LEARNING MADE EASY

Oasis Special Edition

Non-Human Identity Management

for dummies®
A Wiley Brand

- Understand non-human identities
- Recognize gaps in identity management tools
- Learn from real-world security incidents

Brought to you by

OASIS

Lawrence Miller

About Oasis Security

Oasis Security is the management and security solution for non-human identities (NHIs). It is the first solution purpose-built to address the unique challenges of visibility, security, and governance of NHIs across hybrid cloud environments.

Oasis leverages advanced AI-based analytics to automatically discover NHIs, assess their risk, and identify their owners throughout the environment. With its integrated, policy-driven governance capabilities, Oasis orchestrates the entire life cycle of NHIs, including remediation and compliance management, all within a single solution.

Leading organizations across a wide range of industries use Oasis to foster innovation and collaboration among security, identity, and engineering teams, enabling secure digital transformation and cloud adoption.

Non-Human Identity Management

Oasis Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Non-Human Identity Management For Dummies®, Oasis Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-32001-1 (pbk); ISBN 978-1-394-32002-8 (ebk); ISBN 978-1-394-32004-2 (ebk)

Publisher's Acknowledgments

Editor: Elizabeth Kuball
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Jeremith Coward
Production Editor: UmeshKumar Rajasekhar

Table of Contents

Introduction

Identity management is a critical component of enterprise security. Identities are the key construct through which we control how authorized entities — individuals, applications, and devices — can access data and perform actions.

Historically, human identities have been the primary focus of identity and access management (IAM). Although human identities remain strategically important, shifts in infrastructure and workload architecture have driven the exponential growth of non-human identities (NHIs) — NHIs outnumber human identities by 20x — completely changing the identity landscape and opening up new challenges.

The massive scale and dynamic nature of NHIs makes it impossible for traditional IAM tools to maintain holistic visibility and provide insights into the applications and machines that use those NHIs. As a result, organizations can't effectively implement robust security policies without risking system resilience.

About This Book

Non-Human Identity Management For Dummies, Oasis Special Edition, consists of four chapters that explore the following:

- The current state of identity and access management and the challenges of managing NHIs (Chapter 1)
- Real-world NHI security incidents and lessons learned (Chapter 2)
- The Oasis NHI Management Platform (Chapter 3)
- Key features and capabilities you need in an NHI management platform (Chapter 4)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you.

Foolish Assumptions

It has been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

Mainly, I assume that you're a chief information security officer (CISO); chief security officer (CSO); chief information officer (CIO); IAM manager; or IAM/cloud/security analyst, engineer, or architect. As such, I assume that you have a strong understanding of IAM, cloud, infrastructure, and applications issues and topics.

If any of these assumptions describes you, then this is the book for you! If none of these assumptions describes you, keep reading anyway — it's a great book, and after reading it, you'll know quite a bit about non-human identity management.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin.

TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected, and I sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about. Well, probably not, but they do offer practical advice.

Beyond the Book

There's only so much I can cover in this short book, so if you find yourself at the end of it wondering, "Where can I learn more?" check out `www.oasis.security`.

IN THIS CHAPTER

- Exploring the exponential growth of non-human identities
- Recognizing the unique challenges of non-human identities for traditional IAM
- Understanding the limitations of traditional IAM tools in non-human identity management

Chapter 1
Looking at the Current State of Identity and Access Management

Simply put, identity is the new perimeter — and non-human identities (NHIs) are the gaping hole in that perimeter. In this chapter, I explain the basics of NHIs and explore the unique challenges of NHIs, as well as the limitations of traditional identity and access management (IAM) processes and tools.

Understanding Non-Human Identities

NHIs — including service accounts, service principals, IAM users, roles, applications, and so on — serve as digital gatekeepers, enabling secure machine-to-machine and human-to-machine access and authentication within modern enterprise systems (see Figure 1-1).

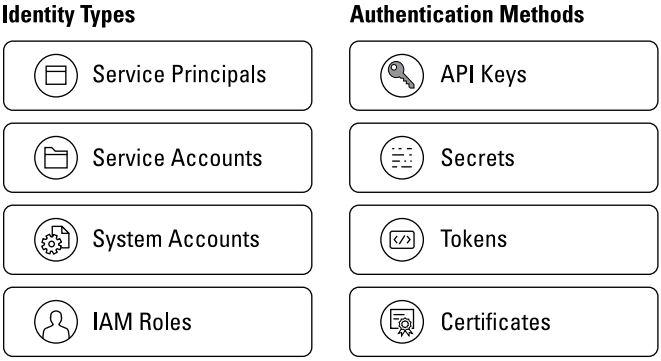


FIGURE 1-1: Different authentication methods for different NHI types.

The push for innovation has led to the adoption of microservices architectures, third-party solutions, hybrid and multi-cloud environments, and continuous integration/continuous delivery (CI/CD) DevOps pipelines, creating a complex web of interconnected systems and fueling the exponential growth of NHIs. NHIs now outnumber human identities in enterprise environments by 20x, according to ESG, with broader access privileges to sensitive data, constituting a massive attack surface. With ever more business processes being automated with artificial intelligence (AI) workflows and accessed by AI-powered services, this trend is likely to accelerate even more. Yet despite the risks, NHIs are still a blind spot for most enterprises because they lack the right tools to manage them throughout their life cycle.

The security risks of unmanaged NHIs are further compounded by the fact that, on average, there are 5x more highly privileged NHIs than there are highly privileged human identities. Further complicating the challenge of securing NHIs is that NHIs can't leverage biometrics or other forms of multifactor authentication (MFA).

Attackers gain access via compromised NHIs using the following threat vectors:

- **Stale privileged NHIs:** Despite their privileged access, stale or orphaned accounts remain unchanged and susceptible to exploitation due to the lack of ownership, accountability, visibility, and credential rotation.
- **Unrotated secrets exposed to offboarded employees:** Secrets left unrotated and exposed to a former employee

pose a significant risk, especially when they can be accessed on the internet and have privileged access.

- **Stale storage accounts:** Stagnant storage accounts present a potential security loophole in which outdated configurations may leave sensitive data vulnerable to unauthorized access or compromise.
- **Active secrets with long expiration dates:** Secrets with excessively long expiration dates pose a security risk because they provide an extended window of opportunity for threat actors to exploit vulnerabilities.
- **Vaults with unused access policies:** Vaults containing unused access policies represent an overlooked security gap that may inadvertently grant unauthorized access to sensitive resources or data.

Being able to find and highlight these vulnerabilities is the first step to proactively managing and securing NHIs to mitigate security risks and safeguard organizational assets.

WARNING

Oasis research reveals that organizations that don't have an enterprise NHI management strategy have a rapidly growing attack surface with numerous toxic combinations of vulnerabilities. In a typical company with 10,000 employees, Oasis Data and Research found, on average:

- **Stale, privileged unrotated NHIs:** 253
- **Unverified third-party vendors:** 207
- **Unrotated secrets exposed to offboarded employees:** 30
- **Access attempts from known threat actors:** 21
- **Critical service outages due to expired credentials:** 24
- **Active secrets with 50+-year expiration dates:** 18

Recognizing the Challenges and Limitations of Traditional IAM

Managing NHI is complex and involves more than just safely and securely rotating secrets. Without the right tool, the operational complexity and overhead of managing NHIs becomes an insurmountable challenge.

The scale and dynamic nature of NHIs poses complex operational challenges that traditional IAM solutions aren't designed to address (see Figure 1-2).

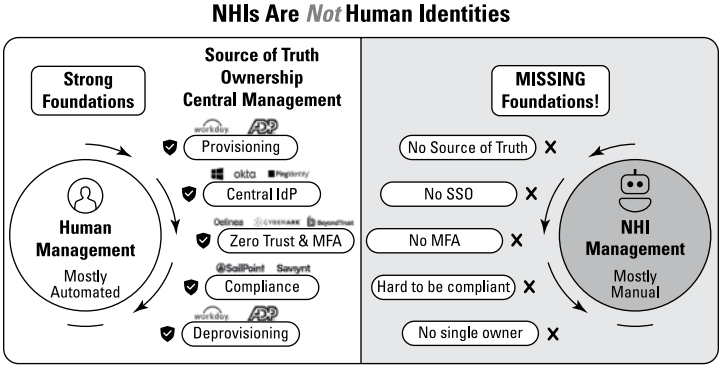


FIGURE 1-2: The traditional IAM security stack doesn't effectively address NHI management.

NHIs differ significantly from human identities in several key aspects that create unique challenges and expose the limitations of traditional IAM, including the following:

- **No source of truth:** NHIs are not centrally managed like human identities; instead, they're created and managed across multiple platforms by various stakeholders. It can be a real challenge to classify whether a user is a human or a machine.
- **No single owner:** Unlike human identities, NHIs are not tied to specific individuals and are often used by multiple administrators or applications.
- **Scale:** The large volume of NHIs creates a massive attack surface that is growing exponentially.
- **Rate of change:** NHIs are subject to frequent creation and deprecation, aligning with the rapid pace of code development, rendering them more challenging to manage. However, NHIs can also persist unchanged for years without rotation, creating further management challenges.
- **Developer-driven:** Unlike human identities, the creation and control of NHIs aren't centralized. In many cases, NHIs are directly created by developers, or even citizen developers

and power users in no-code or low-code applications, who may not be aware of their usage, because they represent the only means for the code they need to interact with systems.

- **Secret expiration:** Frequent password rotation is very common around privileged users, but many NHIs are set to live for a very long time — sometimes without an expiration date.
- **Operational risk:** Engaging with NHIs carries operational risks. In the absence of a comprehensive understanding of all consumers and dependencies, there is a potential for disrupting production systems. Plus, efforts to rotate secrets may unintentionally disrupt established and vital business workflows.
- **Authentication diversity:** NHIs support multiple authentication methods, reflecting technological evolution. Various systems may employ different authentication methods, leading to a wide range of approaches in use. Additionally, whereas MFA can be used to greatly enhance password security in human identities, NHIs cannot take advantage of MFA.

Identifying Gaps in Traditional IAM Tools

NHIs are very different from human identities. NHIs have a more dynamic life cycle that typically spans beyond security teams, directly involving developers, and that is mission critical for business continuity and operational resilience. The scale, speed, diversity, and distributed nature of NHIs brings a whole new set of management requirements that existing security tools alone, like privileged access management (PAM), cloud security posture management (CSPM), and secret managers, cannot address effectively.

Privileged access management

PAM solutions are designed to secure, control, and monitor the activities of human privileged users, such as administrators, root users, and generic accounts with broad access rights, ensuring only authorized personnel can access sensitive data and infrastructure.

At their core, PAM systems integrate with the organization's authoritative identity sources, such as human resources (HR) systems and Microsoft Active Directory (AD), to comprehensively understand human identities and their associated privileges. By enforcing access policies, managing credentials, and providing granular auditing capabilities, PAM solutions mitigate the risk of insider threats and unauthorized access to sensitive data and infrastructure. Ultimately, PAM systems act as the centralized control plane for governing privileged human access across the enterprise environment.

Unlike human users who are provisioned from an authoritative source, such as HR databases or AD, NHIs lack a centralized record system. They're often created in an ad hoc, distributed manner by developers and DevOps teams directly within cloud platforms, Kubernetes clusters, CI/CD pipelines, and other modern infrastructure. This distributed provisioning process results in NHIs being spun up on demand without going through standardized IT workflows. The lack of an authoritative source of truth, combined with how and by whom NHIs are created, fundamentally breaks the data model and governance frameworks upon which traditional PAM tools are built.

REMEMBER

PAM tools are built on the premise of managing dedicated, long-lived privileged accounts mapped to individual human identities and following well-structured provisioning workflows. In contrast, NHIs can be ephemeral, infused throughout dynamic infrastructure, and created outside of legacy identity management processes. Their privileged nature and lack of centralized control make them invisible to PAM tools.

Cloud security posture management

Cloud security posture management (CSPM) tools excel in assessing, managing, and enhancing the security of cloud environments. They focus on identifying and remediating infrastructure misconfigurations, ensuring compliance with security policies, and minimizing the risk of security breaches — not managing NHIs.

Key capabilities and features of CSPM tools include:

- **Continuous monitoring:** CSPM tools maintain a watch over cloud environments, detecting deviations from security best practices.

- **Risk assessment and compliance:** CPSM tools conduct thorough risk assessments, ensuring compliance with industry standards and regulatory requirements.
- **Remediation:** CSPM tools spring into action, automatically remediating security issues and enforcing policy compliance.
- **Policy enforcement:** CPSM tools automate the enforcement of security policies, maintaining a consistent security posture across the cloud ecosystem.

CSPM tools monitor a variety of cloud infrastructure settings, such as network, data storage and encryption, software versions, serverless functions, application programming interface (API) gateways, Domain Name System (DNS), logging and monitoring, and adherence to organizational policy and governance.

Secret managers

Secret managers play a pivotal role in securely storing and managing API keys, passwords, and encryption keys. They can be used effectively to implement security policies or to automate processes like secret rotation. These tools excel in their designated functions but often operate in isolation, leaving a significant security layer — the NHI layer — unaddressed.

Secret managers have long been the go-to solution for securely storing and managing secrets. They provide a centralized repository for sensitive information, encrypting it and enabling controlled access. This approach ensures that secrets are protected against unauthorized access and helps organizations comply with security and data privacy regulations.

Secret managers focus on vaulting secrets, but they aren't identity-aware. Consequently, they lack the context of ownership, usage, permissions, and accessed resources. Although secret managers excel in their specific domain, they may not fully address the unique security concerns associated with unmanaged NHIs. These NHIs often operate within cloud environments, interacting with various resources and systems.

IN THIS CHAPTER

- Ensuring complete and contextual visibility of all non-human identities
- Replacing manual rotation processes with automation
- Securing service accounts

Chapter 2
Exploring Non-Human Identity Security Incidents and Lessons Learned

This chapter looks at some recent real-world breaches involving non-human identities (NHIs) and how to avoid similar incidents in your organization.

Securing Non-Human Identities: Cloudflare

In February 2024, Cloudflare disclosed that it had been breached by a suspected nation-state attacker that exploited multiple unrotated and exposed secrets. The Cloudflare breach actually began in October 2023 with the Okta breach, during which the

attacker gained administrative access to Cloudflare's Okta system. Although the Cloudflare team tried to rotate all relevant credentials within Okta, they missed one access token and three service accounts, mistakenly believing they were unused. Subsequently, the attacker utilized these four NHIs to gain access to Cloudflare's Confluence, Jira, and Bitbucket systems (see Figure 2-1).

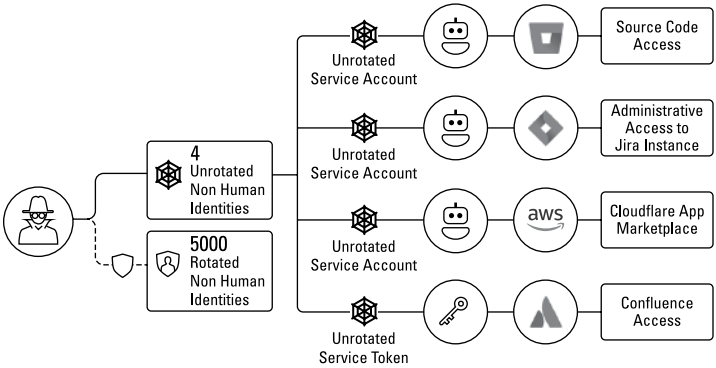


FIGURE 2-1: The Cloudflare breach exploited four unrotated NHIs.

Although the Cloudflare team was aware of the Okta breach in October, they couldn't prevent the subsequent breach. Despite their awareness and the recognized need to rotate all exposed credentials, timely action was impossible to execute quickly enough due to the inherent operational complexity of the task, even for an experienced team like the one at Cloudflare.

Rotating secrets is inherently difficult for a number of reasons:

- They exponentially outnumber human identities by a factor of 10x to 50x. In the Cloudflare case, they had to rotate more than 5,000 NHIs.
- Secrets are everywhere in the environment, making it hard to maintain an accurate and complete inventory of all identities and secrets.
- Rotating an identity without knowing which systems depend on it can lead to business disruptions.

WARNING

The lack of effective management tools leaves most organizations struggling to regularly rotate secrets, especially during security incidents. Furthermore, NHIs lack multifactor authentication (MFA) and often have privileged access, making them prime

targets for attackers seeking to execute supply chain attacks, move laterally, and maintain persistence.

TIP

The best approach for an organization to eliminate the security risk exposure from NHIs is to efficiently manage them throughout their life cycle. This entails implementing several key best practices:

- Make sure that each NHI is dedicated to a single process or application.
- Right-size the NHI privileges for its operation — no more, no less.
- Rotate the identities' secrets periodically to mitigate the risk of unauthorized access.
- Decommission stale identities that are no longer needed.

Automating Key Management: Microsoft Exchange

In the spring of 2023, a sophisticated cyberattack orchestrated by an entity identified as Storm-0558 compromised the Microsoft Exchange Online mailboxes of 22 organizations and more than 500 individuals globally, including key figures in the U.S. Cabinet and prominent U.S. State Department officials. Attributed to China's Ministry of State Security (MSS), Storm-0558 exploited authentication tokens associated with a Microsoft key established in 2016. The stolen key granted the adversary unprecedented access, enabling Storm-0558 to infiltrate Exchange Online accounts worldwide and exert control over sensitive information and systems (see Figure 2-2).

In the wake of this breach, several key takeaways and lessons learned have been identified:

- **NHI management needs to become an integral part of enterprise identity programs.** The Microsoft Exchange Online breach is just the latest example in a rapidly growing trend of attacks that exploit unmanaged NHIs. Even technologically advanced and security-aware organizations, such as Microsoft, can fall victim to attacks against unmanaged NHIs.

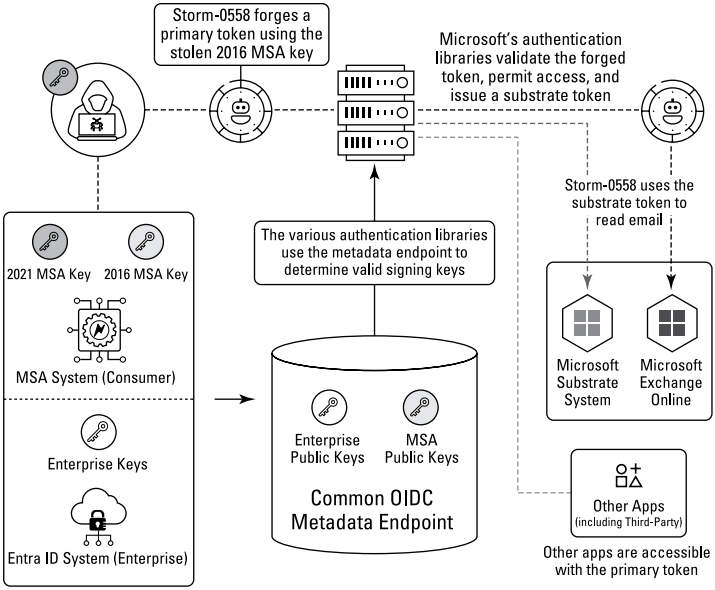


FIGURE 2-2: The Microsoft Exchange Online breach leveraged a stolen 2016 Microsoft Account (MSA) key.

- **Organizations should adopt practices and tools that keep both operational continuity efforts and security best practices aligned.** In 2021, following a large production outage, Microsoft stopped its manual key rotation processes, leaving the key that was later compromised (and many others) vulnerable. Prioritizing operational continuity over security posture is a very common pattern that, in most cases, is caused by lack of contextual visibility, which leads to inaction. The complexity and scale of NHIs requires a purpose-built tool that can automatically discover NHIs, create system dependency maps, and identify high-risk priorities.
- **Automate, automate, automate.** When it comes to NHI management, automation is key because the scale is so vast. Companies can't disregard the limitations of manual processes, which are prone to error and operationally expensive. Adding automating tasks like secret rotation typically requires integrating new tools and capabilities in your stack, but the investment is absolutely critical for the long-term success of the business.

- **Rotation of keys and secrets is only one part of the larger challenge of complete NHI life cycle management.** As environments become increasingly distributed, spanning multiple clouds and hundreds of interconnected services, NHIs grow exponentially in scale. Consequently, security and operations teams need to adopt tools that enable effective cooperation across every phase of the NHI life cycle, from provisioning to rotation and decommissioning.

Addressing Non-Human Identity Risks: Dropbox

In April 2024, a threat actor compromised a service account — specifically designed to execute applications and automate essential services — in an automated system configuration tool within the Dropbox Sign (formerly HelloSign) production environment, and accessed sensitive customer information.

Service accounts, often created in Microsoft Active Directory (AD), serve as a conduit for various system operations, from software installations to database management. Functioning autonomously, these accounts carry out tasks seamlessly, often operating in the background without human intervention. However, their autonomy and extensive access privileges make them susceptible to exploitation if they aren't adequately secured.

In response to the incident, Dropbox took swift action to mitigate risks to its users. This included resetting users' passwords, logging users out of connected devices, and coordinating the rotation of all application programming interface (API) keys and Open Authorization (OAuth) tokens.


TIP

The Dropbox Sign security incident serves as a stark reminder of the critical importance of effectively managing NHIs, like service accounts, throughout their life cycle. Organizations must prioritize robust practices for the creation, assignment, governance, rotation of secrets, and decommissioning of stale service accounts

to mitigate risks and enhance cybersecurity posture. Key lessons learned include the following:

- **Prioritize comprehensive visibility for effective service account management.** Achieving a complete view of the service account landscape is crucial. Organizations should strive for holistic visibility, enabling them to identify all service accounts within their infrastructure. This visibility should extend to various aspects such as account usage, permissions, and associated resources.
- **Ensure safe secret rotation for NHIs.** Regular password/secret rotation is standard practice for human identities, but it's often overlooked for NHIs. Concerns about potential disruptions to critical operations lead to the neglect of secret rotation, allowing compromised service accounts to maintain prolonged and unmonitored access to an organization's network.
- **Understand context to avoid unnecessary business disruptions.** Detailed insight into the context surrounding each service account is essential. Contextual mapping capabilities provide information about service account configurations, access controls, and usage patterns. By understanding the context in which service accounts operate, administrators can make informed decisions regarding their management and access privileges.
- **Strengthen NHI security with proactive posture assessments.** Assessing the security posture of service accounts is paramount. Organizations should conduct automated posture assessments, evaluating factors such as secret rotation, access permissions, and compliance with security policies. This proactive approach helps identify risks and prioritize remediation efforts to enhance the overall security of service accounts.

WARNING

Rotating passwords in outdated environments, especially those heavily dependent on Microsoft AD service accounts, presents a significant challenge. Unlike modern systems that allow for simultaneous rotation of multiple passwords, older systems often impose restrictions, permitting only one password rotation at a time. This limitation not only complicates the rotation process but also heightens the risk of credential exposure due to delayed updates.

CHOOSING THE RIGHT NHI MANAGEMENT SOLUTION

Addressing NHI challenges in modern environments is a multifaceted objective that requires organizations to conquer three critical steps:

1. **Gain a comprehensive understanding of your environment and all identities within it.**

   This means going beyond the data provided by your identity provider (IdP). You do this by incorporating multiple sources of information for deeper visibility into all of an identity's critical usage characteristics.

2. **Understand your perimeter risk exposure.**

   This means developing security policies tailored to your specific business needs, utilizing tools with advanced analytics to identify potential gaps and threats, and establishing a prioritization process for continuous review and assessment of your security posture.

3. **Take control of the NHI life cycle while avoiding operational headaches, preventing risks, and minimizing response times to issues.**

   This means moving beyond slow email-based processes for remediation and adopting a more efficient policy-based automation model that can orchestrate workflows across existing infrastructure and services without disruption.

Use the following checklist to help you choose the right NHI management solution for your organization:

- ☐ **Identity-centric architecture:** Understand all aspects of NHIs. NHIs are the primary asset the solution manages and secures.
- ☐ **Classification:** Categorizes identities as human or non-human and resolves ambiguities.
- ☐ **Discovery:** Scans the environment and automatically creates an inventory across all identity sources.
- ☐ **Usage contextualization:** Adds context to identities based on users' permissions, roles, and resources.

(continued)

(continued)

- ☐ **Ownership assignment:** Assigns clear ownership to each NHI.
- ☐ **Risk posture:** Evaluates security risks and vulnerabilities.
  - ☐ **Toxic combinations:** Detects concurrent risk combinations.
- ☐ **Threat detection:** Identifies suspicious activities in real-time.
- ☐ **Remediation:** Automates the resolution of security incidents and posture violations.
- ☐ **Compliance:** Ensures adherence to regulatory requirements.
- ☐ **Workflows:** Automates security processes and incident management.
  - ☐ **Provisioning:** Manages creation and assignment of identities.
  - ☐ **Rotation:** Regularly updates secrets and credentials based on policy.
  - ☐ **Offboarding:** Removes access to NHI for identities that no longer need exposure and for former employees.
  - ☐ **Decommissioning:** Safely removes inactive or obsolete identities.
- ☐ **Policy-based automation:** Automates tasks using predefined policies.
- ☐ **Cloud-native orchestration:** Integrates seamlessly with diverse cloud-native services and does not require proprietary systems.
- ☐ **Cross-cloud:** Supports all major clouds.
- ☐ **Cross-vault:** Supports cloud-native and third-party cloud vaults.
- ☐ **DevOps tool integration:** Connects with DevOps tools for secure workflows.

IN THIS CHAPTER

- Managing non-human identities with Oasis
- Accelerating enterprise initiatives
- Exploring non-human identity management use cases

Chapter 3
Managing and Securing Non-Human Identities with Oasis Security

This chapter introduces you to the Oasis Non-Human Identity (NHI) Management platform and explore its key capabilities, features, and benefits.

Introducing the Oasis NHI Security Cloud

Oasis is the first enterprise platform purpose-built for managing and securing NHIs. Oasis continuously analyzes your environment to identify, classify, and resolve security risks associated with all NHIs throughout their complete life cycle. Oasis is built with an identity-first approach that starts with cloud infrastructure and extends to Software as a Service (SaaS) and on-premises systems.

Plugging Oasis into your environment is incredibly simple and can be done in minutes. The platform connects with all major public clouds through an agentless interface and can be further integrated with leading identity management systems, secret

management solutions, IT service management (ITSM) systems, and developer platforms.

After those are connected, most of your work is done. The Oasis NHI cloud solution is built on four engines that combine powerful discovery and posture analytics with efficient remediation and life-cycle management:

- **NHI Discovery Engine:** In Oasis, the identity is the starting point and the core unit of management. Identities define the security perimeter and control the access to your resources. Discovering and understanding each identity is the prerequisite to securing the perimeter — only looking at secrets or infrastructure configurations isn't enough. Other solutions focus only on secrets and infrastructure configurations, but Oasis also discovers service accounts, identity and access management (IAM) roles, service principals, keys, tokens, and more. Oasis connects agentlessly to your cloud infrastructure and services to give you complete visibility and actionable context on all the NHIs in your environment.
- **Context Reconstruction Engine:** Oasis doesn't need to have preexisting knowledge about the NHIs in your environment to be able to manage them. Oasis continuously learns about all aspects of each NHI in your environment leveraging its purpose-built analytics engine. The Context Reconstruction Engine (CRE) leverages powerful sets of artificial intelligence (AI), machine learning (ML), large language models (LLMs), and behavioral algorithms to continuously correlate data from audit logs, identity providers (IDPs), vaults, data security posture management (DSPM) platforms, application security posture management (ASPM) platforms, and more, providing a deep business context map of each identity (class/type, usage, consumers, authentication methods, entitlements, and resources) and detecting risk factors, policy violations, and anomalous behaviors.
- **Ownership Discovery Engine:** Many organizations don't maintain an NHI ownership process. The first step in order to manage NHIs, mitigate risk, or initiate remediation processes is to identify its owners. After ownership is established and attested, life-cycle management actions can be implemented with the necessary approvals and without breaking things. Oasis has developed a unique set of purpose-built ML algorithms that, without prior knowledge

and collecting from logs, configuration management databases (CMDBs), and more, can suggest NHI owners in your environment by analyzing the digital footprint and behaviors of who consumes them and for which resources.

- **Policy-driven bring-your-own-identity (BYOI) Orchestration Engine:** Visibility and security alerts alone are not enough to secure NHIs. The toughest hurdle to solve is operationalizing security at cloud scale. Oasis solves this with three key unique capabilities:
  - *Policy-driven control plane:* Oasis normalizes security policies across asset types, allowing for automated enforcement and remediation at scale (set once, enforce many).
  - *BYOI and Outpost architecture:* Oasis does not require the use of proprietary IDPs, vaults, or secret managers. It seamlessly integrates with cloud-native services and existing processes to orchestrate life-cycle management tasks with the least impact to cost and administration. Oasis Outpost manages even the most sensitive aspects of NHIs, such as secrets, without becoming a third-party risk to your environment.
  - *Identity life-cycle management (ILM) workflows:* Built into the Oasis NHI Security Cloud is a complete set of NHI ILM workflows to turn complex processes into very simple, easy-to-understand tasks, such as automatic safe rotation, monitoring, employee/contractor offboarding, recertification, and stale NHI decommissioning.

REMEMBER

Here's how Oasis unlocks real, effective NHI management:

- **NHI-centric:** Identities are the key starting point of the Oasis platform, not infrastructure or secrets. This allows the Oasis platform to create a complete and actionable view of the operational context of how systems are interconnected, allowing it to create a high-fidelity view of dependencies, usage, and entitlements.
- **Cross-system insights:** Oasis is engineered to work without preexisting knowledge of an environment and doesn't depend on a single authoritative source. The Oasis platform connects, aggregates, and analyzes data across various systems — such as IDPs, event logs, secret managers,

application security posture management (ASPM), and data security posture management (DSPM) — providing a holistic inventory with rich contextual information on each identity and its posture.

- **Life-cycle orchestration:** Oasis offers powerful life-cycle management capabilities, automating key processes from creation to decommissioning. This ensures that all identities are properly managed throughout their entire life cycle, reducing the risk of security breaches.
- **Hybrid cloud support:** Oasis supports hybrid cloud environments, allowing organizations to manage NHIs across both on-premises and cloud environments. This flexibility ensures consistent security and compliance in diverse IT landscapes.
- **Fast time-to-value:** The Oasis platform delivers quick and tangible benefits, enabling organizations to see value rapidly. With streamlined implementation and intuitive features, Oasis helps businesses enhance their security posture without lengthy deployment times.

Architecture and components

Figure 3-1 shows the integration points between the Oasis NHI Security Cloud architecture and various systems and teams within an organization, including security teams, developers, and third-party systems.

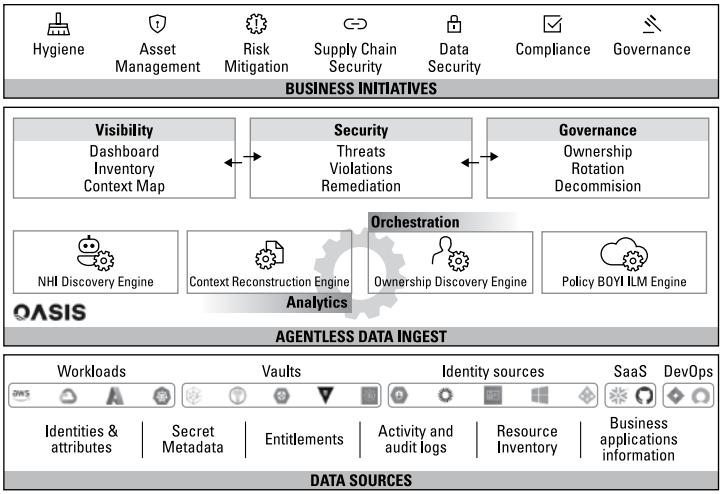


FIGURE 3-1: The Oasis NHI Security Cloud architecture.

Integrations

Oasis integrates with a variety of tools and platforms, ensuring that alerts and remediation guidance integrate into your existing environment and workflows, including the following:

- **Providers**
  - Cloud: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), databases, virtual private connections (VPCs), and Kubernetes
  - On-premises: Active Directory (AD), databases, applications
  - Software as a Service (SaaS)
  - Data platforms
- **Secret management**
  - Secret managers
  - Privileged access management (PAM)
  - Native cloud vaults
- **Workflows**
  - Infrastructure as Code (IaC)
  - IT service management (ITSM)
  - Security information and event management (SIEM)
  - Identity governance and administration (IGA)
- **Context enrichment**
  - ASPM
  - Configuration management database (CMDB)
  - DSPM

Capabilities

Key capabilities in the Oasis NHI Management platform include:

- **Visibility and inventory:** Auto-discovers all identities, resources, secret managers, and workloads to enrich inventory information. Seamlessly connects with your environment and in minutes automatically creates a comprehensive inventory, providing a consolidated single pane-of-glass view.

- **Posture:** Automatically assesses and ranks posture issues based on their severity, allowing for a prioritized approach to addressing risks.
- **Remediation:** Provides tailored remediation plans that can be executed automatically.
- **Integration:** Integrates with a broad set of systems where NHIs are created including IaaS, PaaS, vaults, IDPs, and on premises to create a central view and inventory of all NHIs.
- **Context:** Provides critical contextual information beyond raw data by furnishing essential information including ownership, usage, consumers, resources, and privileged status.
- **Life-cycle management:** Effortlessly orchestrates the entire life cycle with automated onboarding, monitoring, and decommissioning, all through a unified interface.

Benefits

The Oasis NHI Security Cloud helps organizations quickly realize tangible business benefits, including:

- **Stronger security:** Eighty percent reduction of the identity attack surface
- **Simpler compliance:** Continuous access review and attestation
- **Better governance:** One hundred percent policy enforcement
- **Operational efficiency:** Forty percent reduction of time spent on rotations and reviews

Accelerating Critical Enterprise Initiatives

The Oasis NHI Management platform helps accelerate critical enterprise initiatives such as:

- **Asset management:** Discover, inventory, and classify all NHIs for effective asset management.
- **Risk management:** Mitigate risks associated with NHIs through proactive monitoring and management practices.

- **Third-party access management:** Secure management of third-party access to NHIs, ensuring controlled and monitored access.
- **Compliance:** Ensure compliance by managing NHIs according to regulatory requirements and organizational policies.
- **Hygiene:** Ensure optimal identity hygiene by maintaining the cleanliness and security of NHIs.

Planning Your Journey to NHI Management with Oasis

Like many IT and security initiatives, effective NHI management is not a "one-and-done" undertaking; it's a journey that will lead your organization to a greatly improved security posture. Oasis can help you on your journey, addressing key NHI management use cases including:

- **Visibility:** See what you couldn't before:
  - Full NHI inventory
  - Ownership assignment
  - Consumer classification
  - Resources and permissions mapping
- **Security:** Prioritize and remediate existing posture issues automatically:
  - Decommissioning stale accounts
  - Secret rotation
  - Right-sizing overprivileged accounts
- **Governance:** Align and enforce processes to best practices with automation
  - Safe automated secret rotation
  - Enforce by-policy provisioning
  - Safe employee offboarding

IN THIS CHAPTER

- Setting goals, choosing the right tool, and understanding your perimeter
- Defining a framework, strengthening security posture, and automating life-cycle management

Chapter 4
Ten (or So) Steps for Deploying an Effective NHI Management Program

This book covers the ins and outs of non-human identity (NHI) management — what it is, why it matters, and best practices. But how do you translate theory into action? Follow these ten (or so) steps to transform your objectives into a strategic, actionable road map to effectively manage and secure your NHIs:

1. **Define the scope and set goals.**

   Start by defining clear objectives and success criteria to guide your NHI management program. Begin with stakeholder mapping, involving key players like the chief information security officer (CISO), cloud administrators, and security architects to navigate the NHI landscape and implement policies effectively. Then map and document all relevant environments — cloud, on-premises, and hybrid — where NHIs operate.

2. **Select an NHI management tool.**

   Choosing the right tool is critical to your program's success (see Chapter 2). Select a solution that addresses the risks and business priorities identified in Step 1 and that can handle your specific environment. Ensure that the tool supports key areas like identity discovery, ownership assignment, periodic attestation, automatic remediation, and life-cycle management. For hybrid environments, make sure the tool provides seamless management across different systems and integrates with your security stack.

3. **Define and understand your perimeter.**

   With your tool selected, the next step is to gain full visibility into your NHI perimeter. Use the tool to scan, discover, and inventory all NHIs across cloud, on-premises, and hybrid environments. When visibility is achieved, assign ownership of each NHI to ensure accountability throughout its life cycle — from creation to decommissioning. This will help avoid unmanaged or orphaned accounts, which can create security risks.

4. **Define a policy framework and set priorities.**

   Define policies that govern NHI access, attestation, secret rotation or federation, and decommissioning. Implement least-privilege access for all NHIs and automate key processes such as secret rotation, recertification, and auditing. Your policies should align with industry best practices and regulatory standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or Zero Trust Architecture.

5. **Strengthen your security posture.**

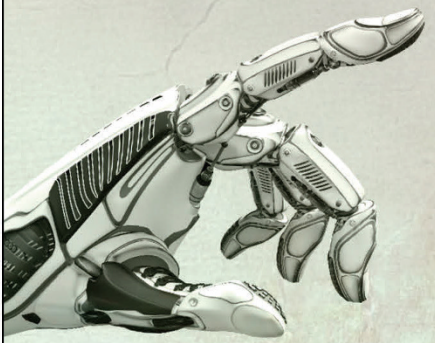
   Evaluate and address NHIs that fall outside established policies, such as over-privileged accounts or unrotated secrets. Break the problem into manageable parts to prioritize and resolve the most critical risks first, ensuring effective and efficient remediation.

6. **Automate life-cycle management of NHIs.**

   Automation ensures that provisioning, secret rotation, compliance, attestation, and decommissioning are consistently applied without manual intervention, minimizing errors and operational overhead. Begin with pilot automation in nonproduction environments to test workflows and policies. After they're validated, scale automation across your organization to streamline operations, enhance efficiency, and maintain compliance as your business grows.

OASIS

Manage & Secure Non-Human Identities



VISIBILITY

Gain a full understanding of your environment across IDPs.

GOVERNANCE

Streamline identity lifecycle management with policy-based automation.

SECURITY

Develop tailored security policies, and continuously assess your security posture.

oasis.security

Discover and manage your non-human identities

Non-human identities (NHIs) serve as digital gatekeepers, enabling secure machine-to-machine and human-to-machine access and authentication within modern enterprise systems. The rapid adoption of microservices, third-party systems, and cloud-based platforms has led to the exponential growth of NHIs, creating a complex web of interconnected systems. But unlike human identities, NHIs typically are not centrally managed and, thus, represent a major risk to organizations. Non-Human Identity Management For Dummies will help you securely manage NHIs across your digital estate.

Inside...

- Secure non-human identities
- Automate key management
- Address non-human identity risks
- Secure the entire identity fabric
- Plan your journey to NHI management

Lawrence Miller served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the coauthor of *CISSP For Dummies* and has written more than 200 *For Dummies* books on numerous technology and security topics.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-32001-1
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.