JOINT SOLUTION BRIEF

Accelerate Response & Remediation for Cloud Security Alerts

Security and DevOps teams must be closely aligned if they're going to optimize the cloud's speed and agility without putting assets at risk. Working together to identify, understand, and respond to security alerts quickly and accurately is critical to reducing security risk in the cloud. This is no small task, but automation can help.

Combining the power of Orca and Torq eliminates silos between security and DevOps teams, standardizes cloud security operations, and accelerates alert response and remediation. With Orca and Torq, organizations can address more risks, and do so faster - delivering significant overall improvements to their cloud security posture.

Deliver accelerated response and remediation, increase efficiency, and improve your cloud security posture with Orca and Torq's end-to-end automation for critical AWS, Azure, and Google Cloud security alerts.

Key benefits of the joint solution:

1. Improve **EFFICIENCY** by automatically routing cloud security alerts to the appropriate teams responsible for responding.
2. Increase **PRODUCTIVITY** by enabling single-click, suggested action buttons embedded within each alert; allowing teams to respond directly within the chat and messaging platforms they are already working in.
3. Reduce **RISK** exposure by reducing the mean time to respond (MTTR) to alerts.

Reduce your cloud security risk exposure with improved security operations by utilizing these combined solutions:

COMBINED FEATURES	BENEFITS
Distribute alerts to teams that are responsible for fixing	Reduce alert fatigue and noise to keep teams focused
Supply context-rich alerts directly within ticketing, SIEM, SOAR, or messaging/chat applications	Reduce the time required to comprehend critical alerts or the need to login to multiple software applications
Recommended semi-autonomous (single-click) or fully autonomous remediation buttons for resolving detected alerts	Reduce MTTR, human-error, and enforce consistency in remediation processes
Built-in response and recommended remediation templates for common cloud security alerts	Reduce configuration time and the need for scripting or API knowledge

Orca + Torq: Use Cases

Distributed Alerting: Connect Orca's findings to the tools the enterprise already uses.

With Torq, the Orca Security Platform connects to ticketing, workflow, SIEM, and messaging applications to distribute critical alerts to the tools cloud teams use. These notifications can be customized to alert only the teams/channels responsible for managing that cloud environment and responding to that specific alert.

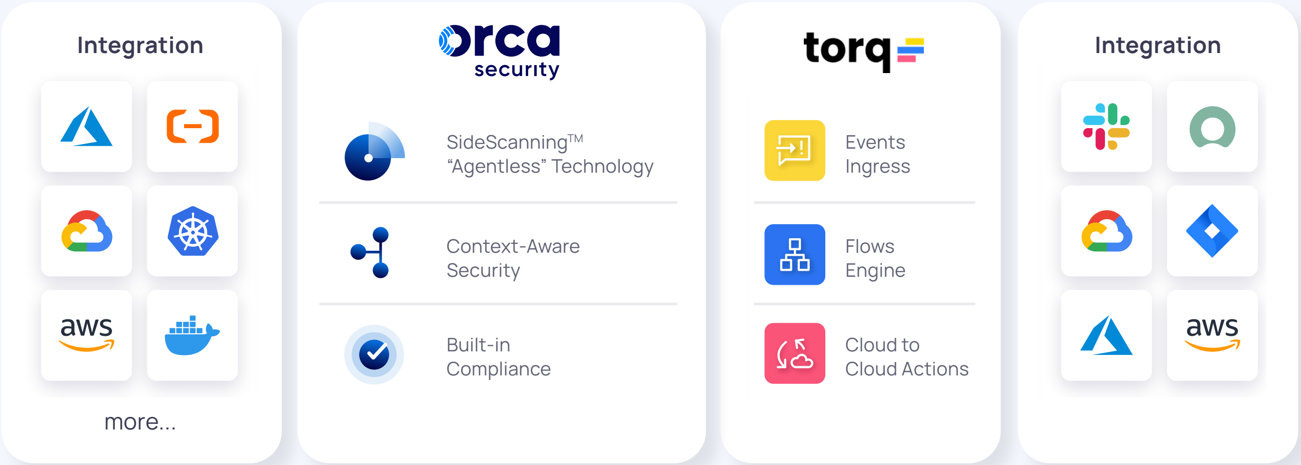
Recommended Action Buttons: Deploy single-click or semi-automatic recommended remediation buttons directly within the distributed alert for fast, convenient, and accurate remediations.

Build powerful automations that route alerts to teams who are responsible for responding; while educating those responders with the recommended cloud security best practices to resolve. Orca sends the full context of the issue, along with optional programmed remediation buttons that are designed to take action without having to leave the alert or messaging platform.

Establish Guardrails: Autonomous Remediations

Enable fully automated remediations for frequent policy violations where only one remediation path is preferred. Resolve misconfigurations and security threats automatically from the Orca Platform. Select from a library of out-of-the-box automated remediation rules, or fully customize your own workflows to auto-enforce cloud security compliance.

How Orca + Torq Work Together



Integration

more...

SideScanning™ "Agentless" Technology

Context-Aware Security

Built-in Compliance

Events Ingress

Flows Engine

Cloud to Cloud Actions

Integration

1. Connect Orca Security Platform to your cloud environments in <5 minutes.
2. The Orca Security Platform automatically and continuously scans for misconfigurations and potential hazardous threats lurking within your cloud environments; notifying with prioritization and mission critical context.
3. Use built-in workflow templates or build your own automated responses to key alerts.
4. Connect Torq to messaging platforms and CSPs for alert distribution and remediation control.

Orca + Torq Scenarios

Example 1: Rotating AWS IAM Access Keys

Orca detects an AWS IAM Key that has not been rotated within the recommended 30 days within an AWS production account. An alert is triggered and a Torq workflow is initiated. Torq registers the specific alert, and forwards the context of that alert to the #PROD-AWS-IAM Slack channel, notifying the specific team members responsible for that environment. The alert surfaces within the channel feed with four preconfigured button choices; Rotate Keys, Investigate, Create a Jira Ticket, Ignore. A member of the channel selects “Rotate Keys,” and a new IAM access key ID for that user is assigned while deactivating the old one. The Slack channel is communicated with an automated message that confirms the rotation of that user’s IAM key, and the alert is logged as resolved within Orca’s Security Platform.

Example 2: Azure Privileged User MFA Disabled

Orca detects a privileged user within Azure Account-Staging1 that has MFA disabled. Using Torq, MFA is automatically enabled for all privileged users within Azure Account-Staging1. Torq recognizes the Orca alert, automatically creates a Jira ticket, enables MFA on the privileged user, returns to comment and close the Jira ticket created (for logging purposes), and notifies the Microsoft Teams #Staging-Azure1 channel that an automated MFA remediation was applied for the specific user.

Connect your first cloud account in minutes and see for yourself.

Visit https://orca.security

Connect your Orca Security account to Torq today and receive your first 3 automation workflows free!

Visit https:torq.io

WHY Orca Security

Orca Security, the cloud security innovation leader, provides cloud-wide, workload-deep security and compliance for AWS, Azure, and Google Cloud — without the gaps in coverage, alert fatigue, and operational costs of agents.

Find critical attack vectors before your adversaries without having to cobble together disparate tools for cloud security posture management, compliance assessments, and workload and data protection. Delivered as SaaS, Orca Security’s patent-pending SideScanning™ technology reads your cloud configuration and workloads’ runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and unsecured PII. SideScanning™ covers all your workloads-VMs, containers, and serverless.

WHY Torq

Torq’s no-code automation platform modernizes how security and operations teams work with easy workflow building, limitless integrations, and numerous pre-built templates.

At Torq, we understand the challenges facing front line security teams, who are often overwhelmed as the number of security events continues to rise within increasingly complex environments.

Our platform helps front line teams and CISOs by delivering lightweight, modern security automation that is easily integrated with their existing tools set, and flexible enough to seamlessly scale as organizations’ needs change.

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