RoonCyber

RUNTIME CNAPP WITH AI WORKLOAD PROTECTION

Many AI security tools focus on prompts and responses, but miss what matters most — how AI interacts with real systems. As AI agents gain access to APIs, data, and services, a compromise can create indirect paths into critical infrastructure.

MAJOR AI SECURITY GAPS

AI Privileged Access

AI agents create a new attack surface, operating as privileged automation with access to critical systems and data.

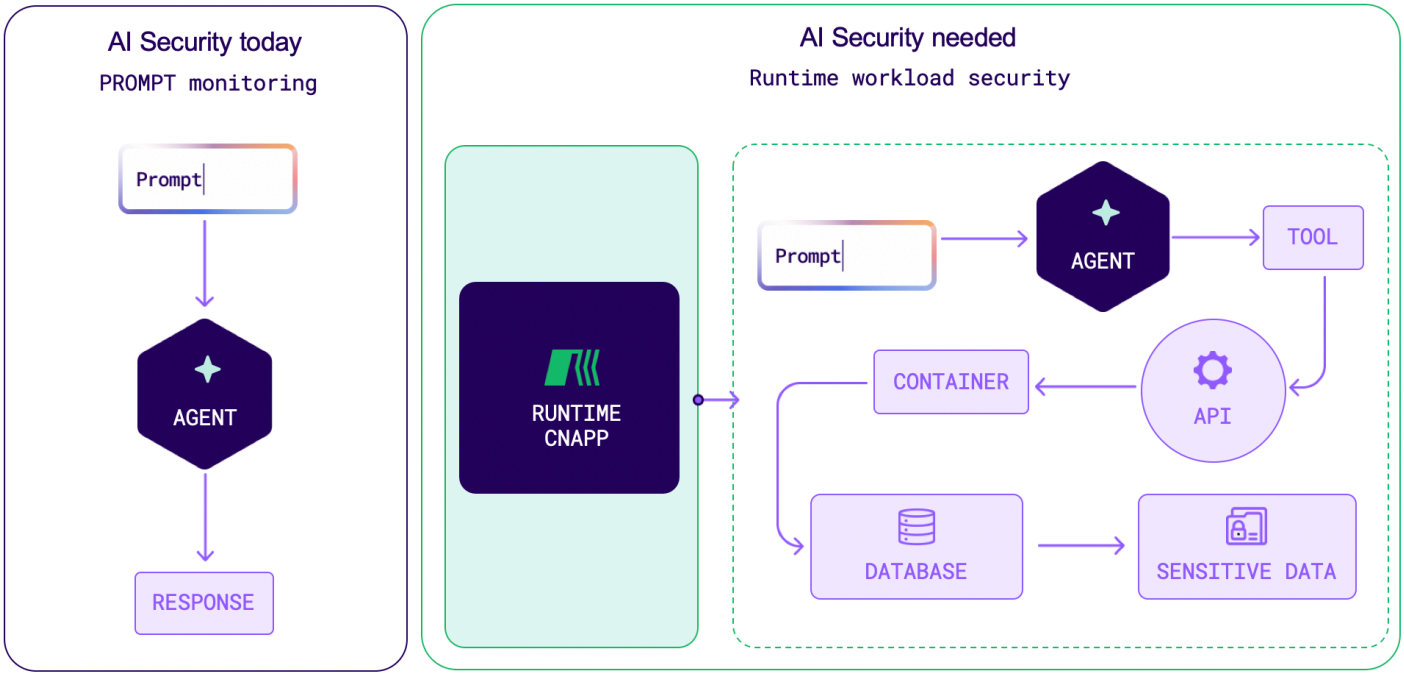
Prompt Blind Spots

If you only monitor prompts, you miss what matters most, what AI actually does in your environment.

Cloud Blind Spots

Without runtime visibility, AI-driven activity moves through your cloud unseen, along with the risk it creates.

WHY RUNTIME VISIBILITY IS NEEDED WITH AI



RoonCyber's Runtime CNAPP + AI Workload Protection

Runtime Detection & Validation

See and validate what AI workloads actually execute.

Attack Path Context

Understand where AI-driven activity can move.

Business Impact

Translate runtime threats into dollars and confidently score risk.

15x Faster MTTR

90% Reduction False Positives

45-50% Lower TCO

One Unified Platform