CERNE™ AGENT ECOSYSTEM

Security Agent

Detects threats, contains them and records every step. Threats hide in a flood of security alerts, user logs and network signals that no team can read in full. The Security Agent correlates user, asset and network behaviour with threat intelligence, classifies severity, and notifies, contains or escalates, with an incident opened automatically.

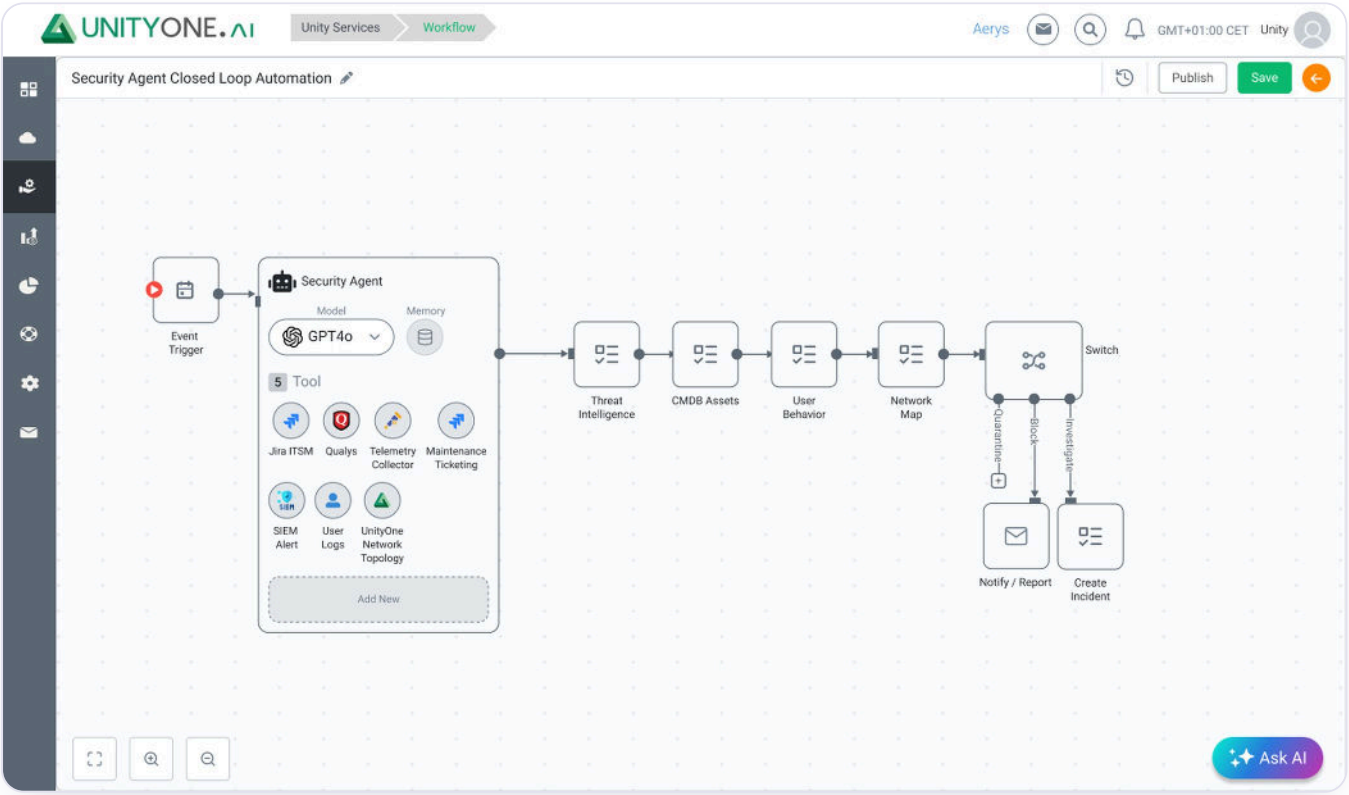
The problem it solves

- Threats buried in SIEM alerts
- Slow correlation of users, assets and network
- Manual containment and incident creation
- Patchy audit trails

241 days

average breach lifecycle;
$4.44M average breach cost

IBM Cost of a Data Breach Report 2025.



Security Agent closed-loop automation: threat intelligence, CMDB assets, user behaviour and network map, then quarantine, block or investigate.

© Copyright 2026 By UnityOne AI | www.unityone.AI

HOW THE SECURITY AGENT WORKS

From trigger to governed outcome

Trigger

- UnityOne event: security anomaly detected
- Security alerts, anomalies and threat intelligence

AI service agent

- Correlates user, asset and network behaviour
- Detects threats and risk patterns

Tool integrations

- SIEM and threat intelligence feeds
- CMDB for asset context
- User logs and behaviour analytics
- Network topology and telemetry; ITSM

Decision engine

- Classifies threat severity
- Decides to notify, contain or escalate

Actions

- Block or isolate
- Create an incident
- Notify and report

Outcome

- Faster threat detection and response
- Reduced security risk exposure
- Automated incident management
- Continuous learning and audit trail

Decision modes: Notify | Contain | Escalate

GET STARTED

Put Cerne™ agents to work

See the agent ecosystem hands-on in the UnityOne AI Playground, or talk to our team about which agents to deploy first in your hybrid and multicloud estate.

▷ Enter Playground | ✉ Contact Us

Email: contact@unityone.ai · Playground: cerne.unityone.ai · Sales: unityone.ai/contact-us

© Copyright 2026 By UnityOne AI | www.unityone.AI