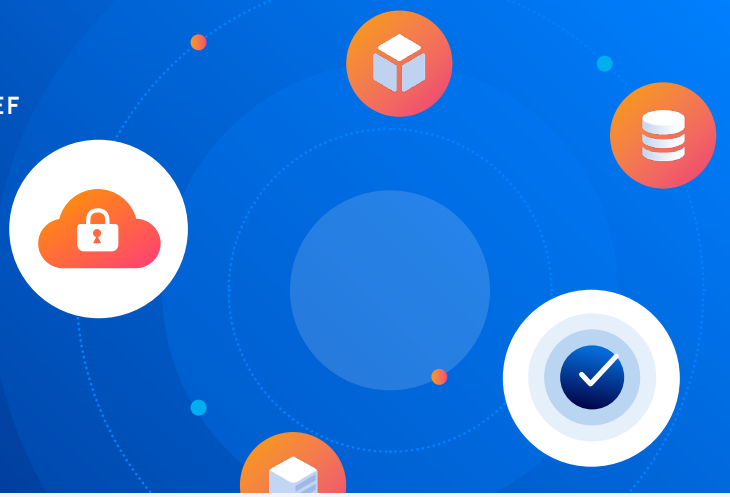
orca security PagerDuty JOINT SOLUTION BRIEF

Agentless Security at the Speed of the Cloud



DevOps programs are under a ton of pressure to release new code to the cloud at scale with little to no delay. These continuous deployments require friction-free monitoring, alerting, and remediation to achieve the program improvements necessary to reach the desired business outcomes.

Orca Security allows DevOps teams to build and release software quickly while enabling security teams increased visibility into projects and the software build process to measure and mitigate risk. Orca's combined agentless visibility and unified data model provide complete and context-rich security, and is your best ally in building trust in your alerts as they are transferred to PagerDuty.

As PagerDuty ingests Orca Security alerts, it brings major incident best practices to your organization, empowering DevOps teams with sophisticated end-to-end response automation that quickly and accurately orchestrates the proper response, every time.

By combining the power of Orca Security and PagerDuty, DevOps and security teams can effectively collaborate to detect, prioritize, notify, and accurately remediate cloud security risks in minutes - not months.

Resolve Cloud Risks Efficiently with Orca Security + PagerDuty

Key benefits of the joint solution:

100% COVERAGE

- Continuously monitor the entire cloud estate for security and compliance risks and send prioritized alerts to PagerDuty – all without agents.
- The zero-touch approach to cloud security provides **100% visibility and coverage** to replace multiple security tools.
- Monitor for vulnerabilities, malware, misconfigurations, lateral movement risk, weak or leaked passwords, overly permissive identities, and more.

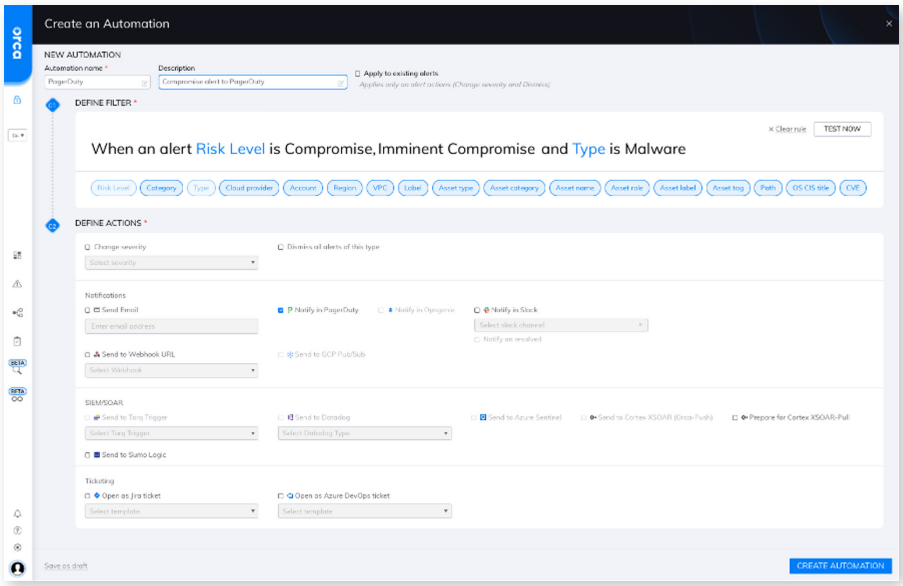
ALERTS THAT MATTER

- Orca considers the **environmental context** of each risk, and surfaces the most critical alerts, eliminating 99% of the noise.
- Alerts created in PagerDuty with different priorities based on **contextual risk analysis** from Orca.

SIMPLIFIED RESPONSE

- Alerts include their **precise path to remediation** for quick, effective resolution by the DevOps team.
- Integrated workflows can be used to **immediately assign issues** to the appropriate teams to improve efficiency, speed up risk remediation, and achieve better ROI.

Unlike other solutions that operate in silos, Orca leverages its full coverage capabilities to provide full comprehension of your entire AWS, Azure, and Google Cloud estates. Combining all your cloud assets, software, connectivity, and trusted entitlements into a single, unified data model, enables Orca to prioritize risks based on the severity of the underlying security issue, its accessibility, and business impact. This approach helps security teams focus on the 1% of critical issues that matter most.



Built-in Compliance

Closed-loop alert management maintains continuous compliance with PCI-DSS, SOC 2, GDPR, NIST, HIPAA, and more.

Get agentless cloud security and compliance for AWS, Azure, Google Cloud, and Kubernetes – in a fraction of the time and operational costs of other solutions.

COMBINED FEATURES	BENEFITS
Notify on-call responders based on alerts sent from Orca	Mobilize the right cross-functional team in seconds to ensure product delivery timeframes remain on track
Create alerts of different severity based on contextual intelligence from Orca	Protect sensitive data, critical applications, and improve customer experiences by resolving critical incidents faster
Alerts in PagerDuty will be resolved and confirmed by Orca, automatically.	Closed-loop remediation helps teams remain operationally efficient and stay within the security, risk, and compliance parameters prescribed by the business

How it works

Whenever automation query rules are met, Orca Security can send the resulting alerts to PagerDuty.

- Orca Security scans your cloud configurations, workloads, and threat activity continuously; risks that are identified get prioritized and send an event to the receiving service in PagerDuty
- Alerts received from Orca Security will trigger a new incident on the corresponding PagerDuty service where the defined incident routing and orchestration will take place.
- Once the issue has been remediated and acknowledged in Orca, a resolution event will be sent to the PagerDuty service to resolve the alert and associated incident on that service.

Connecting PagerDuty to Orca Security

1. Start with PagerDuty
2. Add Orca integration to PagerDuty by creating or selecting an existing service
3. Retrieve your integration key
4. Switch to Orca Security
5. Locate the PagerDuty integration and select Connect
6. Enter your PagerDuty integration key
7. Configure the automation rules

orca security

PagerDuty

Connect your first cloud account in minutes and see for yourself at: https://orca.security