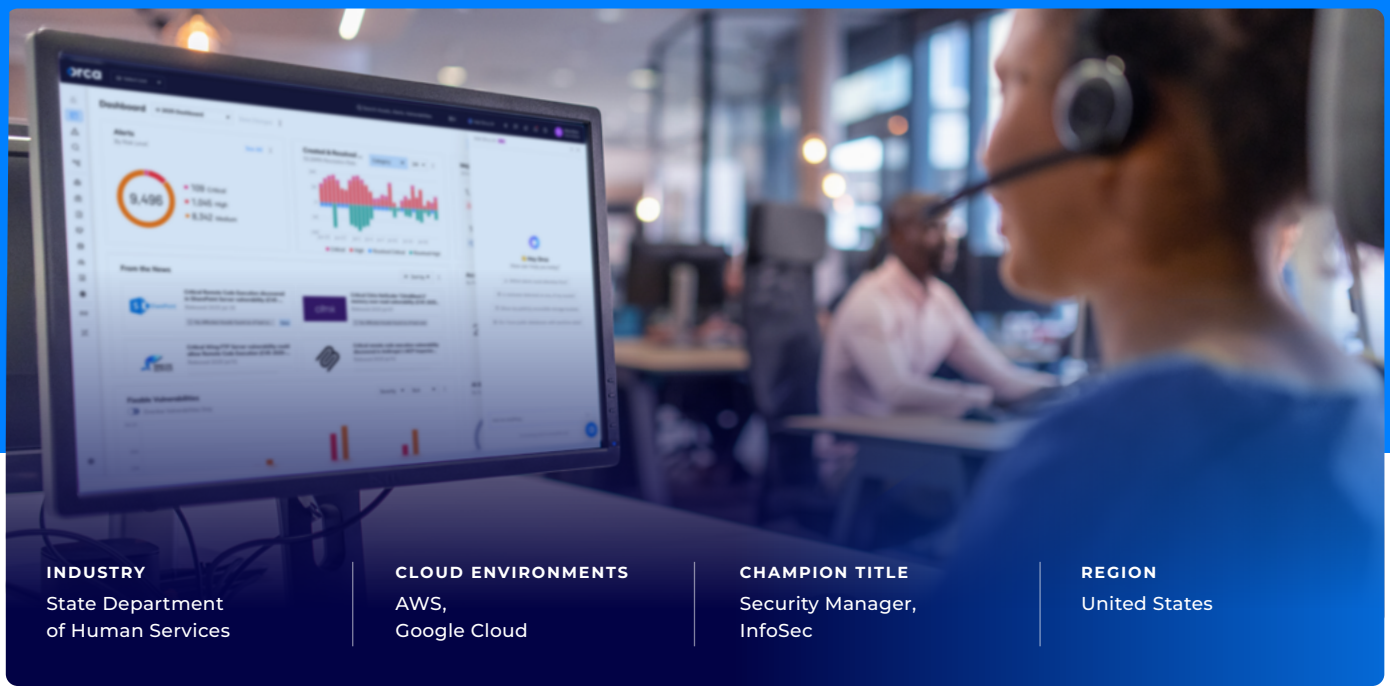
State Department of Human Services Eliminates Overhead and Blind Spots Generated by Legacy Agent-Based Cloud Solution



INDUSTRY
State Department of Human Services

CLOUD ENVIRONMENTS
AWS, Google Cloud

CHAMPION TITLE
Security Manager, InfoSec

REGION
United States

Cloud Security Challenges

- ✕ Blind spots due to legacy agent-based tools
- ✕ Compliance gaps for protecting PHI in AWS and Google Cloud workloads
- ✕ Too much overhead to complete compliance audits for HIPAA and HITECH, distracting the team from delivering digital services for their constituents

Cloud Security Results

- ✓ Visibility increased from ~60% to 100% of workloads
- ✓ Compliance reporting cycles shortened from weeks to days
- ✓ Sensitive PHI exposures were identified and re-mediated before audits
- ✓ Jira integration significantly improved security operations efficiency

State Department of Human Services: Connecting People with the Assistance They Need

State Departments of Human Services often administer social services like welfare, child protection, disability services, and public health programs. They serve as safety nets for vulnerable populations, but struggle with outdated and proprietary technology systems, lengthy wait times, and balancing compliance with genuine human need. The specific State Department of Human Services anonymized for this case study operates a multi-cloud environment, using AWS and Google Cloud to power applications that ensure their citizens access the health insurance assistance they need.

Before partnering with Orca, this team was using an agent-based approach to monitor the security of their cloud workloads. As a result, they could only see about 60% of their cloud estate.

The Challenge: Blind Spots and Compliance Gaps from Legacy Agent-based Tools

Before partnering with Orca, this team was using an agent-based approach to monitor the security of their cloud workloads. As a result, they could only see about 60% of their cloud estate, since they couldn't deploy agents on every workload. The agents also needed to be maintained, increasing overhead for the team. Meanwhile, the agents that were deployed, overloaded the team with too much telemetry without making any threats or risks actionable for remediation.

Because this cloud application focused on health insurance assistance, this team faced pressure to comply with both HIPAA and HITECH regulatory standards. Gathering evidence for each of these audits was time-consuming and resource-intensive, often delaying work to bring new capabilities securely to their application and serve their people.

The Head of Information Security started the search for a solution that would give him full visibility of his multi-cloud estate, save his team time for compliance audits, reduce the overhead of managing agents, and integrate with their ticketing solution, Jira On-Prem, to streamline workflow automation.

Orca Delivers Full Visibility of Cloud Risk, Streamlines Work with Jira On-Prem Integration, and Simplifies Multi-Cloud Compliance

Full Visibility: Since implementing the Orca Cloud Security Platform, this State Department of Human Services has dramatically improved the visibility of their multi-cloud environment—from 60% to 100% of their workloads across AWS and Google Cloud. The numerically scored alerts gave the team clear prioritization to focus on the most important security risks and compliance gaps to address. The alerts also presented and factored in context covering sensitive data detections, asset context, identity and access policies, external exposure, exploitability predictions, and other data, giving them the relevant information they needed to determine the appropriate mitigation steps.

Streamlined Work: During the proof of concept, the team tested the Jira On-Prem integration to share Orca data with their incident response workflows. They were impressed with the depth of data they were able to pass to the Jira tickets, as well as the flexibility of the integration setup. Orca allows admins to create multiple templates so that each use case is covered. Not only can each project be assigned a template, admins can have multiple templates per project if needed.

Simplified Compliance: The Head of Information Security customized out-of-the-box compliance frameworks for HIPAA and HITECH to quickly monitor and triage any compliance drift, like exposed PHI, before audits. By using the Orca Platform, they eliminated emergency disruptions. They were able to efficiently prepare for an audit by streamlining compliance fixes into the workstream of other remediation work. When it came time to share evidence with the auditors, it was a simple click of a button to export the compliance report to PDF or CSV.

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