

TECHNICAL VALIDATION

Menlo Security Enterprise Browser Solution

Streamlined, Zero-trust Access for the Enterprise

By Justin Boyer, Validation Analyst; and Alex Arcilla, Senior Validation Analyst
Enterprise Strategy Group

July 2024

Contents

Introduction.....	3
Background.....	3
Menlo Secure Enterprise Browser	4
Enterprise Strategy Group Technical Validation	5
Manage the Browser	5
Secure Access to Applications and Data	7
Protect the User.....	9
Conclusion.....	11

Introduction

This Technical Validation from TechTarget’s Enterprise Strategy Group documents an evaluation of the Menlo Secure Enterprise Browser. Enterprise Strategy Group reviewed how this solution can help organizations provide zero-trust access for hybrid workers and third-party users by establishing the browser as a layer of defense as well as the secure access method. Specifically, we review how the Menlo Secure Enterprise Browser solution simplifies how to manage browser security policies, secure access to applications and data, and, ultimately, protect the end users from evasive threats and attacks.

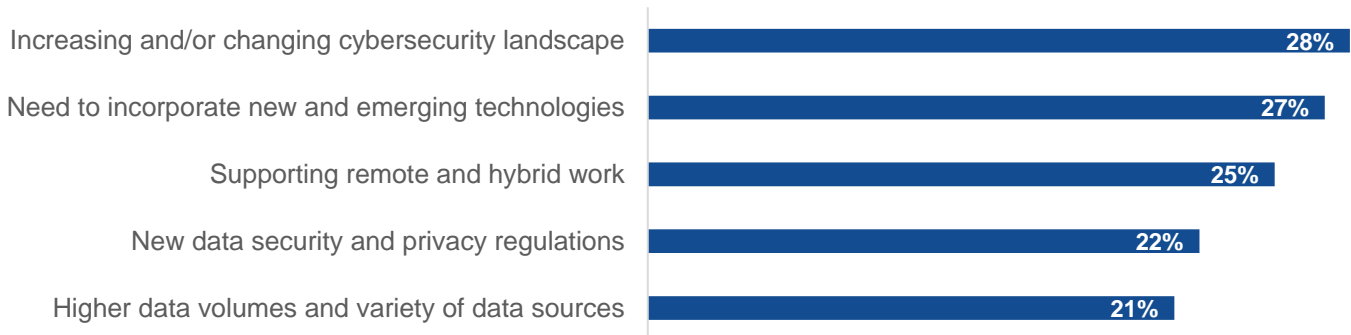
Background

Phishing and malware delivery is top of mind for many organizations: Enterprise Strategy Group research found that 46% of respondents, to the best of their knowledge, have experienced an attempted ransomware attack frequently, whether daily, weekly, or monthly.¹

The increased frequency and sophistication of attacks is no surprise, as organizations are dealing with increased complexity in their IT environments. Not only must they be cognizant of the increased and/or changing cybersecurity landscape, but they also must deal with the need to support remote and hybrid work (see Figure 1).²

Figure 1. Top Cited Reasons for IT Environment Complexity

What do you believe are the biggest reasons your organization’s IT environment has become more complex over the past two years? (Percent of respondents, N=1105, five responses accepted)



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

IT environmental complexity has certainly added to the challenge of securing networks against evolving threats and attacks. With the increase in remote and hybrid work and the use of public cloud services, a fixed IT network perimeter no longer exists.

While organizations have implemented multiple layers of security to monitor and filter traffic in transit between the end user and the application—specifically security at the infrastructure, transport, and endpoint layers—and at

¹ Source: Enterprise Strategy Group Research Report, [Ransomware Preparedness: Lighting the Way to Readiness and Mitigation](#), December 2023.

² Source: Enterprise Strategy Group Research Report, [2024 Technology Spending Intentions Survey](#), February 2024.

secure web gateways (SWGs) to filter content and URLs, the threat landscape has unfortunately expanded beyond what these defenses can address.

With the emergence of SaaS and cloud-native applications, the browser is now widely used as a point of access. Yet, bad actors have found the browser to be another place to initiate cyberattacks. Organizations now need to consider how the browser must be utilized as a critical layer of defense against cyberattacks.

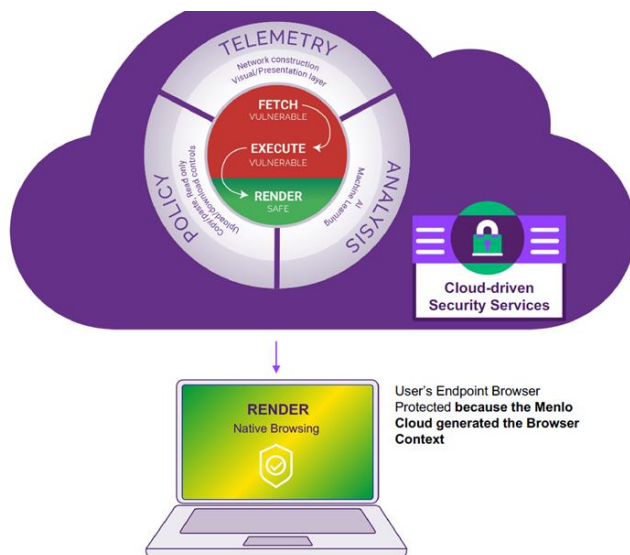
Menlo Secure Enterprise Browser

The Menlo Secure Enterprise Browser solution uses Secure Cloud Browser and other controls to secure access to applications, protect end users, and turn the browser into a layer of security rather than a weakness.

Menlo Secure Cloud Browser provides security via a managed local browser partnered with a hardened digital twin in the cloud (see Figure 2). The secure cloud browser can be deployed with additional security services, but it does not introduce the complexity or performance impact of traditional network proxies.

The Menlo Cloud fetches, executes, and renders all content for the user. This process enables Menlo to analyze and execute the contents of a web page, determine if it is a threat, and remove any potential malicious content before rendering it for the end user. Menlo also provides 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 could try to exploit vulnerabilities.

Figure 2. Menlo Secure Cloud Browser



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

The Menlo Secure Enterprise Browser solution and the Menlo Secure Cloud Browser deliver three categories of capabilities:

- Management.** Administrators can configure policies for local and secure cloud browsers. Organizations choose a configuration based on benchmarks (U.S. Department of Defense, Center for Internet Security, and Menlo-provided) and apply that configuration to all managed browsers. Menlo Secure Cloud Browser also provides instant visibility and forensics.

- **Security.** Menlo Secure Cloud Browser secures access to enterprise web applications and sensitive data with three operating models: access through secure portal authentication, a browser extension for unmanaged endpoints, and a client for non-browser access.
- **Protection.** Secure Cloud Browser provides 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 AI-powered real-time analysis, finding threats such as HTML smuggling, which is an evasive technique used to spread ransomware.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group validated how the Menlo Secure Cloud Browser helps organizations to secure the use of any browser within an enterprise. To complete this validation, we reviewed the processes and workflows that are associated with how organizations can do the following: manage browser security, regardless of the browser used; secure browser access to applications and data; and protect end users.

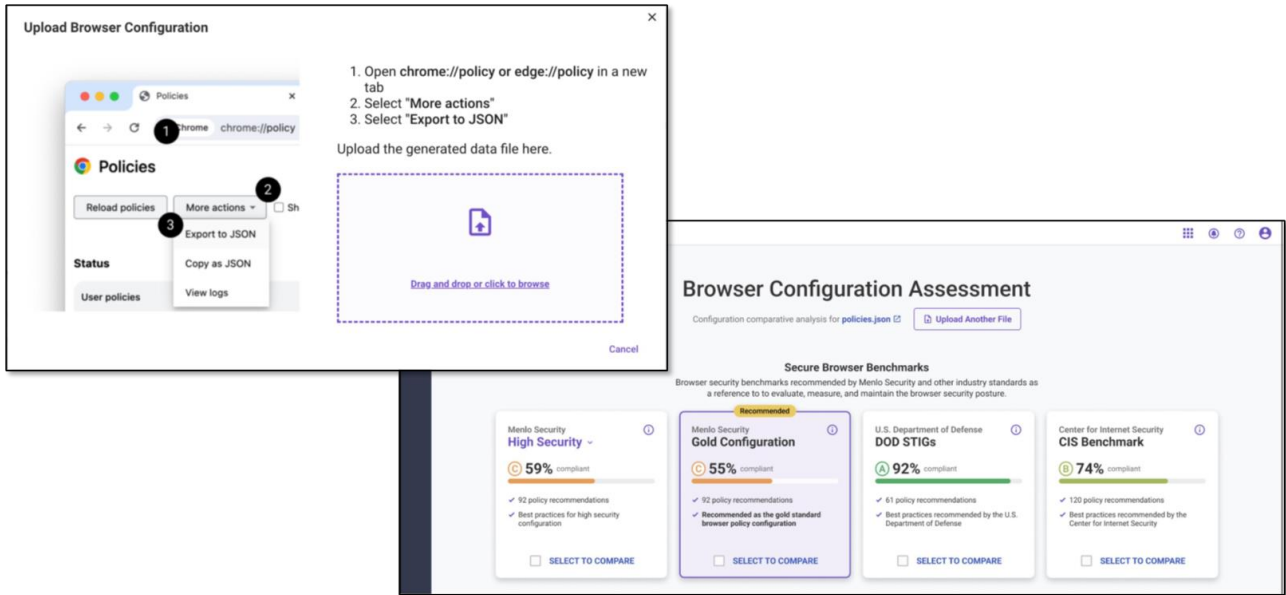
Manage the Browser

The use of browsers has gone beyond just surfing the web. In fact, browsers have become the “operating system” that organizations are using to complete their everyday tasks. Organizations are now using browsers to interface with SaaS and cloud-native applications for completing business-critical tasks as well as using business productivity and collaboration suites to communicate and create documents (e.g., Microsoft Office 365, Google Workspace). Given the amount of work that organizations now accomplish via a browser, they need to focus on securing the browser itself, as it is now a viable enterprise asset that can be attacked. Securing any browser session begins with configuring policies for local and cloud-based browsers, while establishing visibility into browser activity and providing the ability to perform forensic analysis to isolate and remove potential security events.

Enterprise Strategy Group Testing

Enterprise Strategy Group began by navigating to the Menlo Secure Cloud Browser interface to establish browser security policies for a given browser type. Instead of inputting configurations for individual browser types, Menlo Security enables organizations to upload existing policies (via browser configurations) and select a “benchmark” level of security to be implemented (see Figure 3).

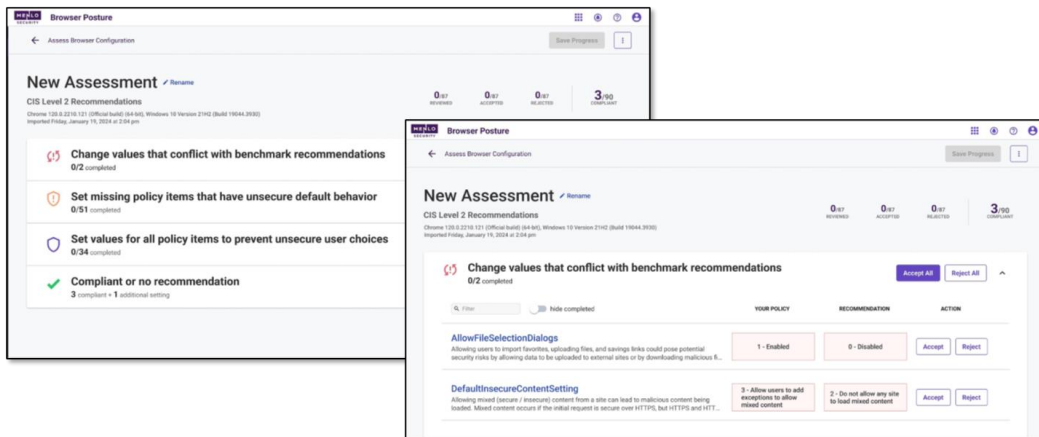
Figure 3. Uploading Existing Browser Configurations for Assessment



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

After selecting the desired benchmark, we observed how the solution assessed the uploaded browser configurations and listed recommendations for new policies to implement (see Figure 4). Recommendations addressing more severe security gaps were listed in decreasing order. Administrators could review the policies chosen before implementing new security policies.

Figure 4. Assessing Current Browser Security Settings Against Benchmark



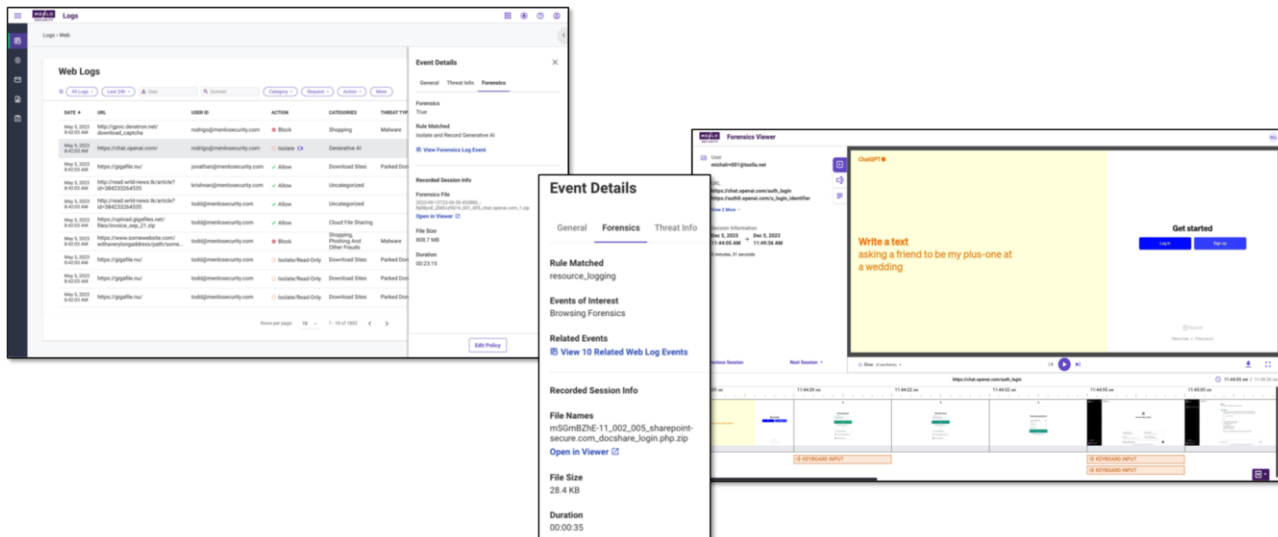
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

After configurations are reviewed, policies can be uploaded through existing channels. For example, they can be published to Google Chrome and Microsoft Edge via Microsoft Intune. Doing this allows end users to continue using familiar browsers.

Next, Enterprise Strategy Group observed how Menlo Secure Browser facilitates forensic analysis. Instead of reviewing packet captures (PCAPs), we could search via recorded events. As shown in Figure 5, we viewed exactly

what occurred during specific browser sessions. This functionality improves and accelerates analysis as session content reveals exactly what occurred, including user input.

Figure 5. Conducting Forensic Analysis via Recorded Browser Sessions



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

Why This Matters

With the increasing use of SaaS applications, web applications, and other web-based services, the browser has become a critical piece of enterprise architecture. Employees use the browser to access business-critical systems, and attackers have taken advantage of this shift to target the browser as a point of entry into organizations' environments.

The first step to secure the browser is hardening it. Enterprise Strategy Group validated that Menlo gives organizations the power to publish browser security policies to protect users. We were able to choose from a list of established industry benchmarks, such as those published by the Department of Defense and the Center for Internet Security, as well as those created by Menlo. These policies can be published to Google Chrome and Microsoft Edge through Microsoft Intune and other management channels.

Managing browser security needs to be easy when dealing with the multiple users working with various browser types. Menlo enables easy administration through security policies that are deployed and updated in a centralized manner. Menlo logs security events, which can be examined using recorded browser sessions, simplifying forensic analysis and reducing the need for relying on PCAPs for investigation.

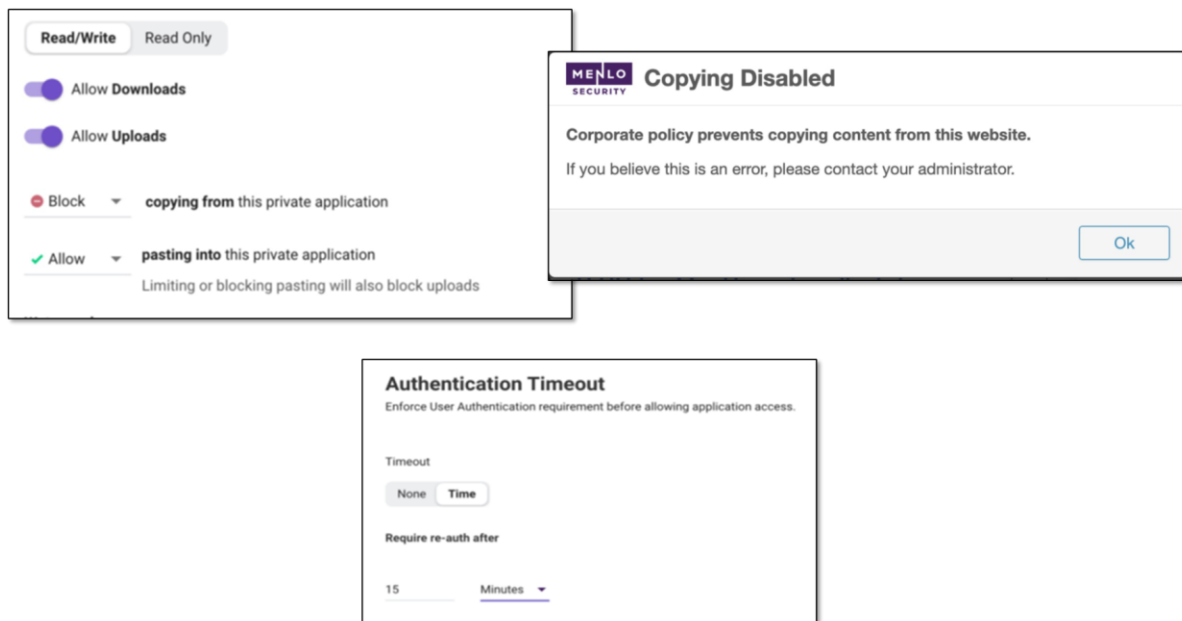
Secure Access to Applications and Data

After the browser itself is secure, organizations still need to ensure that any application accessed via a browser is secure as well. While virtual desktop infrastructure (VDI) and first-generation remote browser isolation (RBI) were meant to address this issue, such legacy approaches can adversely affect both scalability and performance, thus possibly resulting in negative end-user experiences as well as incurring unnecessary costs. With the Menlo Secure Cloud Browser, organizations can simplify how end users securely access applications and data in a scalable and performant manner.

Enterprise Strategy Group Testing

Enterprise Strategy Group proceeded to review how Menlo Secure Cloud Browser can simplify how end users access applications and data. Beyond defining application access control settings—e.g., according to user/group, source IP address, geolocation, and posture assessment—we saw how we could configure multiple settings to secure application and data access. We saw that we could configure multiple application controls, such as read-only versus read/write, file download and upload, and copy/paste permissions. We could also set timeouts per application (see Figure 6).

Figure 6. Configuring Application Controls

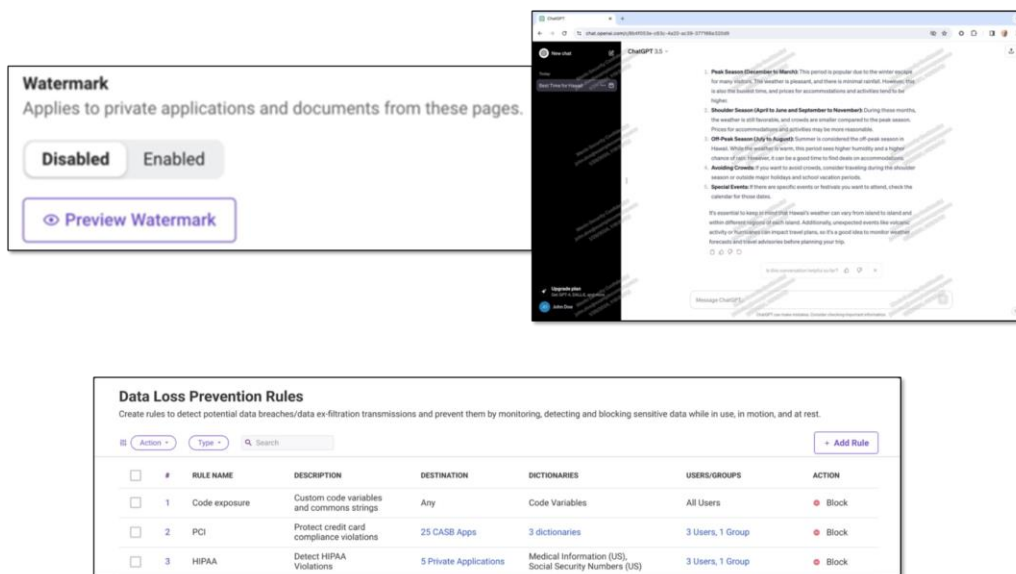


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Menlo Secure Cloud Browser secures applications in both directions, working to protect application servers from infected endpoints. Malware on an infected endpoint can compromise application servers by injecting code into HTTP headers and payloads. Through attacks such as server-side request forgery (SSRF), an attacker can gain control of the application server, steal sensitive data such as session keys, or cause a server to perform actions it wasn't intended to perform by manipulating HTTP requests. Menlo Secure Cloud Browser inspects HTTP headers and payloads before sending them to the application server, blocking file uploads and malicious code as well as sending clean HTTP requests to the server so that application work isn't interrupted. This inspection protects against attacks such as header manipulation, session hijacking, and cookie stealing.

Enterprise Strategy Group next reviewed how Menlo Secure Cloud Browser and Menlo Data Protection work to prevent data loss during a browser session. Menlo supports data loss prevention (DLP) scans and last-mile DLP that prevents data from leaking into the local browser. The Menlo Cloud inspects outbound and inbound traffic to prevent data exfiltration via dictionaries and adjustable templates. Additionally, Menlo Data Protection supports browser function controls, defining copy/paste rules as well as data redaction, and implementing watermarking for files and documents (see Figure 7).

Figure 7. “Last Mile” Data Loss Prevention



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

Why This Matters

Enterprise Strategy Group research found that 63% of cybersecurity professionals feel that working as a cybersecurity professional is more difficult than it was two years ago. The top two reported reasons for this are the increasing workload and attack surface organizations face.³ In the focus on complexity and the attack surface, the browser is often overlooked as a potential attack vector. Organizations need to treat the browser as part of the attack surface and work to protect data and applications from browser vulnerabilities.

Enterprise Strategy Group validated that Menlo Secure Cloud Browser works to keep applications and data secure through multiple vectors. Menlo enables security teams to define application access policies based on user group, IP address, geolocation, or posture assessment. The Menlo Cloud protects application servers by inspecting and cleaning HTTP requests to prevent header manipulation, session hijacking, and cookie stealing. We also observed Menlo’s ability to create data loss prevention (DLP) rules, prevent end-user actions such as copy/paste or file upload, and watermark documents.

Ensuring browser session security does not stop at the browser. Organizations must also secure browser access to applications and data. Menlo Secure Cloud Browser simplifies configuration of application controls and DLP rules so that any data generated during browser sessions is less vulnerable to cyberattacks, without affecting scalability and the end user experience.

Protect the User

During any browser session, bad actors can attempt to extract end-user sensitive information by session hijacking, SaaS phishing, and inline frame injection (i.e., embedding unsanctioned content into legitimate websites). Unfortunately, blocking and filtering URLs is insufficient. With Menlo Secure Cloud Browser, an AI-based neural network extracts and inspects data elements from each website to determine if the webpage is secure for end-user interaction.

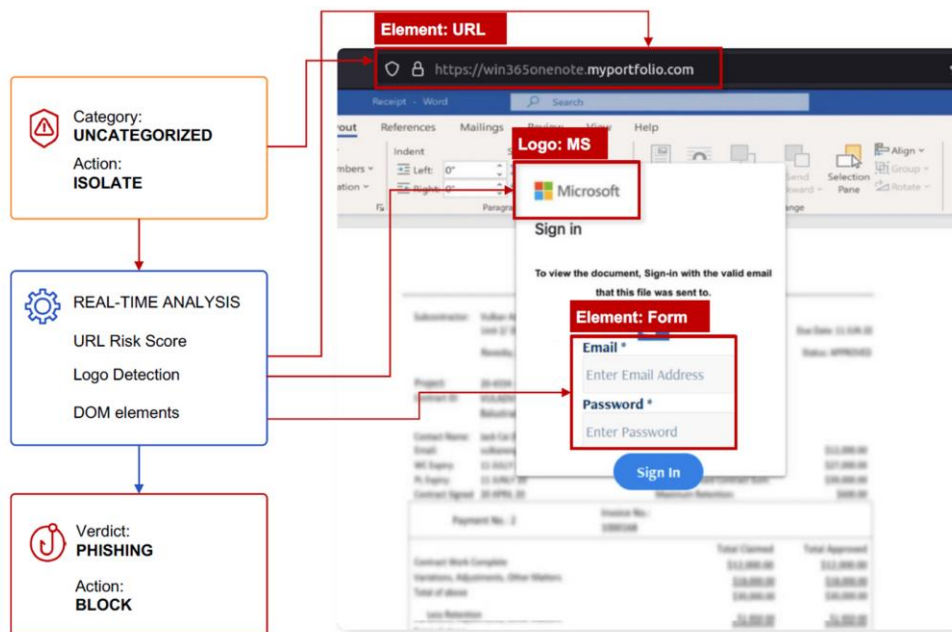
³ Source: Enterprise Strategy Group Research Report, [The Life and Times of Cybersecurity Professionals Volume VI](#), November 2023.

Enterprise Strategy Group Testing

Enterprise Strategy Group finally observed how the Menlo Secure Cloud Browser protects end users from being hacked. The Menlo Cloud supports traditional URL categorization and filtering based on exceptions as well as threat data, reputation, content inspection, and other criteria.

Since URL filtering alone is insufficient to catch all modern, sophisticated attacks, we reviewed how the Menlo Cloud goes further to protect end users from malicious content. The Menlo Cloud maintains a neural network that analyzes data in real time. It utilizes computer vision to inspect content and executes each request and response in the cloud. It then extracts document object model (DOM) elements from the visited website, such as form fields, media objects, and scripts associated with each response. In real time, the neural network within Menlo Cloud processes these elements to verify that the website will not initiate a security event (see Figure 8).

Figure 8. Protecting the End Users Against Threats and Attacks



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

If the network determines that the website poses a security risk, that site will be blocked. Combining a powerful neural network with computer vision and traditional filtering techniques, the Menlo Cloud can detect and stop malware that uses evasive techniques such as HTML smuggling and encrypted payloads often used to bypass legacy SWGs.

Why This Matters

A phishing or social engineering attack was the number one contributing factor indicated by survey respondents when asked what contributed to the compromise of accounts or credentials.⁴ Attackers have become more adept at bypassing legacy web security solutions such as SWGs, which leaves end users vulnerable to browser-based attacks.

Enterprise Strategy Group validated that the Menlo Secure Cloud Browser was built with the goal of overcoming the pitfalls of legacy web security solutions. We found that the Menlo Secure Cloud Browser can improve end-user protection by leveraging an AI-based neural network to continuously examine and evaluate webpage elements for potential security gaps.

The sophistication of threats and attacks that can plague end users during browser sessions has unfortunately decreased the effectiveness of URL filtering and blocking. The Menlo Cloud combats this by fetching and executing every response as well as inspecting all media, DOM elements, and scripts, filtering out malicious content. Using cloud-driven browser security from Menlo, organizations can protect end users from sophisticated attacks without expensive and clunky VDI infrastructure that can negatively influence the end-user experience. Users can access their applications as normal, while the Menlo Cloud protects them in the background.

Conclusion

As IT environments have become more complex and difficult to defend, and as cyberattacks have become more sophisticated, organizations have invested more into infrastructure and cybersecurity solutions. However, the industry has also shifted to more web-based and SaaS applications, making the browser the primary tool used by employees to complete their work. Attackers have continued to work to bypass legacy solutions such as SWGs, thus making the browser a dangerous part of the overall attack surface. Solutions such as VDI and RBI were meant to address this issue, but these approaches often adversely affect both scalability and performance, resulting in both negative end-user experiences and unnecessary costs. Organizations need to focus on securing the browsing experience without limiting the end user's ability to perform their work.

Enterprise Strategy Group validated that Menlo Secure Cloud Browser was built to address the main concerns around protecting end users as they use the browser. Menlo Secure Cloud Browser runs a digital twin in conjunction with a local browser to provide critical security services without hindering performance or user experience. The Menlo Cloud renders and executes requests and responses, using its neural network to analyze page elements and find malicious code. It protects application servers from attack by compromised endpoints by inspecting and cleaning all requests to the server, removing any HTTP header manipulation or malicious code. These techniques help to prevent the sophisticated attacks that often bypass legacy web security solutions. Additionally, the Menlo Cloud enables security teams to configure browsers according to industry benchmarks, create policies to control end user permissions, and prevent data loss through DLP rules and watermarking.

There is no benefit to investing large amounts of time and resources into legacy security infrastructure that attackers have learned to bypass. The Menlo Secure Enterprise Browser solution delivers critical security services such as DLP as well as URL and content filtering. Additionally, it uses its neural network to scan each page, deliver only safe content, and enable users to complete their work safely, using the same browsers they've already been using. If your organization struggles to provide complete browser security for end users, whether remote, hybrid, or in the office, Enterprise Strategy Group recommends that you consider the Menlo Secure Cloud Browser and the other capabilities of the Menlo Secure Enterprise Browser solution.

⁴ Source: Enterprise Strategy Group Research Report, [Passwordless in the Enterprise](#), September 2023.



©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

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