MENLO SECURITY

HEAT Visibility

Providing visibility and action-oriented threat intelligence into highly evasive threats targeting your organization

As browsers continue to expand in sophistication, so do the attacks that threat actors use to target browsers and evade enterprise detection capabilities. Traditional security solutions are reliant on analyzing network traffic that is provided by firewalls and secure web gateways, but lack the visibility needed to capture the wide range of events that comprise a modern web session. Threat actors know this and are outsmarting these solutions by using novel and highly successful approaches collectively referred to as highly evasive and adaptive threats (HEAT). These evasive threats target the web browser as the primary attack vector, circumventing traditional network-based and endpoint solutions that lack visibility into events happening inside the browser. That is why highly evasive and adaptive threats are so potent.

Menlo Security's HEAT Visibility provides visibility and insight into the browser surfacing action-oriented threat intelligence on highly evasive and adaptive threats, providing organizations with the information they need to better secure their users.

HEAT Visibility provides:

- **Visibility into highly evasive and adaptive threats that traditional solutions can't detect** — provides visibility into highly evasive threats that other security tools can't. Dashboard analytics are also provided for security teams to help convey security risk and improve security posture.
- **Integrated evasive threat intelligence into SOC teams for faster Incident Response** — provides actionable alerts and enriched threat intel on different highly evasive and adaptive threat techniques used to improve incident response. Highly evasive and adaptive threat intel can be consumed directly into customer SIEM, SOAR and SOC platforms via the Log API and Splunk TA to use as part of their security response playbook.
- **Optimized security policy control** — As evasive tactics continue to evolve and new threats are detected, HEAT Visibility can help customers identify policy misconfigurations and provide additional recommendations to mitigate risk of evasive attacks.

Product Overview

Menlo Security's HEAT Visibility performs automated analysis of customer web logs in order to identify malicious web and file requests exhibiting evasive tactics and surfaces these through actionable alerts and dashboard analytics inside of the Menlo admin portal. This provides actionable forensic-level information for SOC teams in the form of high-fidelity alerts.

Features include:

HEAT Attack Dashboard

View adversary generated threat intelligence about phishing and malware attacks that use highly evasive threats (such as MFA Bypass phishing attacks, HTML Smuggling, Legacy URL Reputation Evasion (LURE), and malicious password protected files) targeting your users that other solutions can't detect or block.

Continuous scanning of web logs to provide actionable insights and alerts

Analyzes domains, URLs, IPs, browser telemetry, user behavior, file downloads, and other data from over 400B web sessions analyzed each year to provide comprehensive visibility on Highly Evasive Adaptive Threats (HEAT) attacks targeting the browser.

Actionable HEAT alerts & reporting

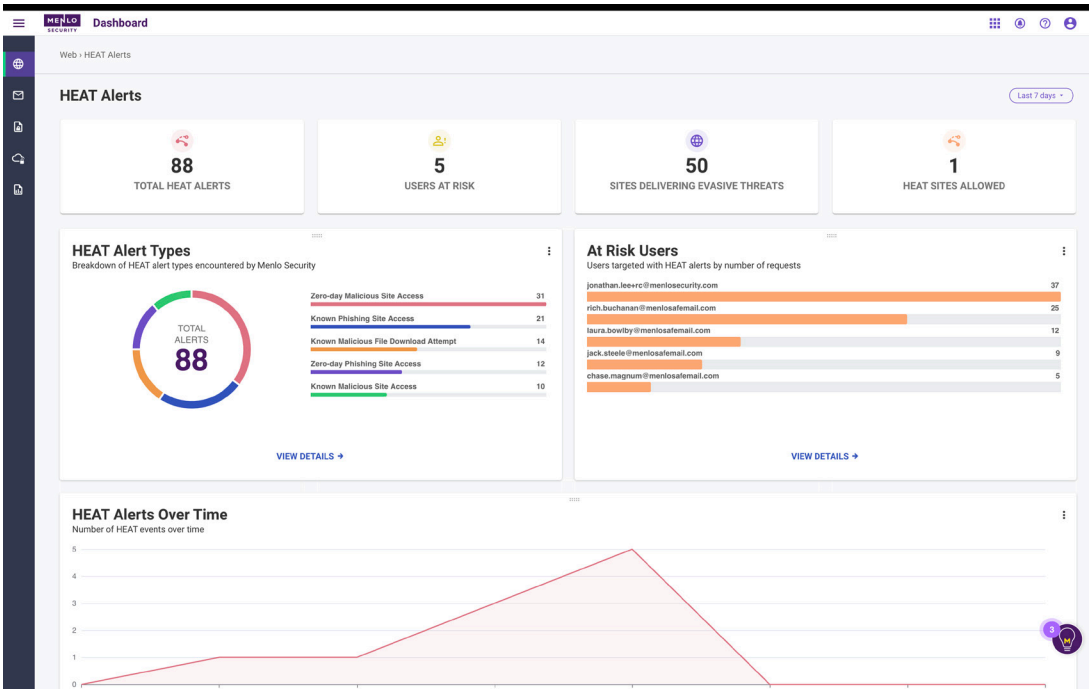
Surfaces alerts to security teams in the event a highly evasive and adaptive threats is detected. Threat type alerts include zero hour phishing site access and password submission, zero hour malicious site access and file access, zero hour file download, known phishing/malicious site access, known malicious file download and Command and Control (C2) traffic. Customers can use these alerts to operationalize the threat intelligence derived from the Menlo platform.

IOCs automatically added to Block List

Domain and URL information automatically added to Menlo's Global Block list.

APIs available for log export capabilities

Integrate HEAT intelligence into your log aggregation, automation and security orchestration tools.



As customers access web pages, their traffic leaves their network and is sent to the Menlo Security cloud platform, which sits inline and surfaces suspicious activity. By providing customers with visibility into highly evasive and adaptive threats they can respond quickly to these critical threats—from initial investigation through to containment. Highly evasive and adaptive threats alerts can also be consumed by security teams through the Menlo Log API or insights reporting and analytics tool—enabling customers to better visualize threat trends and demonstrate the business value of securing your browsers with Menlo Security.

Securing the browser with Menlo

Along with HEAT visibility, Menlo Security converges all secure web gateway capabilities into our isolation-powered cloud security platform providing enhanced security across web, email and SaaS applications—including HEAT Shield, Remote Browser Isolation, Cloud Access Security Broker, Data Loss Prevention, Proxy, Firewall-as-a Service and Private Access—to provide extensible APIs and a single interface for policy management, reporting and action-oriented threat analytics.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to outsmart threats, completely eliminating attacks and fully protecting productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.