

Agentless, Workload-Deep Context-Aware Security for Azure

Are you tired of operating in the dark - with agent-based solutions?

Before Orca Security, enterprises needed multiple, disparate cloud security tools to get visibility into their cloud estate. With agents required for each workload, blind spots are inevitable. Without full visibility, there is no way to know if your configurations are secure, if security groups are hardened, which OS and applications are running, if there's risk of lateral movement... the list goes on. Orca solves this problem with its single, agentless platform that delivers 100% visibility of your entire cloud estate as well as workload and data protection, cloud security posture management, vulnerability management, and compliance management capabilities.

The Orca Cloud Security Platform for Azure

Orca Security provides cloud-wide, workload-deep, context-aware security and compliance for Azure without the gaps in coverage, alert fatigue, and operational costs of agent-based solutions. The Orca Security Platform detects risks in all Azure workloads including, VMs, containers, and serverless, regardless of whether they are idle, stopped, or paused, as well as configuration issues in native Azure cloud services.

Orca Security integrates with Microsoft Azure services and products, including Azure Sentinel and Azure SSO. Orca's integration with Azure Sentinel, Microsoft's SIEM, allows you to load data into Sentinel and monitor and visualize it using Sentinel workbooks. Logging in to the Orca console using Single Sign On is supported by a variety of SSO products to include Azure SSO

Orca Security integrates through the Azure runtime storage layer and combines this with metadata gathered from Azure APIs to detect risks across both the workload and control planes. Customers can easily scan object storage buckets for personally identifiable information (PII) and malware without moving or storing the underlying data. With Orca Security, customers can inspect Identity and Access Management (IAM) policies, generate alerts, and visualize issues simultaneously via an asset risk map.

Detect and prioritize cloud security risks in your Azure environment in minutes, not months.

Orca Security Detects and Prioritizes Against

- ✓ Vulnerabilities
- ✓ Misconfigurations
- ✓ Malware
- ✓ Misplaced Sensitive Data
- ✓ Lateral Movement Risk
- ✓ Identity and Access Management Risk

Azure Integrations

-  Azure Sentinel
-  Azure SSO

Orca Benefits



100% Coverage

Orca covers 100% of your cloud assets – now and in the future. This includes VMs, containers, and serverless, as well as cloud infrastructure resources like blob storage, resource groups, key vault secrets, and much more. Orca even discovers and monitors idle, paused, and stopped workloads, orphaned systems, and devices that can't support agents.

"Orca has taken our cloud environment visibility from zero to 100%. When I discuss with my team what to address first, now I speak from a far more credible position."

Doug Graham
CSO & CPO, Lionbridge



Multiple Tools in ONE

Orca detects and prioritizes the most important security risks at every layer of your Azure cloud estate through a single platform, eliminating the need to cobble together disparate tools. Orca replaces legacy vulnerability assessment tools, CSPM, CWPP solutions, and more.

"For us, the most important criterion was to find a tool that sees different security angles, including infrastructure, applications, and PII. Orca lets us see it all in a single place."

Ran Tenenbaum
CISO, Grand City Properties



Alerts that Matter

Stop wasting valuable time manually correlating high volume, low-risk alert data from multiple security tools. Orca's context engine separates the 1% of alerts that demand quick action from the 99% that don't, enabling security teams to avoid alert fatigue and fix the truly critical security issues before attackers can exploit them.

"Orca risk-prioritizes alerts in a way that's very actionable in terms of both the information that is provided and the level of security that is given. This is top-notch and pure magic."

Caleb Sima
VP of Information Security, DataBricks



Built-in Compliance

Orca ensures regulatory compliance by alerting to threats ranging from vulnerabilities and malware, to file integrity and leaked passwords. Orca also uniquely recognizes where sensitive data is stored across your cloud estate and alerts you to potential exploitation paths, helping you meet compliance mandates such as PCI-DSS, SOC 2, CCPA, GDPR, and HIPAA.

"With Orca, I can easily demonstrate passing cadence. I can demonstrate vulnerability assessment, proper governance of machines, and separation of duties. Orca in itself would convince any EU judge that a company has a more than reasonable security program."

Jack Roehrig
CISO, Turnitin

Orca Azure
Customers

