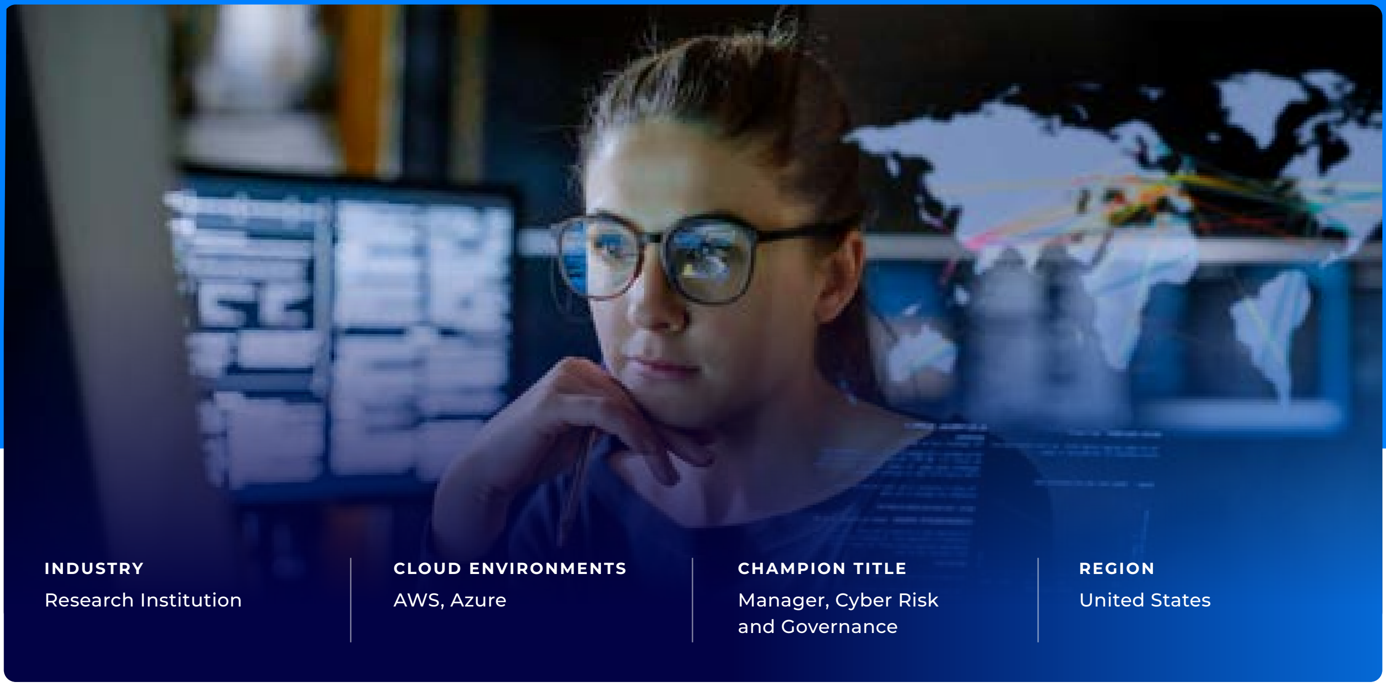
CASE STUDY | RESEARCH INSTITUTION

Federally Funded Research and Development Center Unifies Cloud Risk and Compliance Across 300+ Azure Subscriptions



INDUSTRY	CLOUD ENVIRONMENTS	CHAMPION TITLE	REGION
Research Institution	AWS, Azure	Manager, Cyber Risk and Governance	United States

Cloud Security Challenges

- ✗ Decentralized cloud management across 300+ Azure subscriptions and AWS accounts
- ✗ Limited visibility due to reliance on agents
- ✗ Fragmented legacy toolset with siloed data
- ✗ Mandate to comply with NIST 800 standards

Cloud Security Results

- ✓ Unified visibility across 300+ Azure subscriptions and AWS accounts
- ✓ Eliminated agent overhead in research environments
- ✓ Strengthened compliance posture under NIST 800 standards
- ✓ Enabled collaboration across security, compliance, architecture, and IT teams

The Mission: Ensuring National Security Through Specialized Research and Development

Federally Funded Research and Development Centers (FFRDCs) strengthen national security by conducting research for the United States Government. FFRDCs tackle complex scientific, technological, and analytical challenges requiring continuity, objectivity, and access to sensitive information. Established under long-term contracts with federal agencies, these centers operate independently from government administration while serving the public interest. The specific Federally Funded Research and Development Center anonymized for this case study uses Azure and AWS to power their cloud native applications.

The Challenge: Visibility Fragmented Across Too Many Cloud Accounts to Properly Align with NIST 800 Standards

When the cyber risk and governance team at the FFRDC was mandated to show compliance with NIST 800 standards, it became evident that driving progress across 300+ Azure subscriptions and AWS accounts was untenable. Before partnering with Orca, the team relied heavily on agent deployments to secure their research environments. This meant a lot of overhead to maintain those deployments, as well as siloed data per cloud account and subscription. Additionally, agents only saw the assets they are deployed on, so there were a lot of blind spots across their AWS and Azure environments where agents were not deployed.

Because information was fragmented across the complex cloud environment and in disparate tools, the vulnerability management team struggled to connect the dots from vulnerabilities, misconfigurations, and identity risks to sensitive research assets. Major security risks remained misprioritized or unidentified, while efficient remediation options for known issues stayed obscured in the mess of data and policies that needed to be manually analyzed.

Compliance reporting was also resource intensive, requiring team members to manually gather evidence of compliance while noting failed controls and kicking off the work to fix the compliance gaps. Tracking compliance for such a large, complex environment was impossible without disrupting innovative work to support the compliance team's lean resources and timeline to meet the compliance mandate.

Orca Unifies Cloud Risk and Compliance with Prioritization Baked In

A group of stakeholders across Cyber Risk and Governance, Cloud Architecture, and Enterprise IT joined forces to find a solution that met three key criteria:

- Centralized visibility across all workloads and cloud accounts without creating friction with the individual teams
- Relevant security context presented clearly to understand what sensitive data is at risk and which team to work with to remediate issues
- Eliminate the reliance on agents

While the group considered native cloud security tools like Azure Security Center, as well as other CNAPPs on the market, the team ultimately chose the Orca Cloud Security Platform for three reasons:

- Immediate cloud visibility within minutes of agentless deployment, eliminating the overhead of implementing and maintaining agents
- Attack paths—prioritized by risk level—that showed how vulnerabilities and misconfigurations could be chained together to compromise sensitive research data
- Centralized cloud compliance with alerts automatically connected to controls to update pass/fail statuses

The partnership with Orca transformed the FFRDC's cloud security and compliance posture, enabling the team to achieve NIST 800 compliance across their entire multi-cloud environment efficiently. By eliminating agent overhead and unifying visibility across 300+ accounts, the organization now identifies and prioritizes critical risks while protecting sensitive research assets. This agentless approach improved collaboration across the board, freeing each team to focus on strategic initiatives rather than manual compliance tracking and demonstrating how modern CNAPP platforms support mission-critical government research and innovation.

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, and Kubernetes. The Orca Cloud Security Platform leverages Orca's patented SideScanning™ technology to provide complete coverage and comprehensive risk detection.

Ready to try it out?
Sign up for a demo. Visit orca.security/demo

orca
SECURITY