



CLOUD SECURITY POSTURE MANAGEMENT (CSPM) WITH ORCA

55%

of organizations now manage two or more cloud providers (Orca research)

38%

of organizations with sensitive data have those databases exposed to the public (Orca research)

128 days

average time critical alerts sit before anyone acts on them (Orca research)

THE CHALLENGE:

Visibility Gaps, Alert Noise, and Stalled Remediation

Cloud environments change constantly, and Orca found that 55% of organizations now manage two or more cloud providers, with nearly a third of all cloud assets sitting in a neglected state nobody is actively watching. Every new account, region, and managed service adds another place for a setting to drift out of policy, and most teams push hundreds of configuration changes a week.

Even where visibility exists, most CSPM tools reduce every finding to the same flat severity label. A database holding sensitive data gets flagged "High," the same as thousands of other findings that day. But look closer and the picture changes. That database is also

publicly exposed, and 38% of organizations with sensitive data in their databases have those databases exposed to the public. What looked like one more "High" alert is actually one of the riskiest findings in the environment, and a flat severity label never surfaces that. What's worse, findings like this often sit unresolved for months, with critical alerts averaging 128 days before anyone acts on them.

What teams need instead is unified visibility and context that connects exposure and identity into one picture, and that can speed up remediation inside the tools and workflows they already use.

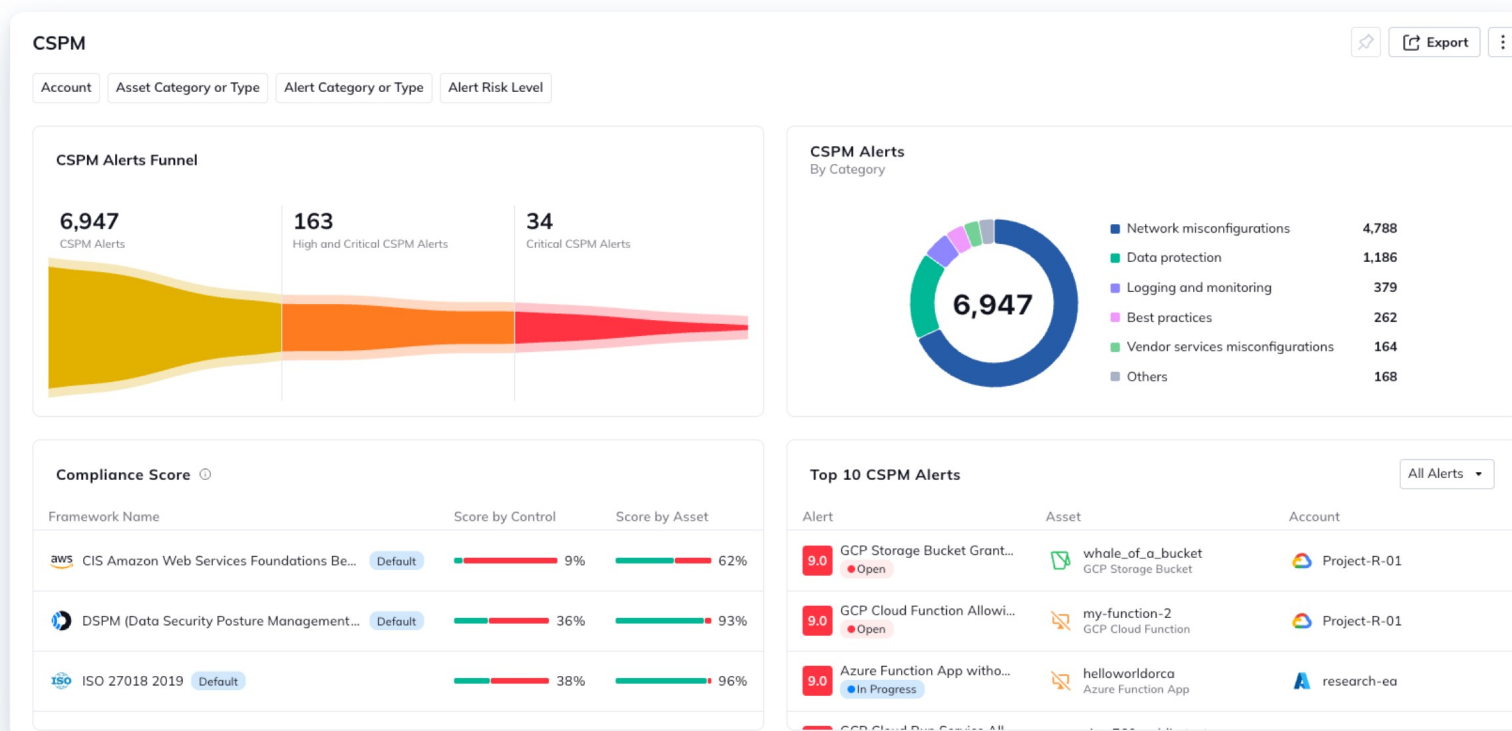
THE SOLUTION:

Visibility, Context, and Automation in One Platform

Orca's CSPM runs on the same agentless SideScanning™ technology and Unified Data Model that power the Orca Platform. Every misconfiguration is automatically connected to the identities that can reach it, the workload it sits on, and the data behind it, so posture findings arrive with an attack path attached instead of a checklist item.

- ✓ **Complete Visibility:** Every cloud account onboards and scans in as little as 15 minutes, agentlessly, with a real-time sensor available if desired, so nothing (idle, orphaned, paused, or stopped) goes unmonitored, and posture stays mapped to 200+ compliance frameworks automatically instead of scrambling before every audit.
- ✓ **Context That Powers Decisions:** Thousands of raw findings become a short, ranked list, because misconfigurations are automatically correlated with identity entitlements and network exposure to surface attack paths, like a public bucket paired with an over-permissioned role, so every finding carries real risk context instead of a static severity label.
- ✓ **Remediation That Closes the Gap:** Findings get step-by-step remediation guidance and route directly into the ticketing, SIEM, and CI/CD tools teams already use, with Workflow Automations and AI Agents handling routine triage and remediation for supported alert types to close that gap faster.





CAPABILITIES:

CSPM Capabilities

- Complete Coverage, Agentlessly:** Connects to AWS, Azure, Google Cloud, Oracle Cloud, Alibaba Cloud, and Tencent Cloud through patented SideScanning™ technology, onboarding in as little as 15 minutes to discover and monitor idle, orphaned, paused, and stopped assets that agent-based and API-only tools typically miss, with zero runtime performance impact on the workloads it scans. Each snapshot is scanned and deleted inside the customer's own cloud account, never shipped to Orca's infrastructure.
- Orca Sensor for Real-Time Detection:** An optional lightweight eBPF sensor adds real-time, in-workload detection on top of the agentless foundation, typically added for regulated workloads that require continuous runtime-level compliance, such as DISA STIG checks on government systems or PCI DSS environments handling cardholder data, and for mission-critical assets.
- Policy Assessment:** Evaluates every resource against 2,500+ out-of-the-box configuration controls, with support for fully custom policies and severity tuning to match internal risk tolerance.
- Compliance Mapping & Reporting:** Maps findings to 200+ pre-built and customizable compliance frameworks and benchmarks, including CIS Benchmarks for AWS, Azure, and Google Cloud, NIST 800-53, NIST CSF, PCI DSS, ISO 27001, HIPAA, FedRAMP, HITRUST, GDPR, and CCPA, with one-click export for audit-ready compliance reports.



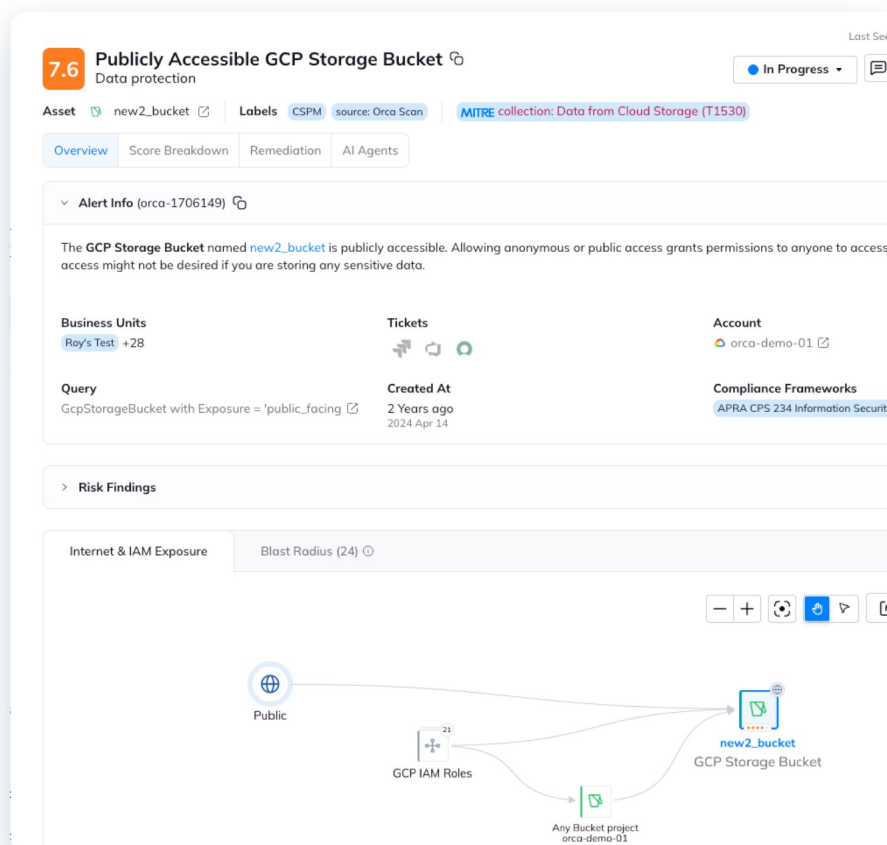
Visibility is a problem every organization has. Orca almost immediately gave us both wide and deep visibility into our threat landscape. When we take that data and show it to folks, their eyes open."

JEREMY TURNER

Senior Cloud Security Engineer, Paidy



- **Drift and Change Detection:** Ingests cloud provider audit logs, such as AWS CloudTrail, Azure Activity Log, and Google Cloud Audit Logs, to trigger rescans and update risk in near real time as configurations change, instead of waiting on the next scheduled scan.
- **Dynamic Risk Scoring:** Every finding's risk score updates in place as the environment changes, keeping a timeline of what changed, instead of the static severity label and “flicker effect” of tools that close and reopen alerts each time something shifts.
- **Attack Path Detection:** Correlates misconfigurations with IAM policies, effective permissions, and network exposure to surface attack paths, like a public bucket paired with an over-permissioned role, instead of listing each policy violation in isolation. Paths can be filtered by whether they cross accounts or cloud providers, and each is scored based on Probability Score (how easily the entry point can be exploited) and an Impact Score (the damage if it is), with the highest-impact path surfacing automatically instead of requiring a manual graph query.
- **Sensitive Data Discovery:** Automatically discovers sensitive data, such as PII, PHI, and PCI, across storage and databases, and flags it specifically when it sits on a viable attack path instead of just tagging that it exists.
- **Multi-Account and Organizational Governance:** Groups accounts and resources into Business Units by cloud provider, account, tag, or custom logic, so posture reporting and policy scope match how the organization is actually structured.



- **Pre-Deployment Policy-as-Code Scanning:** Scans Terraform and other IaC templates, plus container images, against the same policy set used in production, so a misconfiguration is caught in the pull request instead of becoming a live finding to remediate later.
- **Guided Remediation Recommendations:** Every finding comes with step-by-step remediation guidance mapped to its specific misconfiguration and context, so responders know exactly what to fix and how instead of starting from a blank runbook.



We turned [Orca] on. We thought it would take several hours, but it literally was within seconds. We had an overlay of: What is our current status? Which are the things that are noncompliant that we need to address right away?"

BENJAMIN GODARD

Head of Security, Spotnana



- **Automations and AI Agents:** Orca Automations trigger ticketing, notifications, and one-click remediation actions on defined rules, while Orca AI Agents can investigate alerts and generate ready-to-run remediation code, whether a CLI command or an IaC patch, then open a pull request or ticket for supported scenarios. An attack path's full detail, including its timeline and story, can also be pushed into a new Jira ticket in a single action.
- **Integrations:** Expansive integration capabilities include Jira, ServiceNow, Splunk, Slack, and GitHub, and span key categories such as Ticketing, Notifications, SIEM & SOAR, Identity & Access, GRC & Compliance, Storage, CI/CD & Endpoint, and AI & MCP, plus webhooks and a documented API.

ONE PLATFORM:

Part of a Complete Cloud, Code, and AI Security Platform

Orca's CSPM capabilities share the Orca Unified Data Model with the rest of the Orca Platform. Orca is sold as a single SKU, so Orca CSPM also includes the capabilities below, with no separate license or new integration required, delivering complete cloud, code, and AI visibility and context.

- | | | |
|----------------|--------|----------------------------|
| ✓ CIEM | ✓ CWPP | ✓ KSPM & Container |
| ✓ API Security | ✓ DSPM | ✓ AI Security |
| ✓ AppSec | ✓ EASM | ✓ Vulnerability Management |
| ✓ CDR | | |



Previous experience with CSPM tools clarified our requirements and processes needed to make the best use of these tools. Orca more than meets the challenge."

GIORGIO ROCCA
CISO, Banca Progetto

About Orca

Orca Security delivers security for the companies that build. As cloud, applications, AI, and app generation expand the attack surface, Orca transforms security risk into the context teams need to act. The Orca Platform provides complete visibility across cloud, AI, and application environments, correlates risk across every layer, and prioritizes the exposures that matter most so organizations can remediate faster and innovate with confidence. Trusted by hundreds of organizations, including SAP, Autodesk, Gannett, Lemonade, and Digital Turbine, Orca is backed by leading investors including Temasek, CapitalG, ICONIQ Capital, and Redpoint Ventures. Learn more and connect your first account in minutes at orca.security, or book a personalized demo.



Ready to try it out?

Sign up for a demo. Visit orca.security/demo

