OASIS

How Oasis Completes Your PAM Strategy

Non-Human Identity Governance
Across Every Vault, Every Cloud, Every Identity

The Problem in Brief

If you've evaluated your PAM program against the three questions that define Non-Human Identity (NHI) governance readiness, the gaps are likely familiar:

You can't inventory every non-human identity in your environment, only what's inside your vault

You don't have the chain of context For any given secret, you can't trace every consumer, dependency, and downstream system attached to it

You can't safely rotate or decommission any NHI today without risk of an outage

These aren't failures of your PAM investment. They're the natural consequence of an identity landscape that has expanded beyond what PAM was designed to govern. NHIs now outnumber human ones by orders of magnitude, authenticate through secrets scattered across multiple vaults and cloud platforms, and operate without the lifecycle controls that HR and directory systems provide for people.

PAM remains essential for what it does: credential vaulting, session management, and privileged access for humans. **What's missing is a governance layer purpose-built for the non-human identity landscape that sits above and across your existing vault infrastructure.**

That's what Oasis was built to deliver.

How Oasis Works: Architecture Overview

Oasis operates as a governance layer on top of your existing PAM platforms and vault infrastructure. It does not replace your vaults, compete with your PAM solution, or require you to migrate secrets. Instead, it **connects to your environment as-is and provides the visibility, context, and lifecycle automation that no single vault can deliver on its own.**

Oasis connects to your environment through agentless integrations across enterprise PAM vaults, cloud-native secrets managers, SaaS platforms, CI/CD pipelines, code repositories, and on-premises infrastructure. There is no agent deployment, no secret migration, and no disruption to existing workflows.

Oasis builds a unified identity graph that maps the complete relationship chain, from consumer to secret to identity to resource, across every connected system.
This graph is the foundation for every governance action: rotation, decommissioning, policy enforcement, and access review.

Oasis enforces policy across all vaults from a single control plane. Rotation cadence, ownership requirements, least-privilege rules, and expiration limits are defined once and applied consistently, regardless of where the credential is stored.

OASIS

Six Capabilities That Complete Your PAM Program

Each capability below maps directly to a governance gap that PAM alone cannot close.

1. Universal Discovery

The gap:
PAM governs what's in the vault. It cannot see secrets in cloud-native managers, CI/CD systems, SaaS credential stores, environment variables, or hardcoded in application code.

What Oasis does:
Continuously discovers every non-human identity and secret across your entire environment, every cloud, every vault, every platform. Discovery is agentless and ongoing, surfacing the identities and credentials that no team knows about and no single vault can see. New identities are detected as they're created, not at the next audit cycle.

2. Full Context Mapping

The gap:
PAM sees a credential in the vault. It does not see which application consumes it, what the identity does at runtime, what systems depend on it, or what would break if the credential were rotated.

What Oasis does:
Maps the complete relationship chain **consumer → secret → identity → resource**, so your teams understand not just where a credential lives, but what uses it, why it exists, and what depends on it. This is the context that makes every downstream governance action possible: safe rotation, meaningful access review, and confident decommissioning. Discovery tells you what exists. Context mapping tells you what it means. Without both, you have an inventory, not a governance program.

3. Cross-Vault Policy Enforcement

The gap:
Each vault enforces its own policies independently. There is no mechanism to apply consistent governance rules across CyberArk, Azure Key Vault, AWS Secrets Manager, HashiCorp Vault, and every other secrets store in the environment.

What Oasis does:
Applies unified governance policies across every vault and secrets store from a single control plane. Rotation cadence, ownership requirements, least-privilege enforcement, and expiration limits are defined once and enforced consistently across the system.
A secret in Azure Key Vault is governed with the same rigor as a secret in CyberArk.

4. Dependency-Aware Lifecycle Automation

The gap:
PAM can execute a credential rotation. But without knowing every system, application, and pipeline that consumes that credential, rotation causes outages. This fear is why secrets become long-lived and long-lived secrets are among the most exploited attack vectors.

What Oasis does:
Enables safe rotation and decommissioning by accounting for every consumer of a secret before action is taken. Oasis maps all dependencies, coordinates the update across connected systems, and confirms completion. No more outages from blind rotation. No more orphaned identities persisting because teams are afraid to revoke what they can't fully map.

5. Ownership and Accountability

The gap:
Human identities have clear owners, the humans themselves. Non-human identities often have no assigned owner, no responsible party, and no one accountable when they're compromised or need review.

What Oasis does:
Assigns and enforces ownership for every non-human identity. When an identity needs review, rotation, or decommissioning, there is always a clear owner accountable for action. Ownership is not a field in a spreadsheet; it is an enforceable governance control tied to policy and alerting.

6. PAM-Native Integration

The gap:
NHI governance tools that operate independently from PAM create yet another silo. Security teams end up managing two separate systems with no coordination.

What Oasis does:
Works with your existing PAM platform, not around it. Oasis routes secrets into your vaults where appropriate, leverages PAM's strengths for credential storage and session management, and extends your PAM program with the NHI-specific capabilities that complete your privileged access strategy.
Your PAM investment is preserved and amplified, not duplicated or displaced.

In Practice: How Organizations Use Oasis

Insurance Organization: Replacing Vault Complexity with a Unified Governance Layer

Challenge

The organization managed a hybrid infrastructure spanning on-premises CyberArk, Azure Key Vault, and AWS. Azure service principal creation was entirely manual, handled through Jira tickets with no automated provisioning, vaulting, or rotation. Thousands of service principals had accumulated during a period of ungoverned creation, many abandoned and stale.

What changed with Oasis

The organization deployed Oasis as the governance layer above existing vaults, preserving CyberArk as the credential store while shifting lifecycle management into Oasis. For Azure service principals, they implemented end-to-end automated provisioning: once a request is approved in their ticketing system, Oasis creates the identity, generates the secret, stores it in the vault, assigns ownership, sends a secure one-time notification to the requestor, and enrolls the identity in automatic rotation from day one. The stale identity count dropped from over 10,000 to under 4,000 once full-environment correlation was enabled.

Financial Services Company: Ownership, Inventory, and the Path to Automatic Rotation

Challenge

The organization had accumulated roughly 25,000 accounts in CyberArk across a decade of upgrades, alongside secrets in HashiCorp Vault and Azure Key Vault. Ownership was poorly tracked; when employees left, their service accounts were not reassigned. Development teams deployed service principals via Terraform without attribution to an owner, making it impossible to contact the responsible party when secrets were approaching expiration.

What changed with Oasis

Oasis integrated across the full vault landscape and correlated CyberArk-stored accounts back to the identities in Active Directory and cloud environments that consumed them, showing for the first time which accounts were vault-managed and which were not. Ownership became enforceable: every newly provisioned identity requires an owner at creation, and for legacy accounts, Oasis suggests owners based on usage patterns and triggers attestation campaigns to confirm or reassign. The team is now migrating to automatic rotation, starting with AD service accounts, using dependency mapping to identify which credentials can be safely rotated without outage risk.

OASIS

Deployment Model

Oasis is designed for enterprise deployment with minimal friction:

Agentless architecture

no software installed on endpoints, servers, or within vault infrastructure. Oasis connects through API integrations and read-level access to your existing systems.

Time to value

discovery and initial context mapping begin within days of deployment, not months. Organizations typically have full visibility into the environment within the first 30 days.

No migration required

secrets stay where they are. Oasis governs across your existing vault topology without requiring consolidation or re-architecture.

Scales with your environment

designed for enterprises managing tens of thousands to millions of non-human identities across multi-cloud, multi-vault, hybrid infrastructure.

Next Steps

Your PAM program protects your most privileged credentials. Oasis extends that protection to every non-human identity, consuming them across every vault and every cloud.

See what's in your environment. Request a complimentary NHI discovery assessment to map the non-human identities, secrets, and governance gaps across your vault and cloud landscape.

Request Your NHI Discovery Assessment

Or talk to our team about how Oasis integrates with your specific PAM and vault environment.

Schedule a Technical Walkthrough