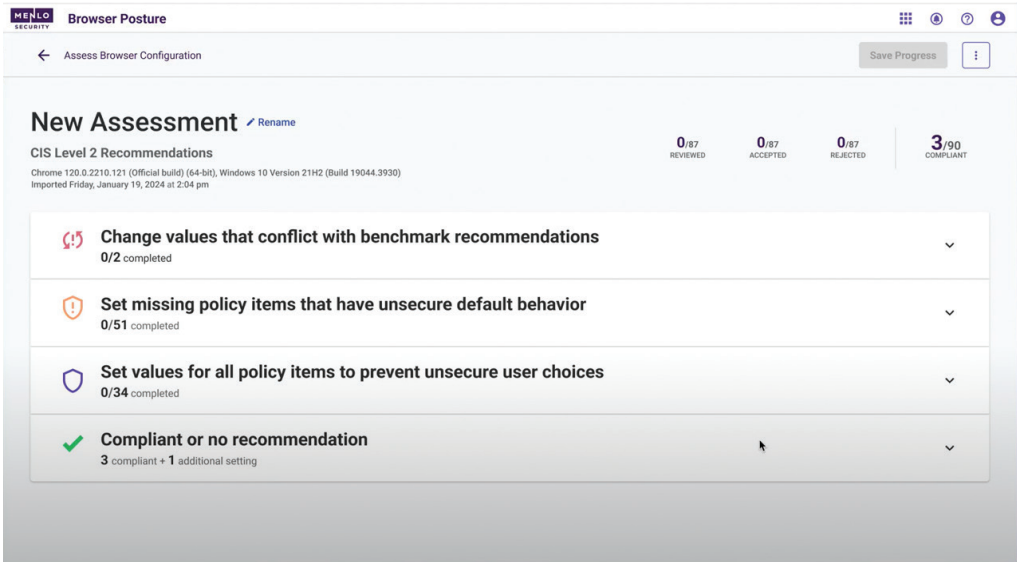
A few comparisons with benchmarked policies include:

- Control use of Web Bluetooth API
- Control use of Web USB API
- Limit access to Chrome remote desktop control
- Require timely application of security updates

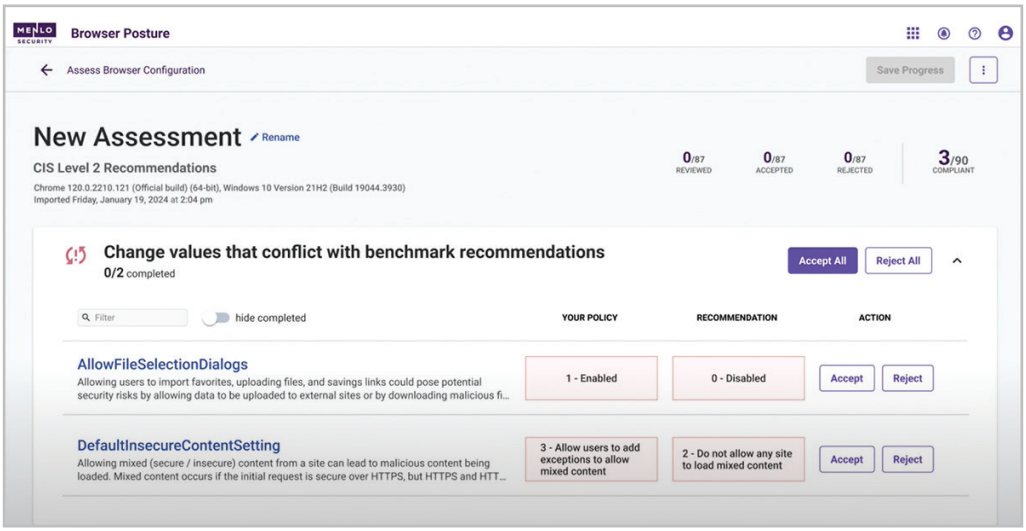
With Menlo Security Browser Posture Manager, you can manage your choice of Chromium-based browsers, including Google Chrome and Microsoft Edge, which make up over 90% of the browsers used at work.



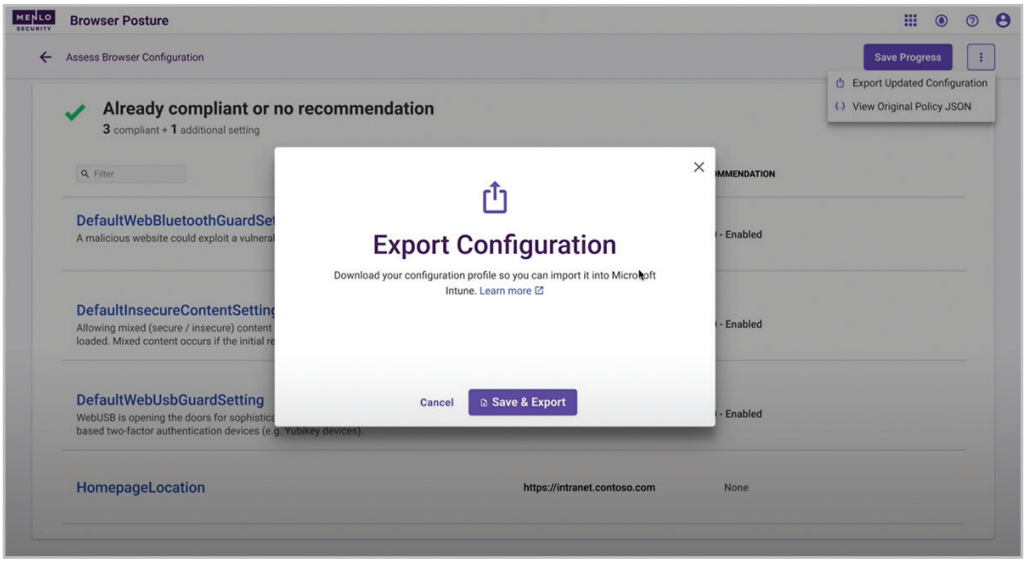
Not only will Menlo call out the disparity between your browser configuration and best practice benchmarks, but we will provide specific suggestions regarding what to change in order of possible security ramifications...



When the user clicks onto the set of assessment, Menlo goes a step further. Not only do we show you each specific policy, we explain it. This can give you enough details to accept or reject policy changes, because you know your environment — and your users — best.



Once you've decided which policies make sense, it is a simple matter to export the configuration.



Menlo Security makes getting — and keeping — secure browser policies as easy as 1, 2, 3

1. **Upload**

   Begin the process by uploading a JSON file listing your browser configuration.

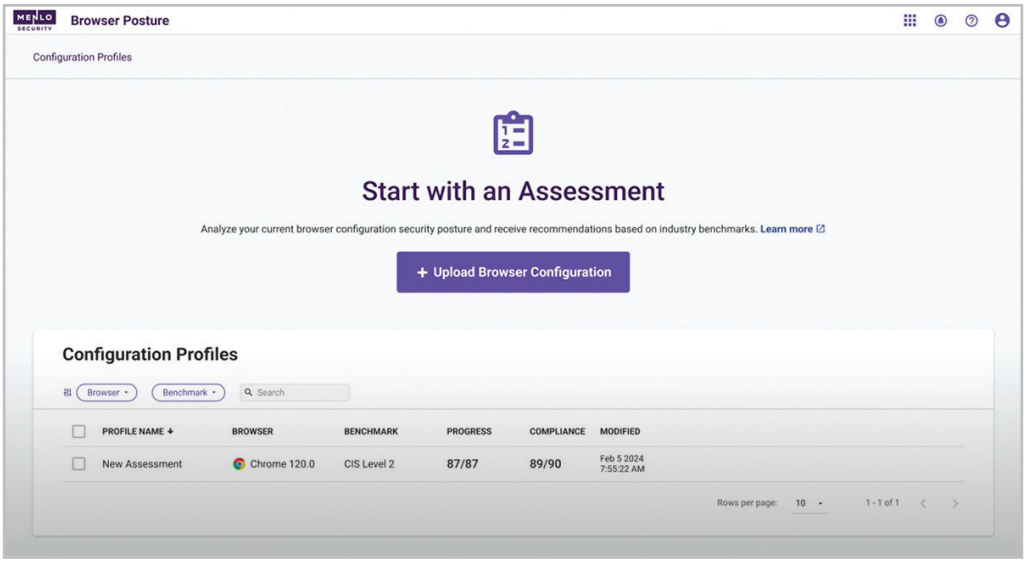
2. **Review**

   Menlo Browser Posture Manager will compare your configuration against those employed by benchmarking experts. Menlo then goes even further, calling out configurations that conflict with benchmarks as well as those that are outside security best practices.

3. **Deploy**

   Once you've selected or adapted the set of security profiles that fit your situation most closely, Menlo Security has simplified the process of deployment. You can leverage Microsoft Intune to handle configuration management of existing browsers, or you can automate the process via Intune integration.

Menlo even reminds you of policy recommendations that have not been reviewed before you push out the configuration. And if you want to review the comparison with these benchmarks at any point, the assessments are automatically saved.



Manage the browser with Menlo Security

With Browser Posture Manager, you can keep your security team, your corporate leadership, and your users happy. As Highly Evasive and Advanced Threat (HEAT) attacks proliferate and target browsers, your attack surface has expanded rapidly. With confidence in enterprise browser security policies and an automated way to deploy and update them, you can finally take control of enterprise browser security — without forcing your users to compromise.

About Menlo Security

Menlo Security eliminates the browser attack surface by allowing IT and security teams to properly manage their existing browsers, protect their users, and secure application access and enterprise data to provide a comprehensive browser security approach.

Menlo allows enterprises to secure their existing browsers by providing real-time dynamic policy controls to effectively stop evasive malware, zero-hour phishing attacks, and ransomware payloads from infecting your endpoints and enterprise systems.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling Zero Trust access that is simple to deploy. The Menlo Secure Cloud Browser 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.

Work without worry and move business forward with Menlo Security.