TECHNICAL BRIEF

Orca Automation and Customization

Get actionable intelligence in front of the right teams at the right time

Executive Summary

As organizations increasingly rely on the cloud for their business critical applications, security becomes paramount. However, security cannot become a roadblock to innovation. Today's cloud security teams are struggling with data overload and inefficient workflows. An abundance of cloud security data is available, but it is difficult to consume and act on. This leads to inefficient workflows between security, DevOps, and IT, resulting in organizational friction and critical alerts being missed.

Orca's Automation & Customization feature solves this problem by allowing you to prioritize, customize, and integrate alerts into your existing workflows to expedite remediation, improve efficiency, and increase ROI.

IDC

Analyst firm IDC recommends:
"Use automation in the right place to handle the high volume of data to help analysts devote more effort to higher-value activities."

The Orca Security Platform includes three core Automation & Customization capabilities: advanced querying, alerting, and automation.

Orca empowers security teams to quickly and easily:

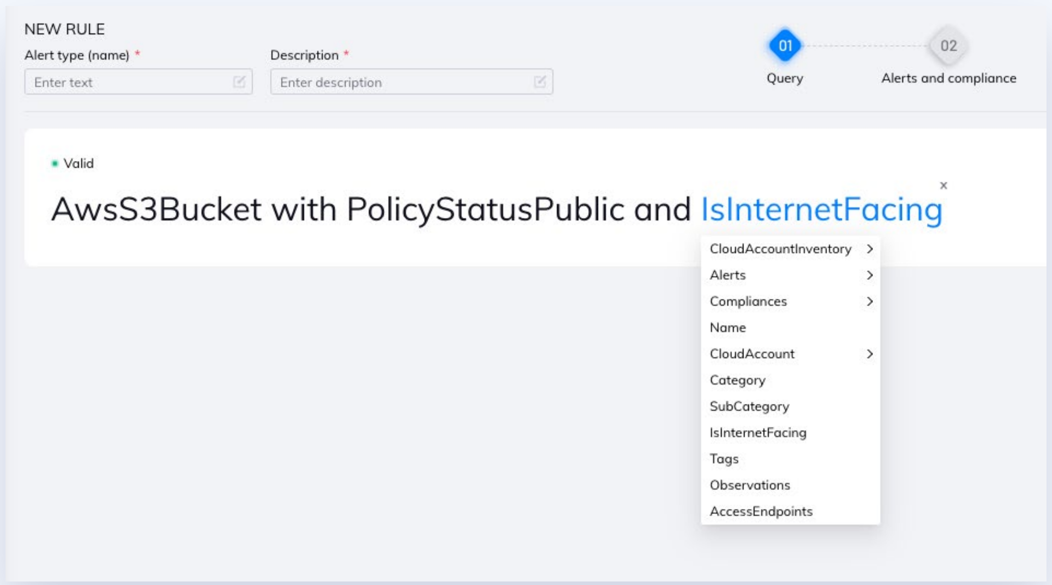
- Query data to filter or search for assets
- Search and investigate security issues using out-of-the-box and custom queries
- Monitor and receive alerts on compliance and standards violations, and other security issues
- Create groups for issues and assets, enabling easy assignment to security, IT, and DevOps teams for remediation
- Automate ticketing with Orca's partner integrations

Orca's Automation and Customization Capabilities

Orca enables security teams to query data to find, investigate, and understand cloud security issues. Queries can be run as one-offs or set up as custom alerts for monitoring. They can also be coupled with Orca's automation capabilities to create highly efficient CI/CD and remediation workflows. These queries allow security teams to create granular alerts that close the gap between security and DevOps/IT teams by automatically routing alerts to the correct team members.

In addition to writing custom alert queries, security teams can leverage over 600 out-of-the-box system queries. These modular building blocks can be combined in limitless ways using Orca's simple, yet expressive query language. System queries also include compliance control rules for the over 35 compliance frameworks and benchmarks that Orca supports, including NIST CSF, NIST 800-53, SOC 2, HIPAA, AWS CIS, Azure CIS, GCP CIS, Windows CIS, Docker CIS, PCI DSS, Orca Best Practices,

and more.



NEW RULE

Alert type (name) * Enter text

Description * Enter description

Valid

AwsS3Bucket with PolicyStatusPublic and IsInternetFacing

FIGURE 1: An example of Orca's Automation & Cutomization query builder and a custom alert query

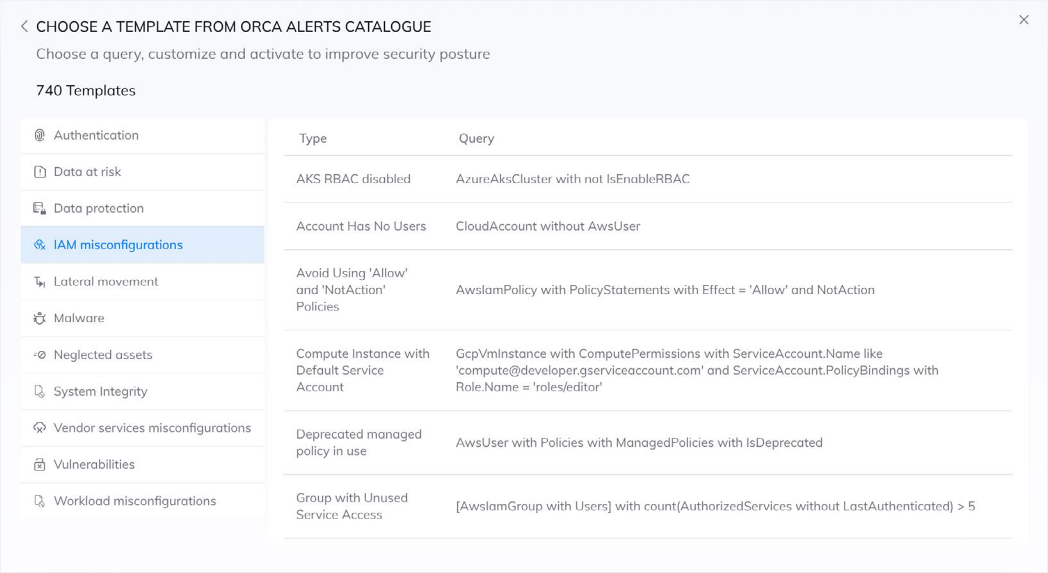
Easy Creation of Queries and Alerts

Orca leverages a Domain Specific Language that enables users to create powerful contextual queries. Orca's simple "<subject> with <condition>" format allows users to easily create custom queries and alerts without any development experience. As users write a query, the query builder tests and validates rules and displays available attributes and commands to assist the user. Here are three examples that demonstrate the simplicity and expressive capabilities of Orca's query language:

`AwsS3bucket with isinternetfacing`	Finds all AWS S3 buckets that are exposed to the Internet.	Example of the simplicity of the query language.
`AwsEc2Instance with Ec2EbsVolumes with Encrypted = false`	Finds all AWS instances that have volumes that are not encrypted.	Another example of a simple, yet powerful query.
`AwsLambdaFunction with (FunctionRole.ManagedPolicy with PolicyStatements with Action containing ‘*’ and Resource containing ‘*’) or (FunctionRole.Policies with PolicyStatements with Action containing ‘*’ and Resource containing ‘*’)`	Finds all AWS Lambda functions that have admin privileges.	Shows the use of grouping using parentheses and the use of logical operators like 'and' and 'or'.

FIGURE 2: Orca Security query language examples

Orca's search functionality includes numerous pre-built query templates and allows users to save queries in a library for reuse. Alerts can be created from queries, providing security, IT, and DevOps teams with limitless monitoring possibilities. And because every compliance control included in Orca's more than 35 supported compliance benchmarks is available in the Orca query language, continuous compliance monitoring is easy to configure and implement.



CHOOSE A TEMPLATE FROM ORCA ALERTS CATALOGUE

Choose a query, customize and activate to improve security posture

740 Templates

Type	Query
AKS RBAC disabled	AzureAksCluster with not IsEnableRBAC
Account Has No Users	CloudAccount without AwsUser
Avoid Using 'Allow' and 'NotAction' Policies	AwsIamPolicy with PolicyStatements with Effect = 'Allow' and NotAction
Compute Instance with Default Service Account	GcpVmInstance with ComputePermissions with ServiceAccount.Name like 'compute@developer.gserviceaccount.com' and ServiceAccount.PolicyBindings with Role.Name = 'roles/editor'
Deprecated managed policy in use	AwsUser with Policies with ManagedPolicies with IsDeprecated
Group with Unused Service Access	[AwsIamGroup with Users] with count(AuthorizedServices without LastAuthenticated) > 5

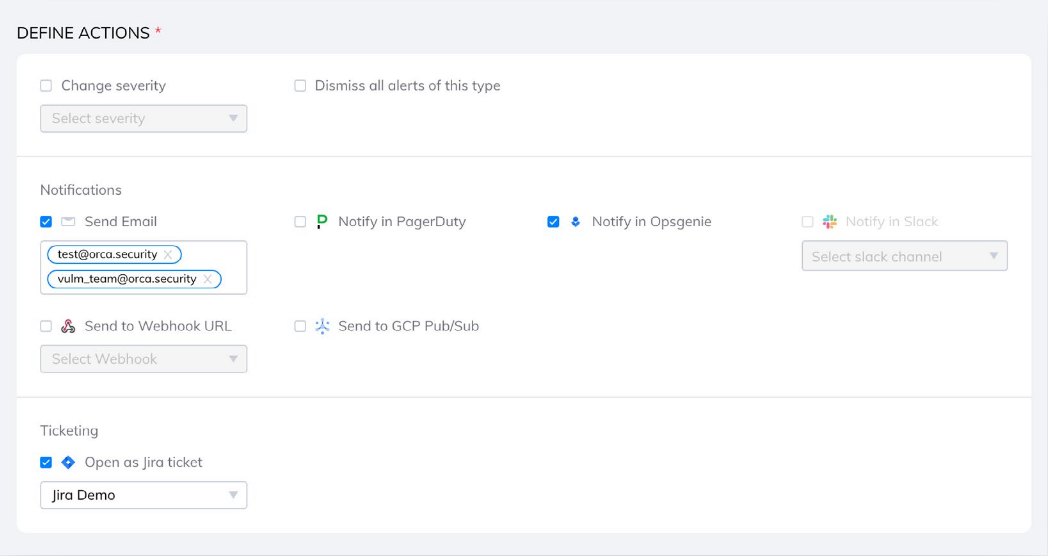
FIGURE 3: Orca Security query templates

By creating queries and using customizable query templates you can create groups of security issues that define tasks that need to be worked on. Rich contextual information is provided with query results to allow remediation teams to operate independently and efficiently.

Automation and Ticketing

Orca can take a query result and automatically send them as as an alert to email, PagerDuty, OpsGenie, Slack, Webhook, or Google Pub/Sub and perform automated ticketing with Jira or ServiceNow.

All functionality is fully supported in Orca's API, which allows for automation integration into your CI/CD and remediation workflows. When using Orca's auto-ticketing functionality, the full context of the issue is populated into the ticket allowing the user to quickly understand the nature of the issue, its criticality, and how to remediate it.



DEFINE ACTIONS *

□ Change severity

Select severity ▾

□ Dismiss all alerts of this type

Notifications

☑ Send Email

test@orca.security ×

vulm_team@orca.security ×

□ Notify in PagerDuty

☑ Notify in Opsgenie

□ Notify in Slack

Select slack channel ▾

□ Send to Webhook URL

Select Webhook ▾

□ Send to GCP Pub/Sub

Ticketing

☑ Open as Jira ticket

Jira Demo ▾

FIGURE 4: An example of Orca's automation configuration options

Automation works by specifying triggers and then assigning an action when the trigger conditions are fulfilled. Available actions include:

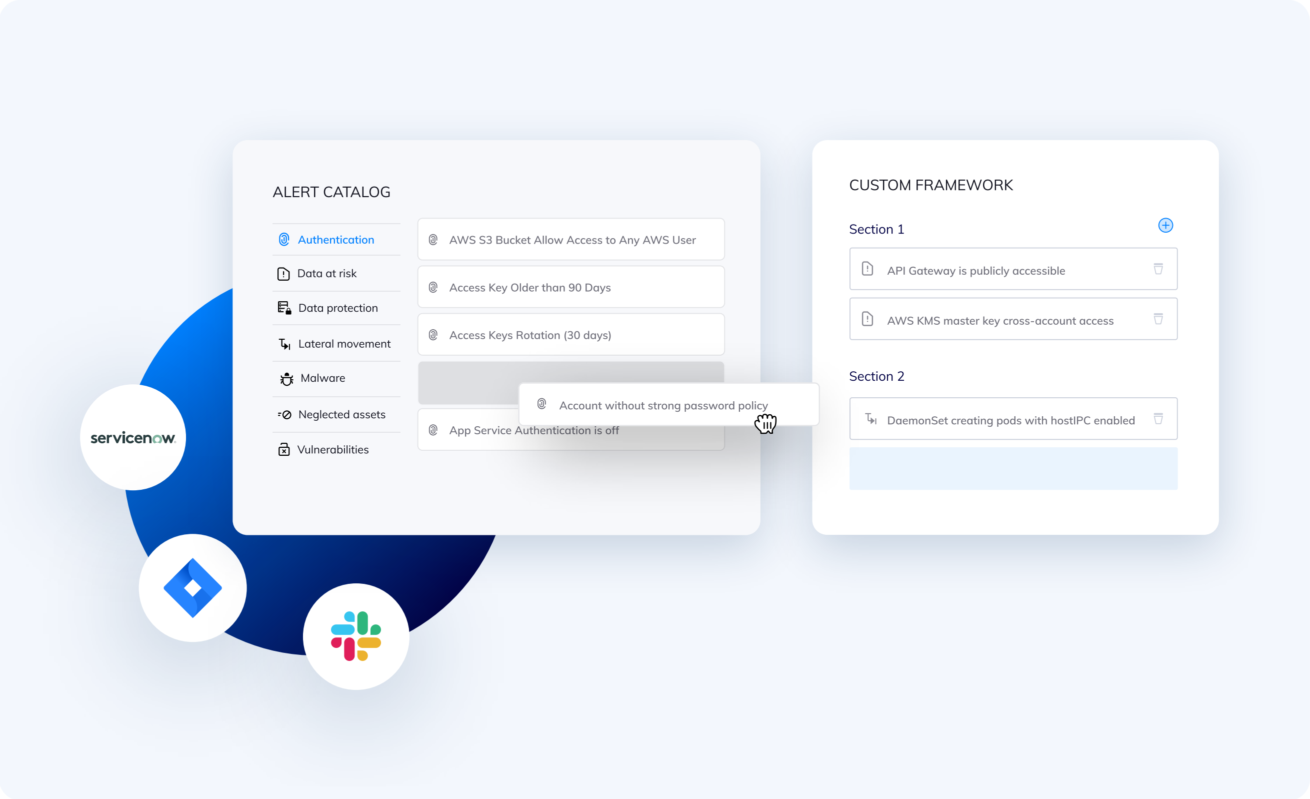
- Change the severity of an alert
- Notifications (email, PagerDuty, OpsGenie, Slack, Webhook, and Google Pub/Sub)
- Ticketing (Jira and ServiceNow)

Using Orca's API, any action can be fully implemented programmatically to support the most complicated CI/CD pipeline and remediation automation requirements.

Continuous Compliance

Orca includes a comprehensive set of queries that map directly to compliance controls. These out-of-the-box templates are available for over 35 supported compliance frameworks and benchmarks, including NIST CSF, NIST 800-53, SOC 2, HIPAA, GDPR, AWS CIS, Azure CIS, GCP CIS, Windows CIS, Docker CIS, PCI DSS, Orca Best Practices, and more.

Users can customize compliance benchmarks by adding, deleting, and modifying controls. Every compliance benchmark can be leveraged as a query, which can be configured to trigger an alert to notify the appropriate individual(s) when a compliance violation occurs. When a control rule fails, the alert indicates all the locations where the control failed.



ALERT CATALOG

- Authentication
- Data at risk
- Data protection
- Lateral movement
- Malware
- Neglected assets
- Vulnerabilities

- AWS S3 Bucket Allow Access to Any AWS User
- Access Key Older than 90 Days
- Access Keys Rotation (30 days)
- Account without strong password policy
- App Service Authentication is off

CUSTOM FRAMEWORK

Section 1

- API Gateway is publicly accessible
- AWS KMS master key cross-account access

Section 2

- DaemonSet creating pods with hostIPC enabled

FIGURE 5: Customize Orca Security compliance benchmarks

Key Benefits

- **Quickly explore data and investigate issues:** Query your entire cloud asset inventory to easily explore, discover, and investigate issues. Find exactly what you're looking for, whether it be all internet-facing assets with a certain vulnerability (CVE), or all internet-facing workloads running a specific version of the sudo package.
- **Receive alerts on security policy violations:** Set up customized alerts to be notified when cloud developers violate internal security policies.
- **Enhance security effectiveness:** Rich contextual information is provided with alerts to allow remediation teams to operate independently and efficiently.
- **Make everyone a cloud security expert:** With Orca's user-friendly interface and query language, anyone can query their asset data and create custom alerts—no development experience required.
- **Improve efficiencies with automated workflows:** All Automation and Customization capabilities are fully supported by Orca's API, allowing you to achieve full integration into your CI/CD pipeline and remediation workflows to include out-of-the box support for auto-ticketing.
- **Realize instant time to value:** More than 600 system query rules are available out-of-the-box. They can be saved as templates, which can then be modified and reused.
- **Ensure continuous compliance:** Continuously monitor and trigger alerts on any supported compliance control. Pre-written queries exist for more than 35 compliance frameworks and benchmarks supported by Orca. These compliance query templates can be used out-of-the-box, or customized to your needs.

orca security

About Orca Security

Orca Security provides instant-on security and compliance for AWS, Azure, and GCP—without the gaps in coverage, alert fatigue, and operational costs of agents. Simplify security operations with a single SaaS platform for cloud security posture management, compliance management, and workload and data protection. Orca Security prioritizes risk based on the severity of the security issue, its accessibility, and business impact. This helps you focus on the critical alerts that matter most. Orca Security is trusted by global innovators, including Databricks, Lemonade, Gannett, and Robinhood. Connect your first cloud account in minutes. Visit orca.security.

Trusted by Organizations Across the Globe

fiverr. Lemonade unity BeyondTrust

LiveOakBank. databricks druva GANNETT

Robinhood Fyber Rapyd paidy

AUTODESK. News Corp duolingo carta