MENLO
SECURITY

Menlo Secure Cloud Browser Executive Brief

Protect users from browser-based attacks, defend your most critical enterprise asset and enable easy zero-trust access.

The adoption of cloud-based applications, alongside the rise of hybrid work environments, has fundamentally altered our work methods. Many of these applications, like email, have shifted from dedicated client apps to browser-based access for increased convenience across various devices. However, network and endpoint security controls often fail to detect browser-based threats, despite the browser's growing importance in enterprise settings. Threat actors exploit this vulnerability with Highly Evasive and Adaptive Threats (HEAT) attacks, such as advanced phishing kits and code obfuscation techniques like HTML Smuggling, evading traditional security tools like firewalls and sandbox analysis. This leads to severe consequences like ransomware infections, account takeovers, and sensitive data breaches.

Secure Cloud Browser Overview

The Menlo Secure Cloud Browser transforms every browser into a secure enterprise browser. Menlo Secure Cloud Browser runs within an elastic and orchestrated cloud-native platform, creating a real time digital twin of your local desktop, executing content away from the endpoint and delivering only safe, reconstructed content to the user's local browser. This allows for lower bandwidth consumption with zero latency allowing users to navigate freely and without fear. It doesn't matter if the web content is good or bad, categorized or uncategorized, the Menlo Secure Cloud Browser treats all content as potentially malicious and handles it accordingly.

The browser represents one of the top attack surfaces in the enterprise. With more than **80% of the Internet attacks targeting end user browsers,** according to Google.


Network and endpoint security fail to provide comprehensive protection inside the browser resulting in a surge of browser-based attacks last year. **75% of phishing links and over 70% of evasive malware** were identified originating from known, categorized or trusted websites.

Commonly deployed security tools consistently lack visibility inside the browser. **Six days is the average** latency between when a zero-hour attack first appears and when it is finally added to the detection mechanism for commonly deployed security tools.
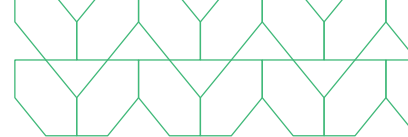
Menlo prevents zero day exploits and HEAT attacks because we analyze data and information in the Secure Cloud Browser. This allows us to use advanced AI techniques, cloud content inspection capabilities, and secure document and archive viewers to identify and block unknown threats or evasive malware that don't have signatures or digital breadcrumbs to detect. By rendering the web page in the Secure Cloud Browser, Menlo is able to see exactly what's happening on the webpage and prevent malicious, dynamic content or payloads, such as javascript or smuggled code, from executing locally on the endpoint. Notorious ransomware and threat actor groups are known for using these evasive techniques to evade traditional security controls. In fact, Menlo Security was the first to identify and block the threat actor group Evil Proxy from using reverse proxy methods on compromised web pages in an attempt to steal user login credentials and gain system access.
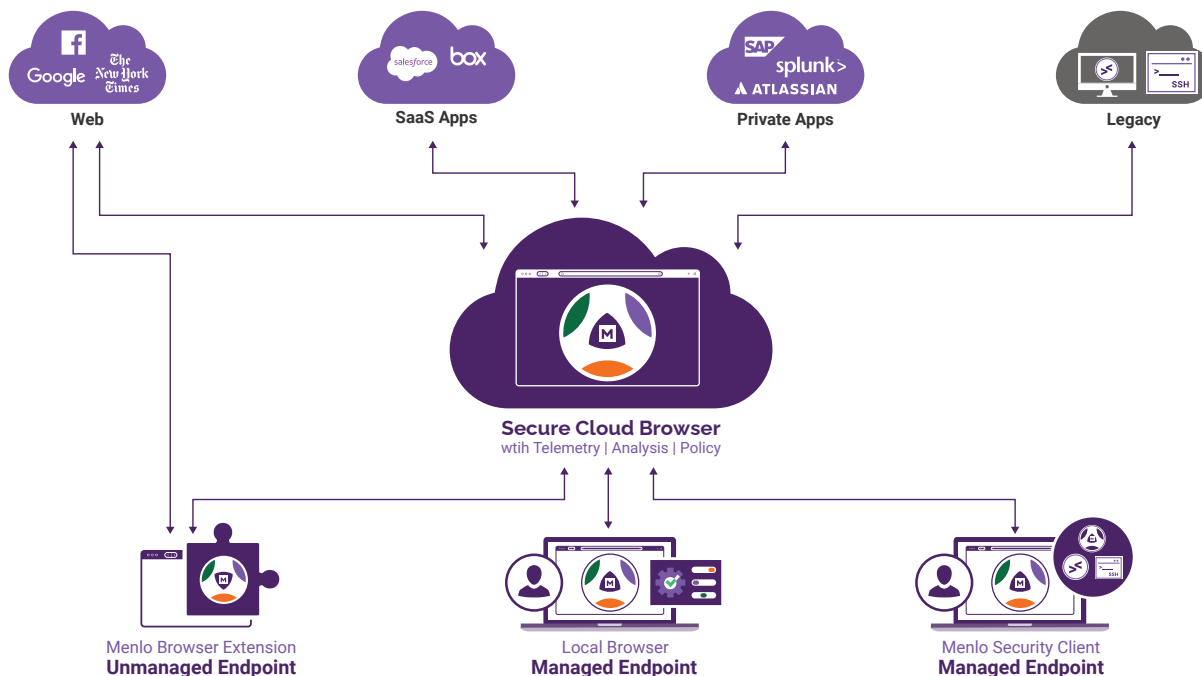
Illustration 1: Menlo Secure Cloud Browser keeps threats off the endpoint

The Menlo Secure Cloud Browser makes it possible to identify evasive techniques by combining AI with advanced URL runtime analysis of the individual web page elements. Using Menlo Computer Vision, a leading object detection model, the Menlo Secure Cloud Browser can identify and locate images and identify logos within web content. The key innovation of the Menlo Computer Vision is its ability to perform logo detection in real-time with high accuracy and then add the classification from this layered model to the larger platform, which makes decisions about how to protect users. The Menlo secure cloud document viewer and archive viewer also enables users to safely view password protected files without ever downloading them to the endpoint. This enables security teams to block evasive techniques used to evade traditional content inspection and close the window of exposure from zero-day exploits.
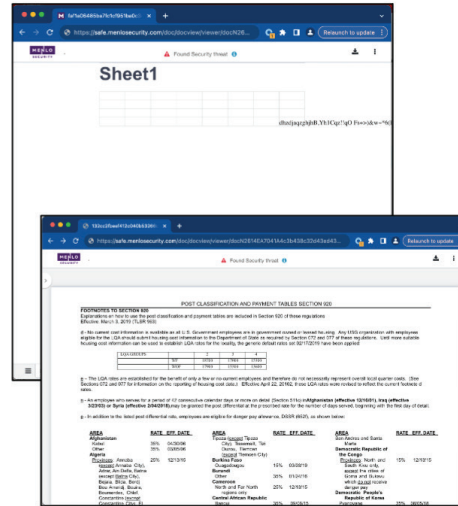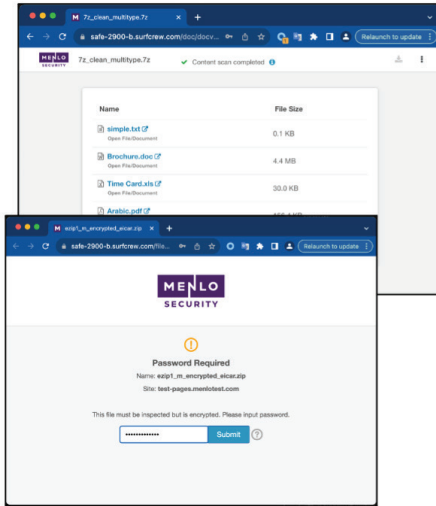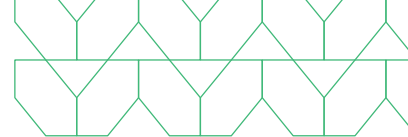
Illustration 2: Menlo secure cloud document viewer and archive viewer

Stop threats before they reach the endpoint. Menlo Secure Cloud Browser eliminates the browser attack surface and delivers modern protection to every single user, no matter where they work.

The Menlo Secure Cloud Browser is easy to use and simple to deploy. It gives administrators the ability to set acceptable use policies to block any malicious activity. Policies can be applied based on user, group, file type, website category, or cloud application to determine when content is blocked, rendered in read-only mode, or accessible in its original form. The Secure Cloud Browser scales globally to accommodate fluctuating workforce needs and traffic volume and can deliver a risk-free local-browsing experience for every user, every tab, and every web session regardless of which browser they choose. Users can continue using the browser they know, and Menlo Security can protect browsers from evasive threats and secure access to applications and data down to the last mile.
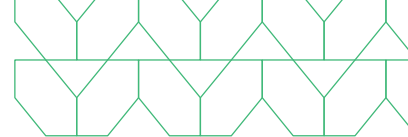
Secure Cloud Browser key capabilities:

Proactive protection against zero-day browser exploits:

Rather than the user's browser accessing websites directly, each web request is sent and executed inside the Menlo Secure Cloud Browser, and only a safe, clean version is brought down to the user's browser. This closes the window of exposure from zero-day browser exploits for all browsers and endpoints ensuring that customers are fully protected before patches are even released or deployed.

Zero-touch code protection:

The Menlo Secure Cloud Browser removes any malicious, dynamic content or payloads, such as javascript or smuggled code, from executing locally on the endpoint, protecting against advanced malware used to evade traditional security tools.

Complete end-to-end browser visibility:

Evasive threat intelligence and actionable alerts are delivered to SOC teams for real time visibility and improved incident response. Detailed threat intelligence and browser forensics can be integrated into existing log aggregation, automation and security orchestration tools for improved optimized performance.

Inline AI-powered protection:

With Menlo, each web request is executed in the Secure Cloud Browser, enabling AI-based real-time analysis of each page, including DOM elements, logos and URL path. If a phishing or malware threat is detected, dynamic policy controls can block the site outright or render the page in read-only mode, preventing any data input.

Multi-layered content inspection:

The Menlo Secure Cloud Browser inspects password protected files, provides malware analysis for documents, and converts files into safe PDFs by applying anti-virus, file hash look up, cloud sandboxing, and file handling policies.

## Secure cloud document & archive viewing:

Open and view any document safely in our secure document and archive viewer without the need to download files to the endpoint. This provides safe viewing of document and archive content, including nested and password protected archives without them ever touching the endpoint.

User/Group policy and authentication control:

Set and fine-tune policies and exception requests for specific users, user groups or content type (all content, risky, uncategorized). Integrates with SSO and IAM solutions with SAML support for user authentication.

Integrated browser forensics:

Incident Response teams can use the Browser Forensics tool for high-fidelity browser session recording to view a complete visual timeline of user browsing sessions including screenshots, user inputs and page resources.
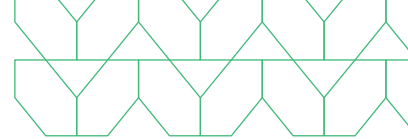
Flexible deployment & ease of management:

Simple to deploy and manage. Supports any browser on any device, desktop and mobile, allowing users to continue working with their browser of choice. No new endpoint software for IT to manage. Once activated, enforcement actions can be easily defined and monitored inside the admin portal.

Seamless API integrations:

Highly extensible set of standards support, API and third party integrations for SSO, SIEM, MDM, firewall, proxy, AV, sandbox, CDR, SOAR, SD-WAN and SASE.

Transform your browser into a Secure Enterprise Browser with Menlo Security

The Secure Cloud Browser stops threats cold, protecting users from zero-day web exploits and browser-based attacks, including the tactics that legacy security tools cannot stop. Using a fundamentally different approach, Menlo Security shrinks the existing risk gap and brings modern protections to every single user, no matter where they work. The Menlo Secure Cloud Browser is the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams.

To learn more about securing the ways people work, visit menlosecurity.com or email us at ask@menlosecurity.com.

MENLO
SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

f 𝕏 in ▶

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.