MENLO SECURITY

DATA SHEET



Menlo Agent Runtime Security (MARS)

Protect AI agents online by detecting prompt injection, sanitizing files, and securing sensitive data in workflows.

Inspect external content before agents use it.

Rebuild files and mask harmful content so useful work can continue.

Protect sensitive data and let teams view agent sessions or take over when needed.

Give Agents Web Access With Runtime Protection

AI agents research suppliers, review documents, and gather information for business decisions. These tasks connect external content with internal information. A supplier page may contain instructions that redirect an agent. A downloaded document may carry malicious code. An upload request may lead the agent to disclose confidential data.

Menlo Agent Runtime Security (MARS) inspects web content, files, and outbound data in agent traffic routed through Menlo. Available controls depend on the connection method and include prompt-injection protection, file sanitization, and data protection.

Where supported and permitted by policy, MARS can mask injected instructions or rebuild a file to remove harmful elements. The agent receives sanitized content it can use to continue its task.

> Cloud-delivered on the Menlo platform for employee assistants, including Claude Code and Cowork, and enterprise-built agents. Protection applies to activity routed through configured Menlo connections.

KEY BENEFITS

Enable Useful Agent Work
Give agents controlled access to external information needed for research and other business tasks.

Reduce Exposure to Malicious Content
Inspect supported pages and files for injected instructions and file-based threats.

Protect Confidential Information
Apply tenant DLP policy, with sensitive-data detection and masking in isolated sessions.

Support Human Oversight
View sessions, take over when assistance is required, and review session recordings.

Three Controls for Agent Runtime Risks

MARS combines prompt-injection protection, file sanitization, and data protection. The selected connection path determines which controls apply.

Security Control	How MARS Applies It	Workflow Value
Prompt-Injection Detection and Masking	Detects injected instructions in supported web content and files. Supports mask, block, or log actions, with deterministic hidden-text removal for PDF and DOCX files.	Reduces the risk that external content redirects an agent's task or induces an unauthorized action.
Menlo File Security	Uses content disarm and reconstruction (CDR) to rebuild supported files from known-good content, alongside antivirus and multi-engine hash reputation.	Removes malicious file elements while preserving useful content for the agent.
Menlo AI Adaptive DLP	Applies inherited tenant DLP policy to agent sessions, with sensitive-data detection and masking in isolated sessions.	Helps prevent regulated information, source code, and other confidential data from leaving through supported interactions.

How MARS Works

01 Route Agent Activity Through Menlo

Connect an agent to a disposable Menlo cloud browser through browser automation or CDP. Configure supported HTTP and LLM-API traffic to use the Menlo cloud proxy.

02 Inspect Content and Enforce Policy

Apply the relevant controls as content passes through Menlo. Depending on policy and the interaction, MARS can mask instructions, rebuild a file, protect sensitive data, or block content.

03 Monitor Sessions and Provide Assistance

Use Agent Monitor for live visibility and human takeover. Review session recordings through Browsing Forensics.

In isolated browser sessions, active web content executes in the Menlo Cloud, separating that execution from the agent's environment.

Protection for Practical Agent Workflows

Apply runtime protection where agents combine external information with sensitive business data.

Workflow	Exposure	MARS Application
Supplier Research and Engineering	An assistant reviews supplier pages and documents while working with confidential designs or bills of materials.	Inspect external content, sanitize supported downloads, and apply DLP to uploads in isolated sessions.
Banking Research and Case Enrichment	An agent combines sensitive customer information with external registries, news, and other sources.	Route the agent's browsing through Menlo isolation to inspect external content and apply sensitive-data controls.
Healthcare Administrative Work	An agent reads external guidelines or payer portals while processing protected health information.	Apply isolation, prompt-injection detection, supported file sanitization, and sensitive-data controls.

Human Oversight and Session Evidence

Security teams manage agent rules by user/group and destination through the Menlo Admin Portal, with upload/download, clipboard, and watermark controls for isolated sessions. Agent Monitor provides live session visibility and human takeover for steps such as login, multifactor authentication, or CAPTCHA completion. Browsing Forensics provides session recordings for review.

Extend the Menlo Security Foundation to Agents

Organizations can extend existing Menlo capabilities to agent workflows, including tenant DLP policy, cloud isolation, file protection, and session visibility.

MARS complements identity providers, agent gateways, and model guardrails by inspecting incoming content and outbound information in agent traffic routed through Menlo.

Connection Options and Deployment

MARS is cloud-delivered. Agents must use a configured Menlo path for enforcement to apply. Coverage depends on the selected path and its supported controls.

The isolated browser, CDP, and cloud proxy connections require no endpoint software. Agents must be configured to route the relevant activity through Menlo.

Available in Early Access

Connection Path	Deployment Approach
Isolated Browser / CDP	Point the agent or its browser-automation connection at a disposable Menlo cloud browser.
Cloud Proxy	Configure supported HTTP and LLM-API traffic to use the Menlo cloud proxy.

Additional Connection Options

MARS Webfetch (COMING SOON)	A Menlo-hosted MCP server will provide Fast direct fetching and Full browser-rendered fetching, returning clean Markdown with destination-policy enforcement and prompt-injection scanning. Deployment requires configuring the agent to use MARS Webfetch and disabling its built-in fetch tool. Initial availability covers web pages; file fetching is a later roadmap capability.
Claude Traffic Attribution (COMING SOON)	Menlo Secure Client attribution will distinguish Claude Code and Cowork endpoint traffic from employee activity for policy and logging.

Start With a Defined Agent Workflow

Choose an agent task that uses external information and sensitive business data. Map its web connections, permitted downloads and uploads, and steps that require human assistance. Test which controls apply to each connection, how policy affects the workflow, and what happens if file sanitization fails. Measure latency on the selected workflow.

Request a Menlo Security demo to explore runtime protection for your AI agent workflows.

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.