Google Cloud

MENLO SECURITY

AI-powered proactive defense inside the browser

Executive summary

Menlo Security HEAT Shield AI, now including generative AI analysis from Google Gemini, delivers expanded protection against never-before-seen social engineering and brand impersonation attacks that target users in the browser.

Tactics employed by threat actors and scammers are constantly shifting and evolving, operating around the world and in every language. This makes attacks increasingly difficult for traditional detection-based security tools, which often rely on known signatures or patterns, to detect novel social engineering attacks and convincing brand impersonation attempts.

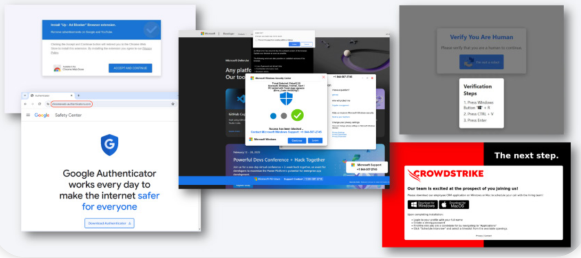
In-browser detection with HEAT Shield AI sees attacks as they happen—even if it's brand new, obfuscated, or is hosted on domains with benign reputations.

Complimenting our existing AI analysis capabilities, this new integration offers access to the latest Google Gemini models through Vertex AI to identify and block web-based attacks in real-time with the highest possible accuracy.

Examples include:

- Fake CAPTCHA/verification pages, such as Clickfix, that attempt to trick users into executing malicious scripts
- Remote technical support scams, also known as Scareware
- Websites impersonating government agencies and well-known brands for nefarious purposes
- Clickjacking that attempts to manipulate a website user's activity by concealing hyperlinks beneath legitimate content
- Sophisticated phishing attacks leveraging advanced toolkits to evade traditional filters and multi-factor authentication (MFA) protections
- QR code phishing attempts

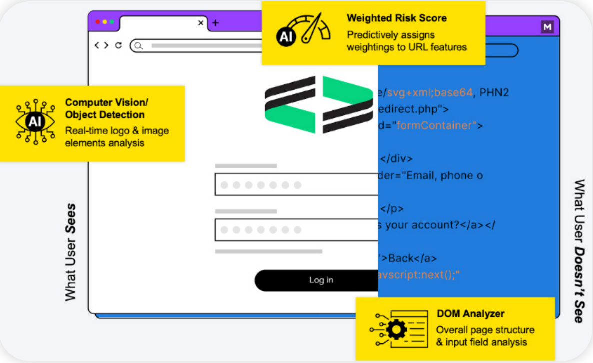
Social Engineering / Brand Impersonation Protection


Google Authenticator works every day to make the internet safer for everyone
Download Authenticator
Verify You Are Human
Verification Steps
1. Press Windows Button + R
2. Press CTRL + V
3. Press Enter
Access has been blocked
Powerful Devs Conference + Hack Together
The next step.
CROWDSTRIKE
Our team is excited at the prospect of you joining us!

Partner and product overview

A pioneer in browser security, Menlo Security prevents web-borne threats and eliminates the complexities of remote access by securing application access and enterprise data using any browser on any device. The Menlo Secure Enterprise Browser solution scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security protects over eight million users and is trusted by major global businesses, including Fortune 500 companies, eight of the ten largest global financial services institutions, and large government institutions, scanning over 400 billion web sessions annually to eliminate threats and ensure a safe, seamless user experience.

HEAT Shield AI is built on the Menlo Secure Cloud Browser, which loads web content within a hardened digital twin of the local browser, protecting the user and the enterprise. The Secure Cloud Browser offers unparalleled visibility into each web session, including document object model (DOM) changes and user inputs, delivering AI-powered analysis inside the browser.

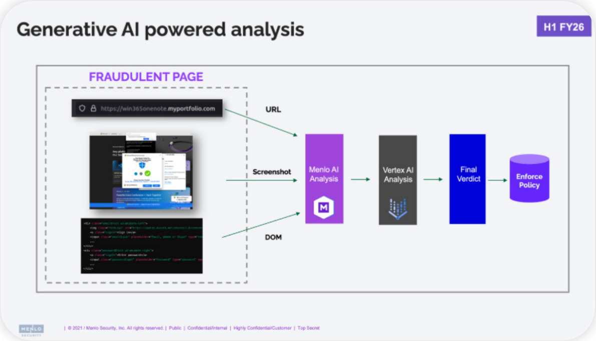


Joint value proposition

Complementing Menlo's existing AI analysis capabilities, this new integration leverages the power of Gemini models through Vertex AI to identify and block never-before-seen social engineering and brand impersonation attacks that target users in the browser. Together, these solutions deliver a new level of proactive defense inside the browser that is both highly effective and seamless for the user.

This enhanced security is delivered right inside the browser you already know, so there's no need for costly and time-consuming applications or clients. Security teams get improved threat prevention and richer threat intelligence with a seamless browsing experience for end users. Our AI-powered capabilities provide advanced phishing and malware prevention, stopping zero-hour phishing attacks and giving you the latest threat intelligence from Google and Menlo to improve incident response..

End-to-end architecture


Generative AI powered analysis
H1 FY26
FRAUDULENT PAGE
https://win365onenote.myportfolio.com
URL
Screenshot
DOM
Menlo AI Analysis
Vertex AI Analysis
Final Verdict
Enforce Policy
| © 2021 / Menlo Security, Inc. All rights reserved. | Public | Confidential/Internal | Highly Confidential/Customer | Top Secret

1. When a user requests a web page, HEAT Shield AI performs an initial analysis using computer vision, a Menlo AI model developed, and examines the heuristics of the DOM of the traffic.
2. If no verdict is returned following the initial analysis, a multimodal request is sent to the Vertex AI Gemini API. This request includes a golden text prompt with specific instructions, page URL (sanitized to remove any query parameters), an image screenshot of the requested page, and a serialized XML DOM.
3. The Gemini AI model processes the prompt and attached artifacts and returns a structured response, including a final verdict: benign, fraudulent, or phishing.
4. Based on this verdict, the customer-configured HEAT Shield policy action, such as Log or Block, is enforced.

Use case 1: Real-time protection against unprecedented social engineering and brand impersonation attacks.
Description: Customers who have deployed Menlo's HEAT Shield AI product to protect end-user browsing now benefit from enhanced, real-time protection against never-before-seen social engineering and brand Impersonation attacks.
Persona: SecOps teams are responsible for protecting their organizations from web-based attacks

Use case 2: AI-enriched threat intelligence and visibility for improved incident response
Description: Menlo Security HEAT Shield AI and Google Gemini together analyze billions of web sessions annually. This continuous analysis generates rich, detailed threat intelligence and alerts about evasive attacks that traditional tools often miss. Security teams get a clear picture of attackers' tactics, techniques, and procedures (TTPs), which can be integrated into their existing Security Information and Event Management (SIEM) or Security Operations Center (SOC) platforms for enhanced real-time visibility.
Persona: Security analysts and threat hunters working in a SOC who investigate security incidents, proactively hunt for threats, and analyze attack trends to protect their organization