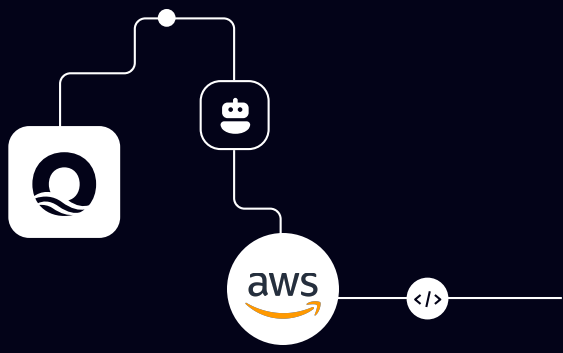
Oasis for AWS



Understanding NHIs in AWS

Identity

IAM User

Entity - human or workload - that interacts with AWS resources

RDS User

Database user account within a specific database instance.

Authentication Method

Access keys

Long-term credentials for an IAM user or the AWS account root user. Such access can be stored in the native AWS vault or not.

Scanned secrets

Plain text credentials stored in AWS Services not properly stored

Role Assumed post authentication method

An identity in AWS with specific permissions can be temporarily assumed by authorized entities, such as IAM users, applications, or services, enabling secure, temporary access to resources. These permissions can only be assumed after the identity has been authenticated in AWS.

Why is managing NHIs in AWS so challenging?

AWS empowers enterprises with unparalleled cloud capabilities, but its complexity can lead to critical security gaps:

Lack Of Centralization & Context

AWS lacks a unified source across accounts & does not provide the necessary context to understand their roles and associated risks.

Generic Insights

AWS tools offer generic insights but lack risk factors context and actionable recommendations.

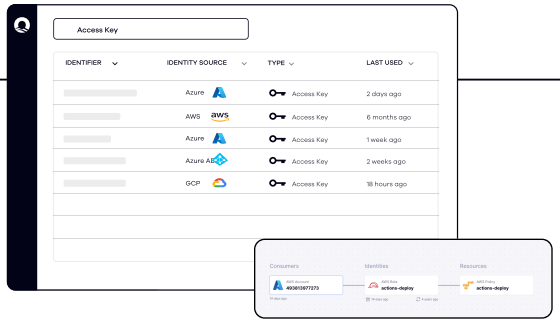
Cross-integration Visibility

Visibility is siloed between AWS & integrations with SaaS and PaaS environments, making holistic security management more complex.

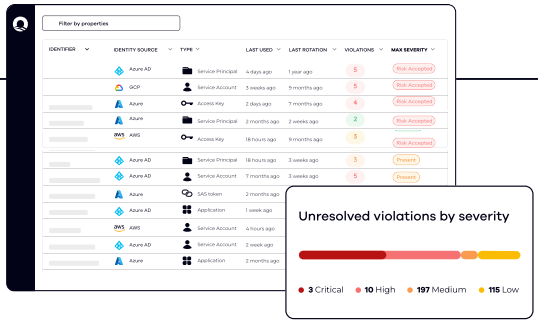
Manual Configurations

AWS setups often demand high technical expertise, leading to increased risks from misconfigurations & oversights.

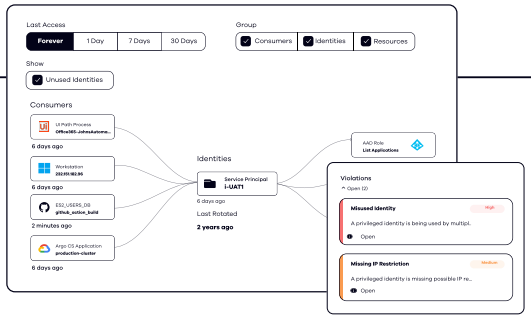
Oasis NHI Security Cloud



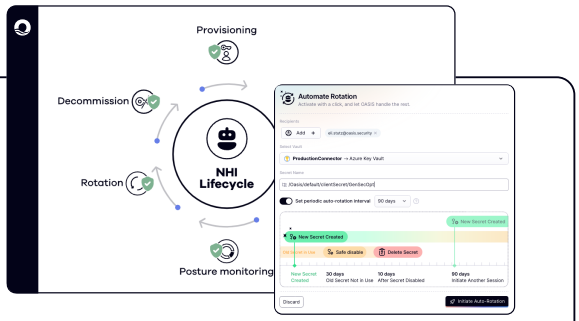
Inventory
Identifies IAM users, roles, and access keys across AWS accounts. Provides a consolidated, real-time view in minutes, enabling better control and governance.



Security Posture And Risk Detection
Prioritizes risks by severity: excessive access, stale users & roles, and unrotated access keys. Offers both preventive security and threat detection capabilities (ITDR).



Context & Ownership
Adds depth to raw data by mapping ownership, usage, resource and privileges. Helps organizations understand "who" or "what" is responsible for each identity.



Lifecycle Management
Automates AWS access key rotation, and decommissioning of stale users & roles. Ensures NHIs stay compliant with policies driven by business justification thorough attestation campaigns

> The challenges of managing AWS NHI are more operational than technical. With Oasis, we've seen up to a 90% increase in operational efficiency, enhanced reliability, and significant reductions in risk exposure by automating the discovery, ownership, and safe rotation of credentials. **It's not just about compliance; it's about securing cloud operations without disrupting them.**
>
> Chief Information Security Officer

Ready to secure your AWS environment?
Contact us at sales@oasis.security or
visit our website at oasis.security