MARS USE CASES

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

01 Browser Sidebar Agent

MARS governs the sidebar's web connection bi-directionally. Examples: Copilot, Gemini, Atlas, Comet.

THE RISK

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

WHAT MARS DOES

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

02 Autonomous Agents

Agents built for business process automation with browser/web access for scraping, data gathering, and SaaS.

THE RISK

Access to sensitive data. Vulnerable to prompt injection via the web.

WHAT MARS DOES

Controls website access, prevents prompt injection, blocks data exfiltration, masks sensitive data, and sanitizes files against malware.

03 Claude CoWork

AI assistant with browser access and internet/SaaS privileges similar to human users.

THE RISK

Access to sensitive data and collaboration tools (email, messaging). Prompt injection via the web.

WHAT MARS DOES

Controls website access, prevents prompt injection, blocks data exfiltration, masks sensitive data, and sanitizes files against malware.

04 Claude Code

Used by professional developers to build code and agents. Internet access via browser, web fetch, and similar channels.

THE RISK

Access to intellectual property. Prompt injection via web. Can be hijacked to exfiltrate code and sensitive data.

WHAT MARS DOES

Controls website access, prevents prompt injection, blocks data exfiltration, masks sensitive data, and sanitizes files against malware.

05 File Sanitization

AI agents consume corporate files (OneDrive, SharePoint) as context for their workflows.

THE RISK

Goal hijacking via indirect prompt injection in files. Sensitive data exposure. Malware propagation.

WHAT MARS DOES

Sanitizes files at rest by removing prompt injection, masks private and sensitive data, and eliminates malware and zero-day attacks.