MENLO SECURITY

Menlo Cloud Executive Brief

Protect Users from Browser-Based Attacks, Defend your Most Critical Enterprise Assets, 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 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 expanded importance in enterprise settings.

Threat actors exploit the browser's insufficient security with highly evasive and adaptive threat (HEAT) attacks. HEAT attacks may include advanced phishing kits and code obfuscation techniques, including, for example, HTML smuggling, that evade firewalls, sandboxes, and other traditional security tools. Such evasive threats can lead to severe consequences, such as ransomware infections, account takeovers, and sensitive data breaches.

Menlo Cloud Overview

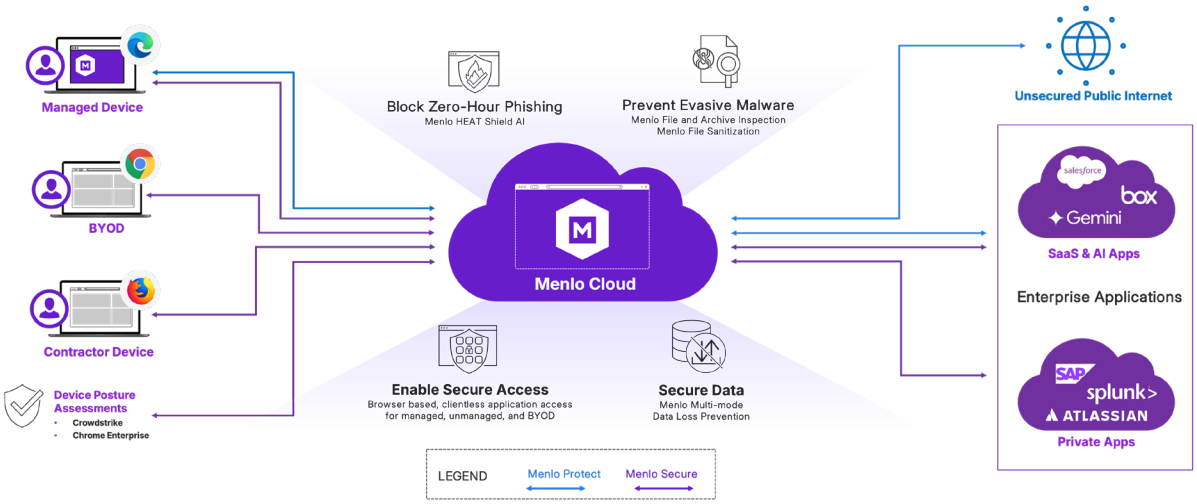
Menlo cloud-based Browser Security transforms any browser into a secure enterprise browser. The Menlo Cloud is an elastic and orchestrated cloud-native platform, creating a real-time digital twin of the user's local browser, executing content away from the endpoint and delivering only safe, reconstructed content to the browser. The Menlo Cloud delivers browser security invisibly to end users who can browse freely without introducing risk to their organization. Regardless of whether if the web content is good or bad, or categorized or uncategorized, the Menlo Cloud treats all content as potentially malicious and handles it accordingly.

Phishing attacks attempt to steal credentials and deliver ransomware, and they continue to grow by triple-digit percentages.

GenAI is changing the workforce. Read this report, based on Menlo Cloud telemetry, that provides the latest trends in enterprise GenAI use, and discusses immediate issues including data loss/leakage, regulatory compliance, and malware vectors.

Your team can get ahead of many security threats posed by the exploding use of GenAI, particularly in browsers. Read this brief.

Menlo Security prevents zero-day exploits and HEAT attacks because data and information are analyzed within the Menlo Cloud. Leveraging advanced AI techniques and cloud content inspection, the Menlo Cloud identifies and blocks novel threats and evasive malware that do not yet have signatures or digital breadcrumbs that legacy defenses rely upon for threat detection. Integrated services in the Menlo Cloud render and execute web page content, providing full analysis of page content and code actions, and then preventing malicious dynamic content and payloads such as JavaScript or smuggled code from executing on the endpoint. Notorious ransomware and threat actor groups are known for using these 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 webpages in an attempt to steal user login credentials and gain system access.



Menlo Cloud Keeps Threats Off the Endpoint

The Menlo Cloud identifies evasive techniques by combining AI with advanced runtime analysis of the individual web page elements. Using Menlo Computer Vision, a leading object detection model, the Menlo Cloud locates and identifies images and logos in web content. The key innovation of 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 cloud document and pantented archive viewer also enables users to safely view plain text and password-protected files prior to downloading them to the endpoint. Security teams can block evasive techniques used to evade traditional content inspection and close the window of exposure from zero-day exploits.

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

Menlo cloud-based browser security is invisible to users and requires no software deployment. 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. All Menlo Cloud services scale 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 users choose. Users can continue using the browser they know, and Menlo Security protects browsers from evasive threats and provides secure access to vulnerable internal applications.

Menlo Cloud Key Capabilities

Proactive protection against zero-day browser exploits: Close the window of exposure from zero-day browser exploits before patches are even released or deployed. Menlo removes any malicious, dynamic content or payloads, such as JavaScript or smuggled code, from executing locally on the endpoint, protecting against advanced malware that can evade traditional security tools.

Inline AI-powered protection: Stop attacks from and losses to fraudulent web sites with AI-based runtime analysis, enhanced with Google Gemini, of each page, including DOM elements, logos, and URL path. If a fraudulent site is detected, dynamic policy controls can block the site outright or render the page in read-only mode, preventing any data input.

Document and Archive Security: Files and archives, in particular any that are password-protected or nested archives, carry the risk of embedded malware. Menlo File Security takes cloud content inspection a step further by assuming all files are malicious. Advanced Content Disarm and Reconstruction (CDR) with patented Positive Selection® technology, disarms and reconstructs files. The patented Menlo Archive Explorer enables a user to select any file for sanitization, delivering only clean, safe content to the user while maintaining any full functionality for nearly any file.

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

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 Menlo Browser Forensics to review high-fidelity browser session recordings that include a complete visual timeline of user browsing sessions, including screenshots, user inputs, and page resources.

Flexible deployment and ease of management: The Menlo Cloud is software as a service with no endpoint deployment, configuration or management and supports any browser on any desktop and mobile device, allowing users to continue working with their browser of choice. Once activated, enforcement actions can be easily monitored and modified inside the admin portal.

Transform Every User's Browser into a Secure Enterprise Browser

The Menlo Cloud protects 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. Menlo cloud-based Browser Security is the only solution that delivers on the promise of browser security by providing a zero trust approach to preventing malicious attacks, making security invisible to end users as they work online, and removing many operational burdens for security teams.

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

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Cloud. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Cloud 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.