MENLO SECURITY

Data Sheet

HEAT Shield

Protect users and defend your enterprise against targeted zero-hour phishing attacks and other evasive threats.

The browser is the most widely used enterprise application and the primary entry point for internet-borne attacks. Such browser-based attacks can result in data exfiltration, credential theft, and account takeover. Traditional network and endpoint security tools cannot stop these attacks because they often exhibit no signature or digital breadcrumbs to detect. Known as Highly Evasive and Adaptive Threat (HEAT) attacks, they leave enterprises that rely on network firewall and endpoint security tools exposed to browser-based threats and zero-hour phishing attacks.

Traditional security infrastructure relies on signatures or pattern matching of known attacks to detect and block threats, but they lack visibility into specific browser signals. Security teams need a solution that provides end-to-end visibility and that is as dynamic as the threats targeting users. Menlo Security HEAT Shield delivers real-time protection against zero-hour threats without impacting productivity.

Three things to know:

The browser is your most critical enterprise asset. Last year, browser-based phishing attacks surged by more than 198% with 30% of these attacks displaying evasive techniques used to evade commonly deployed security.

Traditional detection-based security approaches fail to protect against zero-hour phishing attacks, including other evasive browser-based threats. In fact, 75% of phishing links were identified originating from known, categorized or trusted websites.

Six days is the average latency between when a zero-hour phishing attack first appears and when it is finally added to the detection mechanism for traditional security tools.

Product overview

Menlo Security HEAT Shield puts AI-powered “eyes” on browser activity and dynamic web content, so users can focus on work, not threats. By providing a complete picture into each web session and enabling dynamic policy controls, HEAT Shield eliminates the browser attack surface and brings modern protections to every single user, no matter where they work. HEAT Shield leverages AI-powered analysis and computer vision capabilities to prevent phishing attacks and provides comprehensive visibility into evasive threat signals from inside the browser, a telemetry source that is invisible to traditional network security tools.

Based on this telemetry, Menlo Security mitigates even the most sophisticated phishing attacks, detecting them well before traditional feeds based on indicators of compromise (IOC) and other approaches. HEAT Shield uses real-time dynamic controls to shrink the exposure window by as much as six days, providing an unmatched protection buffer.

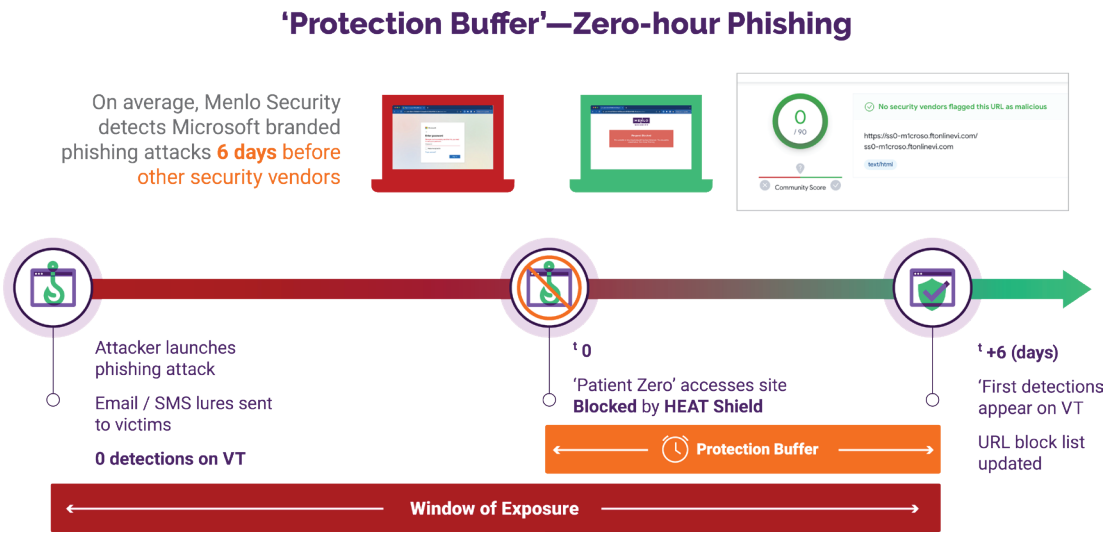

Illustration 1: The protection buffer from Menlo Security protects against zero-hour phishing attacks

Menlo Security manages browsers, protects your users, and secures access to applications and enterprise data, while providing a transparent browser security experience for any browser, across any device.

HEAT Shield intelligence is generated from analyzing more than 400 billion sessions annually to enable real-time protection against browser-based threats and to improve overall security. Enterprises can be assured that they're protected against zero-hour phishing attacks when HEAT Shield is activated. Granular access and security policies are enforced, and web sessions are monitored and protected, providing a risk-free internet experience for users. HEAT Shield supports policy compliance across all devices and locations because it leverages the Menlo Secure Cloud Browser to defend against evasive threats.

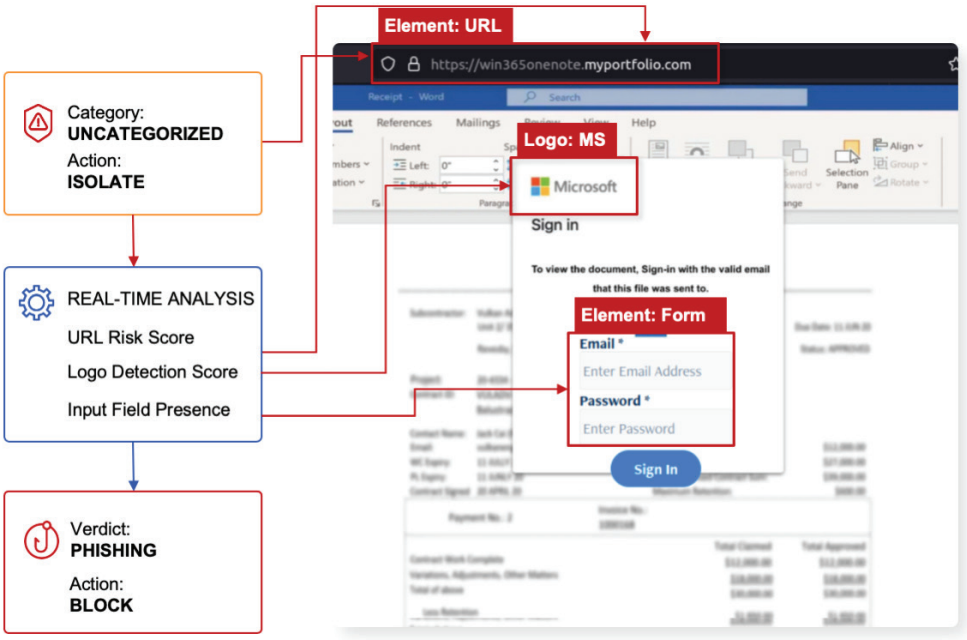

Illustration 2: Example of how HEAT Shield works against an uncategorized website

HEAT Shield key capabilities:

Zero-day exploit protection:

Rather than a local browser accessing websites directly, each web request from the user executes inside the Menlo Secure Cloud Browser. Only safe, clean content is delivered to the user's local browser. This approach prevents any malicious activity from ever reaching the endpoint.

AI-powered On-click inspection:

Each web request is executed in the 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. 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.

Zero-hour phishing protection buffer:

Menlo Security mitigates the threat of zero-hour phishing attacks by detecting such attacks before other security vendors and threat-intel feeds, in some cases up to six days, using real-time dynamic policy controls.

End-to-end browser visibility:

Provides evasive threat intelligence and alerting for real-time visibility and improved incident response. Detailed threat intelligence and alerts can be viewed via a dedicated dashboard inside the Menlo Security admin portal, as well as consumed via API directly by your SIEM/SOC tools for improved performance.

Effortless deployment and ease of management:

Menlo HEAT Shield is simple to deploy and manage, supporting any browser on any device and allowing users to continue working with their browser of choice. There's no new endpoint software for IT to manage. After activation, enforcement actions can be easily defined and monitored inside the admin portal.

Globally available:

HEAT Shield scales seamlessly across >50 global points of presence (PoPs), providing security coverage throughout 145 countries and territories.

Securing the browser with Menlo Security

Along with HEAT Shield, Menlo Security converges browser security capabilities into the Secure Cloud Browser to effectively manage your existing browsers, protect your users, and secure application access and enterprise data, all from a single interface for easy policy management, reporting, and action-oriented threat analytics.

Protecting against modern security threats is a top priority for businesses, but existing solutions are limited and reactive. Using a fundamentally different approach, Menlo Security eliminates the browser attack surface and is the only solution to deliver on the promise of cloud security: by providing a simple to deploy Zero Trust approach that stops attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams.

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.