RUNTIME GOVERNANCE & THREAT DEFENCE

Sentinel

Sentinel is a security control plane for a running agent estate. It watches every tool call and trajectory, classifies threats in real time, shields data at the boundary, and streams governance events straight to your SIEM.

WITHOUT IT

A compromised or misbehaving agent keeps acting until a human notices – usually from a log review, long after the damage is done.

WITH IT

Every tool call and trajectory across your agent estate is watched and threat-classified in real time and streamed to your SIEM, so misbehaviour is caught as it happens. Automated identity revocation and runtime containment are the next step on the roadmap.

WHAT IT IS MCP-native agent security control plane	**WATCHES** Tool calls, trajectories, data at the boundary
STREAMS TO Your SIEM (CEF over TCP/TLS)	**STAGE** Working prototype · containment on roadmap

WHERE IT FITS

Sentinel is the enterprise wedge beside the stack: it consumes the same identities and the same audit-of-record every other layer does, and turns them into live defence.