MENLO SECURITY

DATA SHEET

Menlo IRIS Browser Extension

Vital Security for Your Users, Your Data, and Your Organization Where Work Happens—in the Browser



Works on browsers users already have—no replacement needed

Built on Menlo's trusted enterprise platform used by top security firms

Enhances your security stack with browser-specific control and visibility

The Browser Touches Everything, But Belongs to No One

Every organization faces the same browser-based issues: GenAI data leakage, malicious extensions, phishing, social engineering, malvertising, credential harvesting, and the need for file and data security. The browser has become almost an operating system of its own and the portal to nearly every business function, yet its security doesn't clearly belong to any one team. IT manages the browser, network security filters web traffic, endpoint security watches the device, the identity team owns logins, and data protection sits with compliance. Each team sees only part of the problem, and each assumes the existing stack covers the rest. That's the browser security gap, and attackers are counting on it.

The gap keeps widening because new web tools show up faster than policy can follow. GenAI is the most visible example.

> Regular use of AI on corporate devices tripled from 15% to 45% of employees in one year, and 67% of that use runs through non-corporate accounts. The average organization has more than 15% of users with unauthorized AI browser extensions installed.[1]
>
> Shadow AI was involved in one in five breaches, and high levels of shadow AI added USD 670,000 to the average breach cost.[2]

[1] Verizon 2026 Data Breach Investigations Report (DBIR)
[2] IBM Cost of a Data Breach Report 2025, researched by Ponemon Institute

KEY BENEFITS

- Go from proof of value to deployment in hours, not months
- Stop data loss at the point of action—copy, paste, upload, download, print, and screenshot
- Steer users toward sanctioned GenAI tools and control what data goes into them
- Inspect files inline for DLP violations, viruses, and malware
- Deliver clean, usable files with Content Disarm and Reconstruction (CDR), available as an add-on
- Stop phishing and zero-day threats before they're cataloged, with the HEAT Shield add-on
- Inventory every browser extension your users have installed, and the risk each one carries
- Centrally log every web session by user, device, destination, and activity

Why Your Existing Security Stack Misses the Browser

Firewalls, secure web gateways, and EDR were built for the network and the endpoint, not for what happens inside a browser session. Everyday actions like copy, paste, upload, print, and screenshot go unseen, which is especially concerning when the destination is GenAI. Files moving through the browser can carry DLP violations out and malware in. And most teams can't even inventory the extensions users have installed, let alone judge the risk each one carries—a risk that can change at any time with a silent update.

Built-in browser controls help, but they're specific to one vendor's browser, and most organizations run more than one. They also can't deliver zero-day exploit protection or full content disarm and reconstruction. And if nothing is watching the browsers the first sign of trouble may be a breach or a data leak.

The shared root cause is simple: enterprise-grade browser protection hasn't come in a form that deploys quickly on all the browsers people already use. What's missing is focused, browser-level visibility and control that a team can deploy and run without retooling, replacing browsers, or weeks of concentrated effort.

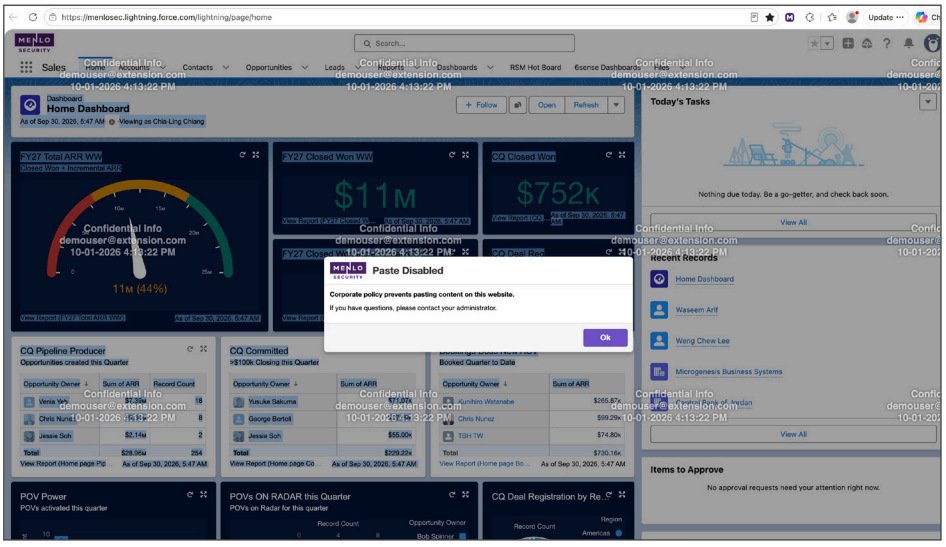
One Browser Extension. Enterprise-Grade Browser Security.

Menlo IRIS brings the essential capabilities of a secure enterprise browser to the browsers your users already have, in a flexible, easy-to-deploy extension. It installs via the Chrome Web Store, MDM, Intune, JAMF, or other UEM tools, and enforces data protection, file security, web governance, threat prevention, and extension visibility right where work happens, with every policy managed from a single console. Users keep the browsers and tools they know, and they'll likely never notice Menlo IRIS until it stops an attack. Because it works alongside your network, endpoint, and identity tools without a proxy or inline decryption, Menlo IRIS fills gaps instead of duplicating controls.

The Capabilities You Need, in a Form Factor You Can Work With

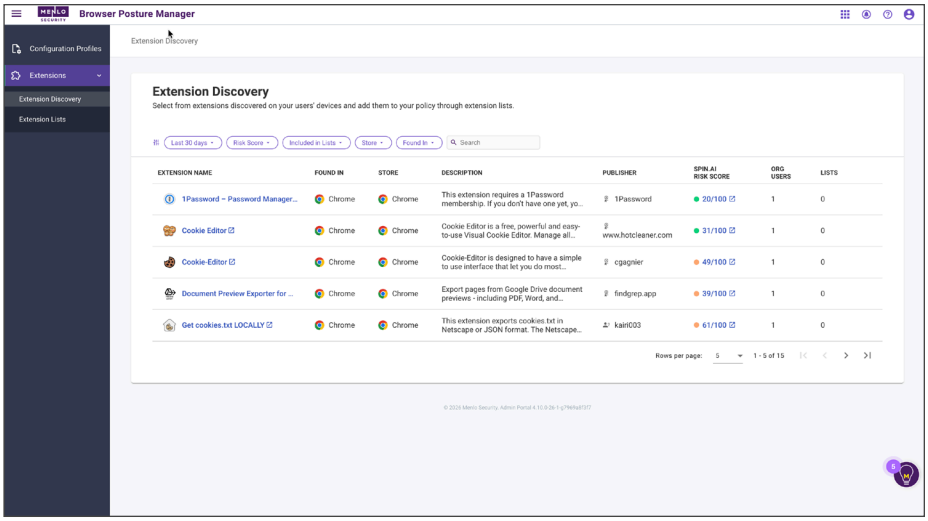
DATA LOSS PREVENTION

With Menlo IRIS, data loss prevention is enforced directly in the session and can be customized for different users, groups, domains, and locations.



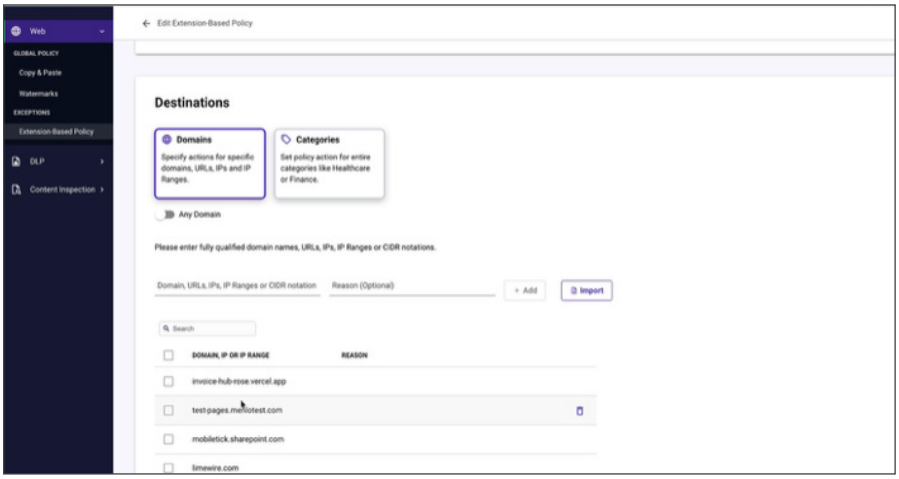
- Enforcements include clipboard (copy/paste), file upload/download, watermarking, print, read-only pages, developer-tools restrictions, and screenshot deterrence, with predefined and custom dictionaries to protect your crown jewels.
- **Why It Matters:** These everyday actions must be managed and controlled, particularly when the destination is GenAI. Menlo IRIS also gives you visibility into what users tried to do.

THIRD-PARTY EXTENSION VISIBILITY AND RISK



Because Menlo IRIS is on the endpoint, it delivers visibility into the other extensions deployed on user devices.

- Maintain an enterprise-wide inventory of third-party extensions, with risk insight for each one.
- **Why It Matters:** Extensions can be hacked, developer licenses stolen, or an existing extension purchased by threat actors. Because extensions update via a silent push from the web store, neither you nor your users will know until it's too late.



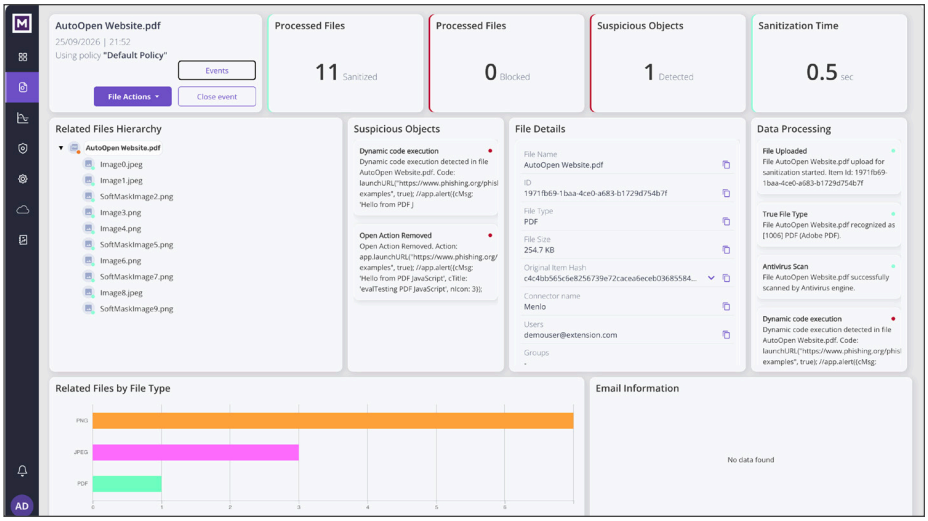
WEB GOVERNANCE AND GUARDRAILS FOR AI USE

Menlo IRIS makes it easy to steer users as they browse.

- Domain- and category-based policies steer users away from risky and unsanctioned sites and toward sanctioned ones, including GenAI destinations.
- When an action is blocked, users are alerted to the cause, which reduces helpdesk tickets.

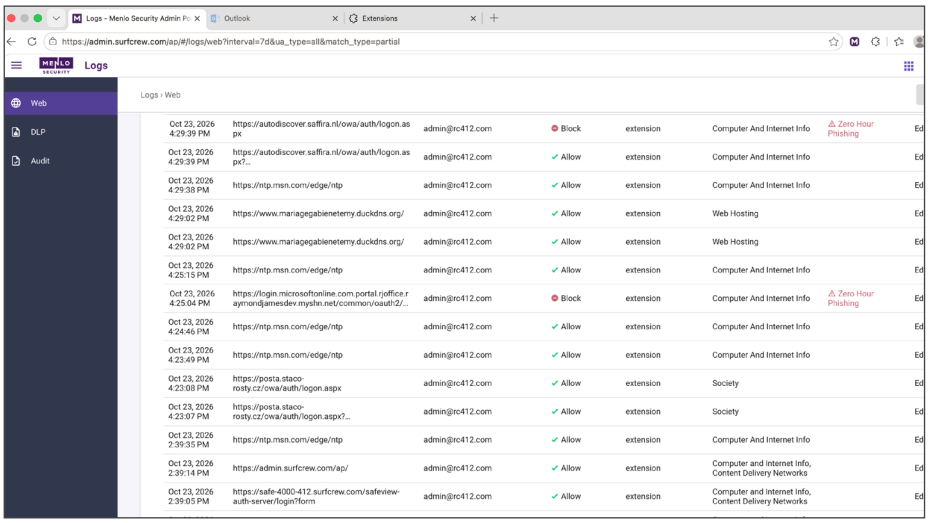
Why It Matters: See which GenAI tools are in use and control what data moves into them, without banning the tools people rely on and breaking workflows. The same controls apply to any web destination.

FILE SECURITY THAT GOES BEYOND BLOCK AND ALLOW



Blocking risky files is vital to security, but it can also break workflows. With Menlo IRIS, inspection is built in, so you don't have to make assumptions or take chances.

- Inline dictionary- and regex-based DLP inspects content moving through the browser.
- Integrated hash matching, antivirus, and cloud sandbox analysis are automatically applied to files.
- Add Content Disarm and Reconstruction (CDR) to go further. CDR removes malicious content and reconstructs a clean, fully usable file, rather than simply blocking it.
- **Why It Matters:** Attackers embed links and exploits in files to evade common filters.



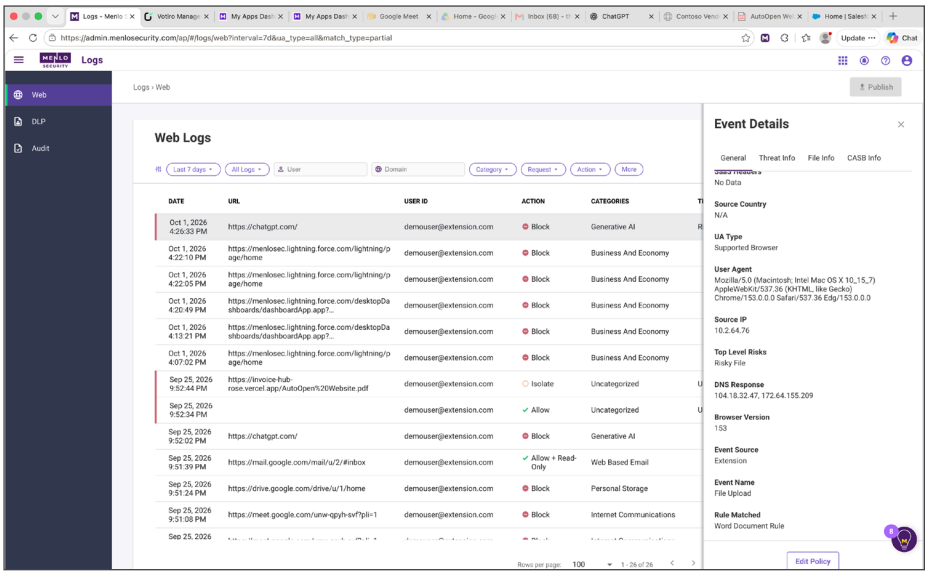
AI-POWERED THREAT DETECTION THAT STOPS EVEN ZERO-DAY THREATS

Add AI-powered threat detection via HEAT Shield AI to Menlo IRIS for protection that stays ahead of new exploits, well before they're cataloged.

- Real-time, intent-based detection stops phishing, malvertising, and social engineering attacks before users can click on them.
- HEAT Shield looks at what a page is actually doing, rather than waiting for URL lists, signatures, or known indicators to catch up.
- **Why It Matters:** Most browser security tools rely on static lists. Proactive detection identifies malicious behavior before anyone has cataloged it.

THE VISIBILITY AND GOVERNANCE THAT LEADERSHIP EXPECTS

Getting visibility into user activity in the browser has long been difficult or impossible with your existing security stack. With Menlo IRIS, every browser and extension event is logged and searchable.

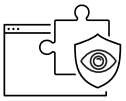


- Centralized web logging covers user, device, destination, and activity, with an audit trail and fleet-wide extension inventory on demand.
- Teams working toward SOC 2, HIPAA, GDPR, and other requirements get the audit trail they need through Insights and custom reports.
- **Why It Matters:** Compliance violations can be costly and audits are time-consuming. Visibility shouldn't require standing up a full SOC.

MANDATORY AUTHENTICATION TO MENLO IRIS

Because Menlo IRIS lives on the endpoint, you can require users to authenticate before they browse the internet, corporate SaaS, private applications using their browser.

- Mandatory authentication to Menlo IRIS, enforced automatically.
- Integration with authentication providers for identity context and login.
- **Why It Matters:** Ensure that all users authenticate to Menlo IRIS so their web activity can be monitored and the required data security controls can be enforced



Simple to Deploy, Simple to Run

Menlo IRIS deploys via the Chrome Web Store, MDM Intune, JAMF, other UEM tools, or managed browser controls. Configure easily and go from proof of value to deployment fast. Push policy through the tools you already use, manage everything from one console, and get logs for every event across managed and BYOD devices alike. There's no hardware to add and no browser to replace, and because users stay on their own browsers, each vendor's security patches reach them as soon as they're released.

Enterprise-Grade Browser Security

The browser is where work happens, and it's where attackers, data leaks, and risky extensions meet your users. Menlo IRIS gives you visibility, security, and control over how people actually use the browser, without a browser migration or a new platform project to staff.

Menlo IRIS is built on Menlo's proven enterprise platform, which protects some of the world's most security-conscious organizations. As your risk profile changes, Menlo gives you room to grow, from differentiated add-ons to hybrid deployments and full isolation, so you always get exactly the security you need.

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.

© 2026 Menlo Security, All Rights Reserved.

MENLO SECURITY

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