DATA SHEET

# Menlo Cloud

## Transform Any Browser into a Secure Enterprise Browser

Keep evasive threats off the endpoint

Full Visibility into Browser Activity

Transparent user experience

## The Challenge

The shift to cloud-based applications and hybrid work has transformed how we work. Many enterprise applications, like email, have shifted from dedicated client apps to browser-based access for convenience across devices. However, network and endpoint security often fails to detect browser-based threats, despite their growing importance in enterprise settings. Cybercriminals exploit this vulnerability with highly evasive and adaptive threat (HEAT) attacks, such as advanced phishing and HTML smuggling, which bypass firewalls, sandboxes, and other traditional security measures. Such threats leave organizations vulnerable to ransomware, account takeovers, and data breaches.

### Modern Cloud Based Browser Security is the Only Way to Deliver Preemptive Security

The Menlo Cloud delivers the next generation of remote browser isolation with patented technology that can secure all web traffic by replacing inefficient pixel-streaming with safe HTML rendered at the endpoint.

The Menlo Cloud secures local browsers by creating a real-time, hardened digital twin of the local browser in the cloud, executing content away from the endpoint and delivering only safe content to be rendered by the user's local browser. With each click, every page that is opened in the local browser is mirrored and opened first in the cloud, providing complete protection against web exploits or HEAT attacks that target users through the browser.

## KEY BENEFITS

The browser represents one of the top attack surfaces in the enterprise, with more than 80% of internet attacks targeting end-user browsers, according to Google. With Menlo, employees and contractors can access applications through a browser portal or extension, with no need for installation on their devices.

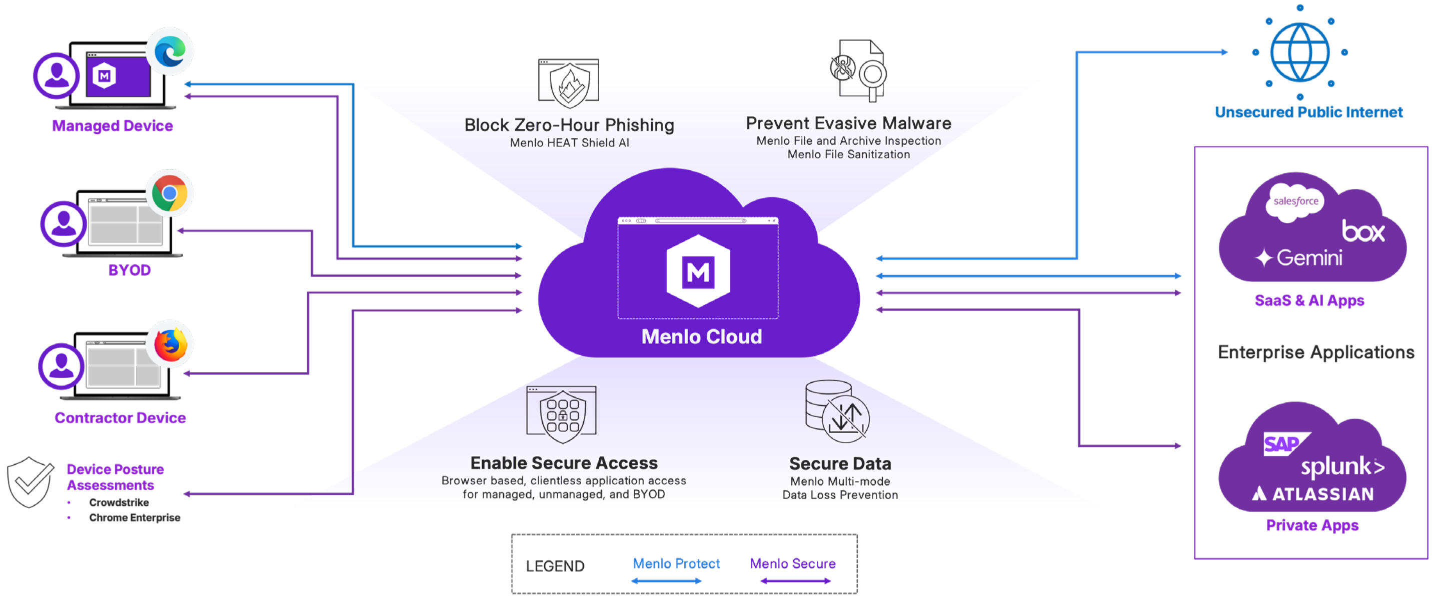
Network and endpoint security tools fail to provide comprehensive protection inside the browser, resulting in a surge of browser-based attacks. In fact organizations during 2024 faced 140% growth in browser-based phishing attacks and scary 130% growth in zero-day phishing attacks through browsers.

When a zero-hour attack first appears, it takes six days on average to add it to the detection mechanisms for common security tools.

The Menlo Cloud delivers a transparent user experience 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 Cloud treats all content as potentially malicious and handles it accordingly.

Multiple services in the Menlo Cloud collaborate to prevent threats, specifically the growing number specifically designed to avoid detection by legacy network and endpoint security solutions. Many attacks occur on fraudulent web sites that users are lured to with zero-day techniques such as polymorphic phishing and GenAI-enhanced social engineering or compromised sites hosting drive-by downloads. Menlo Heat Shield AI is integrated with Google Gemini analysis to deliver highly effective fraudulent site detection long before signature- or category-based defenses can identify them. Evasive malware embedded in site code is never delivered to endpoints. Files and archives carried in web traffic, even password-protected, are rendered safe with Menlo File Security. And in the era of GenAI, Menlo DLP prevents data loss to GenAI with inspection of both the GenAI prompt inputs and any files uploaded from a browser to a GenAI portal.

Menlo cloud-based browser security is a SaaS service with no endpoint software deployment for most use cases. The Menlo Cloud management portal gives administrators the ability to set acceptable use policies to block 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. Every service in the Menlo Cloud 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 end user browser choice. Users can work with the browser they know, and Menlo Security can protect browsers from evasive threats, while securing data and applications down to the screen level, controlling copy/paste actions, forbidding file uploads and downloads and watermarking web pages.



## Menlo Cloud Keeps Threats off the Endpoint

## Key Features

**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 Your Browser into a Secure Enterprise Browser

The Menlo Cloud protects users and organizations from zero-day web exploits and browser-based attacks. Using a fundamentally different cloud-based approach, Menlo Security brings modern protections to every user, no matter where they work. The Menlo Cloud is the only solution to deliver on the promise of browser security—by providing the most secure zero trust approach to preventing malicious attacks—by making security invisible to end users as they work online and removing many operational burdens for security teams.

## 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.

Work without worry and move business forward with Menlo Security.

MENLO SECURITY

Learn more: https://www.menlosecurity.com
Contact us: ask@menlosecurity.com