APONO

Datasheet

Securing Non-Human Identities (NHI)

Discover and manage all principals in modern cloud environments

The Challenge of Scaling NHIs

As organizations accelerate cloud adoption and automation, Non-Human Identities (NHIs)—like service accounts, API keys, IAM roles, and machine credentials—are multiplying rapidly. Often outnumbering human identities by 40:1 or more, these NHIs operate behind the scenes across cloud, SaaS, CI/CD, and GenAI environments.

Without centralized visibility or control, NHIs quickly become over-privileged, untracked, and vulnerable to compromise. Traditional IAM solutions struggle to scale with the complexity of managing machine access, especially in production environments where speed and stability are critical.

The Consequences:

- Lack of visibility across NHI usage and ownership
- Widespread over-privilege
- Unclear accountability
- Elevated blast radius in the event of compromise

NHI Risk Snapshot

60% of machine identities are over-permissioned[1]

62% of cloud breaches involve service accounts[2]

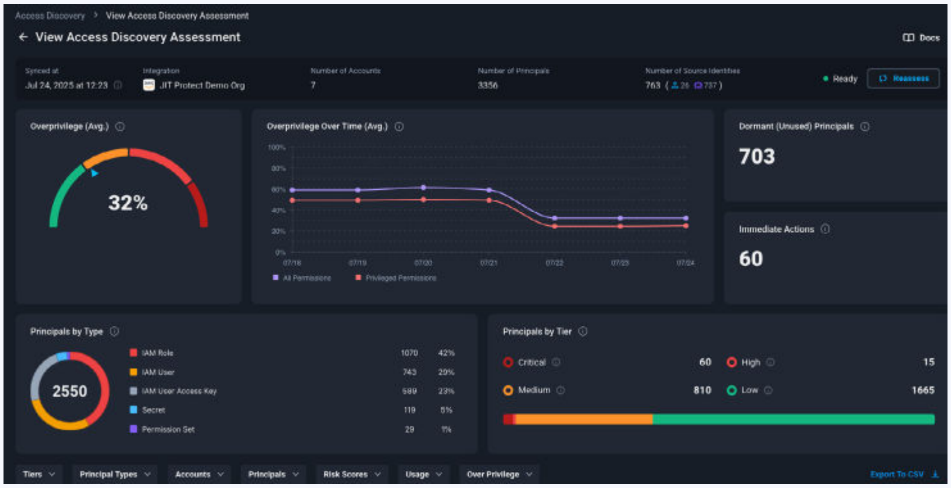
171K+ secrets discovered across SaaS & GenAI environments[3]

Apono Brings Order to NHI Access

Apono's Cloud Access Management Platform gives security and DevOps teams complete control over both human and non-human access through a single interface. With continuous discovery, contextual risk scoring, and actionable insights, Apono helps organizations:

- Unify visibility across all principals in your cloud
- Connect NHIs to their human owners
- Detect dormant, overprivileged, or orphaned identities
- Prioritize remediation with risk-based context

Whether you're dealing with IAM roles, tokens, secrets, or service accounts, Apono treats every identity as a manageable, measurable access surface.



Access Discovery > View Access Discovery Assessment

View Access Discovery Assessment

Synced at	Integration	Number of Accounts	Number of Principals	Number of Source Identities
Jul 24, 2025 at 12:23	JIT Protect Demo Org	7	3356	763 (26 737)

Ready

Overprivilege (Avg.): 32%

Overprivilege Over Time (Avg.)

Dormant (Unused) Principals: 703

Immediate Actions: 60

Principals by Type: 2550

IAM Role	1070	42%
IAM User	743	29%
IAM User Access Key	589	23%
Secret	119	5%
Permission Set	29	1%

Principals by Tier

Critical	60	High	15
Medium	810	Low	1665

APONO

Datasheet

Smart Remediation, Built for Scale

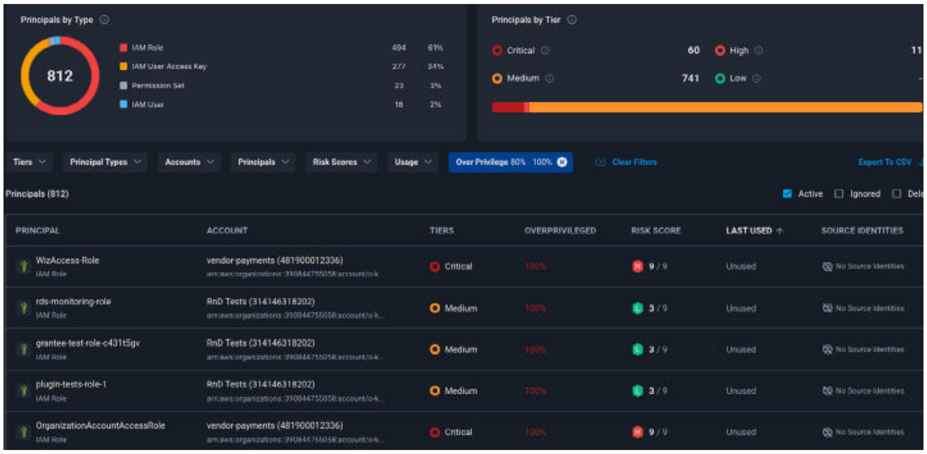
Traditional tooling makes remediation risky or manual. Apono gives teams the ability to safely eliminate risky access without disruption.

Risk Scenarios We Detect

Dormant principals unused for 90+ days

Unused privileges that add unnecessary exposure

Overprivileged IAM & Admin actions beyond actual usage



Principals by Type

812			
🟥	IAM Role	494	61%
🟧	IAM User Access Key	277	34%
▨	Permission Set	23	3%
🟦	IAM User	18	2%

Principals by Tier

Critical	60	High	11
Medium	741	Low	-

Principals (812)

☑ Active ☐ Ignored ☐ Dele

PRINCIPAL	ACCOUNT	TIERS	OVERPRIVILEGED	RISK SCORE	LAST USED ↑	SOURCE IDENTITIES
WizAccess-Role IAM Role	vendor-payments (481900012336) arn:aws:organizations::390844755058:account/o-k	Critical	100%	H 9 / 9	Unused	No Source Identities
rds-monitoring-role IAM Role	RnD Tests (314146318202) arn:aws:organizations::390844755058:account/o-k...	Medium	100%	L 3 / 9	Unused	No Source Identities
grantee-test-role-c431t5gv IAM Role	RnD Tests (314146318202) arn:aws:organizations::390844755058:account/o-k...	Medium	100%	L 3 / 9	Unused	No Source Identities
plugin-tests-role-1 IAM Role	RnD Tests (314146318202) arn:aws:organizations::390844755058:account/o-k...	Medium	100%	L 3 / 9	Unused	No Source Identities
OrganizationAccountAccessRole IAM Role	vendor-payments (481900012336) arn:aws:organizations::390844755058:account/o-k...	Critical	100%	H 9 / 9	Unused	No Source Identities

Remediation Actions

Quarantine dormant or unknown identities using autogenerated Access Flows and JSON deny policies ready for cloud deployment

Rightsize policies based on actual usage

Delete access paths that no longer serve a valid purpose

Each remediation is reversible, trackable, and fully auditable. No guesswork, no production risk.

Platform Capabilities

Cross-Environment Visibility
Unify access visibility across cloud providers, databases, SaaS, CI/CD pipelines, and more.

Contextual Risk Prioritization
Assess privilege risk using real-time context like usage frequency, access type, and resource sensitivity.

Unified Principal Management
Govern human and non-human identities through a single platform with policy enforcement, tracking, and investigation.

Continuous Least Privilege Enforcement
Usage insights keep access continuously right-sized.

Streamlined Auditing & Reporting
Track every access change to simplify compliance and reduce audit overhead.

1. Gartner Identity Governance Research, 2023 I 2. Palo Alto Networks Unit 42 Cloud Threat Report, 2024 I 3. Nightfall AI's 2024 State of Secrets Report

About Apono

Founded in 2022 by Rom Carmel and Ofir Stein, Apono delivers a Cloud Privileged Access Platform purpose-built for modern, fast-moving environments. With support for both human and non-human identities, Apono helps security and DevOps teams enforce least privilege at scale without slowing down delivery.

Trusted by Fortune 500 enterprises and recognized in Gartner's Magic Quadrant for Privileged Access Management two years running, Apono is shaping the future of secure cloud access.

APONO

www.apono.io
@Apono_official
@aponoio