MARS PROGRAM · USE CASES

MARS Use Cases

Where MARS fits, what is at risk, and what it protects against

AI agents are moving fast. They browse the web, interact with SaaS tools, read files, and handle data that is often sensitive. That speed and access creates real risk, and most security tools were not built for it. MARS (Menlo Agent Runtime Security) sits between the agent and whatever it is trying to reach, inspecting content, enforcing policy, and stopping threats before they cause damage.

In all cases, the focus is on agents that have browser and web access. The five use cases below show where MARS fits and what it protects against.

01 Browser Sidebar Agent

Menlo MARS governs the sidebar's connection to the web, bi-directionally. Example sidebars include Copilot, Gemini, Atlas, and Comet.

THE RISK

Sensitive data leakage and loss through data exfiltration. Agent poisoning through prompt injection.

WHAT MARS DOES

- Real-time sensitive data detection and masking
- Prompt-injection stripping

02 Autonomous Agents

Building agents (with Claude Code or any Agent Development Environment) for business process automation. The agent has browser and web access for web scraping, data gathering on the internet, and SaaS.

THE RISK

The agent has access to sensitive data and is vulnerable to prompt injection via the web.

WHAT MARS DOES

- Controls access to specific websites
- Prevents prompt injection on web pages and files

- Blocks data exfiltration and masks sensitive data (DLP controls)
- Sanitizes files and web pages to prevent malware poisoning

03 Claude CoWork

The CoWork desktop app is used as an AI assistant. It can use the browser on the endpoint and has access to the internet and SaaS with similar privileges as human users.

THE RISK

Claude CoWork has access to sensitive data, is vulnerable to prompt injection via the web, and has access to collaboration tools such as email and messaging.

WHAT MARS DOES

- Controls access to specific websites
- Prevents prompt injection on web pages and files
- Blocks data exfiltration and masks sensitive data (DLP controls)
- Sanitizes files and web pages to prevent malware poisoning

04 Claude Code

Claude Code is used by professional developers to build code and agents. Claude Code has internet access for research via browser, web fetch tools, and similar channels.

THE RISK

Claude Code has access to intellectual property, is vulnerable to prompt injection via its web access, and can be hijacked to exfiltrate code and sensitive data.

WHAT MARS DOES

- Controls access to specific websites
- Prevents prompt injection on web pages and files
- Blocks data exfiltration and masks sensitive data (DLP controls)
- Sanitizes files and web pages to prevent malware poisoning

05 File Sanitization & Preparation for AI Use

AI agents consume data from corporate resources (OneDrive, SharePoint) as context. Files pulled from these sources are fed directly into agent workflows.

THE RISK

Any AI agent with access to files can have its goal hijacked via indirect prompt injection hiding in files. It can also surface sensitive or private data and carry malware across the organization.

WHAT MARS DOES

- Sanitizes files at rest by removing prompt injection
- Masks private and sensitive data
- Eliminates malware and zero-day attacks