MENLO SECURITY

DATA SHEET

Menlo AI Agent Security

Secure AI Agent Workflows, Unlock Data for Agentic Use, and Enable Browser Agents Safely

The Challenges of the AI-Powered Enterprise: Invisible Threats, Inadvertent Data Loss, and Inaccessible Data

As enterprises plan and execute their agentic AI strategies, security teams and developers are grappling with unprecedented security and data access gaps posed by autonomous agents and browser agents. They face three key challenges:

The Vulnerability of Machine Ingestion: AI agents lack human skepticism and interpret web code literally. Malicious actors hide "invisible" prompt injections or poisoned data within a website's HTML to hijack an agent's logic, turning a trusted tool into a conduit for account takeovers, malware distribution, data exfiltration, and credential theft.

The API Trap and Technical Debt: 80% of enterprise data is trapped in legacy "Systems of Record" lacking APIs. Developers face expensive and prolonged application modernization. This burden stalls AI innovation and prevents agents from accessing high-value data.

Data-Hungry Agents and Data Loss: Agents are naturally "data-hungry," scraping any reachable application without strict governance. This allows agents to move laterally across the network or ingest unauthorized content. Simultaneously, unmanaged browser agents act as proxies that can silently leak proprietary code and PII to public models.

KEY BENEFITS

Deploy AI with Absolute Confidence: Eliminate the risk of autonomous agent goal hijacking and logic manipulation, allowing your organization to adopt agentic workflows without compromising security.

Prevent Costly Agentic Data Exfiltration: Ensure sensitive data, PII, and valuable corporate IP never leave your environment through autonomous AI agents or agents in the user's browser, eliminating machine-speed data loss.

Accelerate AI Time-to-Value: Skip months of expensive API development and custom integration work by instantly connecting AI agents to your existing API-deficient applications.

Scale Without Infrastructure Limits: Support millions of simultaneous AI sessions across the globe with zero performance impact, allowing your AI workforce to grow at the speed of your business.

Introducing Menlo AI Agent Security

Menlo AI Agent Security provides a managed cloud runtime that scales the agentic enterprise by simultaneously protecting agents from web-borne threats and unlocking data from API-deficient legacy applications.

- Secures the Autonomous Agent: Menlo Agent Runtime Security (MARS) acts as a protective cloud runtime that executes all agent browser sessions in remote, disposable containers. It strips malicious scripts, hidden instructions, and steganography from the pages and files requested by the agent before the agent processes them, neutralizing threats at machine speed and empowering the enterprise to scale their agentic strategy safely.
- Bridges the Agentic Data Gap: MARS helps agents access valuable data trapped behind web UIs and places controls on agent application and data access. It navigates web UIs for the agent to retrieve the data, and exerts policy controls over the retrieval, masking sensitive data from agents without appropriate permissions and providing explicit instruction/data separation. MARS allows teams to accelerate AI time-to-value across the enterprise.

Key Use Cases

- **Prevent Ingestion of Malicious Content:** Neutralize “invisible” commands or malware hidden in HTML and files by executing sessions in the Menlo Cloud.
- **Control Agent Access to Internal Applications:** Apply Least-Privileged Access to “data-hungry” agents, air-gapping them from application servers to prevent lateral movement.
- **Enable Agents to Access API-Deficient Applications:** Use MARS as a managed abstraction layer to instantly connect agents to ERP and CRM systems without backend refactoring.
- **Govern Browser Agent Assistants:** Apply local governance and AI-powered data redaction to integrated sidebars (like Gemini and Copilot) to prevent silent exfiltration of proprietary code or PII.
- **Prevent Data Exfiltration by Agents:** Interpose between the agent and data sources to mask sensitive information before the agent can harvest it.

GLOBAL SCALABLE INFRASTRUCTURE

Menlo has already built a global elastic cloud infrastructure designed to spin up browser sessions. This means Menlo can globally support millions of transient agentic sessions, lasting anywhere from seconds to hours, without any performance degradation. This high-performance infrastructure is built to absorb 100% of malicious code while delivering clean, sanitized data to your AI at machine speed.

Secure and Scale Your AI-Enabled Workforce

The move toward an agentic enterprise requires more than just new AI tools; it demands strict security controls. Menlo AI Agent Security provides the only unified runtime that simultaneously neutralizes sophisticated logic attacks, prevents critical data loss, and bridges the gap to legacy data. By centralizing AI execution in the Menlo Cloud, you can confidently scale your autonomous and assisted AI initiatives without compromising on security, performance, or data sovereignty.

About Menlo Security

Menlo Security is the pioneer of unified browser security, protecting the modern enterprise's dual workforce: humans and AI agents. Our Browser Security Platform is the only solution that provides a unified trust layer for the modern enterprise, delivering architectural immunity to all actors, both agents and humans.

By focusing security on where the work happens- the browser session- Menlo provides industry-best zero-day threat prevention that eliminates threats before they reach the user device or agent, advanced file and data security that keep users safe and productive, and secure access to applications. These key capabilities are tailored for the security and access needs of users and agents, within a unified control, visibility, and policy framework.

Menlo doesn't just bundle security features; we collapse the distance between security, productivity, and innovation.

This is Menlo. Let's get started.

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