

✦ NEW

Redflags® AI Governance Suite

Turning AI Adoption Into Secure Behaviour

Employees across every enterprise are rapidly adopting AI from web-based services like ChatGPT, Copilot, Claude, Gemini, and DeepSeek to locally-installed desktop applications and agentic models like Ollama and LM Studio. This momentum drives innovation, but it's also outpacing corporate security policy, creating an urgent new layer of behavioural risk.

The Challenge

Security teams have limited visibility and no mechanism to intervene at the point of risk. As a result, several vulnerabilities are emerging.

Vulnerabilities

Data leakage: Users upload sensitive files, proprietary code, and confidential data into unsanctioned AI platforms lacking enterprise data protections.

Shadow AI: Employees use personal accounts or sign into unmanaged AI tools with corporate credentials, sidestepping DLP, identity, and audit controls.

Unmanaged local AI: Desktop apps and locally-hosted models operate beyond cloud monitoring, with agentic capabilities acting autonomously on endpoints.

Security teams need more than policies, they need real-time behavioural control.

Discover the new

Redflags® AI Governance Suite

The AI Governance Suite equips enterprise security teams to manage AI risk at the human layer, bridging the gap between policy and practice through behavioural intelligence and timely intervention.



Redflags enables CISOs, SOC analysts, and behavioural risk practitioners to move from reactive detection to proactive risk prevention, empowering organisations to embrace AI confidently and securely.



Deploy a pre-built AI campaign from the Redflags catalogue targeting the most common risk behaviours.



Intervene in real time with contextual nudges that guide secure behaviour.



Gain baseline telemetry on AI tool use across departments (see which tools, how often, and by which users).



Distinguish sanctioned vs. unsanctioned AI usage across web and desktop environments.

➔ To find out more, visit redflags.io