Major Federal Agency Protects Cloud Migration Program with Orca

INDUSTRY
Federal Agency

CLOUD ENVIRONMENTS
AWS, Google Cloud, Azure, Oracle Cloud

REGION
United States

Cloud Security Challenges

- ✕ Limited cloud visibility with agent-based approach
- ✕ Lacked depth of data into software packages
- ✕ Fragmented view across multi-cloud inventory and compliance
- ✕ Data sovereignty requirements

Cloud Security Results

- ✓ Comprehensive multi-cloud inventory in minutes
- ✓ Deep intel about vulnerable software packages
- ✓ Centralized compliance view
- ✓ Private mode deployment to satisfy data sovereignty requirements

The Mission: Modernize Cloud Infrastructure

This Agency is critical to maintaining a strong economy. They started its cloud migration program because several individual bureaus were pursuing their own cloud solutions to modernize their applications. This created duplicative contracts that ignored opportunities for cost reduction and consolidated procurement.

The Challenge: Fragmented Agent-based Visibility of Risk Across Multi-Cloud Environments

While the cloud migration program pushed for adoption across AWS, Azure, Google Cloud, and Oracle Cloud, the Agency had historically relied on an agent-based approach to vulnerability scanning. Agents only saw security gaps on the resources where they were deployed. Additionally, agents didn't scale. Instead, they increased overhead on the lean team to deploy and maintain the technology. The agent-based approach to cloud security meant the Agency could only see a fraction of their cloud estate, leaving them blind to serious security threats.

Driving compliance across multiple cloud service providers proved untenable. This Agency maintains strict adherence to NIST 800-53/171/172, DISA STIGs, CMMC, and BOD 22-01, enforcing aggressive 30-day remediation SLAs.

Siloed tools meant investigations had to be manual, causing extended remediation SLAs.

The Agency was looking for a solution that was easy to deploy, easy to use, and delivered deep visibility across their multi-cloud estate. However, they also had strict data sovereignty requirements. The chosen solution had to keep all scanning and data processing within the Agency's boundaries.

Orca Unifies Multi-Cloud Inventory, Security, and Compliance

The Agency selected Orca's agentless Cloud-Native Application Protection Platform (CNAPP) because it uniquely addresses federal challenges with proven, public-sector differentiators:

- **Orca Private Mode Deployment:** In this mode, the Orca Platform backend and scanning operate entirely in the Agency's accounts, ensuring no data or metadata leaves their environment, ensuring alignment with their FedRAMP High boundary.
- **Deep Risk Context, Agentlessly:** Orca's patented SideScanning™ technology provides workload-deep visibility (OS vulnerabilities, misconfigurations, IAM, secrets, malware, lateral movement paths).
- **Attack Path Analysis:** More than just simple graph connections, Orca evaluates what combinations of security issues pose the highest risk to the organization's crown jewels and prioritizes which attack paths are most critical.
- **Dynamic Risk Prioritization:** Orca goes beyond CVSS and EPSS scores to determine the risk of alerts and assets. Aside from general severity groupings (i.e. critical, high, etc), Orca calculates the risk of alerts and assets based on factors like asset context, exposure details, attack paths, and data sensitivity at risk. By calculating a prescriptive risk score with environmental context, the Agency teams can trust they are focused on the most important issues at hand.
- **Built-in Federal Compliance Acceleration:** Out-of-the-box support for 200+ frameworks, including NIST 800-53/171/172, DISA STIGs, and CIS Benchmarks. Continuous monitoring validates patching status in real-time and generates audit-ready evidence with the click of a button.

Orca augments this technology with a resident Orca engineer. This “high-touch + high-tech” model ensures:

- **Strategic alignment** specific to Agency directives
- **Operational excellence** through alert tuning and hands-on triaging alongside the Agency teams
- **Knowledge sharing** through workshops, training, and documentation within Agency’s boundaries

This model drives a new level of rigor to the Agency’s vulnerability management program. With this approach, Orca has been able to respond quickly with new features as their cloud adoption and long-term partnership grows.

About Orca Security

Orca offers a unified and comprehensive cloud security platform that identifies, prioritizes, and remediates security risks and compliance issues across AWS, Azure, Google Cloud, Oracle Cloud, Alibaba Cloud, and Kubernetes. The Orca Cloud Security Platform leverages Orca’s patented SideScanning™ technology to provide complete coverage and comprehensive risk detection.


orca
SECURITY