MENLO SECURITY

Secure Enterprise Browser Executive Brief

Prevent Evasive Threats that Target the Browser

The web browser has become the most widely used enterprise application, making it a prime target for threat actors. Despite the billions of dollars spent each year on cybersecurity, the web browser is the least protected attack surface in the enterprise today, primarily because dominant network security tools have no visibility into browser traffic. It should come as no surprise that threat actors target the web browser as the focus of ransomware and phishing attacks, and they are using highly evasive threats to avoid detection and maximize their success rate.

Traditional network and endpoint security tools, including web gateways, endpoint detection and response (EDR), and firewalls, are blind to browser-based activity because these tools rely only on detection capabilities, such as pattern matching of known threats, and lack complete visibility into specific browser behaviors. The Menlo Secure Enterprise Browser solution closes this gap and stops malware and phishing by providing visibility into actions inside the browser. This visibility enables you to identify and block malicious websites, regardless of known signatures or pattern-based detection.

Why Browser Security

Because browsers play an outsize role in the digital economy, they are often the target of threats. The enterprise browser is a critical component of enterprise security, protecting users in a variety of ways:

Phishing Attacks: Phishing has become a popular tool for adversaries to compromise user systems, steal data, or gain unauthorized access by deceiving users into revealing sensitive information, usually through fake websites or emails.

Zero-Day Exploits: Zero-day phishing attacks and other vulnerabilities are unknown or never-before-seen phishing attacks that have not yet been categorized as malicious. They they may also include security flaws that have not yet been patched by developers. Ensuring strong browser security helps defend against such zero-day exploits by implementing inline browser security and dynamic security enforcement for users.

Malware and Viruses: Browsers can be susceptible to malware and viruses, which can infect devices and cause various issues, such as data theft, system damage, or loss of control over user devices. The robust security features of the Menlo Secure Enterprise Browser help to prevent such malware attacks and ensure safer browsing experiences.

Secure Access to Sensitive Information: Browsers are the primary tools used to access the internet and online services, including corporate information, SaaS applications, email, social media, banking, and more. Users often enter sensitive information, such as passwords, credit card details, and personal data, and browser security is essential for preventing this information from falling into the wrong hands.

Protecting Privacy: Browsers can track users' activities, store cookies, and gather personal information, raising privacy concerns. The Menlo Secure Enterprise Browser solution can help users and organizations control their online privacy, block unwanted tracking, and protect their data from misuse.

Why Menlo

Menlo Security provides end-to-end visibility into all web traffic and enables dynamic policy controls, allowing you to identify browser-based threats and prevent them from reaching your end users. Menlo is unlike on-premises and cloud-based network security tools that rely on signatures of known threats or systems that employ network-based telemetry alone, which fail to detect unknown phishing threats and other evasive techniques. Instead, Menlo Security offers a simple-to-deploy cloud-based browser security service that supports any browser, anywhere in the world.

Given the shift toward evasive threats, we introduced Menlo Protect with HEAT Shield AI, an industry-first suite of threat prevention capabilities designed to detect and block evasive threats targeting the browser. Using multiple AI-based techniques, including Computer Vision, URL risk scoring, and analysis of web page elements, HEAT Shield AI can accurately determine in real time if a link being opened is a phishing site designed to steal user credentials. If so, HEAT Shield AI applies dynamic policy enforcement—either displaying the page in read-only mode or blocking it completely. HEAT Shield AI provides real-time protection for the browser, surfacing action-oriented threat intelligence on highly evasive threats and zero-hour phishing attacks, enabling you to improve security while providing a seamless browsing experience for end users. Menlo Secure Application Access adds similar protections for users of all types to get least-privileged access to the apps they need. Controls include application access, rather than network access, as well as read/write, upload/download, copy/paste, and watermarking.

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 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. © 2025 Menlo Security, All Rights Reserved.

MENLO SECURITY

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