DATASHEET

orca security

Generative AI-Driven Cloud Security for AWS with Orca Security & Amazon Bedrock

Orca Security's AI, generative AI, and LLM capabilities serve as a 'security co-pilot' to simplify cloud security operations

aws PARTNER

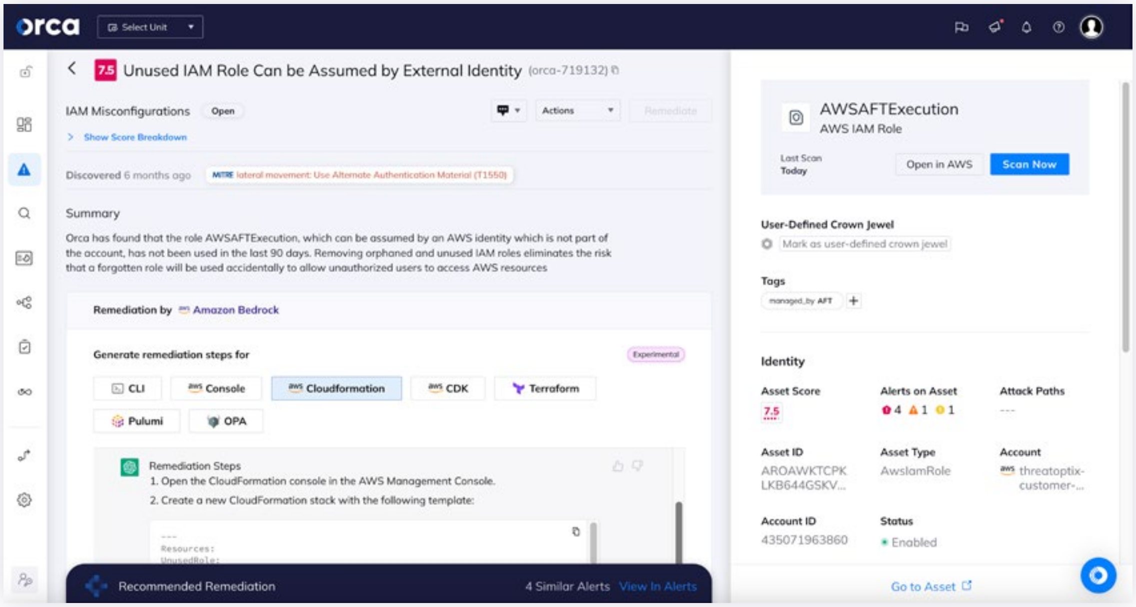
2022 Global Security Partner of the Year

The challenge

While short-staffed cloud security teams receive hundreds of alerts each day that require investigation, remediation, and response, they often have to rely on cloud security tools that are challenging to operationalize. This can result in burnout and turnover with cloud security falling behind and the potential of critical alerts being missed.

How Orca's generative AI-driven cloud security helps

Orca is at the forefront of leveraging AI, generative AI, and LLMs to augment cloud security operations. Orca's [AI-Driven Cloud Security Platform](#) lowers required skill thresholds, simplifies tasks, accelerates remediation, and uses AI to calculate optimal cloud configurations, thus dramatically alleviating daily workloads and burnout, and significantly improving cloud security posture.



7.5 Unused IAM Role Can be Assumed by External Identity (orca-719132)

IAM Misconfigurations Open

Discovered 6 months ago MITRE lateral movement: Use Alternate Authentication Material (T1550)

Summary

Orca has found that the role AWSAFTExecution, which can be assumed by an AWS identity which is not part of the account, has not been used in the last 90 days. Removing orphaned and unused IAM roles eliminates the risk that a forgotten role will be used accidentally to allow unauthorized users to access AWS resources

Remediation by Amazon Bedrock

Generate remediation steps for

Remediation Steps

1. Open the CloudFormation console in the AWS Management Console.
2. Create a new CloudFormation stack with the following template:

```
---
Resources:
UnusedRole:
```

AWSAFTExecution
AWS IAM Role

Last Scan
Today

User-Defined Crown Jewel

Tags

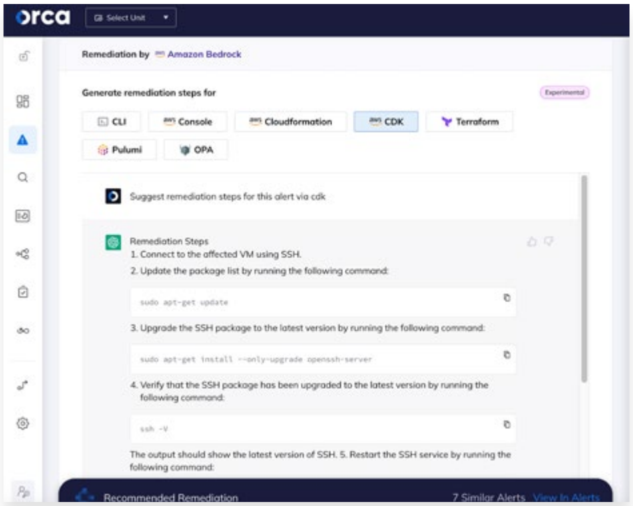
Identity

Asset Score	Alerts on Asset	Attack Paths
7.5	4 ▲1 1	---
Asset ID	**Asset Type**	**Account**
AROAWKTCPK LKB644GSKV...	AwsIamRole	threatoptix-customer-...
Account ID	**Status**	
435071963860	● Enabled	

Orca alerts on an overprivileged IAM Role and provides ready-to-use AI-generated remediation code

Accelerate remediation with Orca and Amazon Bedrock

Orca leverages Amazon Bedrock to deliver turnkey remediations for each cloud risk that the Orca platform detects. Orca feeds the cloud security alert data to Amazon Bedrock, including information about the risk and its contextual environment such as affected assets, attack vectors, and potential impact. Amazon Bedrock then generates instructions and code that can be followed in the console or copied and pasted into a command line interface or Infrastructure as Code (IaC) provisioning tool. To ensure privacy, all requests to Amazon Bedrock are anonymized, and any sensitive information is removed or masked before submitting.



Remediation by Amazon Bedrock

Generate remediation steps for

Suggest remediation steps for this alert via cdk

Remediation Steps
1. Connect to the affected VM using SSH.
2. Update the package list by running the following command:

```
sudo apt-get update
```

3. Upgrade the SSH package to the latest version by running the following command:

```
sudo apt-get install --only-upgrade openssh-server
```

4. Verify that the SSH package has been upgraded to the latest version by running the following command:

```
ssh -V
```

The output should show the latest version of SSH. 5. Restart the SSH service by running the following command:

Supercharge your cloud security operations with Orca

- ✓ Help your security team increase productivity, reduce burnout, and improve cloud security.
- ✓ Allow teams across the organization, regardless of their skill level, to benefit from Orca's cloud insights and improve decision making.
- ✓ Simplify and accelerate responding to zero-day risks, performing audits, optimizing cloud assets, and understanding exposure to threats.

About the Orca Platform

The Orca Cloud Security Platform is trusted by hundreds of organizations and identifies, prioritizes, and remediates risks and compliance issues across your AWS cloud estate - without requiring a single agent. Orca deploys in minutes, and detects vulnerabilities, malware, misconfigurations, lateral movement, API risks, sensitive data at risk, anomalous events and behaviors, overly permissive identities, and more.

Orca Security is available on AWS Marketplace. Learn more at https://orca.security.

Connect your first cloud account in minutes
See why so many Orca customers rave about our platform.
Visit orca.security/demo