andromeda

Rightsize Your Permissions for Human Users + NHI

A FREE analysis of your cloud environment with actionable insights to implement least privilege and right-size roles based on permissions usage and risk

- Full discovery and inventory human users and NHI
- Quantified risk scores reflecting identity posture, behavior, and privileges
- Prioritized findings and detailed remediation steps
- Fine-grained visibility into roles and permissions
- Fast and Easy to Run, with no impact on your environment

Why Conduct a Permissions Rightsizing Exercise?

A comprehensive IAM risk assessment and role right-sizing exercise will identify security, compliance, and overprivilege issues across human and non-human identities in your cloud environment.

It will help you understand your risk and attack surface and provide actionable recommendations to reduce your blast radius and secure your environment.

This is critical step in your journey to zero-trust for human and non-human identities.

With this actionable data, you can investigate identity security issues and discrepancies, prioritize remediations, improve your identity security posture, and communicate risk to the C-suite.

Strategic Benefits: value-driven security transformation initiative

- Immediate risk identification
- Precise permission rightsizing
- Actionable remediation roadmap
- Continuous security improvement

Simple Set Up

- Identify the cloud you want to use for your rightsizing exercise.
- After a few minutes of setup, the solution will connect to your environment through API.

- Within hours, we will identify all human and non-human identities' security, compliance, and overprivilege issues.
- If available to you, connecting your IdP will result in richer insights.

*Note: Limited to one cloud environment, 100 identities, and 100 roles.

Actionable Findings and Recommendations

Human Users

Category	Example Finding	Recommendation
Stale Identities	Users who have left the organization but still have access to cloud resources	Delete stale identities
Overdue Key Rotation	Keys unrotated for over 6 months	Rotate keys with regular frequency
Inactive Access Keys	Keys inactive for 1 year or never used	Delete inactive and never-used access keys
Inactive IAM Users	Local accounts not used for over 1 year	Enforce SSO access and remove unused local accounts except in break-glass case
Shadow Admin Privileges	Users who inherit admin privileges through local accounts and/or lateral movement	Reduce the number of Admin users; enforce SSO access with step-up MFA, remove standing access, and move to JIT access
MFA Issues	Inconsistent MFA use across SSO access and local account access	Enforce consistent MFA use

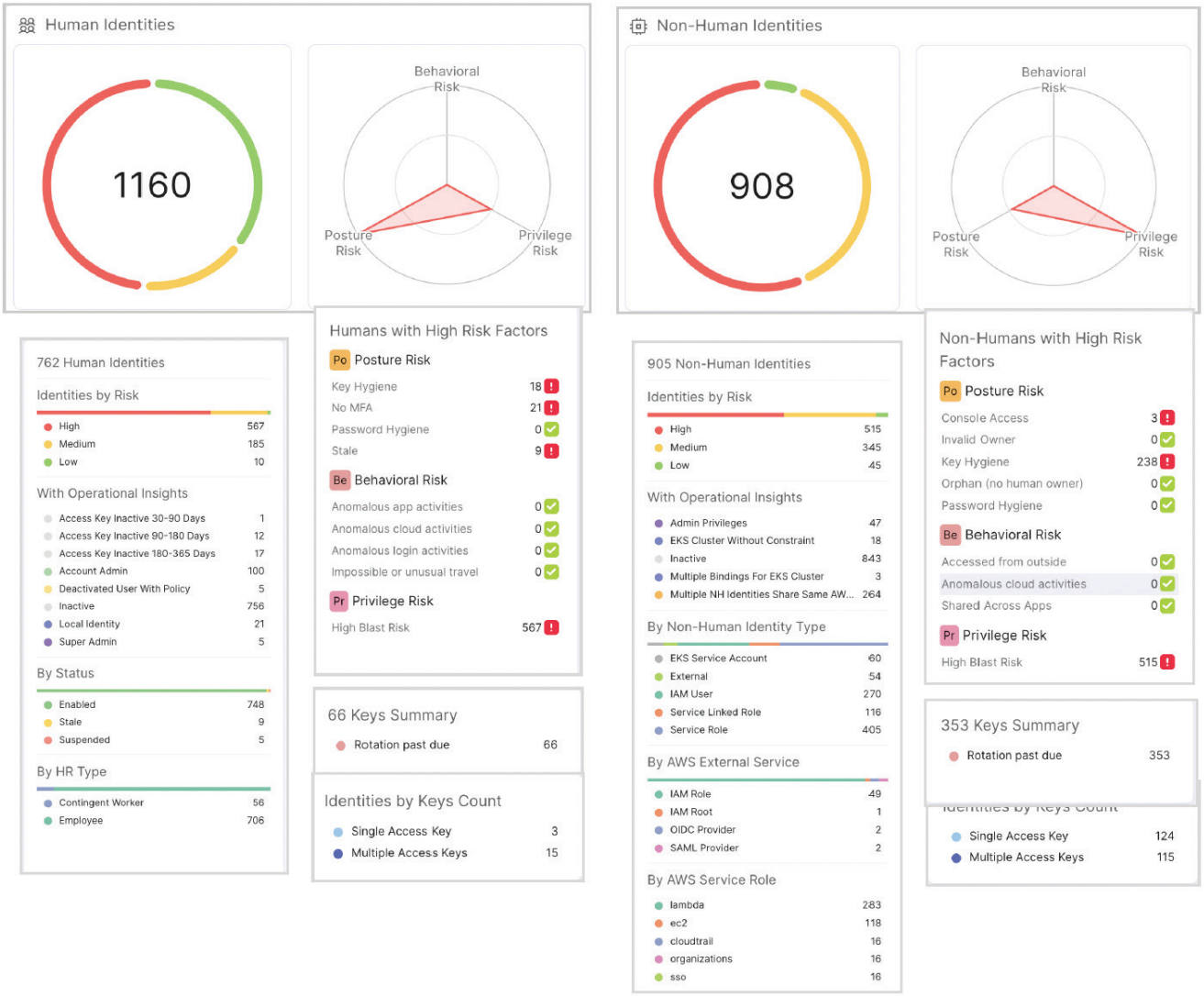
NHI

Category	Example Finding	Recommendation
AWS Console Access	NHIs flagged with console access and high blast risk	Remove console access for NHIs
Overdue Key Rotation	Keys unrotated for over 6 months	Rotate keys with regular frequency
Inactive Access Keys	Keys inactive for 1 year or never used	Delete inactive and never-used access keys
Inactive NHI	NHIs are inactive	Deactivate inactive NHIs; prioritize those with high blast risk
NHI with Admin Privileges	NHIs with admin access, including those with unrotated keys	Remove IAM and data deletion permissions from NHI
External NHIs with Privileged Access	NHIs with root trust or roles with the ability to escalate privileges	Evaluate if these roles are necessary; reduce the list of permissions to prevent privilege escalation
Lateral Movement	NHIs with lateral movement from test to production environment	Right-size the privileges to eliminate lateral movement to higher criticality environments

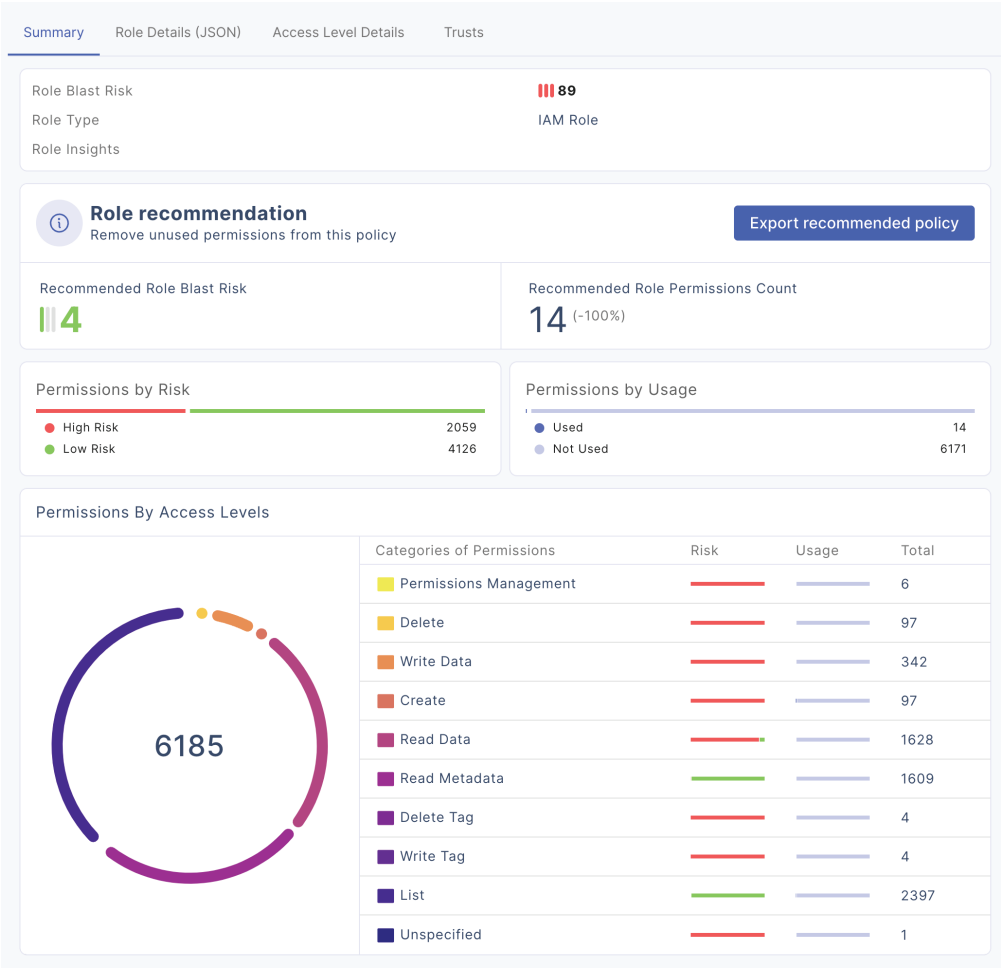
Roles and Permissions

Category	Example Finding	Recommendation
Unused Roles	IAM Roles unused for 1 year	Delete roles
Over-privileged Roles	IAM Roles with unused permissions	Right-size the roles based on actual permissions usage information

Human and Non-Human Identity Discovery and Risk Analysis



Role Right-Sizing Recommendation and Remediation



Lateral Movement with Privilege Escalation Detection