Brought to you by Informa Tech

Where next in the evolution of enterprise browsers?

Publication Date: 20 Fed 2024

Rik Turner

Senior Principal Analyst, Cybersecurity

Omdia view

Summary

This whitepaper surveys the burgeoning market in browser security technology. While remote browser isolation (RBI) has become a mainstay for securing web usage, newer technologies have come along in recent times to address the broader requirements represented by cloud-based (and thus browser-accessed) applications, as well as hybrid and remote working patterns.

We consider both browser extensions and enterprise browsers in this context, and consider where else browser security technology is headed beyond those two approaches.

Browser security has gained a newfound urgency

After a period of relative calm, the browser security sector has undergone a burst of innovation recently, and with good reason.

The world of work has gone from:

> Web browsing for information, alongside client-server apps in the data center for enterprise functionality,

to:

> a combination of cloud-native and software-as-a-service (SaaS) apps for almost all business requirements and, increasingly, remote working as the norm.

In this new scenario, the browser has become the perfect on-ramp for the majority of cyberattacks. Even if the first point of contact with their target is a phishing email, threat actors all too often direct victims to a website from which malware will inadvertently be downloaded, systems can be compromised, and the next stage of penetrating the infrastructure can begin.

In other words, if the eyes are the windows to the soul of a human being, then an organization's "eyes" onto the internet are also the windows through which attackers can nowadays see into its soul, i.e. the sensitive and/or confidential information residing at its heart, whether it be its intellectual property (IP), its customer database, or the input data it uses to train its machine learning models.

Purloining that IP or customer list can cause serious competitive or legal issues, while tampering with the AI training data can seriously skew strategic business decisions. In any case, the incentive for attackers to leverage the browser as their way in has grown dramatically thanks to app cloudification and the work-from-anywhere trend.

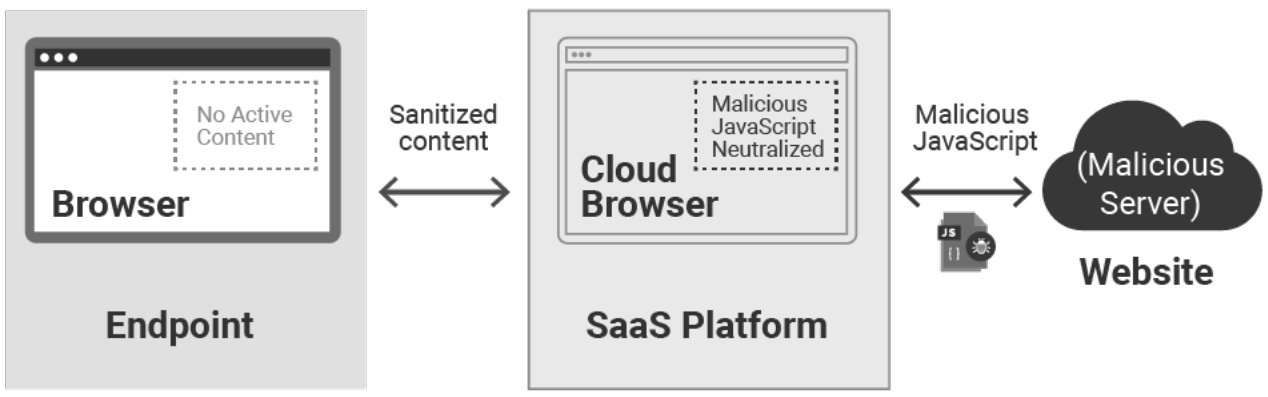
Isolation got the ball rolling in browser security

The World Wide Web has worked its way into the very epicenter of modern business and, along the way, has opened up an entirely new flank in many organizations' attack surface. After all, why run into a bank with a weapon and a nylon over your head, when you can filter millions from multiple bank accounts from the comfort (not to mention security) of your own home?

The first technical response to Web-based attacks was to isolate the browser. Only static content could go straight through to the end user's machine, while dynamic content was rendered in a sandboxed environment on a remote server, where it could do no harm to that device. The server would then send a sanitized stream of display data (pixels for some, Chromium display objects in the

more advanced systems) for the dynamic part of content to the endpoint, with anything malicious having been removed before they got to the person's lap- or desktop.

Figure 1: Remote browser isolation puts each tab or session into a cloud-secured process or VM



Source: Menlo Security

RBI finds its way into SASEs galore

RBI has enjoyed considerable success over the years, evidenced by both the number of M&A deals, as large security vendors sought to add the technology to their portfolios, and the number of modern, cloud-based platforms that have now introduced RBI as an option within their broader range of services.

In particular, there has been a marked trend in recent times for vendor of so-called secure access service edge (SASE) technology and its humbler sibling, secure service edge (SSE), to add RBI into the mix. The rationale is a simple one: SASEs and SSEs are proxies, making them a logical place from which to deliver RBI, while RBI rounds out their service offering alongside capabilities such as data leak prevention (DLP) and cloud access security broker (CASB).

That said, it is an open question as to whether, in this scenario, the RBI add-on can isolate every tab and session, and indeed whether it can scale to every user. If not, there is clearly the risk of it resulting in a poor end-user experience, leading to dissatisfaction and a desire to circumvent the security control.

Meanwhile, with the browser now being the primary conduit for the majority of knowledge work activities, whole new types of browser security have emerged since the late 2010s.

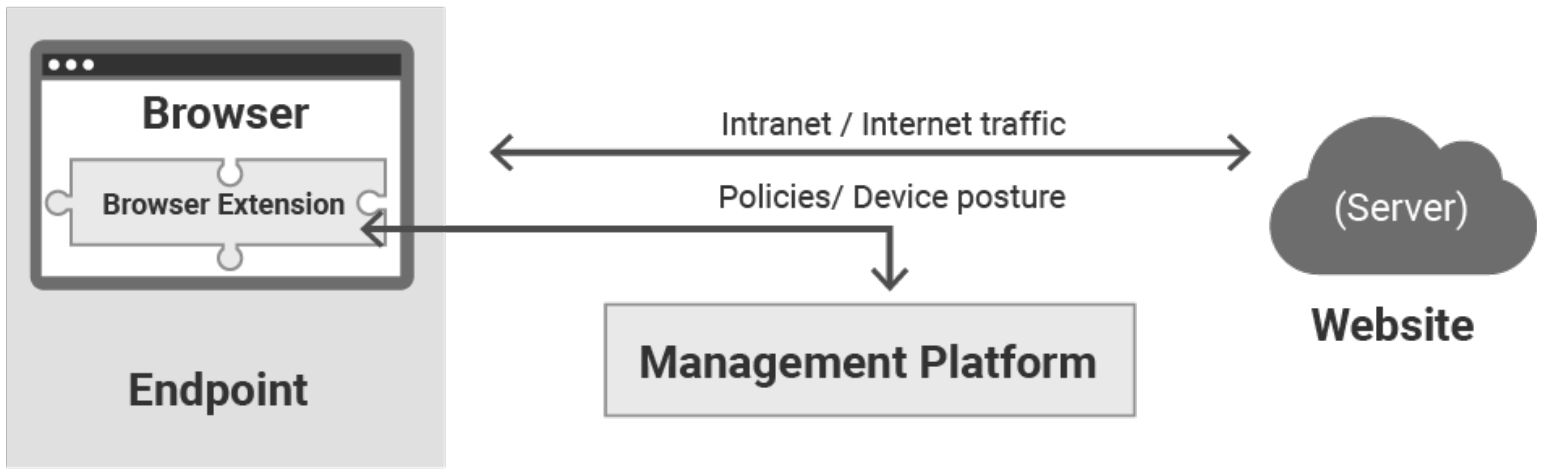
How browser extensions work

First up in chronological order is browser extension technology, which injects security policy as code into the standard browsers that ship with laptops, provided they are Chromium-based (Chrome and Edge being the most common).

The extension can then enforce an organization's security policy around access to websites and what interactions the user of the device can have with them. They may allow read-only access, for instance, blocking any attempt to upload data.

Representative vendors of browser extension technology include LayerX and SlashNext. Menlo Security also offers an extension, with the difference that it combines it with a cloud-based browsing component.

Figure 2: How standalone browser extension technology works



Source: Menlo Security

Strengths and weaknesses of browser extensions

Omdia endeavors to highlight both the strengths and weaknesses of each technological approach. In the case of browser extensions, their strengths include the fact that users can continue to use their regular browsers, so there should be no perceptible impact on their normal working habits.

Extensions are also better suited for unmanaged devices and BYOD or contractor zero-trust access needs than full replacement browsers. For obvious reasons, they are also financially less onerous for the organization deploying them than full replacement browsers.

In terms of their weaknesses, it is an open question whether a user, armed with a certain amount of technical knowledge, can in fact circumvent, or indeed "turn off" the extension's features.

The enterprise browser proposition

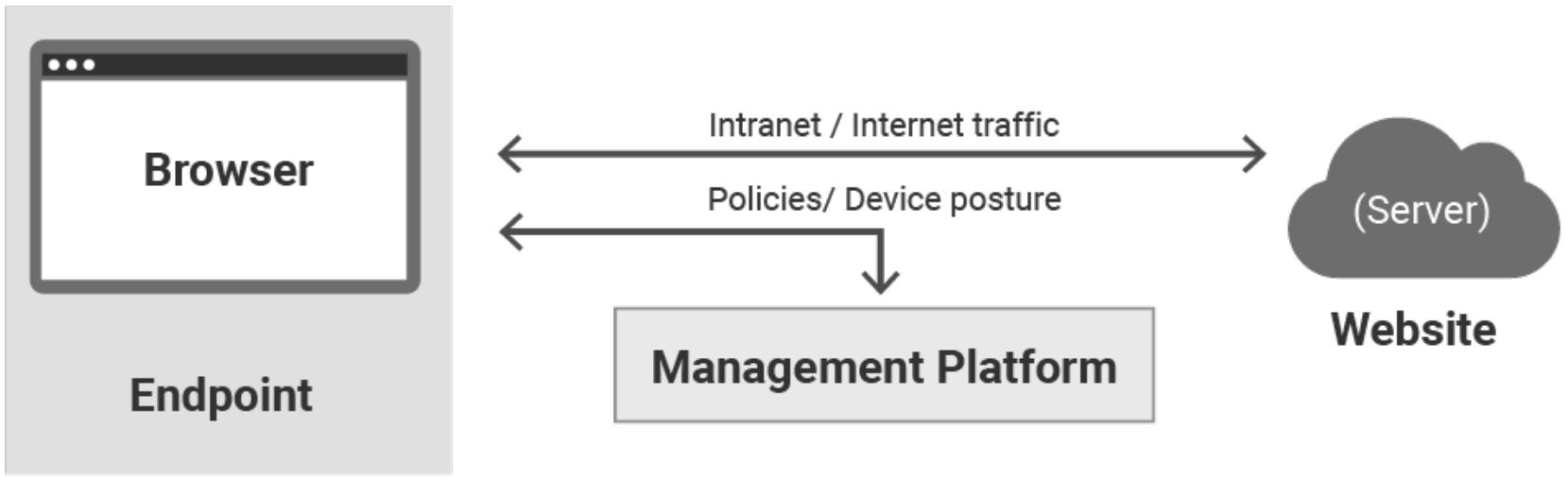
Next to arrive on the scene, starting in just the last couple of years, was enterprise browser technology. The approach here is to propose an entirely new browser, based on the Chromium framework, that enterprises can download to all the endpoints in their environment to enforce corporate security policy. The options they have are to replace all the standard "consumer" browsers on their company laptops, or to have the enterprise browser live alongside those regular browsers yet enforce any corporate work to flow through itself, blocking the other browsers if a user tries to go through them to the website or application.

Enterprise browsers can also block copying content that a user is viewing in the enterprise browser if they open a consumer browser on the same device, avoiding the situation in which a user could cut and paste it into the regular browser and forward to someone outside the company, for instance. Now, such controls would seem to provide support for the coexistence of browsers. However, since the information has already left the enterprise and is now housed on that endpoint; it is now on contested ground. This limitation, together with other risks associated with relying solely on endpoint controls, makes the technology less applicable in BYOD environments, or indeed for contractor and partner scenarios.

Representative vendors of enterprise browser technology are Island and Talon (which was acquired by Palo Alto Networks in December 2023). Google and Microsoft should also be mentioned here, since they offer enterprise-specific features that can be added to their regular browsers. Menlo Security is also in this group, though it opts not for the replacement route, but rather that of

promoting all the standard browsers to enterprise browser status via a combination of an extension and cloud-based functionality (see below in the section **Further innovation arrives in browser security**).

Figure 3: How enterprise browsers work



Source: Menlo Security

Strengths and weaknesses of enterprise browsers

As for the strengths and weaknesses of enterprise browsers, on the plus side they instinctively feel like a more secure alternative to extensions by virtue of the fact that they are a distinct browsing environment, ordained and managed by the organization deploying them. Sort of how a SCIF is more secure than a reading room in a library, or how a company phone should be more easily controlled by the company than one that's owned by the employee.

Admittedly, this may be more of a perception than a reality, of course: people can choose to blab about what they saw while they were in a SCIF, while a determined employee can usually circumvent his company's security controls if he or she is minded to use that phone inappropriately.

On the minus side, the organization is now paying to duplicate a technology that has hitherto come free with every laptop. And from a security perspective, even the anti-tampering controls that come with enterprise browser may be defeatable: some critics argue that if a user has the knowledge, via the regular browser on their device, to access its memory and use the data available there, they can effectively hijack a session or steal information, bypassing the enterprise browser altogether.

Another issue to consider here is the fact that replacement browsers usually require a policy management console that may not integrated be with unified endpoint management systems, raising the unwelcome prospect of swivel-chair management.

Can you rely entirely on local software on the device?

What both these approaches have in common is that they rely on changes to the browser on the user's device to enforce security policies there on the entire online experience. In the case of the extension, this is done by incrementing the existing browser with some extra software, while the enterprise browser camp advocates an entirely new browser, either replacing the regular browser altogether or suppressing it whenever corporate activity is taking place.

Both scenarios raise the philosophical question of whether, as a CISO, you feel happy trusting a software app running on the end user's laptop, smartphone, or tablet as your single line of browser defence. This is particularly the case when the software is running on an untrusted device,

such as a BYOD endpoint.

Further innovation arrives in browser security

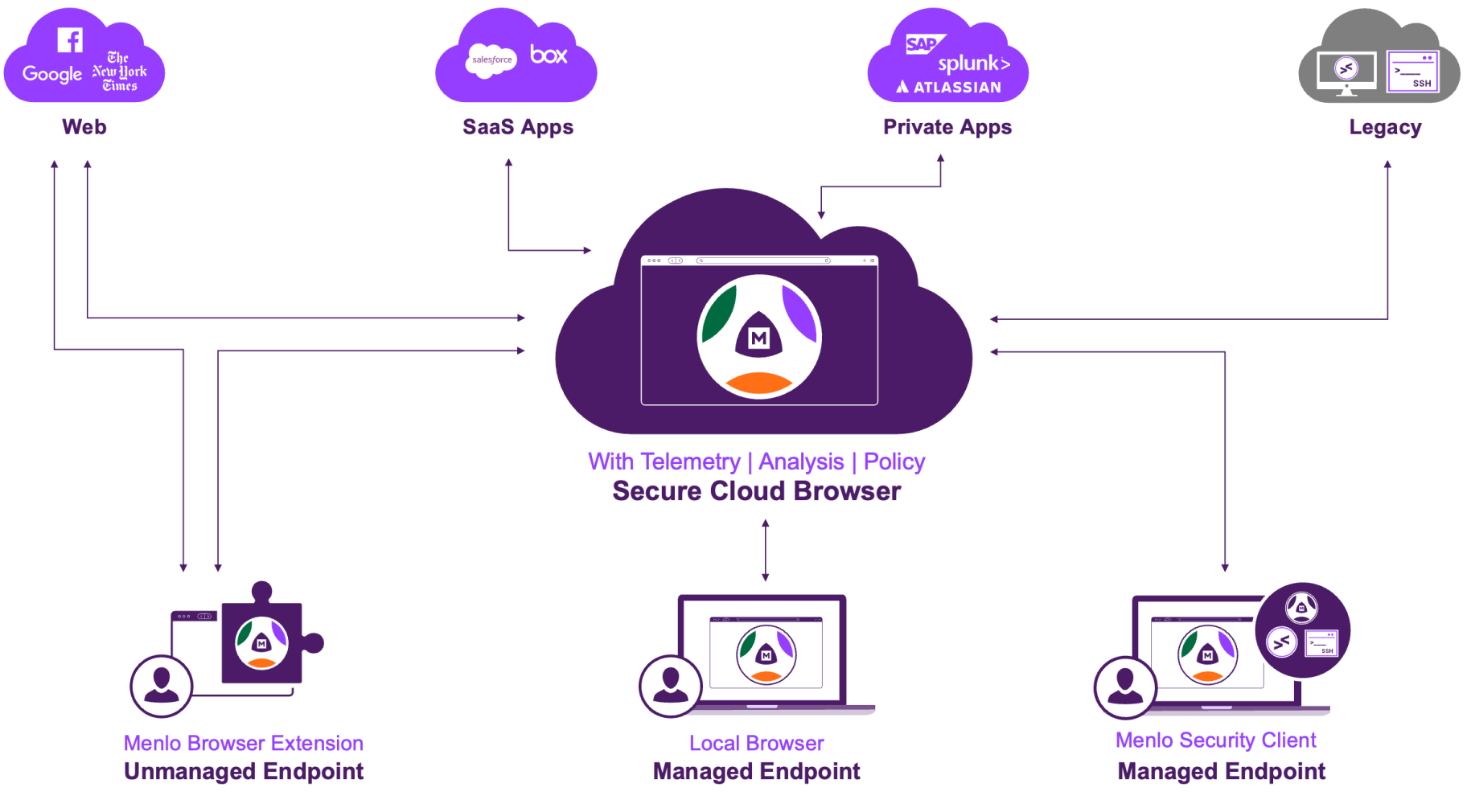
As can be seen from this brief summary of recent developments, browser security has been a hotbed of technological innovation in the last few years. However, neither extensions nor enterprise browsers should be thought of as the end state here, since there is still more evolution to come.

For instance, to address the perceived weakness of both these approaches to browser security, one idea is now to combine a secure cloud-based browsing capability and a centrally-managed software module, packaged as an extension for all local browsers and, ideally, available from extension marketplaces.

The argument here is that by coupling an extension with a cloud-based security element, an organization can add defense in depth to browser security and ensure policy enforcement. The cloud component takes care of a large part of the security requirements for an enterprise browser, while the centralized management capability sets the security policies the extensions will enforce on the traffic that has been allowed through to them.

In essence, this approach holds the promise of turning every regular browser, i.e. the ones that ship as default on all mobile devices, into an enterprise browser, without the cost or operational overhead of deploying or maintaining the latter.

Figure 4: How the combination of cloud-based browsing and a local browser extension works



Source: Menlo Security

Further reading

Omdia Market Radar: Browser Security 2023 (August 2023)

Developments in Browser Security: From Isolation to Enterprise Browsers (March 2023)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com