Enterprise Strategy Group by TechTarget

SHOWCASE

JULY 2024

Transforming the Browser From a Point of Attack to a Layer of Defense With Menlo Secure Enterprise Browser

Justin Boyer, Technical Validation Analyst

Abstract: The browser has become an essential part of enterprise IT environments. End users use the browser to access email, the internet, web-based applications, and SaaS applications to perform business-critical tasks. Despite the investments made to secure IT infrastructure, organizations still struggle to protect the browser from sophisticated attacks that bypass legacy web security solutions. To move forward, organizations must focus on turning the browser into a security layer, hardening it against attacks legacy web gateways can't detect. The Menlo Security Secure Cloud Browser provides a layer of defense against common browser-based attacks while also optimizing end-user productivity and enabling secure use of Gen AI tools.

Cybersecurity Still a Chief Concern

As the threat landscape continues to change rapidly and IT environments grow more complex, cybersecurity is on the minds of many organizations. According to research from TechTarget's Enterprise Strategy Group, 57% of organizations said cybersecurity has become significantly more important to their organization's future over the past two years. Additionally, 68% indicated that their cybersecurity spending will increase in 2024.[1]

As remote work and SaaS usage increases so does dependence on browsers to complete critical work functions. Attackers can use the browser to bypass security controls and trick users into introducing malware into an organization's environment or to steal account credentials. For example, a recent Enterprise Strategy Group research survey identified phishing and social engineering attacks as the No. 1 reason for account credential compromise among survey respondents.[2]

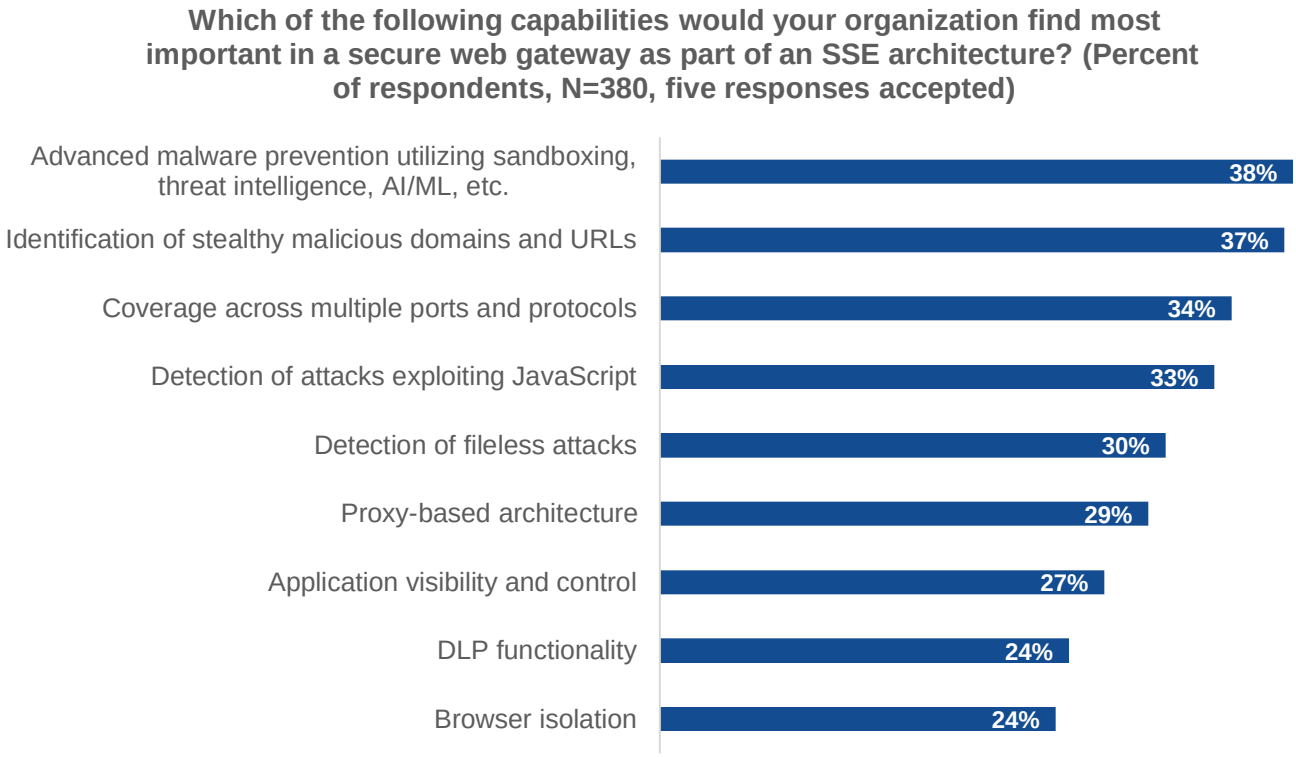
SSE and SASE May Leave Remote Workers Exposed

Security service edge (SSE) and secure access service edge (SASE) have emerged as two models used to secure remote workers. These services include secure web gateway (SWG) technology, which is a core component of SSE and SASE controls. SWG is no longer sufficient to secure web browsing for remote workers. SWG has value for filtering content and maintaining compliance with use policies, but sophisticated threats evade such traditional controls today.

Expecting SWGs alone to help protect remote workers and employees using web-based technologies leaves them exposed to a variety of attacks. Chief among those identified include advanced malware, malicious URLs, and advanced JavaScript attacks (see Figure 1).[3]

[1] Source: Enterprise Strategy Group Research Report, *2024 Technology Spending Intentions Survey*, February 2024.
[2] Source: Enterprise Strategy Group Research Report, *Passwordless in the Enterprise*, September 2023.
[3] Source: Enterprise Strategy Group Research Report, *Security Services Edge (SSE) Leads the Way to SASE*, November 2023.

Figure 1. The Most Important Secure Web Gateway Capabilities



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

However, traditional, network-focused security doesn't protect against browser-based attacks and does not effectively provide the capability requirements expressed by organizations. Enterprise Strategy Group research showed that 65% of survey respondents are open to or actively evaluating alternatives to their current web security solution, showing that current web security technologies still leave something to be desired.[4]

Secure Browsers Critical to Modern Enterprise Security

Network-focused approaches, such as SSE and SASE, can greatly increase cost and complexity. These strategies put the focus on transport security, along with various controls and technologies along the network path, to find and prevent potential attacks.

But the threat landscape has evolved. Attackers have become proficient in evading content scans and malicious link analysis. Social engineering is still a risk, with seemingly legitimate websites that make it through network-based protections becoming sources for phishing attacks. Malicious actors also use ephemeral or compromised websites that aren't marked as malicious by SWGs. These sites use dynamically generated JavaScript code and images to bypass network protections and launch the attack through the browser upon the page rendering.

Because of these changes in the landscape, protecting the browser has become an essential part of modern cybersecurity, with a third of companies using secure browsers to ensure endpoint device and laptop security.[5] Securing the browser ensures that the most used enterprise asset is getting the protection it warrants.

[4] Ibid.
[5] Source: Enterprise Strategy Group Complete Survey Results, *Endpoint Device Trends*, February 2024.

Menlo Security: Secure Cloud Browsing

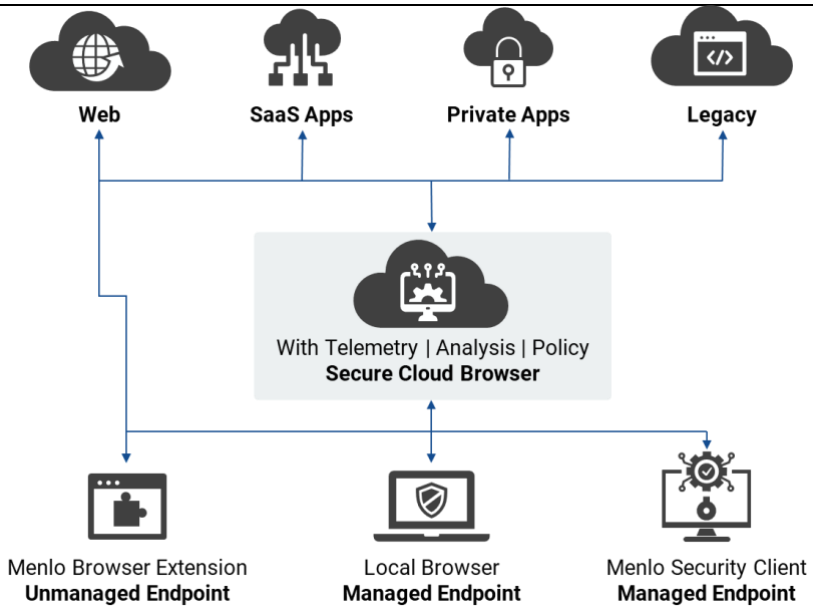
Menlo Security offers an enterprise browser solution built to secure the browser, protect end users, and turn the browser into a layer of security rather than a weakness. The Menlo Secure Enterprise Browser solution provides security via a managed local browser partnered with a hardened digital twin in the cloud—the Menlo Secure Cloud Browser. Secure cloud browsing is a significant advancement beyond network proxies and remote browser isolation, which lack the full browser context and have been known to degrade performance.

The Secure Cloud Browser fetches, executes, and renders all content for the user. This process enables Menlo to inspect the contents of a webpage, determine if it is a threat, and remove any potential malicious content before rendering it for the end user. In addition to adding the browser context to its enforcement, Menlo also provides additional security services, such as content filtering. The page execution happens within the Menlo Cloud, not on the endpoint device, protecting the endpoint from any malicious code that might try to exploit vulnerabilities.

The Menlo Secure Enterprise Browser solution, rooted in the Menlo Secure Cloud Browser, delivers three categories of capabilities:

- **Manage.** Configure policies for local and secure cloud browsers. Organizations choose a configuration based on benchmarks (Department of Defense, Center for Internet Security, and Menlo-provided) and apply that configuration to all managed browsers. The Menlo Secure Cloud Browser provides instant visibility and forensics to aid investigations.
- **Secure.** Secure access to enterprise web applications and sensitive data. Menlo Secure Cloud Browser offers three options: a secure portal, a browser extension for unmanaged endpoints, and a client for non-browser access.
- **Protect.** Advanced protection against modern sophisticated attacks. In addition to protecting users, Menlo Cloud protects application servers against header manipulation, session hijacking, cookie stealing, and malicious file uploads. The hardened digital twin browser executes code and performs real-time analysis to find threats, such as HTML smuggling used to spread ransomware or potential phishing attacks. The Secure Cloud Browser automatically separates personal and work sessions, siloing sensitive business data and applications.

Figure 2. The Menlo Secure Cloud Browser



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Conclusion

Modern workforces are increasingly remote and are using primarily SaaS and web-based applications. The browser has become the "operating system" of corporate work and an essential part of the enterprise's end-user ecosystem.

Traditionally, organizations have used network-based security solutions, along with SSE and SASE, to provide security services to a hybrid workforce. Unfortunately, security gateways and transport security don't stop browser-based attacks. Sophisticated attackers can use various techniques to bypass traditional web security solutions to execute code directly within the browser, exposing end users to malware and ransomware. Organizations should be looking to secure the browser to protect against advanced threats that bypass typical network-based security controls.

The Menlo Secure Enterprise Browser solution combines a managed local browser with a hardened digital twin in the Menlo Cloud to fetch, execute, and render web content before it reaches the endpoint device, ensuring that any malicious elements won't be executed on the endpoint device.

By combining configuration management with cloud security services and real-time threat detection, Menlo Security provides a secure browsing experience without performance impacts commonly found in browser isolation solutions and which avoids the high costs and complexity of SSE and SASE infrastructure. By partnering with Menlo Security, organizations can transform the browser from a forgotten weakness to a robust security layer.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com