OASIS Solution Brief

Manage and Secure All Non-human Identities

The Challenge

Despite the critical nature of non-human identities, most organizations struggle to manage them effectively due to a lack of suitable technology. Oasis Security steps in to bridge the gap between development, operations (DevOps), and security, providing a comprehensive platform to control the lifecycle of Non-Human Identities.

What are Non Human Identities

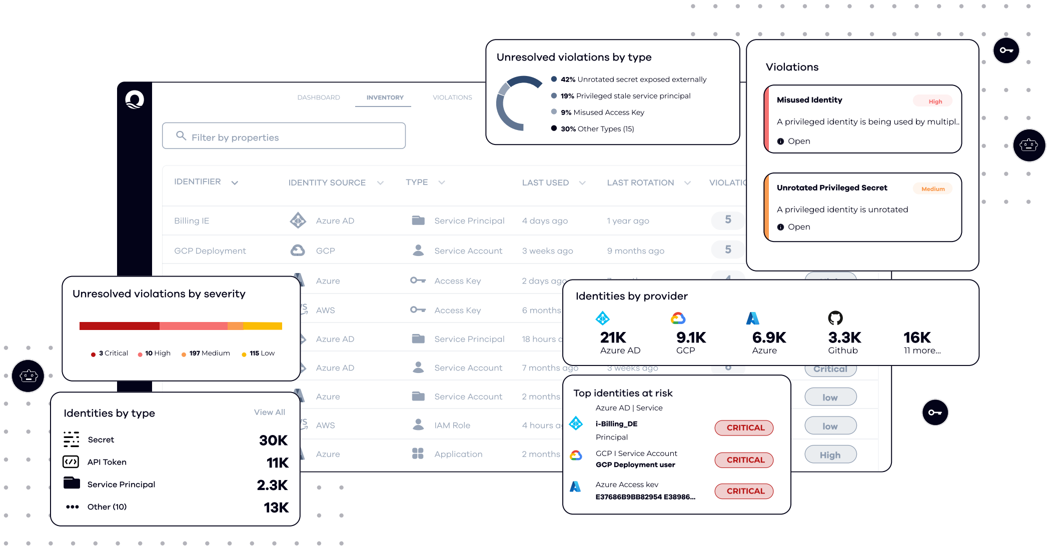
- Service Principals
- Service Accounts
- Storage Accounts
- System Accounts
- IAM Users
- IAM Roles
- API Keys
- Secrets
- Tokens
- Certificates
- RDS Users
- Vaults

Non-human identities are different

Human		Non-human
Slow moving	vs.	Lightning-fast proliferation
Centralized	vs.	Decentralized
small percentage of privileged accounts	vs.	Mainly privileged
Created by both developers and systems	vs.	Created by identity team
Structured identity lifecycle management (ILM)	vs.	**Sparse management (no ILM)**

The Solution

Oasis Security introduces the industry's first Non-Human Identity Management platform designed to secure the complete lifecycle of Non-Human Identities. Through continuous analysis of the environment, Oasis identifies, classifies, and resolves security posture risks associated with all non-human identities.



IDENTIFIER	IDENTITY SOURCE	TYPE	LAST USED	LAST ROTATION	VIOLATIC	
Billing IE	Azure AD	Service Principal	4 days ago	1 year ago	5	
GCP Deployment	GCP	Service Account	3 weeks ago	9 months ago	5	
	Azure	Access Key	2 days ago			
	AWS	Access Key	6 months			
	Azure AD	Service Principal	18 hours			
	Azure AD	Service Account	7 months ago	3 weeks ago		Critical
	Azure	Service Account	2 months			low
	AWS	IAM Role	4 hours			low
	Azure	Application	2 months			High

Unresolved violations by type
- **42%** Unrotated secret exposed externally
- **19%** Privileged stale service principal
- **9%** Misused Access Key
- **30%** Other Types (15)

Violations

Misused Identity High
A privileged identity is being used by multipl..
Open

Unrotated Privileged Secret Medium
A privileged identity is unrotated
Open

Identities by provider

21K	9.1K	6.9K	3.3K	16K
Azure AD	GCP	Azure	Github	11 more...

Unresolved violations by severity
● **3** Critical ● **10** High ● **197** Medium ● **115** Low

Identities by type View All

Secret	30K
API Token	11K
Service Principal	2.3K
Other (10)	13K

Top identities at risk

Azure AD | Service **i-Billing_DE** Principal	CRITICAL
GCP I Service Account **GCP Deployment user**	CRITICAL
Azure Access kev **E37686B9BB82954 E38986...**	CRITICAL

Key Capabilities

Cloud And On-Prem Support

Versatile Support For Both Cloud And On-Premises Environments.

Holistic Visibility With Context

Automatic Identification Of All Identities Within The Ecosystem. Comprehensive Insights Into Non-Human Identities, Including Context On Owners, Consumers, Resources, And Privileges.

Active Posture Management

Active Risk Management Through Posture Observability, Vulnerability Detection, And Automatic Remediation.

Non Human Identity Lifecycle Automation

Oasis Secures The Full Lifecycle Of Both New And Pre-Existing Non-Human Identities

Easy To Use And Developer Ready

Streamlined Onboarding Process For Quick Deployment.

Top Use Cases And Benefits

Rapid Incident Response

Swift Identification And Resolution Of Security Incidents.

GRC Enforcement

Enforcing Governance, Risk, And Compliance (GRC) Policies, Such As Secret Rotation, On Non-Human Identities

Out-Of-The-Box Remediation

Gives Out-Of-The-Box Remediation Plans To Shorten Resolution

Secure Employee Off-Boarding

Seamless Management Of Identity Transitions During Employee Exits.

Safe Secret Rotation And Decommissioning

Automated Resolution Plans And Code For Secure Secret Rotation And Decommissioning.

Security Posture Management

Continuous Monitoring And Evaluation Of Risk Posture, Prioritizing Vulnerabilities Based On Configurable Policies.