MENLO SECURITY

DATA SHEET

AI-powered intent detection

ClickFix and clipboard protection

Zero-day phishing prevention

AI-Powered Proactive Defense Against Evasive Browser Attacks

Real-time browser protection in a lightweight browser extension

The Browser Blind Spot in the AI Era

As enterprises rush to adopt AI-powered workflows, the browser has become the central workspace—and the primary attack vector. Attackers are constantly evolving their tactics, employing AI-generated phishing kits, zero-day URLs, and convincing social engineering to trick even vigilant users. Traditional defenses, reliant on outdated IOCs and easily manipulated heuristics like domain age and reputation, are increasingly ineffective against threats that are evasive by design.

Real-Time Intent Detection, Powered by Gemini

HEAT Shield Agent is a standalone security capability, available directly through the Google Cloud Marketplace. It isn't a phishing filter—it's an intent engine. Rather than checking a page against a list of known-bad URLs, the Agent captures the URL, DOM, and a real-time screenshot of the page and sends that telemetry directly to Google Gemini for analysis, returning a verdict before the user ever interacts with the threat. This "browser-first" approach requires no isolation or proxy infrastructure; it deploys as a lightweight extension within the browser itself.

HEAT Shield AI intelligence catches what a reputation score can't—including zero-day phishing, AI-generated lures, brand impersonation, clickjacking and fake software-update prompts, and ClickFix / malicious copy-paste attacks. If a session is deemed malicious, the Agent instantly blocks the page before the user can interact with the threat—a direct extension of the Menlo ecosystem, with a frictionless deployment model.

KEY BENEFITS

The browser is your most critical enterprise asset—and increasingly the first thing attackers target. Nearly 1 in 3 phishing domains on .com and .net were originally registered for legitimate use, so reputation-based filtering alone can't catch them.

The median phishing site lives online for just 5.5 hours before any blocklist catches up—gone long before traditional detection ever sees it.

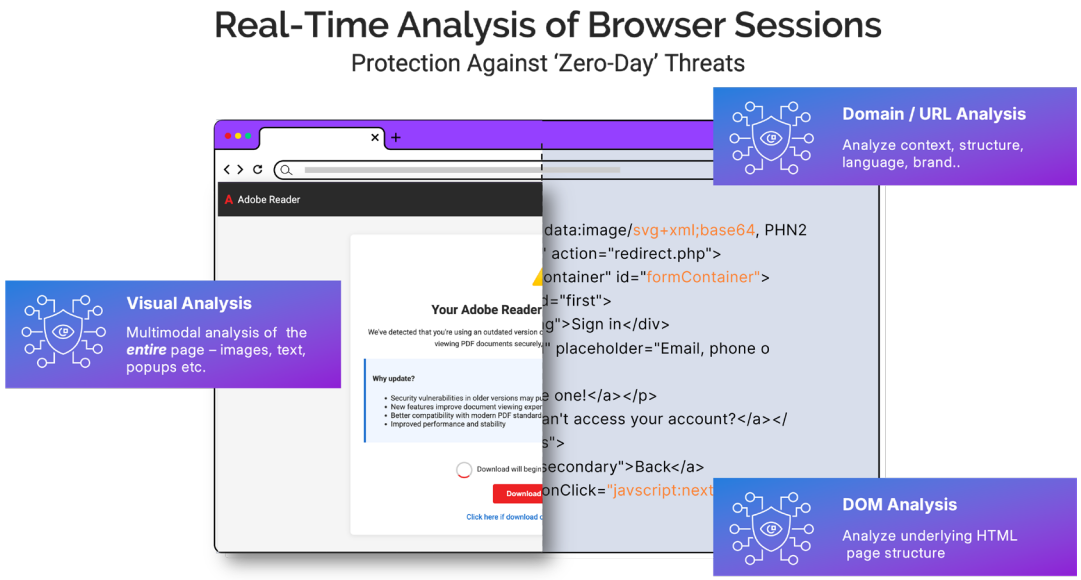
Fake CAPTCHA gates built to stop crawlers, not people, have risen 563% in the past year—a sign attackers are engineering pages specifically to evade automated security scanning.

Every verdict HEAT Shield Agent returns categorizes the request and gives a clear reason for the block—and that intelligence isn't siloed. Once a domain is flagged, the block applies tenant-wide, and it feeds a crowdsourced blocklist that updates for every HEAT Shield tenant globally.

Key Capabilities

- **Real-Time Intent Detection:** Captures the URL, DOM, and a real-time screenshot of the page and sends that telemetry directly to Gemini—always the latest available model—for analysis. A verdict returns before the user ever interacts with the threat.
- **Stop Evasive Social Engineering with a Two-Punch Defense:** Detects the social-engineering lure as the page renders—flagging fake CAPTCHA gates, deceptive error prompts, invisible clickjacking overlays, and AI-generated impersonation attempts before the user ever acts—including blocking clipboard-based attacks like ClickFix from reaching a terminal or Run dialog.
- **Zero-Day Phishing & Brand Impersonation Protection:** Gemini multimodal analysis reads logos, login forms, and page layout alongside DOM elements and URL paths—identifying sophisticated impersonation and zero-day phishing attempts without relying on signatures or reputation checks.
- **Tenant-Wide, Crowdsourced Blocklisting:** Once a domain is flagged, the block applies instantly across your tenant and feeds a global crowdsourced blocklist shared by every HEAT Shield customer, with a clear, specific reason for every block, not a generic 'blocked' page.

HEAT Shield Agent Analyzes the Live Page—Not Just the URL—to Catch Threats Other Tools Miss.



Menlo HEAT Shield Agent analyzes uncategorized websites in real time to determine whether they're legitimate or malicious

Deployable Without a Rip-and-Replace: A lightweight browser extension, pushed via Intune, JAMF, or the Chrome Web Store. No proxy or isolation infrastructure required, and available directly through the Google Cloud Marketplace. Menlo Security is the 2026 Google Cloud Partner of the Year.

Comprehensive Detection Visibility: Detections are viewable via a dedicated Log Viewer and Dashboard inside the Menlo admin console, with 30-day log retention, and can be consumed via the Logging API directly by your SIEM or SOC tools.

Available Everywhere Your Users Browse: Because it's a browser extension rather than a network dependency, HEAT Shield Agent works the same way for every user, on every managed desktop, wherever they work.

HEAT Shield Agent Closes the Gap Traditional Tools Miss

HEAT Shield Agent seamlessly augments your current SWG, SSE, and endpoint tool investments — no rip-and-replace required. It closes the specific browser-layer gap those tools can't see: evasive, intent-based threats — including zero-day phishing — that bypass network and endpoint controls entirely and defeat legacy, reputation-based detection. By dynamically identifying and stopping these attacks in real time, it's a fast, low-friction way to close that gap today, with a clear upgrade path to the full Menlo Browser Security Platform when your requirements grow.

About Menlo Security

Menlo Security is the pioneer of the Browser Security Platform (BSP), the industry's first infrastructure designed to govern a hybrid workforce of humans and autonomous AI agents. By centering the browser as the new enterprise operating system, Menlo provides a "Guardian Runtime" that resolves the unique risks created when AI agents operate at machine-speed without human skepticism. The Menlo platform enables the agentic enterprise to scale AI with confidence, providing universal connectivity to legacy data and unified zero-day threat prevention across every session. Trusted by over 1,000 global enterprises—including eight of the ten largest financial institutions and major government agencies—Menlo protects over 8 million users and millions of simultaneous AI agent sessions. Headquartered in Mountain View, California, and backed by investors including JPMorgan Chase, American Express Ventures, and Vista Equity Partners, Menlo is securing the browser for the agentic age. Learn more at www.menlosecurity.com.

MENLO SECURITY

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

© 2026 Menlo Security, All Rights Reserved.