MENLO SECURITY

Browser Security Executive Brief

Prevent evasive threats that target the browser

The web browser is 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. It should come as no surprise that threat actors target the web browser as the focus of ransomware and phishing attacks, and are doing so using highly evasive threats to avoid detection and maximize their success rate.

Traditional network and endpoint security-based solutions, including web gateways, endpoint detection and response (EDR) solutions, and firewalls, are blind to browser-based activity because they rely only on detection capabilities, such as pattern matching of known threats, and they lack complete visibility into specific browser behaviors. Browser security 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. Browser security 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 or security flaws that have not yet been categorized as malicious by web filters or not yet been patched by

50%+ of evasive threats come from categorized websites within the browser.

70% increase in attacks using reputable websites to evade URL reputation engines.

20% of web malware attacks are categorized as highly evasive and can bypass existing network security controls.

Every minute, a new phishing site is created that impersonates a well-known brand.

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. Robust browser security helps prevent such malware attacks and ensures 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. Effective browser security solutions can help users and organizations control their online privacy, block unwanted tracking, and protect their data from misuse.

Why Menlo

Menlo Security provides complete end-to-end visibility into all web traffic and enables dynamic policy controls, allowing you to identify and prevent browser-based threats from reaching your end users. Unlike on-premises and cloud-based network security solutions that rely on signatures of known threats, or AI trained on network-based telemetry, which fails to detect unknown phishing threats and other evasive techniques, 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, Menlo Security introduced HEAT Shield, 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 can accurately determine in real time if a link being opened is a phishing site designed to steal users' credentials and apply dynamic policy enforcement — either displaying the page in read-only mode or blocking it completely. HEAT Shield provides real-time protection for the browser, surfacing action-oriented threat intelligence on highly evasive threats and zero hour phishing attacks, enabling organizations to improve security while providing a seamless browsing experience for their end users.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com
(650) 695-0695
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.

© 2024 Menlo Security, All Rights Reserved.