

MAS has set the bar for AI risk. Menlo MARS helps you clear it.

Third-party AI and agents are now in scope. Here is how MARS maps to what MAS expects.

WHAT MAS NOW EXPECTS | ISSUED 7 OCTOBER 2026

You stay accountable

FIs remain accountable for AI used in the services they deliver, including AI developed, operated or provided by third parties.

Assure, then compensate

Obtain sufficient assurance from providers, assess fit for purpose and apply compensating controls where gaps remain. If risk stays outside appetite, limit, suspend or replace the service.

Proportionate and phased

Controls scale to risk. Effective 7 Oct 2027 and phased: Sections 3-4 (oversight, AI inventory) from 2027, Sections 5-6 (life cycle controls, capability) by 7 Oct 2028.

Agents are called out. MAS flags autonomous agentic AI that accesses tools as a reason to review controls regularly.

The browser is where your AI actually runs.

01

Shadow AI hides from vendor reviews

Copilot, Gemini and AI browsers act as privileged, unmanaged agents, and AI is embedded across SaaS.

02

Agents obey hidden instructions

Agents read page code literally. Invisible prompts can hijack their goal and move data out of open tabs.

03

Legacy tools can't see the session

SASE/SSE secure the pipe, EPP/EDR the machine. Neither sees inside the browser session.

THE ANSWER

Menlo Agent Runtime Security (MARS)

A guardian runtime for the agentic economy

01

Secure the agent

- Disposable cloud container for every agent session
- Strips hidden prompts, scripts and steganography before the agent reads a line
- Now covers Copilot, Gemini in Chrome and Claude Code

02

Govern the data

- Least-privilege access scoped to the task
- AI Adaptive DLP masks sensitive data before agents see it
- Level 3 file sanitization (CDR)

03

See and control

- Browser Session Observability and Shadow AI Prevention
- Tamper-proof audit logs, kill switch, Google SecOps integration

PROVEN WHERE THE STANDARD IS SET

8 of 10

of the largest global financial institutions secure their sessions with Menlo

1,000+

enterprises and 8 million+ users, including leading local and foreign banks in Singapore

Millions

of simultaneous sessions on an elastic global cloud built for agent swarms

Google Cloud Security Partner of the Year 2026

Data Protection. Second consecutive year

Leader and Fast Mover

GigaOm Radar, Secure Enterprise Browsing. Second consecutive year

Global Leader and Company to Action

Frost Radar™ 2025, Zero Trust Browser Security

Inc. 5000 2026

Fastest-growing private companies in America

Enterprise Security Solution of the Year

CyberSecurity Breakthrough Awards 2025

Six MAS priorities. One agent runtime.

Read across: what the Guidelines expect, and the Menlo control that helps you meet it.

MAS priority	What MAS expects	How Menlo helps
1. Find your AI, including shadow AI Sections 2 and 4	Discover AI across the firm, even inside third-party software, and keep an inventory of each agent's tools, access and guardrails.	Browser Detection and Response auto-discovers Copilot in Edge, Gemini in Chrome, Claude and AI embedded in SaaS at the DOM level. Shadow AI Prevention and Agent Registration support the inventory.
2. Red-team it 5.14, 5.15, 5.22	Run red teaming and adversarial tests, and validate that guardrails hold against data leaks, manipulation, evasion and poisoning.	MARS is built to withstand the attacks red teams simulate: it strips hidden white-on-white prompt injection, resists goal hijacking and enforces instruction-data separation.
3. Secure the runtime 5.4, 5.16, 5.22	Control inputs, outputs, access and plugins, with least-privilege design and pre-go-live checks.	Guardian Runtime moves security into the browser session and neutralizes zero-day threats before AI reasoning begins. Agents get least-privilege access scoped to the task.
4. Watch your agents 5.3, 5.23	Monitor agent actions and tools, log prompts and responses, and test the kill switch for high-risk AI.	Deterministic visibility at the DOM and file level: prompts, responses and tool calls are logged, with tamper-proof audit trails, a kill switch and Google Security Operations integration.
5. Test your vendors' AI 5.10, 5.11	Obtain sufficient assurance from third-party AI providers, assess suitability, and apply compensating controls where gaps remain.	Level 3 CDR sanitization and DLP as agents browse let you test vendor AI in an isolated environment, without sensitive data leaving.
6. Control change and drift 5.23, 5.25	Prevent unauthorized changes to models and data, with rollback, tiered alerts and incident management.	Orchestrator Agent on Gemini Enterprise adds conversational enforcement: what happened, who else is exposed, apply the fix.

Where Menlo fits. Menlo complements your AI governance; it does not replace it. Board oversight, risk materiality assessments, model validation and vendor due diligence remain the institution's responsibility. Menlo provides the runtime controls and session-level evidence that make them enforceable.

MEET US AT GOVWARE 2026 | BOOTH F07

See MARS against your MAS readiness plan.

Book a customized demo and we will walk through your AI inventory, agent workflows and third-party AI against the six priorities above.

Web menlosecurity.com/demo Email apac@menlosecurity.com



Scan to book a custom demo

Capability descriptions reflect Menlo product information as of October 2026 and may change. This material is not legal or regulatory advice. Section references are indicative; refer to the MAS Guidelines on AI Risk Management published 7 October 2026. The 8-of-10 figure refers to the largest global financial institutions. Awards and rankings as announced by Menlo Security (menlosecurity.com/about/press-releases). Inc. 5000 ranks U.S. private companies by three-year revenue growth. Frost Radar™ is a trademark of Frost & Sullivan.