REBURA | orca security

aws PARTNER Advanced Tier Services

- Immersion Day Solution Provider
- Migration Services Competency
- Well-Architected Partner Program
- Digital Workplace Services Competency
- AWS Marketplace Skilled Consulting Partner
- AWS Microsoft Workloads Services Competency

CLOUD SECURITY SIMPLIFIED

Three-quarters of organizations are concerned about their ability to secure public clouds, furthermore 82% of organisations say that existing security tools either don't work at all or can only provide limited functionality in the cloud.[1]

We believe that there is a better, simpler way! We are so confident that we are offering you an AWS Cloud Security Risk Assessment. Rebura's complimentary 30-day offer is based on Orca's unique agentless technology. It's a simple 3-step process:

1. We'll assist you with the installation of the Orca Cloud Security Platform in an AWS account of your choice.

2. You'll get complete visibility into your cloud estate and its most critical security risks, including vulnerabilities, misconfigurations, malware, exposed data, secrets, weak passwords, and lateral movement risk.

3. After 30 days a Rebura security expert will walk you through the findings, focusing on high-risk items and compliance misconfigurations - discussing remediation and the next steps giving you a clear action plan for improving your cloud security posture.

[1] Gilad Maayan,"The Future of Cloud Security: 2022 and Beyond" ReadWrite, November 12, 2021

ORCA will uncover issues such as:

- Vulnerabilities in operating systems and applications, including the packages and libraries that make up your applications
- Misconfigurations that present a security or compliance risk
- Malware-infected machines – even neglected or orphaned workloads that have flown under the radar
- Poor security hygiene that can enable an attacker to move through your cloud environment

The ORCA Cloud Security Platform

Delivered as SaaS, Orca Security's patent-pending SideScanningTM technology reads your AWS cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and unsecured PII.

There are no agents to install, no overlooked assets, no DevOps headaches, and no performance hits on live environments. This does away with thousands of meaningless security alerts to provide just the critical few that matter, along with their precise path to remediation.

GET STARTED TODAY

T 020 3911 9850 E info@rebura.com W www.rebura.com in Follow us on LinkedIn