MENLO SECURITY

White Paper

Menlo Security Browser Posture Manager

Browsers in the enterprise

Web browsers have become a vital component of business today. According to Gartner, by 2027 the enterprise browser will be a central component of most enterprise superapp strategies.[1] The browser is used today to access a variety of apps and content that previously required everything from VDI deployments to endpoint clients.

As of 2024, Chromium-based browsers, including Google Chrome and Microsoft Edge, are the most prevalent, with Google Chrome holding over 63 percent of the global browser market share, with more than 3.2 billion internet users.[2] Microsoft Edge has a desktop market share of approximately 11 percent.[3] While we may believe that we know these browsers — and many of us have been using them since we were old enough to reach a keyboard — there are elements of these powerful apps that are unfamiliar to most people, including security staffers.

These elements matter for several reasons. Browsers have become unbelievably complex, and they do their jobs exceptionally well. Unfortunately, in some cases, the browser's job centers around enabling consumer behavior and building the browser vendor's ecosystem. This may not be a negative — it is arguable that by turning the browsers that users know and love into Secure Cloud Browsers, it's possible to ensure an experience that satisfies end users as well as enterprise security.

As browsers evolve, they are becoming less like an app, and more like an operating system.[4] The browser offers many features, from direct app access and built-in use of GenAI, to remote desktop capabilities and integration with other services. All of these capabilities are great for consumers (and Chromebooks), but they can compromise enterprise security in potentially unexpected ways.

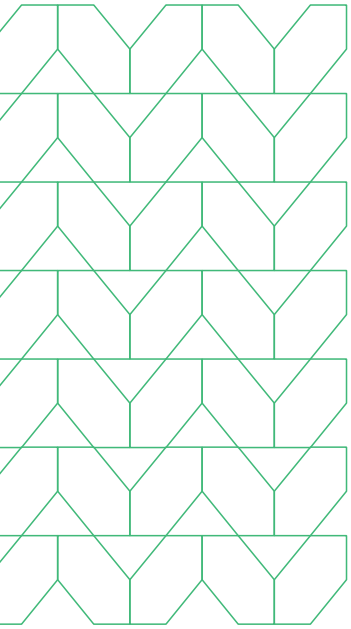
Another complication is that browsers have so many policies that can be implemented. Truly managing these policies – to get the most functionality without damaging security or data privacy requirements – requires time and focus for often oversubscribed IT teams managing the network, security, or desktops. At the same time, these policies must be managed to meet compliance requirements. In many cases, new features are enabled by default and must be explicitly sought out and judged on a policy-by-policy basis. Doing nothing about browser policies is rapidly becoming an unacceptable approach.

[1] Emerging Tech: Security — The Future of Enterprise Browsers – Gartner, April 23

[2] https://www.demandsage.com/chrome-statistics/

[3] https://www.browserstack.com/guide/understanding-browser-market-share

[4] They are the operating system of Chromebooks, for example.



The local browser and the Menlo Secure Cloud Browser

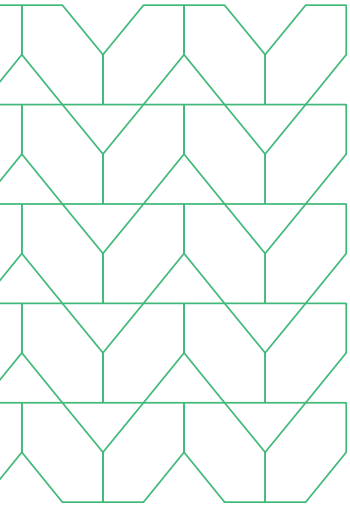
Browser posture control is an important piece of end-to-end browser security and a layered security stance in general. The Menlo Secure Cloud Browser provides a critical security capability, taking the execution of web content off the endpoint and into the Menlo cloud. This protects critical corporate data and defends against malware exploits. But even when isolating web sessions, the endpoint browser controls many aspects of how users interact with the web, including managing passwords, validating HTTPS connections, determining what types of data are shared with external services, and more. Menlo Browser Posture Manager adds a vital layer to any enterprise defense-in-depth strategy and contributes important context to security overall.

The Menlo Browser Posture Manager simplifies the process of controlling browser policies with a central dashboard, step-by-step instructions, and detailed information on how your current configuration differs from those established by benchmarking experts. At the same time, you remain in control. No two enterprises are identical, and they should not be treated as such. You have the option to accept or reject policy suggestions, because you know what will work for your users.

Types of browser policy controls

When describing the many browser posture settings, Menlo uses three broad descriptive categories to highlight the effect that these settings can have in the enterprise; note that some settings touch on several categories. Categories include:

- **Settings that affect data privacy:** These settings impact how the content within web pages is controlled. The key consideration here is to ensure that site data stays within the browser on the desktop and is not sent to external services. Leading browsers include consumer-oriented features that are enabled by default, including settings to allow sites to query available purchase methods or sharing site data with an external service to assist with shopping recommendations.
- **Settings that extend the attack surface:** Some browser policies pertain to features that manage optional security controls or disable optional features, including those available in the JavaScript execution environment. One example is JavaScript APIs, which can give websites access (or allow the site to ask for access) to endpoint Bluetooth or USB devices if enabled or not explicitly disabled.
- **Feature enablement:** Browsers have many security-related features that act as meaningful layers in the security stack. These can include TLS and certificate behaviors, or file upload/download controls. Controlling these settings properly contributes to the overall defense-in-depth stance of the enterprise. But some features may allow capabilities more suited to consumers than to enterprises.



Policy classifications

Menlo Browser Posture Manager classifies policies when performing a browser assessment, ranking them in terms of their importance to review and manage when considered against an established benchmark, such as the Center for Internet Security (CIS). The policies are then displayed in order, along with a concise explanation and the opportunity to accept or reject the suggestion. Classifications include:

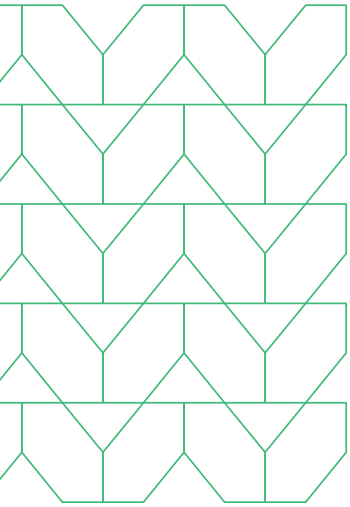
- **Highest priority: Managed settings that conflict with the benchmark.**
  These are settings that may have been explicitly configured in an MDM tool, but conflict with benchmark recommendations. There may be valid reasons for a setting in the enterprise, but these policies are important to review. You can then choose whether the benchmark setting should be used or if you would prefer to stay with the previous configuration.

- **Medium priority: Browser defaults that conflict with benchmark recommendations.**
  These are settings that have not been managed by corporate MDM, but are defaults chosen by the browser vendor. Some of these may seem helpful at first glance, but it's important to review them prior to determining whether to keep them enabled. Some such settings may change the end-user experience. Another consideration is that some settings, if not explicitly accepted or rejected, are assumed to be enabled.

- **Lower priority: Browser defaults that match benchmark recommendations.**
  Many of the browser vendors have chosen to implement policies that are consistent with the recommendations for secure configuration. However, browser defaults can often be overridden by an end user manipulating settings within the endpoint browser. To prevent that action, these settings should be included in MDM management, which controls these settings in a way that cannot be overridden by a user. Because these settings do not modify standard browser behavior, they require less review; often the "Accept All" option in Browser Posture Manager can be used to take control of these policies.

- **Informational: Already compliant and additional policies.**
  "Already Compliant" settings already match the benchmark guidelines and do not require modification. These may be settings that are already managed by corporate MDM, or browser defaults that do not require a modified setting to control them.

  The "Additional Policies" section displays any other policies that were included in the policy export, but do not align with policies managed by the benchmark. These may include policies that are part of corporate Windows endpoint management, customization of home pages, or new tab URLs.



Browser policy examples

The following section includes representative examples of browser policy settings, what they control, and why they are important. These examples illustrate the types of data that is being managed by these policies and why enterprises should review them to determine their own browser posture rather than relying on manufacturer defaults. As mentioned earlier, some settings have ramifications that fall into more than one of Menlo's categories. In those cases, we have listed the policies with security implications (those that affect data privacy or the attack surface) first. Note: these are merely examples of policies and not an exhaustive list, as there are thousands to consider.

Examples of policies that affect data privacy

- **Policy:** TranslateEnabled
  Classification: Data Privacy
  Description: Control page translation capabilities

  Browsers can translate the content within a webpage to convert it into the user's language of choice. When this translation is performed, the content from the page is transferred to a cloud service and the content is returned in the desired language. This sharing of content can apply to any site loaded by the browser, including internal private sites or those requiring corporate logins. Each organization should decide if this level of sharing is appropriate.

  If you set this policy, users cannot change the function. If it is left unset, users can change the setting.

- **Policy:** SearchSuggestEnabled
  Classification: Data Privacy
  Description: Control browser search suggestions

  Browsers can offer search suggestions based on what is being input into the address bar. This capability submits data about the content being submitted to cloud services to provide suggestions to the end user. This process can divulge internal information about a user's browsing behavior, including internal sites, services, and topics.

  If you enable or disable this policy, the user cannot change it. However, if it is left unset, users will get suggestions (though they can disable them). To maintain data privacy, it is usually best to specifically disable it.

Examples of policies that broaden the attack surface

- **Policy:** SSLErrorOverrideAllowed
  Classification: Attack Surface
  Description: Control the ability to proceed beyond browser HTTPS warnings

  Users will see a warning page when certificate errors occur on requested page loads. This can happen when the browser URL does not match the domains within the site's certificate or when a certificate has expired.

  If this policy is not specifically disabled, the user can proceed to load the website in question. If the policy is left unset, the user may choose to ignore the warning. Rather than allowing each end user to proceed and judge whether the site is malicious, the option to proceed should be removed by disabling this policy.

- **Policy:** DefaultInsecureContentSetting
  Classification: Attack Surface
  Description: Control whether parts of sites can be loaded insecurely

  Browsers warn the user when a site is loaded without HTTPS encryption, but the security of data loaded within a page is harder to determine. An HTTPS site can load resources or upload info via HTTP sessions. By default, mixed content is permitted, and can leave site data open to observation or modification. It's not obvious because there is no visual indicator of what is going on under the covers.

  This setting blocks those background requests if they are not HTTPS encrypted. As an example, if a user were on a secured site, such as a banking site, the site might try to load an image or video over HTTP.

  This setting can block insecure sessions from being used.

- **Policy:** ConfigureOnlineTextToSpeech
  Classification: Attack Surface
  Description: Disable online text-to-speech APIs to reduce attack surface

  Websites can control the operating system text-to-speech capabilities from within the JavaScript execution environment, which allows the site to manipulate the settings related to the spoken content. This function increases the attack surface within the JavaScript execution environment, and this API has been shown to be vulnerable to remote code execution. Endpoint tools should be used for this accessibility function, without allowing the website or the JavaScript within it to directly manipulate APIs. A Microsoft blog on the related vulnerabilities with this API can be found here.

- **Policy:** AudioSandboxEnabled
  Classification: Attack Surface
  Description: Enable sandboxing of audio processes

  Chromium browsers separate the execution of key components into distinct processes for security. This model can be extended to include more aspects, such as processing of audio data for processes that could include audio playback from websites, audio recording with input like video calls or web conferencing, audio processing for things like online audio editing tools, and audio routing which directs output to different devices like speakers or headphones.

  While setting this policy to enabled could marginally increase resource usage, it is good security practice to do so, as the isolation provided helps to make sure that the audio data is not misused.

- **Policies:** DefaultWebBluetoothGuardSetting, DefaultWebUSBGuardSetting
  Classification: Attack Surface
  Description: Control use of web Bluetooth and USB APIs

  The modern browser includes interfaces to communicate with endpoint devices via USB and Bluetooth. These capabilities expose APIs to the JavaScript execution environment, which can allow websites to interact with physical devices. There may be consumer use cases where this will be useful, but for corporate devices it represents a new area of complexity and an increased attack surface.

  Within an enterprise setting, both policies should be set to "2," which does not allow a site to ask the user for access. If the policy is set to "3," any site may ask for access. If left unset, sites can ask for access, but users can disable that function.

- **Policy:** PaymentMethodQueryEnabled
  Classification: Attack Surface, Data Privacy
  Description: Allow websites to query available payment methods

  Websites can use JavaScript APIs to query information about configured payment methods. This capability can be used to streamline the online shopping experience for consumers, but it also divulges information to internet sites.

  In an enterprise setting it is generally best to disable this policy. If the setting is enabled, or not set, then the website can ask if the user has payment methods saved.

- **Policy:** DefaultGeolocationSetting
  Classification: Attack Surface, Data Privacy
  Description: Control use of HTML5 location API

  Browsers can share their physical (latitude/longitude) location with websites. This can be used for services to optimize location-based content, such as finding a nearby store or weather information, but sharing location information may not be desirable in an enterprise environment.

  If this policy is set to "1," sites will track the user's physical location. If the policy is set to "2," sites are not allowed to track physical locations. If the policy is set to "3," the user is consulted. Leaving this policy unset has the same effect.

- **Policy:** CryptoWalletEnabled
  Classification: Attack Surface, Feature Enablement
  Description: Manage the Microsoft Edge browser Crypto Wallet feature

  The Microsoft Edge browser has a built-in CryptoWallet functionality targeted at consumers.

  Unless used in a sanctioned corporate function leveraging crypto currency, this capability should be disabled as it adds unnecessary complexity and expands the attack surface, both of which are inappropriate for corporate use. If the policy is left unset, it is the same as enabling it.

- **Policy:** EdgeShoppingAssistantEnabled
  Classification: Data Privacy, Feature Enablement
  Description: Manage Microsoft Edge Shopping Assistant

  The Microsoft Edge browser can use browsing and search history to provide guidance, assistance, and suggestions for online shopping. This functionality shares potentially sensitive user access information with a third-party service to provide this functionality.

  This policy is inappropriate for corporate use and should be disabled. Note that if it is not set, the policy is enabled by default.

- **Policy:** ShowMicrosoftRewards
  Classification: Data Privacy, Feature Enablement
  Description: Manage Microsoft Rewards service

  The Edge browser includes a "Microsoft Rewards" program which allows users to earn points when searching on Bing.com. These points can then be used in the microsoft.com online store. This program relies on tracking user activity, which may involve sensitive corporate information.

  This service is not appropriate for enterprise use and should be disabled. If it is left unset, it is enabled by default.

Examples of policies that pertain to feature enablement

- **Policy:** RemoteAccessHostAllowRemoteAccessConnections
  Classification: Feature Enablement
  Description: Control desktop sharing functions built into the browser

  Browsers include built-in remote access services for sharing and remotely controlling the user's system, without the need to install additional software. This feature could be useful – for example if a user was working from home and needed to access their office computer. It is, however, dangerous — convincing users to allow a third party to remotely view or control their system is a common aspect of phishing or malware campaigns.

  Many environments tightly control the installation of Windows applications to protect against this tactic, and browser desktop sharing capabilities should be managed to enforce similar controls.

Protect your enterprise with layered browser security, made simple by Menlo Security

As these examples have illustrated, today's browsers include powerful capabilities, and not all of them are desirable in an enterprise setting. The sheer number of these policies and the necessity of reading them carefully to understand their full effect can be a daunting prospect. Complicating things further, setting browser policies is not a "one-and-done" scenario, as new features are enabled frequently. It is no longer good security practice to let the user decide, either.

With Menlo Security Browser Posture Manager, it is now easy to ensure that your policies get the best that the browser has to offer while minimizing your corporate attack surface and retaining data privacy. Find out more about Browser Posture Manager, at www.menlosecurity.com.

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.