Complementary Security Assessment with Orca FAQ

What is the VividCloud Complementary Security Assessment with ORCA offering?

The complimentary security assessment involves a single, agentless deployment of the Orca security platform. This assessment offers a comprehensive inventory of an organization's cloud assets, detecting potential issues such as misconfigurations, vulnerabilities, insecure authentication, and malware. The results are compiled into an Executive Report by VividCloud, including guidance for remediation.

What is Orca Security?

Orca Security offers an agentless approach to cloud security and compliance, ensuring complete visibility across cloud configurations and workloads. It identifies security risks at various layers, including cloud infrastructure, operating system, applications, and data, eliminating the need for multiple tools like Cloud Security Posture Management (CSPMs) and Cloud Workload Protection Platforms (CWPPs).

What problems does Orca Security solve?

The Orca platform solves several problems with current cloud security solutions:

- Cumbersome deployment: Installing and maintaining agents on every cloud workload results in performance degradation, and high TCO.
- Coverage gaps: Partial deployment of agents causes blind spots. Less than 50% of assets are covered by agent-based solutions
- Performance degradation: Cloud security solutions based on agents or network scanners have a significant impact on application performance and system resources
- Alert fatigue: Security teams waste valuable time manually sifting through high volume, low-risk alert data resulting in missed critical issues
- Multiple tools: Security teams face the complexity and burden of managing multiple point-solution tools.

What are the benefits of the Orca Security platform?

- Agentless: Security without the need for agents, simplifying deployment and reducing operational overhead.
- Deep visibility: Deep packet inspection and vulnerability scanning to identify security risks across cloud workloads.
- Continuous monitoring: Continuous monitoring allows organizations to detect and respond to incidents in real-time.
- Compliance: Support for 100+ frameworks ensuring compliance with industry standards and regulations.
- Risk prioritization: Prioritize risks based on severity, allowing organizations to focus on the most critical issues first. In fact, Orca's context-aware engine prioritizes the 1% of alerts that need immediate attention.
- Unified platform: Orca includes the core capabilities of CSPM and CWPP solutions, including vulnerability and compliance management, in a single platform.
- Scalability: Provides security solutions that adapt to changing workloads and environments.

Which risks does Orca Security detect?

Orca specializes in detecting and prioritizing various risks in cloud security, including vulnerabilities, misconfigurations, malware, unprotected sensitive data, lateral movement risk, and identity and access management (IAM) risk.

Which assets does Orca cover?

Orca provides comprehensive coverage for all cloud infrastructure assets, encompassing virtual machines (VMs), containers, and serverless components. It extends to various cloud resources such as storage buckets, security groups, Virtual Private Clouds (VPCs), Identity and Access Management (IAM) roles and permissions, Key Management Service (KMS) keys, and more. Orca goes beyond typical coverage by identifying and monitoring idle, paused, and stopped workloads, as well as identifying orphaned systems and devices that cannot support agents.

Does Orca help organizations achieve cloud compliance?

Orca facilitates regulatory compliance by identifying various threats such as vulnerabilities, malware, compromised passwords, and file integrity issues. It supports over 100 key frameworks and CIS benchmarks by default, with customizable compliance templates to adapt to specific requirements. Additionally, Orca aids in meeting data privacy mandates, including PCI-DSS, GDPR, CCPA, and HIPAA, by detecting sensitive information like Personally Identifiable Information (PII) and potential exploitation paths.

What is Context-Aware security?

Unlike traditional solutions that focus solely on the severity of security issues (e.g., CVSS score), Orca considers each asset's role within its environment. Allowing Orca to prioritize critical security issues based on three factors: the severity of the issue, accessibility by attackers, and impact of a potential breach. By analyzing these factors, Orca ensures that alerts are prioritized based on their actual significance to the security posture, rather than alerting to all threats indiscriminately. This approach allows Orca to provide a more nuanced and effective security prioritization.

Does Orca provide a visual representation of cloud assets?

Yes. For response to each alert, Orca offers an attack vector graph that provides contextual information about the asset. This includes details such as the asset type, whether it is public-facing, and any lateral movement risk, presenting a comprehensive view of the security landscape.

Does Orca support multi-cloud configurations?

Yes, Orca supports multi-cloud estates from IaaS providers AWS, Azure, and Google Cloud, allowing you to manage your cloud security and compliance from a single platform.

How long does it take to deploy Orca Security?

Because there are no agents to install Orca Security deploys in minutes and you start seeing results almost immediately.

Can VividCloud provide additional customization and implementation services for this offering?

Yes. The initial offering involves a one-time assessment, resulting in an Executive Report along with guidance for remediation. VividCloud also provides supplementary services for addressing and resolving misconfigurations, vulnerabilities, and risks identified in your cloud environment.

What differentiates VividCloud's offering from other Cloud Security Assessments?

VividCloud's initial security assessment is FREE, unlike many others in the industry. Others providers will help implement Orca and generate findings. VividCloud goes further, in addition to implementing Orca in your cloud environment we will deliver an Executive Summary with remediation guidance. More important, VividCloud has the expertise and can offer professional services for addressing and resolving the issues and risks identified during the assessment.

Can VividCloud help with compliance?

Certainly. VividCloud has a track record of assisting customers with their compliance needs, including but not limited to AWS Well Architected, CIS Controls, FedRAMP Moderate, HIPAA, HITRUST, and NIST 800-53. Additionally, VividCloud is capable of collaborating with your team to create a custom compliance framework tailored to meet your specific requirements.

How does VividCloud’s Cloud Security Assessment with ORCA help remediate risk and compliance issues?

VividCloud offers a comprehensive approach to compliance. Initially, we can help configure a compliance template to establish a baseline. Simultaneously, we can deploy our AWS Audit Manager solution to detect and alert on any changes in compliance resulting from modifications to cloud resources. Our Compliance Pack includes rules and policies designed to automatically address up to 80% of misconfigurations and compliance issues. Finally, VividCloud's engineers are skilled in cloud security and are available to address any additional remediation needs that may arise.

Can VividCloud help implement custom instrumentation and CI/CD workflows for deploying a centralized solution?

Yes. VividCloud has expertise in implementing custom instrumentation and can assist you in creating or enhancing CI/CD (Continuous Integration/Continuous Deployment) workflows to ensure resources are compliant when deployed or modified. We understand the importance of streamlined, VividCloud is positioned to assist in achieving a robust and efficient solution within your production environment.

Can VividCloud guarantee compliance?

No. The VividCloud solution builds upon AWS Audit Manager and assists you in gathering and preparing evidence for audits, saving thousands of hours needed for evidence collection. Further, VividCloud's offering can automatically remediate several compliance issues and detect drift, helping to ensure that once an asset is compliant it stays that way.