MENLO SECURITY

DATA SHEET

Menlo Remote Browser Isolation

Protect Work by Eliminating the Threat of Malware and Phishing Against the Browser

Keep evasive threats off the endpoint

Safeguard user data

Provide a seamless browsing experience for users

The Challenge of Protecting the Enterprise's Most Critical App: The Browser

There's no way around it: the internet is a mission-critical business tool for today's enterprises. Widely distributed users need fast, reliable access to websites, cloud apps, and software-as-a-service (SaaS) platforms to complete their day-to-day tasks. But the internet is rife with malicious threats and highly evasive and adaptive threat (HEAT) attacks that pose an enormous risk for enterprises. Security teams need a new approach for securing web browsing without impacting users' ability to work harder and smarter wherever business takes them.

Evasive Phishing and Malware Defense Wherever Users Work

Menlo Security Remote Browser Isolation provides security teams with the visibility and control they need to enable a zero trust approach to protecting against malware. To capitalize on the growing threat landscape, threat actors are targeting web browsers with HEAT attacks that bypass traditional security defenses and exploit the standard capabilities of modern browsers to deliver ransomware, steal credentials, and deploy malware.

Rather than trying to identify threats after the fact, Remote Browser Isolation works together with the Menlo Secure Cloud Browser to prevent threats from reaching their target. By driving all web traffic through a cloud-based digital twin of the local browser, Menlo delivers only safe content to the endpoint. It doesn't matter if the web content is good or bad, categorized or uncategorized—Menlo Security adopts zero trust principles by assuming that all content is malicious and treating it accordingly.

KEY BENEFITS

To be productive, users need safe and reliable access to web-based information, SaaS applications, online documents, collaboration tools, and other business resources.

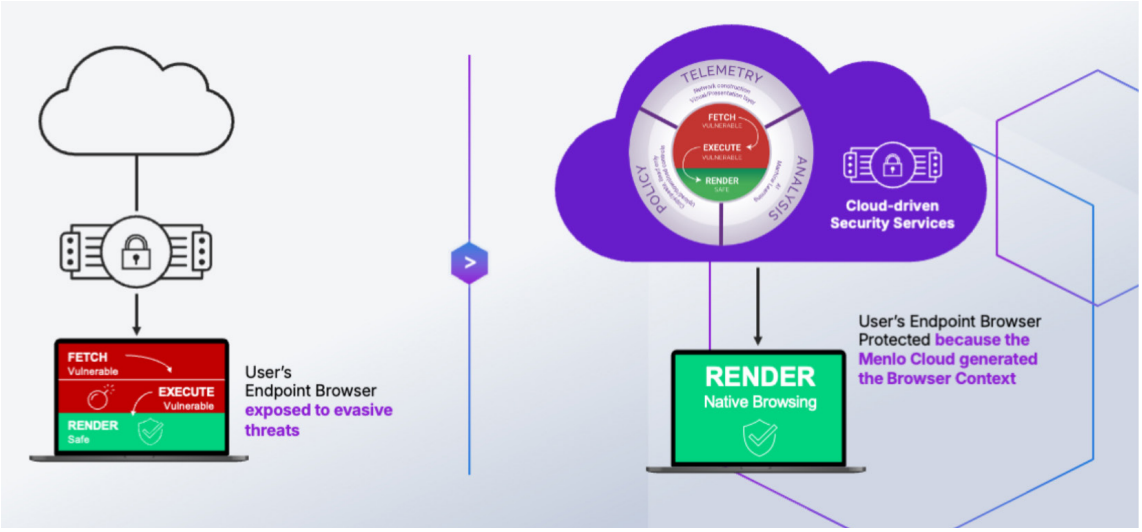
Legacy detection-based security approaches fail to protect against modern-day threats, such as highly evasive and adaptive threat (HEAT) attacks, ransomware, zero days, and credential theft.

Menlo Remote Browser Isolation together with the Menlo Secure Cloud Browser uses a fundamentally different approach to help you stay ahead of the game and eliminate browser-based threats completely.

Along with Remote Browser Isolation, Menlo Security converges secure web gateway (SWG) capabilities into a single cloud-native platform—including CASB, DLP, RBI, proxy, FWaaS, and private access. The Menlo Cloud provides extensible APIs and a single interface for policy management, reporting, and threat analytics. In addition, fluctuating workforce needs and traffic volumes are accommodated without requiring capacity planning or configuring clients deployed on endpoints. This scalability ensures that granular access and security policies are enforced, data leaks are prevented, cloud apps are secure, and compliance is ensured across all devices and locations—while allowing users to access the web-based information and productivity tools they need.

In addition to fully enabling the way people work, Menlo Remote Browser Isolation together with the Menlo Secure Cloud Browser gives administrators the ability to set acceptable use policies to block malicious activity, including compromised websites, cybersquatting, file uploads and downloads, inappropriate sharing, and other unknown threats. Policies can be applied based on user, group, file type, website category, or cloud application to determine when content is blocked, when it is rendered in read-only mode, or when the original content should be accessible.

Menlo Security does this with unmatched performance and scale, ensuring direct-to-cloud internet access while providing core proxy capabilities, running traffic through security checks, including URL filtering, sandboxing, data loss prevention, antivirus scanning, CASB, and other converged technologies.



Menlo Secure Cloud Browser Isolation keeps evasive threats off the endpoint

Key Capabilities

Proactive protection against browser-based threats: Shrink the existing browser risk gap by executing all web content in a secure, cloud-based environment. Menlo prevents any malicious, dynamic content or payloads, such as those hidden in JavaScript or smuggled code, from executing locally on the endpoint, protecting against advanced malware used to evade traditional security tools.

Secure cloud document and archive viewing: Open and view any document safely in our Secure Document and Archive Viewer without the need to download files to the endpoint. Provide high-fidelity, secure versions of files with support for printing, search, copy/paste, and sharing, accessible on both desktop and mobile devices.

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 optimal performance.

Integrated browser forensics: Incident response teams can use Menlo Browser Forensics for high-fidelity browser session recording to view a complete visual timeline of browsing sessions, including screenshots, user keystrokes, and page resources.

Flexible deployment and ease of management: Menlo supports any browser on any desktop or mobile device, allowing users to continue working with their browser of choice. There's 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: Menlo provides highly extensible standards support, API, and third-party integrations for SSO, SIEM, MDM, firewall, proxy, AV, sandbox, CDR, SOAR, SD-WAN, and SASE.

Protect Against Evasive Threats and Prevent Risky User Activity Inside the Browser

Menlo Security's Remote Browser Isolation technology is the core of the Menlo Secure Enterprise Browsing solution, protecting users from browser-based threats by isolating all internet browsing activities in a remote, cloud-based environment. Instead of executing web content directly on the user's device, Remote Browser Isolation processes it in a secure virtualized container. This approach prevents evasive malware, sophisticated phishing attacks, and other threats from ever reaching the endpoint, while allowing users to interact with websites and applications seamlessly. By keeping potentially harmful content away from the user's device, Menlo Security provides strong protection with zero impact on browsing performance.

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.

MENLO SECURITY

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