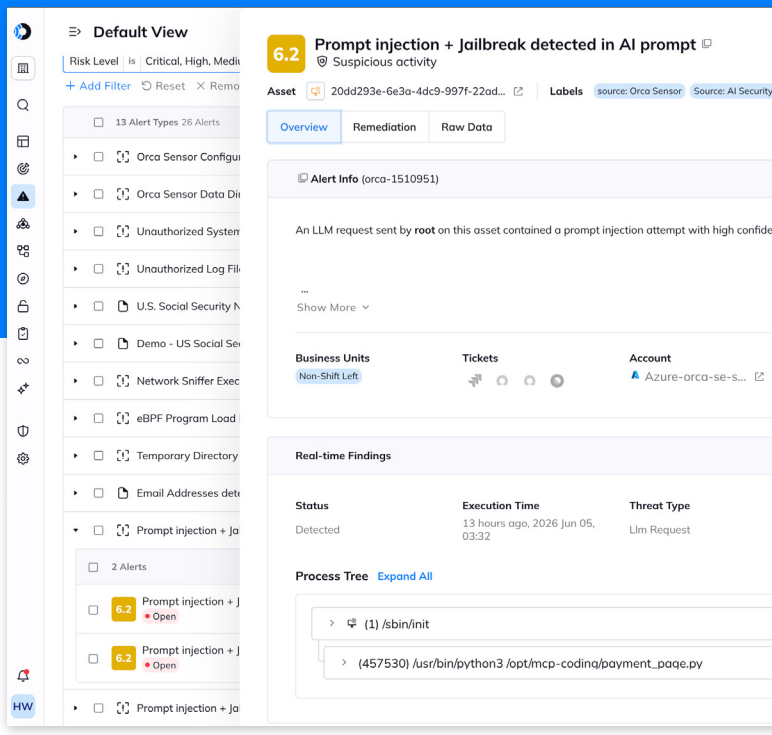
DATASHEET

ORCA SENSOR



Extend the Orca Platform with runtime visibility and protection for advanced Cloud Detection and Response (CDR) and Runtime AI Security.

Unified Runtime Protection for Multi- and Hybrid Cloud

- Deeply integrated with the Orca Cloud Security Platform
- Coverage for public cloud, private cloud, on-premises, and FedRAMP environments
- Support for Linux, Kubernetes, and Windows
- AI-driven features for enhanced threat detection, investigation, and response
- Extensive library of built-in and customizable detections
- Fast and simple deployment
- Automatic updates for minimal maintenance
- eBPF-based for minimal performance impact
- Local decision-making for near-immediate detection and resilience to networking issues
- Meet compliance requirements for NIST 800-53, CMMC, PCI-DSS, HIPAA, CIS Kubernetes Benchmark and more.

A Unified Platform for Runtime and Agentless-First Protection

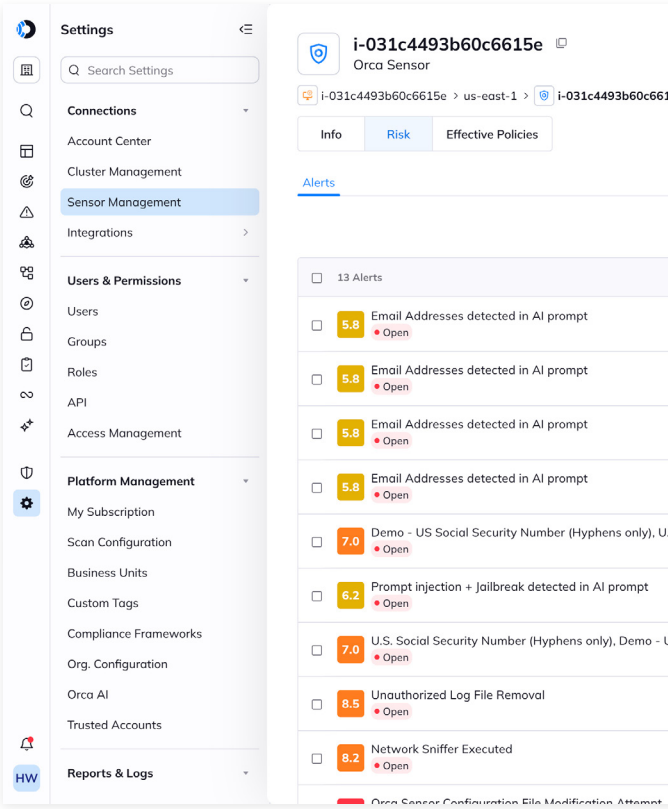
Sensor offers runtime protection that extends the agentless-first capabilities of the Orca Cloud Security Platform, all without the cumbersome deployments, tedious maintenance, high total cost of ownership (TCO), and performance degradation of heavyweight agent-based solutions.

Real-Time Monitoring, Detection, and Protection for Critical Workloads

Sensor provides a real-time view of activity, threats, and malicious behavior flows; extensive and advanced detections; and multiple actions, including the option to terminate processes. While many exploits occur entirely in memory, Sensor can detect and prevent memory persistence and execution even for fileless attacks.

Support for Multi-Cloud and Hybrid-Cloud Infrastructures

Sensor delivers advanced runtime security for diverse multi-cloud and hybrid-cloud architectures, supporting all major and niche public cloud providers, as well as private cloud deployments and on-premise environments. Additionally, Sensor offers full parity across Linux, Kubernetes, and Windows environments, eliminating OS-specific coverage gaps.



Comprehensive and Customizable Detection Policies

Sensor offers an extensive library of built-in runtime detections with the ability to create custom policies as needed, allowing organizations to tailor detections by type, scope, and desired enforcement.

File Integrity Monitoring (FIM)

Define policies once, enforce them everywhere. Detect unauthorized changes to critical system files, configurations, and binaries in real time.

Flexibility for Future Innovation and Improvements in Security

Sensor enables organizations to stay innovative and secure. It offers the flexibility to support future advancements in vulnerability management, non-cloud workload visibility, and more. At the same time, it delivers emerging capabilities through AI-driven features, powered by Orca AI, which enhance threat detection, investigation, and response.

About Orca Security

Trusted by hundreds of organizations, Orca is an enterprise-scalable platform designed to secure large multi-cloud estates efficiently and with low-overhead. With over 50 out-of-the-box third-party integrations, including Slack, OpsGenie, Jira, and ServiceNow, Orca seamlessly integrates with your existing workflows.

Ready to try it out?
Sign up for a demo. Visit orca.security/demo