Unmasking insights from security log chaos

The modern security landscape is riddled with billions of security logs and countless alerts, leaving organizations scrambling to keep their defenses intact. Meanwhile, traditional methods for incident investigation and response can’t keep pace with dynamic cloud environments. Without the proper tools, it can be difficult for security teams to extract meaningful insights and take action.

How can you ensure your security team has the tools it needs to recognize the potential risk and act in time?

Secure your cloud environment with Orca Security

Orca Security, the 2022 AWS Global Security Partner of the Year, is revolutionizing cloud security for Amazon Web Services (AWS) customers. Through the Orca Cloud Security Platform, customers gain the ability to quickly identify, prioritize, and remediate security risks and compliance issues across their AWS cloud estate. Orca’s agentless Sidescanning™ technology and Unified Data Model cover the entire AWS environment, including assets, data, identities, and workloads.

With Orca’s comprehensive platform delivering complete coverage and visibility into the entire cloud estate, enterprises no longer need to be concerned by limited visibility. Orca’s solution provides 24/7 monitoring of the cloud and addresses key concerns about its customers’ AWS environment, including security configurations, potential risks, and compliance management.

Orca reduces operational costs by replacing siloed solutions and multiple disjointed tools with comprehensive risk coverage in a single solution. Additionally, with context-driven prioritization, incident management is efficient and effective.

Customers can operate confidently with Orca knowing that it fills the gaps found in solely agent-based security solutions, which provide only partial coverage and lack full visibility and context, causing alert fatigue.
Smarter security insights with Orca-Amazon Security Lake integration

Orca is now integrated with Amazon Security Lake—a new AWS service that centralizes security data from various sources, including cloud, on-premises, and custom systems, into a purpose-built data lake owned by the customer.

Security Lake has adopted the Open Cybersecurity Schema Framework (OCSF), an open standard that normalizes and combines security data from AWS and a broad range of enterprise security data sources. This integrated solution provides customers with valuable cloud security data and telemetry in OCSF format.

DATA-DRIVEN DECISIONS, INSTANT ACTION

By feeding Orca’s context-rich and comprehensive cloud security data into Security Lake, organizations can eliminate the need for time-consuming data normalization efforts. This integration empowers security teams with increased data intelligence, enabling faster and smarter decision-making.

In addition, Orca’s alert prioritization ensures that critical anomalies and detections, which could have otherwise been overlooked or missed, are promptly brought to the forefront. This capability enables accelerated investigation, triage, and response to potential threats. The platform also offers long-term security data storage, facilitating better forensics for comprehensive analysis and insights.

Customer-focused cloud security

This integrated solution equips customers with advanced cloud security capabilities, simplified operations, and enhanced threat detection. It also facilitates rapid response to safeguard their critical assets and data in the dynamic cloud environment.

UNMATCHED CLOUD SECURITY

- **Effortless data normalization:** Eliminates the burden of data normalization with OCSF, saving time and resources
- **Increased data intelligence:** Provides access to context-rich cloud security data for smarter decision-making
- **Swift incident response:** Accelerates investigation, triage, and response to potential cloud threats
- **Comprehensive cloud coverage:** Achieves security coverage of all AWS assets, data, identities, and workloads
- **Stronger cloud security:** Supercharges organizations’ cloud security data lake with insights for enhanced protection
See for yourself

→ Learn more about the Orca-AWS Security Lake solution on AWS Marketplace.

→ Sign up for a free AWS Cloud Security Risk Assessment.

→ Check out the Orca/AWS partner page and discover why Orca achieved AWS Global Security Partner of the Year.

ABOUT Orca Security

Orca Security is the industry-leading Cloud Security Platform that provides complete coverage and centralized context of your entire cloud estate, enabling security practitioners to spend less time correlating long lists of disconnected alert and focus on remediating the actual risks that have the most impact on the business. Founded in 2019, Orca is trusted by hundreds of customers globally.

Connect your first cloud account in minutes and see for yourself at: https://orca.security