SOLUTION BRIEF

MULTI-CLOUD SECURITY AND COMPLIANCE FOR PUBLIC SECTOR: AUSTRALIA

The 2023-2030 Australian Cyber Security Strategy outlines how the Australian government plans to build national cyber resilience in the wake of rising cybercrime. Part of this initiative is to ensure Australian citizens can trust digital products and software, protect the most valuable datasets, and adopt emerging technologies safely.

According to TechTarget, "over 140 Commonwealth, state and territory agencies already use AWS for critical services in transport, health, education and tax collection." Cloud adoption will only increase as citizens desire more modern digital services.

Orca Completes IRAP Assessment at Protected Level

Australian government agencies and contractors can now use the Orca Platform to command their cloud with confidence that our security practices meet national security standards. Orca takes an agentless-first approach to identify, prioritize, and remediate risks across the entire application lifecycle, from cloud to developer environments. Teams, whether they are developers, DevOps engineers, IT Ops managers, security architects, security analysts, or security engineers, can operate from a Unified Data Model to easily find and fix security and compliance gaps efficiently.

How Orca Delivers Australian Public Sector Security & Multi-Cloud Compliance

Experience quick time-to-value

Orca gives Australian government agencies and contractors an agentless-first approach to the most comprehensive coverage of their cloud estate by detecting misconfigurations, vulnerabilities, malware, lateral movement, data risks, API risks, AI risks, active breaches, and more—without the overhead of agents. Our patented SideScanning™ technology delivers an inventory of assets, risks, and compliance gaps in just minutes of deploying.

The Orca Platform has completed the IRAP assessment at the Protected level. Read the blog

Why Orca?

- ✓ **Pre-production and production coverage:** Secure from cloud to dev environments
- ✓ **Prioritization:** Focus on what risks matter most
- ✓ **Persona-based views:** Tailored for each member of your organization
- ✓ **Prevention mindset:** Stop risks before they happen
- ✓ **Performance, scale & privacy:** Unmatched by any other platform

Orca Detects & Prioritizes the Following Risks:

- ✓ Vulnerabilities
- ✓ Misconfigurations
- ✓ Malware
- ✓ Unsecured Sensitive Data
- ✓ Lateral Movement Risk
- ✓ API Risk
- ✓ Overprivileged Identities
- ✓ AI Risk

Supported Platforms

- ✓ AWS
- ✓ Google Cloud
- ✓ Azure
- ✓ Oracle Cloud
- ✓ Alibaba Cloud
- ✓ Kubernetes

Precisely prioritize risks

The Orca Platform pulls together data across cloud configurations, cloud event logs, CI/CD scans, network, cloud entitlements and privileges, agents, and our SideScanning technology into a Unified Data Model. Orca uses this depth of data to visualize attack paths and precisely prioritize risks with a calculated risk score that keeps the root cause of a security issue and dynamically updates as the context changes. Whether teams use an asset-focused approach or risk-focused approach to remediation, Orca makes sure that teams focus on what really matters.

Discover, classify, and protect sensitive data

The Orca Platform provides a Data Security dashboard that shows an overview of cloud data stores, sensitive data, and security and compliance alerts. When Orca's SideScanning™ technology detects sensitive data, it classifies what type of sensitive data was detected, keeps a masked sample, and deletes the rest. The data sample, paired with deep contextual data, gives team members confidence in any alerts sent their way to fix. All customer data is handled securely complying with ISO certified techniques and procedures.

Adopt AI safely

The Orca Platform supports the safe adoption of emerging technologies like AI in two ways: AI-SPM and AI-driven discovery and remediation.

AI-SPM

Orca identifies deployed AI models in your multi-cloud environment to protect against data tampering and leakage. Orca covers 50+ AI models and software packages—including Pytorch, TensorFlow, OpenAI, Hugging Face, scikit-learn, and many more—allowing you to confidently adopt AI tools while maintaining visibility and security for your entire tech stack.

AI-DRIVEN DISCOVERY & REMEDIATION

Orca uses AI across the platform to make teams more effective, even when they are earlier in their cloud journey. Developers and security practitioners alike can lean on ready-to-use remediation steps, simplified search, and suggested IAM policy configurations. Orca even uses AI to detect anomalous activity and provide cloud detection and response capabilities with an agentless-first approach.

Drive continuous multi-cloud compliance

Instead of hopping across multiple tabs, projects, and environments to collect evidence for audits, Orca provides 185+ customizable compliance and data privacy frameworks, including the Australian ISM, NIST CSF, ISO 27001, GDPR, PCI-DSS, CIS Benchmarks, and more. Compliance gaps are connected directly with Alerts, making it easy to align remediation with existing alert workflows.

Integrate with existing tools

Make sure the right intelligence gets to the right person to efficiently remediate security and compliance gaps. Pass granular context and risk scores of Orca alerts into bi-directional integrations with Jira and ServiceNow. Give developers the information they need to fix security gaps in the environments they're already using, like GitHub, GitLab, Azure DevOps, and BitBucket native apps. Deliver alerts into notification channels like Slack or Microsoft Teams, or your SIEM or SOAR tools like Splunk or Sumo Logic. Explore our integrations directory, and if you don't see a managed integration for your techstack, use our REST API to get the information you need into the places where your teams work.