MENLO SECURITY

Stop Zero-Hour Phishing and Malware Attacks

Block phishing and prevent attacks from malware hidden in web traffic and downloads without compromising business productivity.

Generative AI Is Fueling a New Wave of Phishing Attacks

Generative AI (GenAI) has increased malicious actors' level of sophistication, as hackers use the technology to create more convincing emails, SMS messages, and social posts that deceive even the most seasoned users. These sources contain links that, when clicked, lead the user's browser to phishing sites, which may be designed to steal credentials, sensitive content, or intellectual property (IP).

The Persistent Challenge of File-borne Threats

GenAI is also being used to generate malicious web downloads, embedding malware directly into seemingly safe and legitimate files. In today's dynamic threat landscape, file-borne malware in the web stream continues to be a significant vector for cyberattacks. Highly evasive and adaptive threat (HEAT) attacks and zero-hour ransomware can readily bypass traditional detection-based security solutions. Organizations struggle to balance user productivity with the imperative to prevent these insidious threats from reaching endpoints and compromising data. The challenge is compounded by the sheer volume of files exchanged daily, making manual inspection impossible.

More sophisticated phishing vectors and websites, combined with file-borne threats, create a dual attack methodology that makes it easier for bad actors to steal credentials, extract sensitive data, or deliver malware, dramatically increasing organizational risk.

SOLUTION BRIEF

Menlo Security Unifies Malware Detection, Phishing Prevention, and File Sanitization for Umatched Threat Protection

Menlo Security, the pioneer in browser security, has created a comprehensive browser security solution that proactively eliminates file-borne threats before they reach the user's endpoint, ensuring protection for web downloads without compromising user experience or productivity.

The unified solution leverages:

- **Menlo Secure Cloud Browser:** This foundational technology executes all web content in a secure, cloud-based environment, executing threats away from endpoints. This "assume breach" mentality ensures that no web-borne malicious code can ever directly interact with user devices.
- **Menlo Heat Shield AI:** Dynamically blocks zero-hour phishing attacks, regardless of source (email, SMS, documents) in real time using a combination of AI, computer vision, and real-time analysis of web page elements to identify and neutralize threats before they can reach the user.
- **Menlo Advanced Content Disarm and Reconstruction (CDR):** Patented Postive Selection™ technology from Menlo goes beyond typical malware detection mechanisms. It disarms files by examining all active, executable content, such as macros, scripts, and embedded objects, and then reconstructs a new, clean, and fully functional version of the file. This process ensures that only safe, sanitized data reaches the user.

Unrivaled Protection from Malicious Links in Email Bodies and Attachments

Email remains one of the most successful attack vectors, with weaponized links and attachments being a primary delivery mechanism for ransomware and phishing. Menlo Security offers:

- **Protection against malicious links in email bodies:** Users are protected regardless of how links are delivered, because every link, including those found in the body of an email, opens in the Secure Cloud Browser the moment that the user clicks. Menlo HEAT Shield AI then examines the target website, considering JavaScript elements, Document Object Model (DOM) content, logos and graphics, input fields, and URL paths. All analyses are run in parallel, ensuring that verdicts are both fast and accurate. Rules set in the Menlo administrative portal set the threshold for subsequent actions, including blocking the site or rendering it read-only, to prevent malicious activities, credential theft, data exfiltration, and more.
- **Protection against malicious links in attachments:** In the event that Menlo CDR is not in use, an attachment deemed potentially safe by email content inspection may include a malicious link. If the user opens the attachment in an application and clicks on the malicious link, Menlo HEAT Shield AI phishing detection provides comprehensive protection.

Comprehensive Protection Against Malware Embedded in Files and Archives

Files and archives carried in web traffic are a common entry point for malware. The Menlo Secure Cloud Browser, in concert with Menlo Advanced CDR, offers protection against malware embedded in files and archives carried in web traffic:

- **Comprehensive zero trust file handling:** Every file downloaded can be automatically routed through Menlo Security Advanced CDR, ensuring only clean, sanitized versions are delivered to the user's device.
- **True file fidelity:** Unlike simple file flattening to create a safe PDF, Menlo Advanced CDR performs file analysis among file components, including content, templates, and objects, identifying harmless file components. It then creates a safe, new file in the source file's native format (e.g., Word, Excel, PDF), and rebuilds the source file's safe content in the new file. This process preserves full functionality, formatting, and usability, without disruption or feature loss. Over 200 file types are supported with vendor-endorsed understanding of complex file structures, such as Microsoft Office and the most complex image types.
- **Protection for evasive threats:** Menlo Protect with Advanced CDR eliminates threats that leverage obfuscation, polymorphic malware, or zero-day vulnerabilities that traditional signature- or sandbox-based solutions might miss.
- **Seamless user experience:** As needed, prior to CDR, users are prompted for passwords to open and examine encrypted files and archives. The Menlo Secure Cloud Browser offers a patented archive viewer so that users can review any files that should be delivered for sanitization. The CDR process is transparent to end users, who receive clean, safe files without delay or degradation in performance.

A Fundamentally Superior Approach to Threat Prevention

The integration of native capabilities in the Menlo Secure Enterprise Browser solution—including HEAT Shield AI—and Advanced Content Disarm and Reconstruction with Positive Selection technology marks a significant leap forward in file-borne threat prevention. By unifying high-performance cloud-based browser security with proactive file sanitization, organizations reach the next level of security and user productivity. The Menlo secure-by-design approach frees up security teams, reduces operational burden, and empowers your workforce to browse, click, download, and open files with complete confidence.

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.

MENLO SECURITY

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