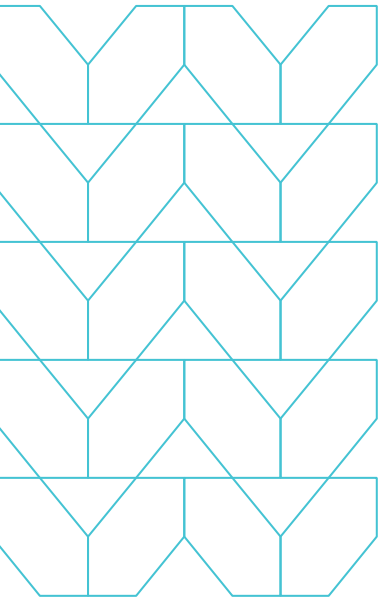
MENLO SECURITY

Defending browsers against zero-hour phishing attacks

Protect the user and defend your enterprise against targeted phishing attacks that traditional approaches cannot stop.

Solution Brief



Most organizations that run web browsers rely on network-based security controls to protect against internet-borne threats. Attackers know these detection-based tools are reliant upon the existence of known bad signatures and are using evasive techniques, including zero-hour phishing attacks to circumvent these controls. These techniques — called Highly Evasive and Adaptive Threat (HEAT) attacks — are becoming increasingly used to evade commonly deployed security controls.

While existing network and endpoint solutions do offer partial protection, these tools ultimately rely on block lists, containing previously convicted phishing URLs, to protect against unknown or never-before-seen phishing attacks. Some secure web gateway (SWG) solutions use more advanced inline phishing detection engines but are limited due to performance requirements.

Even AI models trained on network-based telemetry fall short because firewalls and SWGs lack sufficient visibility into web sessions and don't provide full browser telemetry.

This lack of visibility and control inside the browser has dramatically increased the browser attack surface. Phishing attacks are becoming more sophisticated with the use of cloaking, URL rotation, code obfuscation, and dynamic code generation. These techniques make it difficult for traditional phishing detection tools that rely on signature-based or classic feature extraction techniques to detect evasive pages. Without improved visibility and dynamic control inside the browser, security teams will remain exposed to zero-hour phishing attacks and other evasive threats.

Menlo Security HEAT Shield provides complete visibility into each browser session and enables dynamic policy controls, stopping zero-hour phishing attacks and other evasive threats. HEAT Shield does this by putting AI-powered "eyes" on browser activity and dynamic web content to:

- Better correlate events and end-user actions, including data and credential entry session, for real time decision making on how to best protect users
- Quickly identify and block impersonated brand logos and images using real time logo detection
- Integrate context-rich browser telemetry into existing security tools for accelerated incident response

Key Benefits

Real-time protection against zero-hour threats, credential theft, and previously unseen phishing attacks

Full visibility into every web session, delivering comprehensive browser security and protection against evasive threats that commonly circumvent traditional security solutions

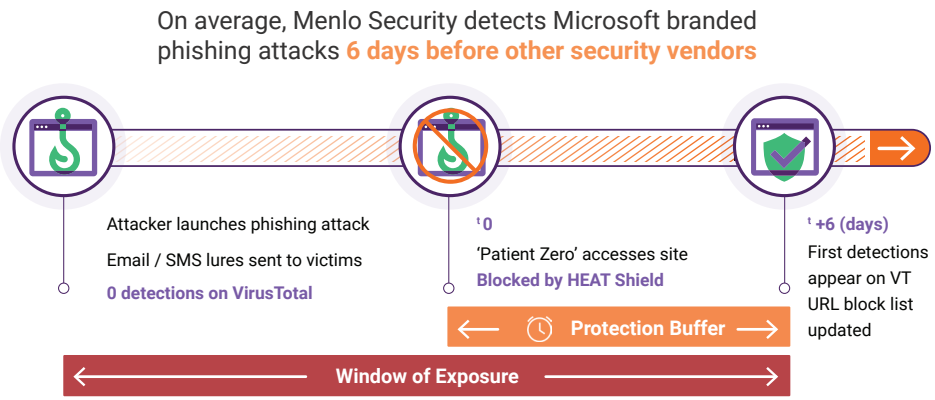
Context rich, evasive threat intelligence and actionable alerts provided to accelerate incident response workflows

HEAT Shield provides comprehensive visibility and intelligence into evasive threat signals from inside the browser, a telemetry source that is invisible to common network security solutions. By doing so, HEAT Shield is able to identify and block zero-hour phishing attacks by as much as six days before other detections mechanisms or threat intel feeds like Virus total are able to pick it up, providing an unmatched protection buffer and bringing modern protection to every single user, no matter where they work.

Key Capabilities

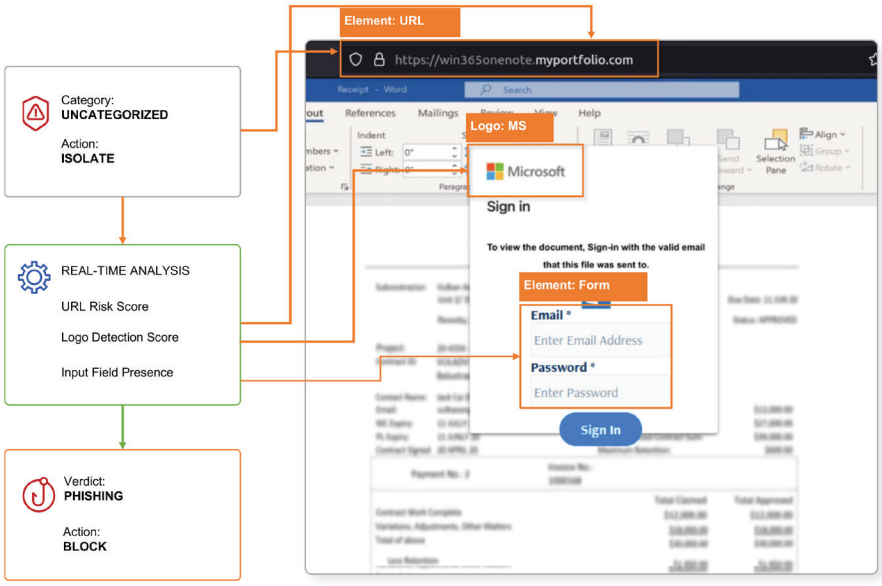
Zero-hour phishing protection buffer

Rather than a local browser accessing websites directly, each web request is sent to our Secure Cloud Browser, where a digital twin of your local browser is created executing the request away from the endpoint and delivers only safe, reconstructed content to the user's local browser. This approach prevents any malicious activity and phishing attempts from ever reaching the endpoint. In fact, Menlo Security mitigates the threat of zero-hour phishing attacks by detecting phishing attacks before other security vendors and traditional feeds based on indicators of compromise (IOC) — in some cases up to six days sooner — providing an unmatched protection buffer.



AI-powered On-click inspection

HEAT Shield uses AI to block zero-hour threats, credential theft, and previously unseen phishing attacks in the browser, before they can gain a foothold in your network. Each web request is executed in the Menlo Secure Cloud Browser, enabling AI-based runtime analysis of each page, including JavaScript DOM elements, logos, input fields, and URL paths. If a phishing or malware threat is detected, dynamic policy controls can block the site outright or render the page in read-only mode, preventing any data input.



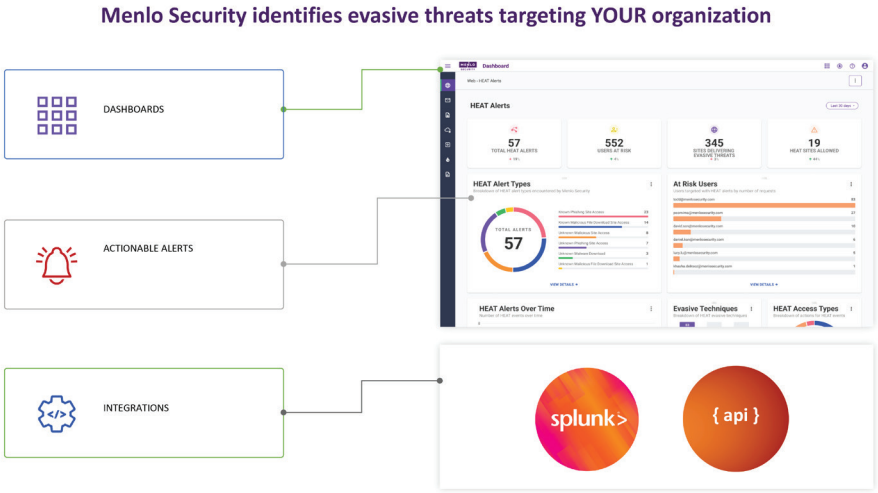
Real-time logo detection

HEAT Shield uses computer vision to identify websites impersonating known brands and services. This allows Menlo Security to put AI-powered "eyes" on browsers and dynamic web content to protect users and their systems. Computer vision-based classification provides fast and accurate protection at scale against dynamic attacks that trick users with images. Custom logos are supported to protect users against attacks targeting your organization.

Complete end-to-end visibility into every web session

HEAT Shield performs continuous analysis of customer web traffic to correlate events and identify the presence of highly evasive threats from inside the browser - a dataset which is invisible to traditional security solutions. Security teams get actionable, real time alerts, which reduce mean time to detect (MTTD) and mean time to respond (MTTR). Context rich, evasive threat intelligence is delivered for improved incident response and overall security posture.

Solution Brief



Protect users against zero-hour phishing by securing your most critical enterprise asset

Many browsers lack essential safeguards against cyber threats, making users vulnerable to increasingly sophisticated attacks. Traditional network and endpoint security tools fall short in offering insight into browser telemetry and leave enterprises susceptible to zero-hour phishing attacks and other evasive threats.

Menlo Security minimizes the browser attack surface by providing a Zero Trust approach to preventing browser-based phishing attacks and other evasive threats. HEAT Shield and Secure Cloud Browser deliver modern protection for users on any browser and remove the operational burden of managing existing browsers for security teams. Menlo Security is simple to deploy, easy to manage, and allows users to continue working with their browser of choice, regardless of where work takes them.

To learn more about securing the ways people work, visit menlosecurity.com or email us at ask@menlosecurity.com.

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.