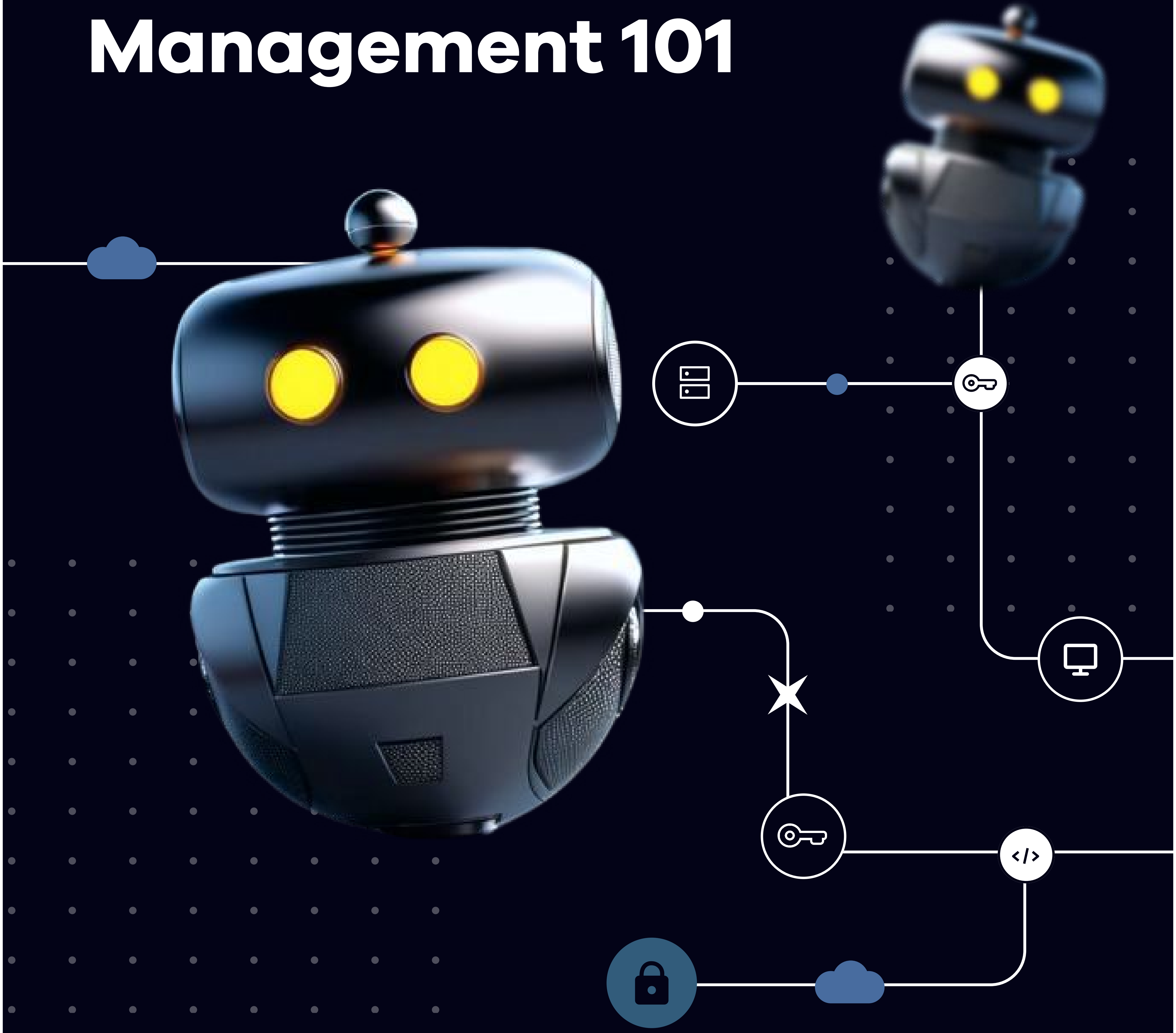
QASIS

Ebook

Non-Human Identity Management 101



2024

Table Of Contents

Introducing Oasis: the Non-Human Identity Management Platform 03

What's Broken with Identity Management? 07

What are Non-Human Identities? 11

Decommissioning orphaned and stale Non Human Identities 16

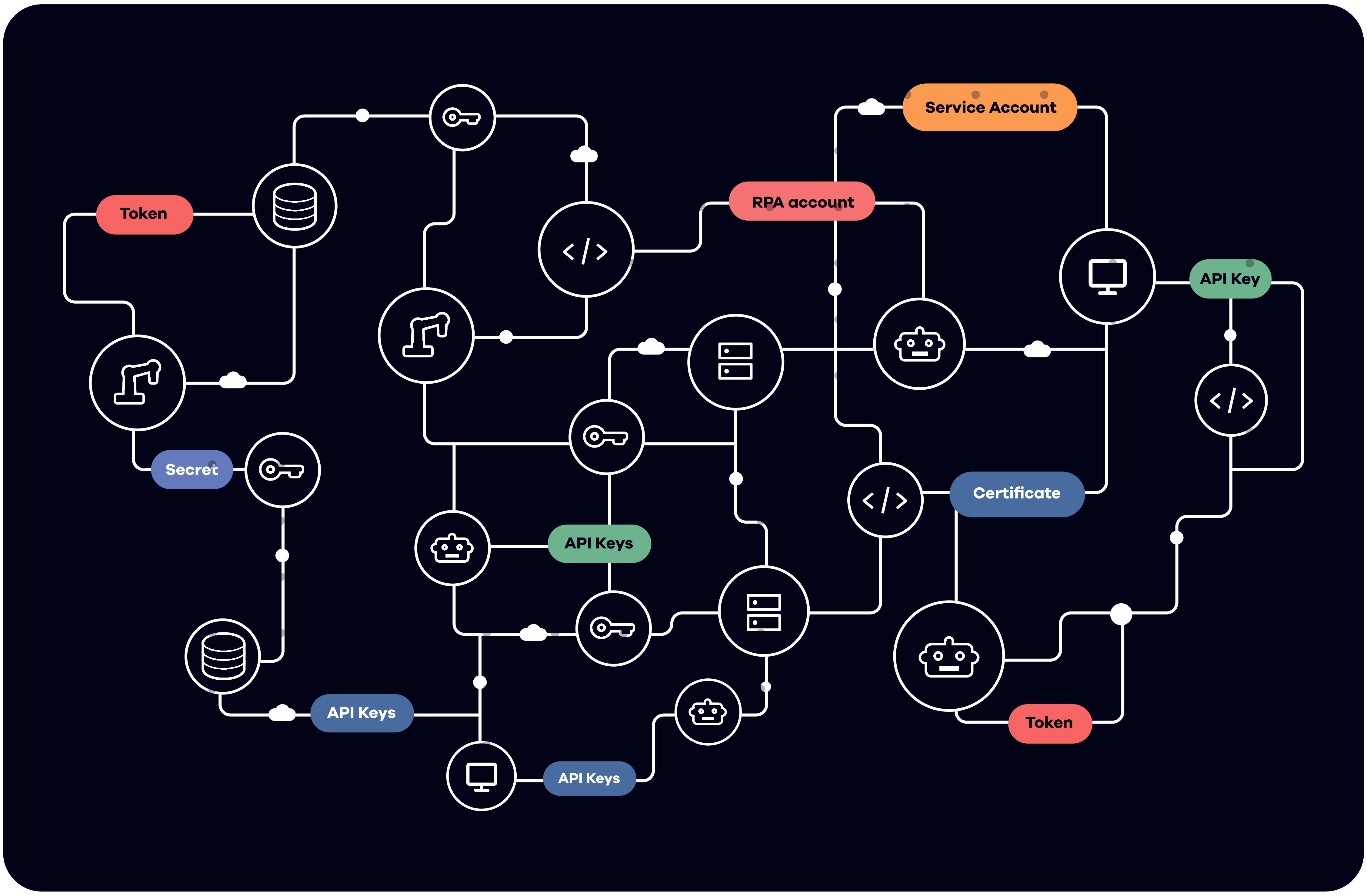
Securing Generative AI with Non-Human Identity Management and Governance 20

What Are Storage Accounts And How To Secure Them? 24

CSPM vs. NHIM (Non-Human Identity Management) 28

How does Non-Human Identity complement Privileged Access Management for 360-degree security? 33

What are Service Accounts and how should you secure them? 37



01

Introducing Oasis: The Non-Human Identity Management Platform

Why Is A Non-Human Identity Management Platform Now Necessary?

To put it in simple terms: identity is the new perimeter and Non-Human Identities (NHIs) are the gaping hole in that perimeter.

NHIs (Service Accounts, Service Principals, IAM Roles, Secrets, Tokens, Keys, etc.) , now outnumber humans by a factor of 10-50x, and constitute a massive attack surface that needs to be secured.
The security risks are further compounded as, on average, there are 5 times more non-human identities with broader access privileges to sensitive data than there are humans. Despite the risks, NHIs are a blind spot for most enterprises because they lack the right tool to manage them through their lifecycle.

Non-Human Identities are very different from human identities. NHIs have a more dynamic lifecycle - that typically spans beyond security teams directly involving developers - and are mission critical for business continuity. The scale, speed, diversity and distributed nature of NHIs bring a whole new set of management requirements that existing security tools, like CSPMs, PAMs, IAMs, and Secret Managers, were simply not designed to address.

This leads to several critical issues that we hear about all the time in our customer engagements:

Lack of visibility

> - I don't know if all NHIs have been on-boarded in my vault
> - I don't know who is using this NHI and how easy it is to steal it
> - I don't know which permissions have been given to each identity

Inability to detect and assess vulnerabilities

> - I don't know if we have long-lived secrets
> - I don't know if secrets given to 3rd parties are in use and have the right permissions
> - I don't know if we are using NHIs that were owned by off-boarded employees

Guesswork and uncertainty

> - I'm not sure if these identities require these permissions
> - I'm not sure if I can rotate this secret without causing outage

Inability to efficiently operationalize security

> - I don't have a way to enforce best practices
> - Operations to execute rotation, right sizing permissions and removing stale NHIs are too complex and time consuming”
> - I can't convince R&D and Ops to adopt our security policy because they generate too much overhead”

Enter Oasis Non-Human Identity Management Platform

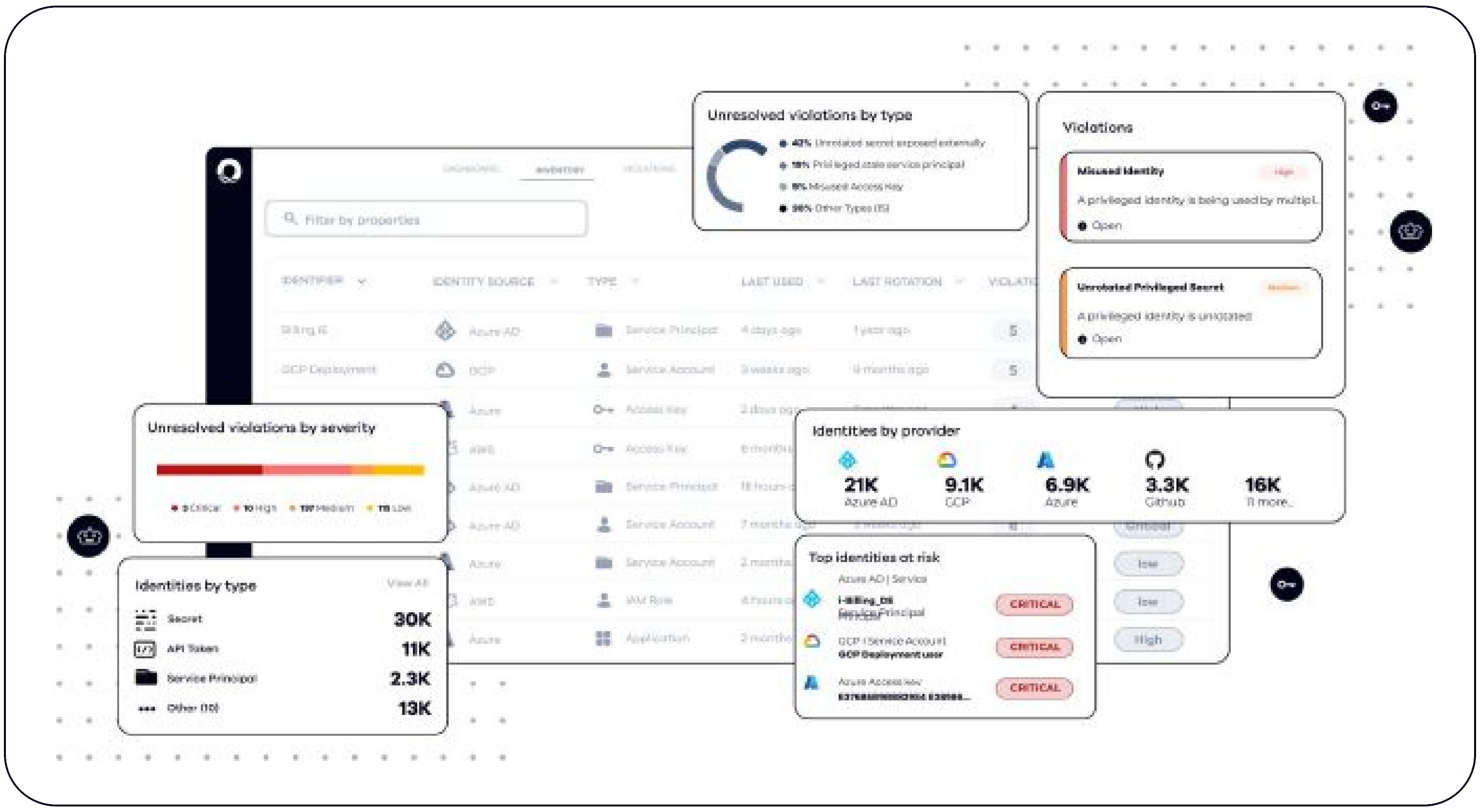
Oasis is the first enterprise platform purpose-built for Non-Human Identity Management. Our goal with Oasis is to empower organizations to secure NHIs throughout their lifecycle removing the operational barriers that have so far prevented security and engineering teams from addressing this critical domain.

We built Oasis with an “identity-first” approach that starts from your cloud infrastructure and extends to SaaS and on-premise systems. With operational complexity being a critical pain point that enterprises are facing, we have placed a ton of emphasis on making the product extremely easy to use, super-smart and automation rich out-of-the-box. As developers are core stakeholders of the NHIs lifecycle, we strived to create a solution that is by-default developer ready and programmable.

Plugging in Oasis in your environment is super simple and can be done in minutes. The platform agentlessly connects with all major public clouds (AWS, Azure, GCP) and can be further integrated with leading identity management systems, secret management solutions, ITSM systems, and developer platforms.

Once connected, most of your work is done! Oasis’s built-in Posture & Remediation Intelligence (PRI) engine begins to continuously analyze your environment to:

- discover all NHIs (new and legacy)
- create a comprehensive inventory of all NHIs providing rich contextual information on who owns it, consumes it, what resources it grants access to and how privileged it is
- Identify any security posture vulnerabilities classifying them by severity
- generate tailored remediation plans that can be executed in manual, semi-automated and fully automated mode


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

Unresolved violations by severity

● 3 Critical ● 10 High ● 137 Medium ● 115 Low

Identities by provider

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

Identities by type — View All

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

Top identities at risk

Azure AD | Service Principal I-Billing_DE	CRITICAL
GCP | Service Account GCP Deployment user	CRITICAL
Azure Access key E37685f09002f04 E38f66…	CRITICAL

IDENTIFIER	IDENTITY SOURCE	TYPE	LAST USED	LAST ROTATION	VIOLATIO…
Billing IE	Azure AD	Service Principal	4 days ago	1 year ago	5
GCP Deployment	GCP	Service Account	3 weeks ago	8 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		
	Azure	Service Account	2 months		
	AWS	VM Role	4 hours		
	Azure	Application	3 months		

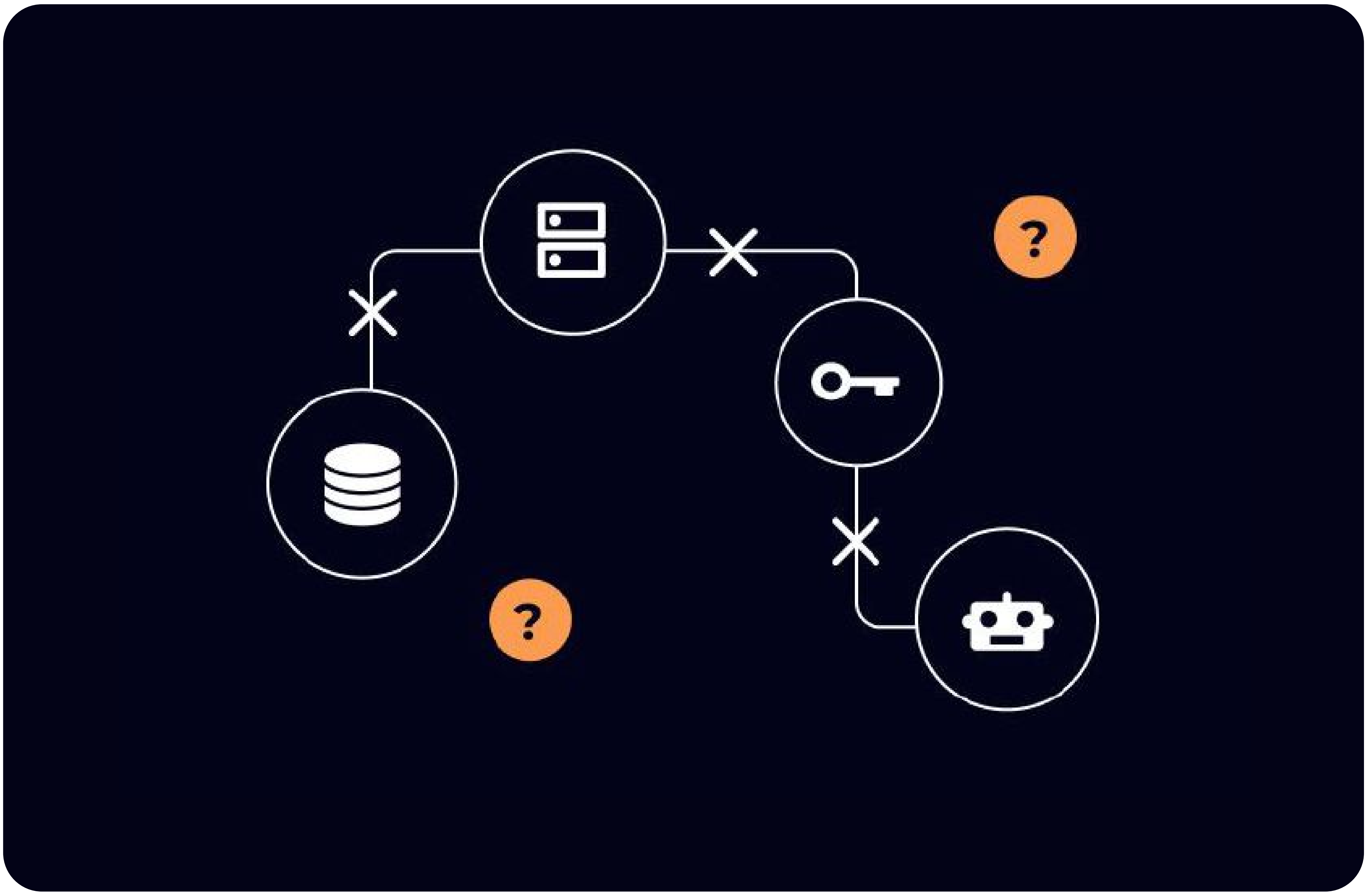
Thanks to these capabilities, Oasis customers have been able to quickly "clean up the mess" in their environments, gaining unprecedented visibility and rapidly eliminating the risk exposure from NHI related vulnerabilities.

Fixing what's broken it's just the first step, though. The second is about "stop the bleeding". In other words, manage NHIs securely from the start, taking control and automating the full lifecycle of NHIs. This is why another critical focus area for R&D is lifecycle management automation to streamline operations and provide holistic governance from provisioning, to rotation to decommission.

Oasis Delivers Unmatched Value. Don't Just Take Our Word For It!

We pride ourselves on being a customer centric organization. Since the early days, we've been working in close collaboration with many CISOs, CIOs, identity and security teams to build the best in class solution for NHI management. While still in the early days, we are excited to witness the amazing results that our customers were able to achieve

> "Oasis has revolutionized our approach to non-human identity management, effectively addressing security challenges that remained unsolved by conventional methods. Their solution has significantly enhanced our security and governance framework, providing us with holistic visibility and lifecycle automation. This represents a new paradigm in non-human identity management, far surpassing the capabilities of traditional legacy systems.
>
> **Chris Mosteller,** Head of Identity Security, JLL



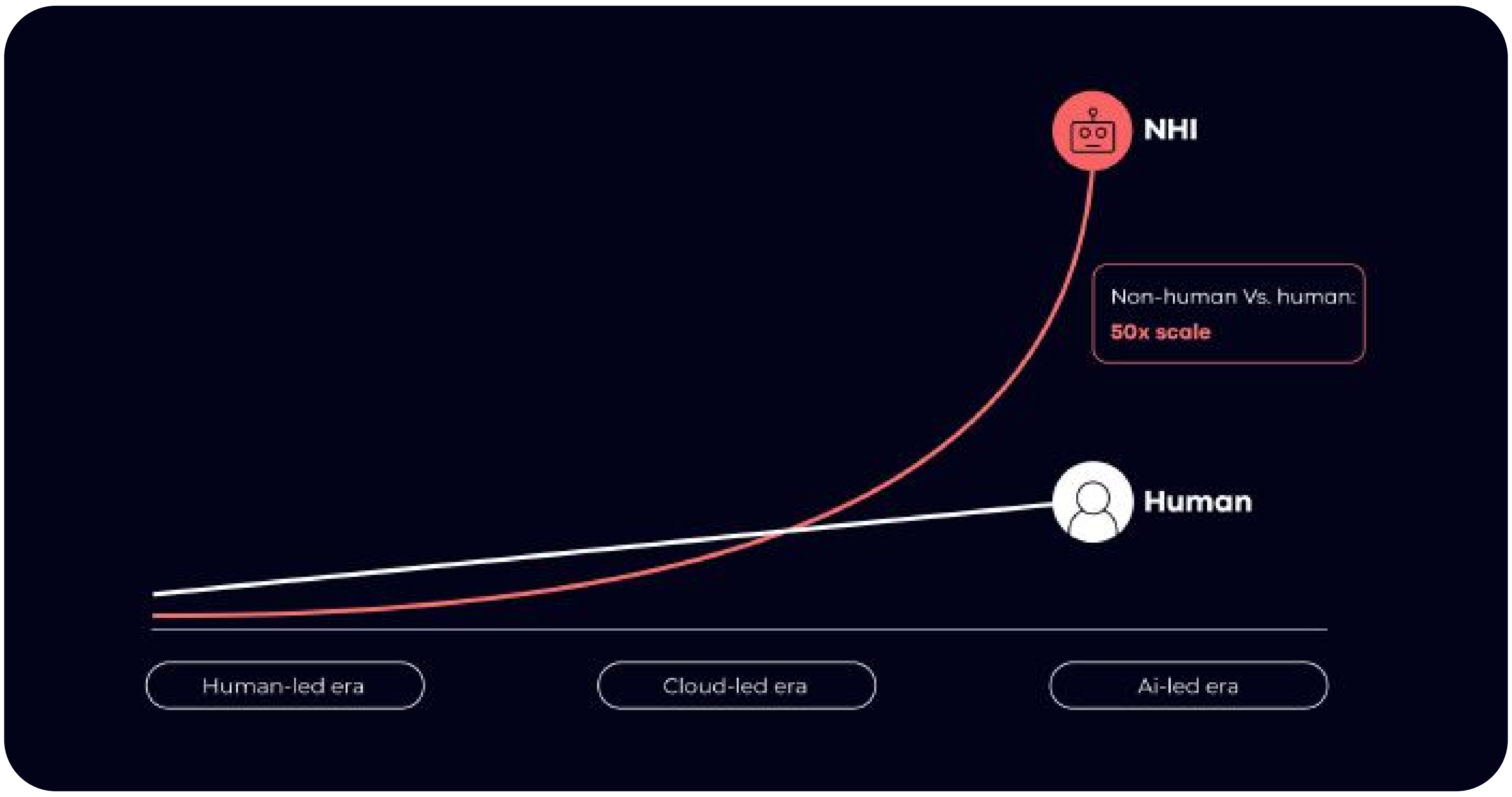
02

What's Broken With Identity Management?

Identity management is a critical component of enterprise security. Identities are the key construct through which we control how authorized entities (individuals, software or devices) can access data and perform actions. Historically, human identities have the primary focus of identity access management. While human identities remain strategically important, shifts in infrastructure and workload architecture have driven the exponential growth of non-human identities, completely changing the identity landscape and opening up new challenges.

Non-Human Identities Bring New Security Challenges

The shift to hybrid multi-cloud, microservices architectures and agile development has fueled the exponential growth of non-human identities, such as service accounts, principal accounts, IAM roles, secrets, tokens, keys, etc., which now outnumber human identities by 10-50x, opening a massive attack surface. With more and more business processes in the future being automated via AI-workflows and accessed by AI-powered services, this trend is likely to accelerate even more.



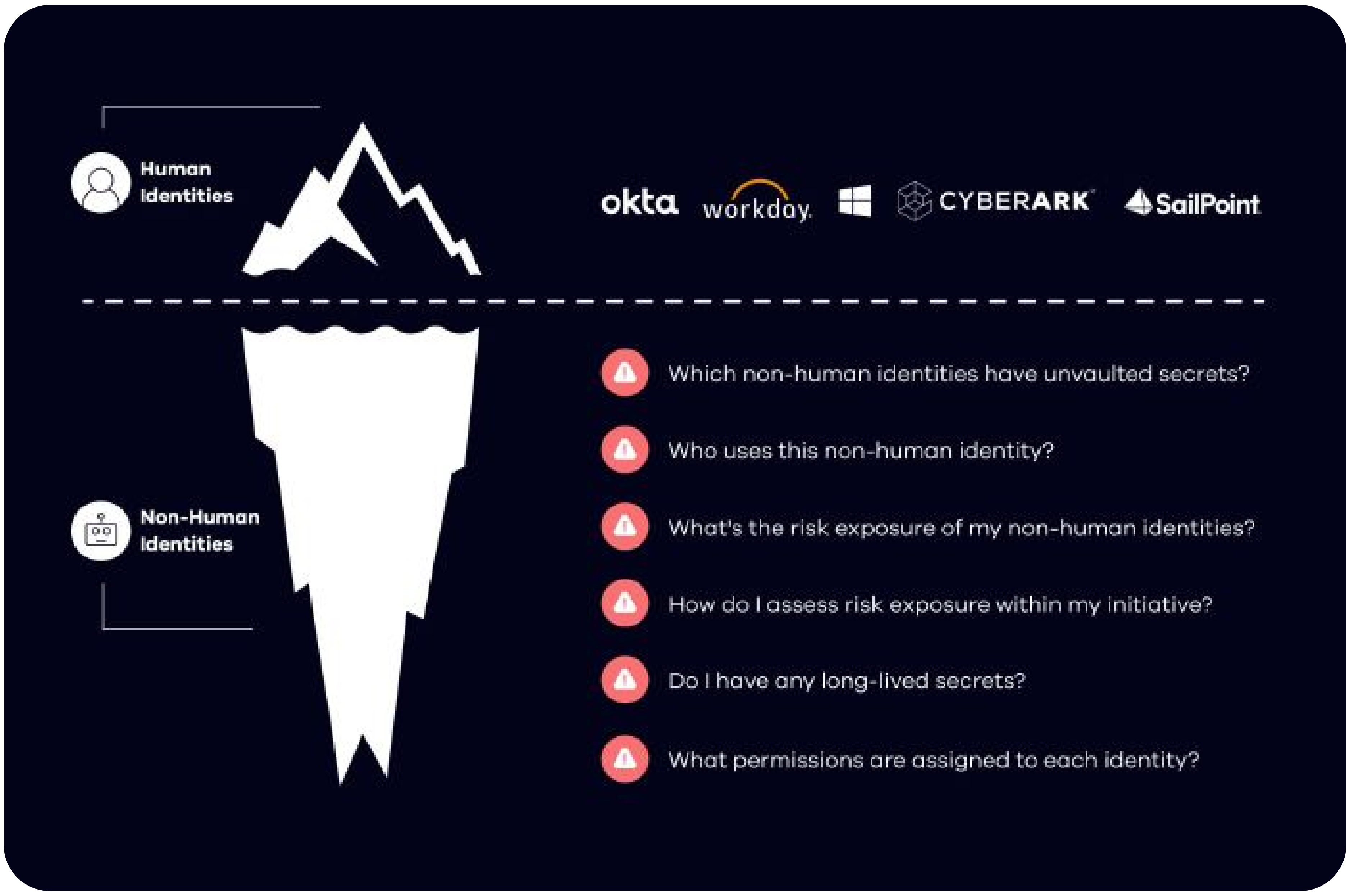
The security risks of unmanaged NHIs are further compounded by the fact that, on average, there are 5x more highly privileged NHIs than there are humans and that with NHIs organization can't leverage biometrics or other forms of secondary verification. Oasis research with organizations that don't have an NHI management enterprise strategy shows a rapidly growing attack surface with numerous toxic combination vulnerabilities.

It is not surprising to see an increase in the number of cyber attacks that involve exploitation of NHIs:

- 38TB of data accidentally exposed by Microsoft AI researchers
- Okta says hackers stole customer access tokens from support unit
- Slack employee tokens stolen, GitHub repository breached
- CircleCI incident report for January 4, 2023 security incident

Given their pivotal role, securing NHIs has consequently become a critical objective with high stakes, as a breached NHI could easily lead to data exfiltration and compromised business operations.

The Security Stack Doesn't Address Non-Human Identity Management


Human Identities
okta
workday.
CYBERARK
SailPoint
Non-Human Identities
Which non-human identities have unvaulted secrets?
Who uses this non-human identity?
What's the risk exposure of my non-human identities?
How do I assess risk exposure within my initiative?
Do I have any long-lived secrets?
What permissions are assigned to each identity?

The scale and dynamic nature of NHIs poses complex operational challenges that existing security solutions, such as IAM, PAM, CSPM, IAG, Secret Manager, aren't designed to address.

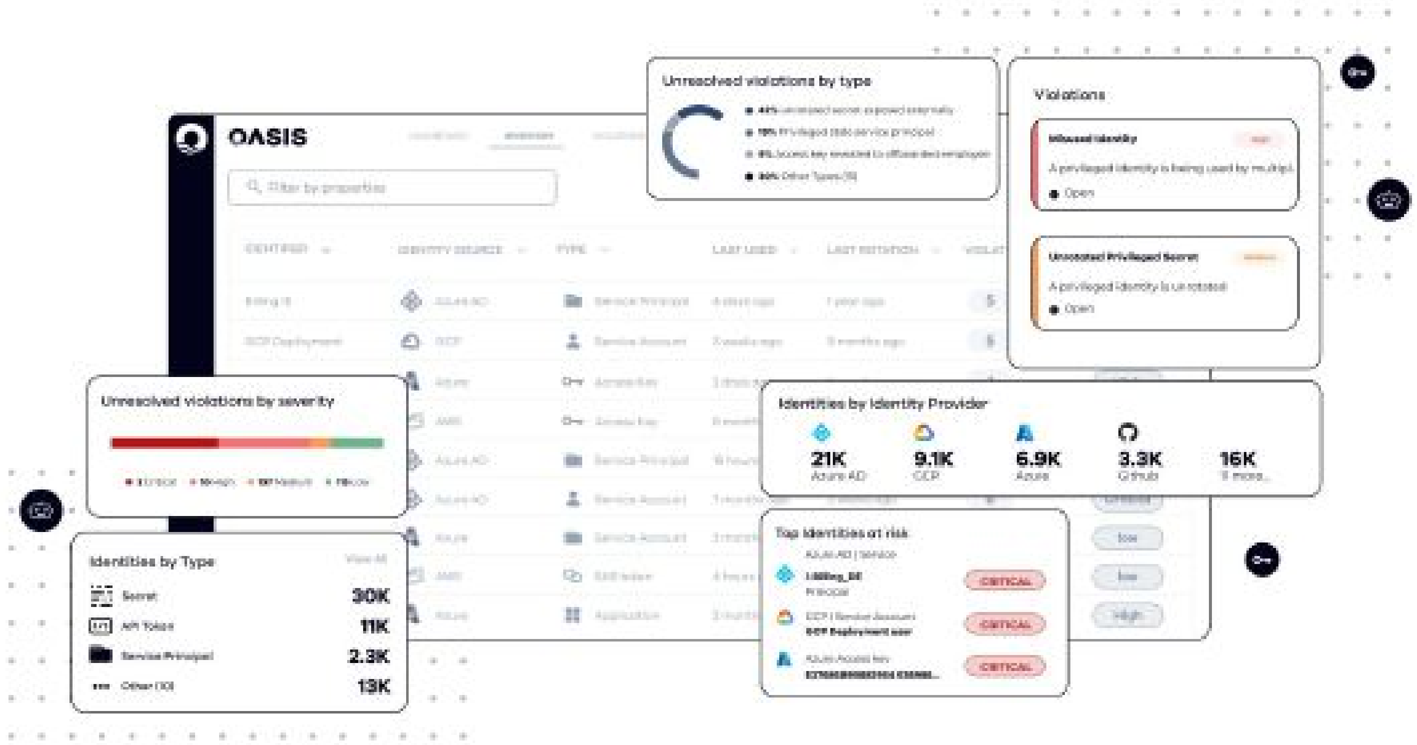
- **IAM and PAM** solutions focus on human identities and "break-glass" accounts used by humans. They are designed around a centralized management model where identities are provisioned and managed by a central team and are associated with an identifiable individual with the ability to leverage MFA.
- **Secret Managers** focus on vaulting of secrets, but are not identity-aware. Consequently, they lack the knowledge of ownership, usage, permissions and accessed resources. As a result, they can be used effectively to implement security policies or to automate processes like secret rotation.

- **CSPMs** are focused on cloud - not all NHIs live in the cloud - and take an infrastructure-first vs. identity-first approach. While CSPMs can show certain posture issues, they won't help to actually remediate the threat. As a result issues will just continue to pile up to the never ending list that the security team needs to take care of, with no solution or fix.

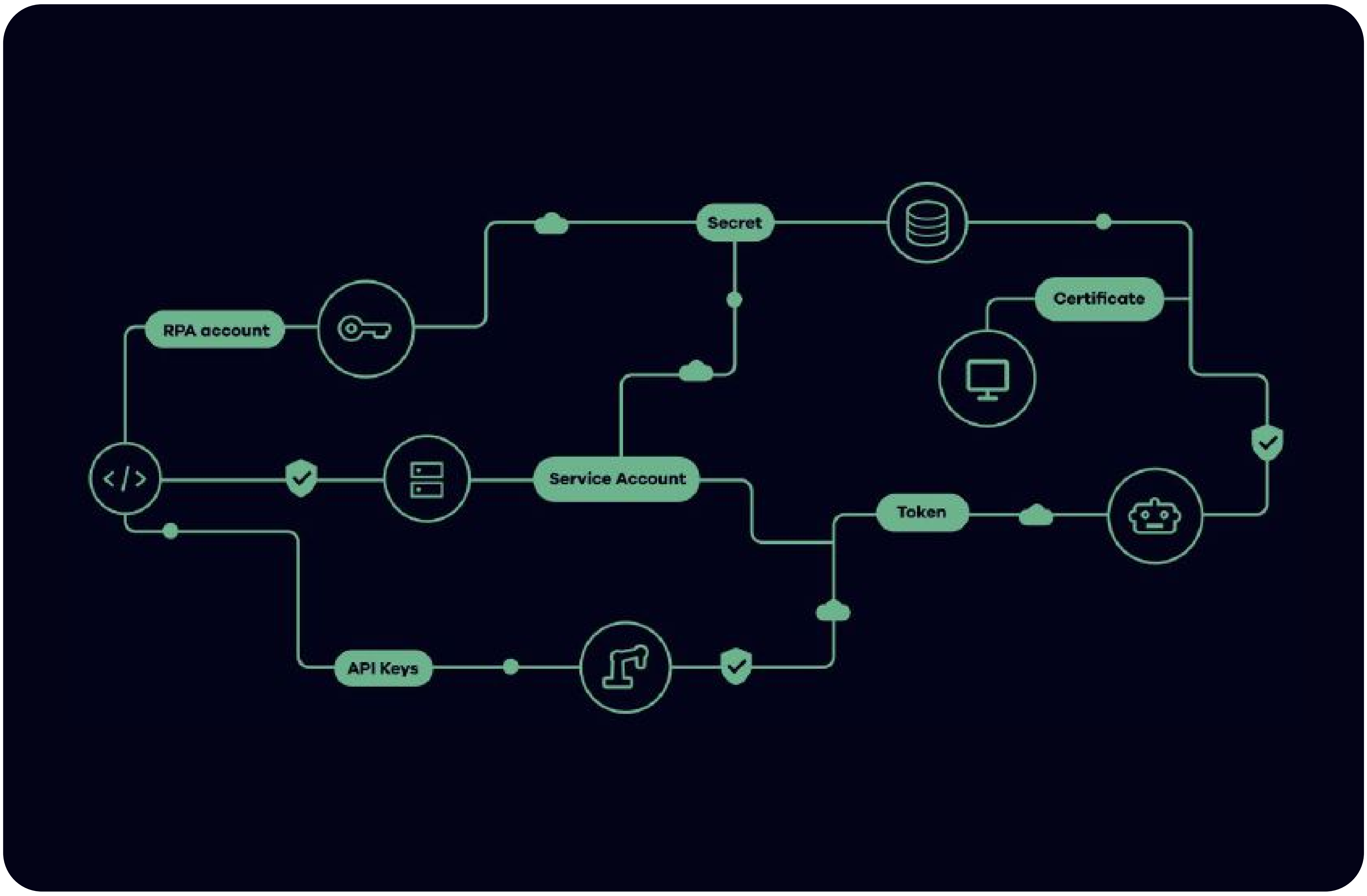
Non-human identities are deeply ingrained into operational systems and software. Lack of holistic visibility with relevant contextual information and control over their lifecycle could mean significant downtime for business critical applications when reacting to a threat or even during regular maintenance operations.

Comprehensive, Actionable Non-Human Identity Management With Oasis

Our goal at Oasis is to solve the NHI security gap. Our mission is to fortify cybersecurity defenses while simplifying security operations by giving security, identity and operations teams the visibility and automation they need to manage non-human identities at scale and throughout the complete lifecycle.



Our breakthrough platform is the first enterprise Non-Human Identity Management platform, purpose-built to secure the complete lifecycle of NHIs across the hybrid cloud. Simple to set up in minutes and natively integrated with major cloud and enterprise SaaS providers, Oasis automatically discovers all NHIs and continuously analyzes your environment to identify, classify and resolve security posture risks with auto-generated, tailored remediation plans that can be executed in manual, semi-automatic or fulling autonomous mode.



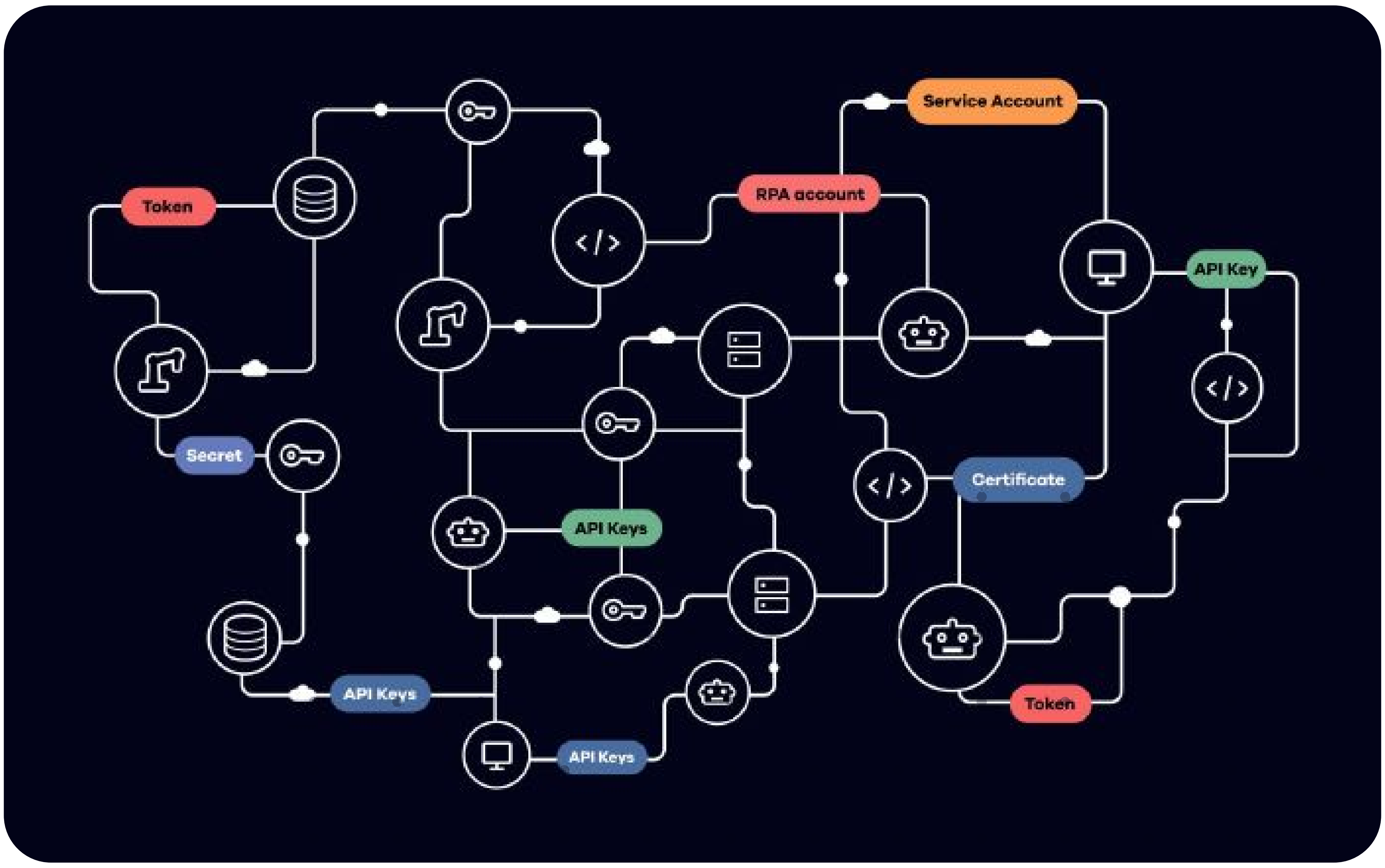
03

What Are Non-Human Identities?

A **Non-Human Identity** (NHI) is a digital construct used for machine-to-machine access and authentication. NHIs are pivotal in today's evolving enterprise systems, especially as organizations transition towards machine-centric architectures. The need for rapid innovation has spurred the proliferation of microservices, 3rd-party services, and cloud-based solutions, creating a complex network where secure machine-to-machine access is governed by diverse NHIs that now form a vast ecosystem that outnumbers human identities by 10x-50x.

The landscape of NHIs is intricate, with definitions and constructs dependent on factors such as cloud providers, SaaS platforms, and on-premises systems. Cloud providers (AWS, Azure, GCP), SaaS (Snowflake, Databricks, Github, etc.), on-prem systems (ActiveDirectory, etc.) all use different models to create and manage NHIs. Unlike Human Identities, NHIs utilize a broader array of authentication mechanisms, lacking the security safeguard of Multi-Factor Authentication (MFA) commonly found in Human Identities.

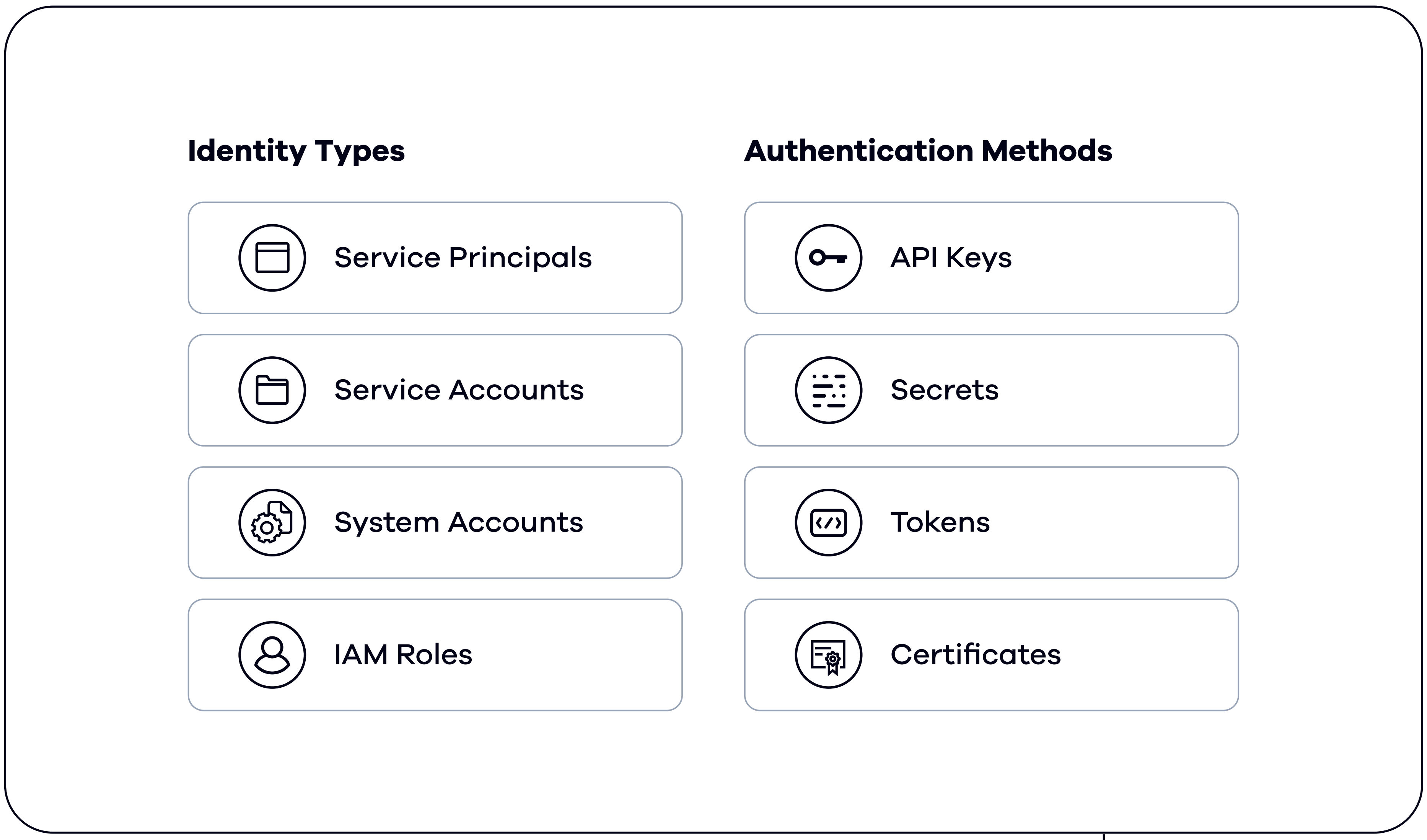
Non-human identities are a crucial aspect of modern security frameworks and the identity stack, presenting a distinct paradigm from traditional human identities within organizational ecosystems.



Examples Of Non-Human Identities

Examples of NHIs include Service Accounts, System Accounts, Application Accounts, and Machine Identities. Authentication methods for NHIs vary, incorporating secret information and federation mechanisms. Examples of authentication methods for NHIs encompass Secrets, Keys, Access keys, Certificates, and Tokens, each serving specific purposes in secure communication and authorization.

Special considerations arise in scenarios where identities are inseparable from the authentication string, as seen in Storage account access keys, Shared Access Signatures (SAS) tokens, and API keys for Software as a Service (SaaS) applications like Snowflake. In such instances, the authentication mechanism encapsulates permissions configuration, complicating identity management and access governance. As organizations continue to automate business processes with AI, the growth of Non-Human Identities is expected to accelerate, underscoring their critical role in the evolving landscape of enterprise systems.



Identity Types

- Service Principals
- Service Accounts
- System Accounts
- IAM Roles

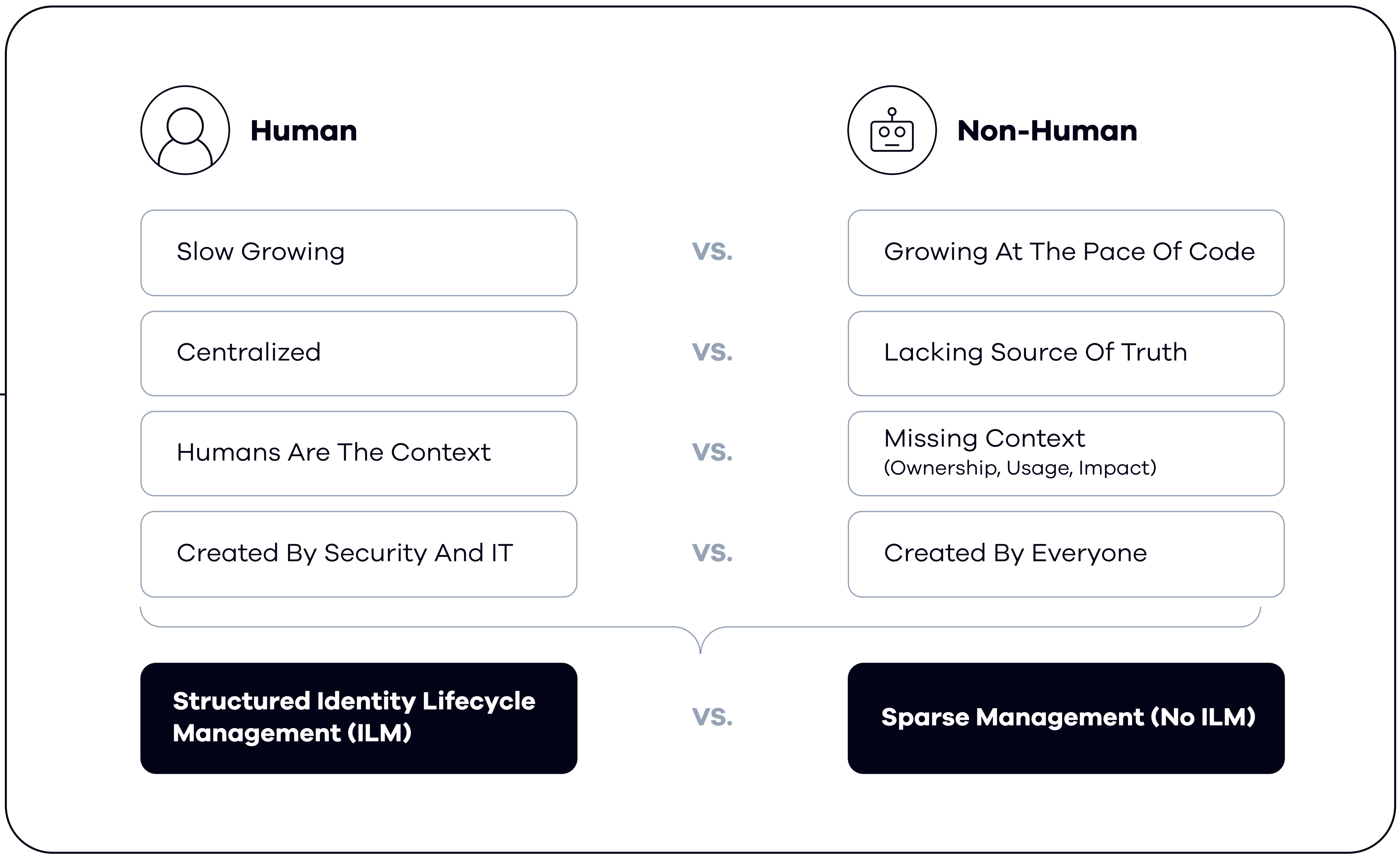
Authentication Methods

- API Keys
- Secrets
- Tokens
- Certificates

Human Identities Vs. Non-Human Identities

NHIs differ significantly from human identities in key aspects:

- **Decentralization:** NHIs are not centrally managed like human identities; instead, they are created and managed across multiple platforms by various stakeholders. It can be a real challenge to classify if a user is a human or a machine.
- **Ownership:** Unlike human identities, NHIs are not tied to specific individuals, evading regulatory requirements and often used by multiple administrators or applications.
- **Scale:** the large volume of NHIs (10x-50x more than human) 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 evolution, rendering them more challenging to govern. However, it's worth noting that NHIs can also persist unchanged for years without rotation or imposed consumer limitations.
- **Developer driven:** unlike with Human Identities, the creation and control of NHIs aren't centralized to IT or Identity Team. In many cases, NHIs are directly created by developers or even citizen developers in no-code low-code who may not be aware of their usage, as they represent the only means for the code they need to interact with systems
- **Secret expiration:** while frequent password rotation is very common around privileged users, many of the NHI are set to live for a very long time, and sometimes even without an expiration date.
- **Operational Risk:** Engaging with NHIs carries inherent operational risks. In the absence of a comprehensive understanding of all consumers, there is a potential for disrupting production systems. Moreover, 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. The basic concept of Human Identity security relies on the fact that you can use these three factors to secure the authentication: 1) something you know (for example, password) 2) something you are (for example, face recognition) 3) something you have (for example, mobile phone) and then do multi-factor authentication. With NHIs the only protection is the secret that the user (in most cases a developer) gave to the machine - there is no SSO or MFA in the middle. This means that if attackers get hold of a Service Account and the secret there isn't anything else that can stop them. In the cloud era, where APIs are the gatekeepers of access, identity becomes the new perimeter.



Human		Non-Human
Slow Growing	vs.	Growing At The Pace Of Code
Centralized	vs.	Lacking Source Of Truth
Humans Are The Context	vs.	Missing Context (Ownership, Usage, Impact)
Created By Security And IT	vs.	Created By Everyone
Structured Identity Lifecycle Management (ILM)	vs.	**Sparse Management (No ILM)**

The Need For Non-Human Identity Management Solutions

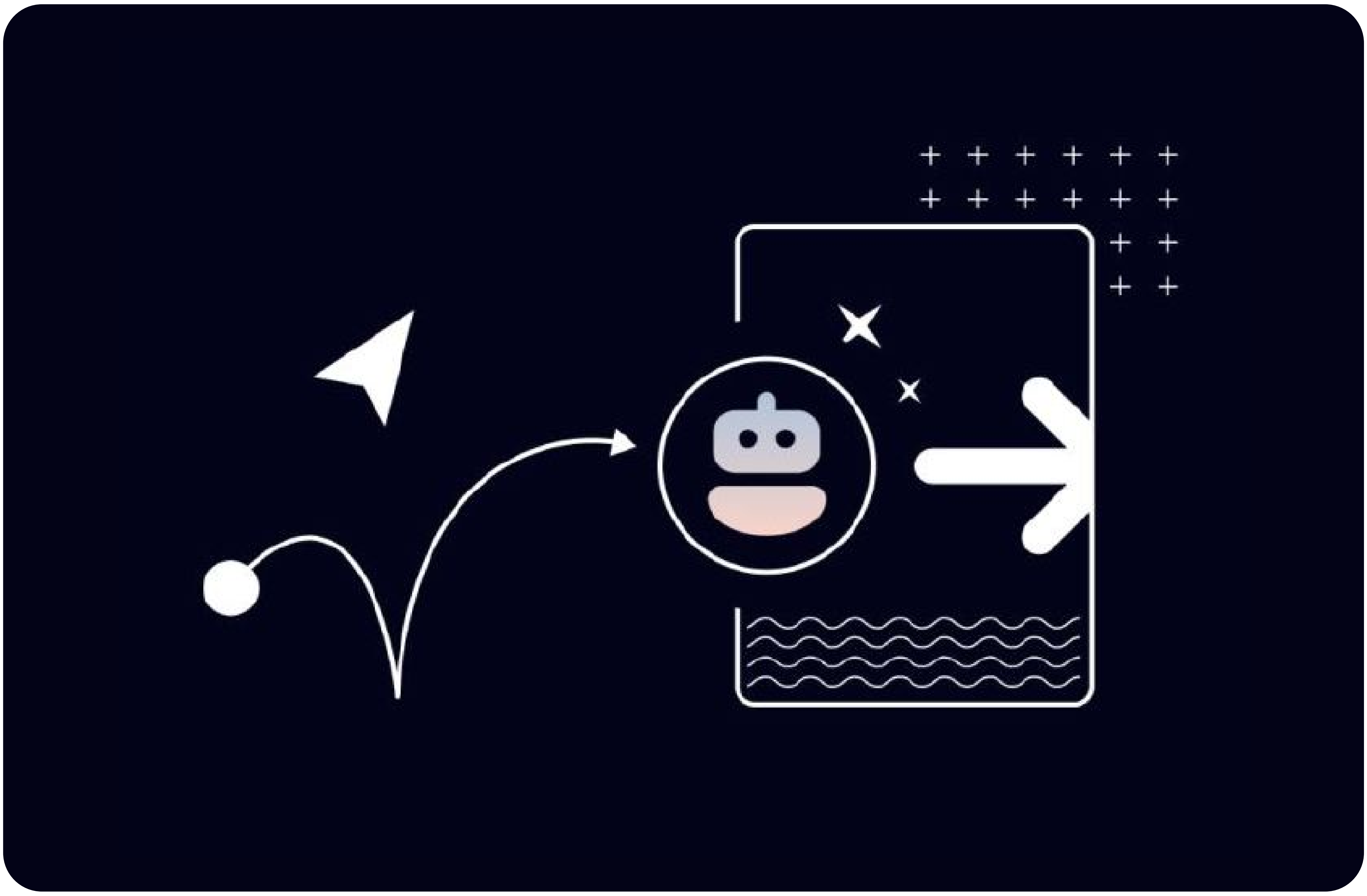
Due to their characteristics and the nature of their lifecycle, NHIs pose several new operational challenges:

- How to discover and inventory all NHIs across cloud providers
- How to identify and prioritize violations and risks
- How to gain critical context metadata information, such as usage, dependencies, owners, consumers and resources accessed, to be able to remediate vulnerabilities without breaking things
- How to take control and automate of the lifecycle of new and legacy NHIs

Despite the risks, non-human identities are often blind spot for most enterprises because they lack the right tool for the job. Existing security tools in the stack, such as CSPMs, PAMs, Secret Managers, IAMs, were not designed to address the new lifecycle management requirements of NHIs and, as result, fall short of the goal leaving organizations vulnerable.

Given the unique operational challenges posed by NHIs, there is a pressing need for specialized Non-Human Identity Management solutions. These solutions should address key requirements, including discovery and inventory management, risk assessment, lifecycle automation, and developer readiness.

Oasis platform for Non-Human Identity Management is now available to close this gap. Oasis takes an NHI-first approach with purpose-built capabilities for discovery, inventory, posture assessment, lifecycle automation, and developer readiness.



04

Decommissioning Orphaned And Stale Non Human Identities

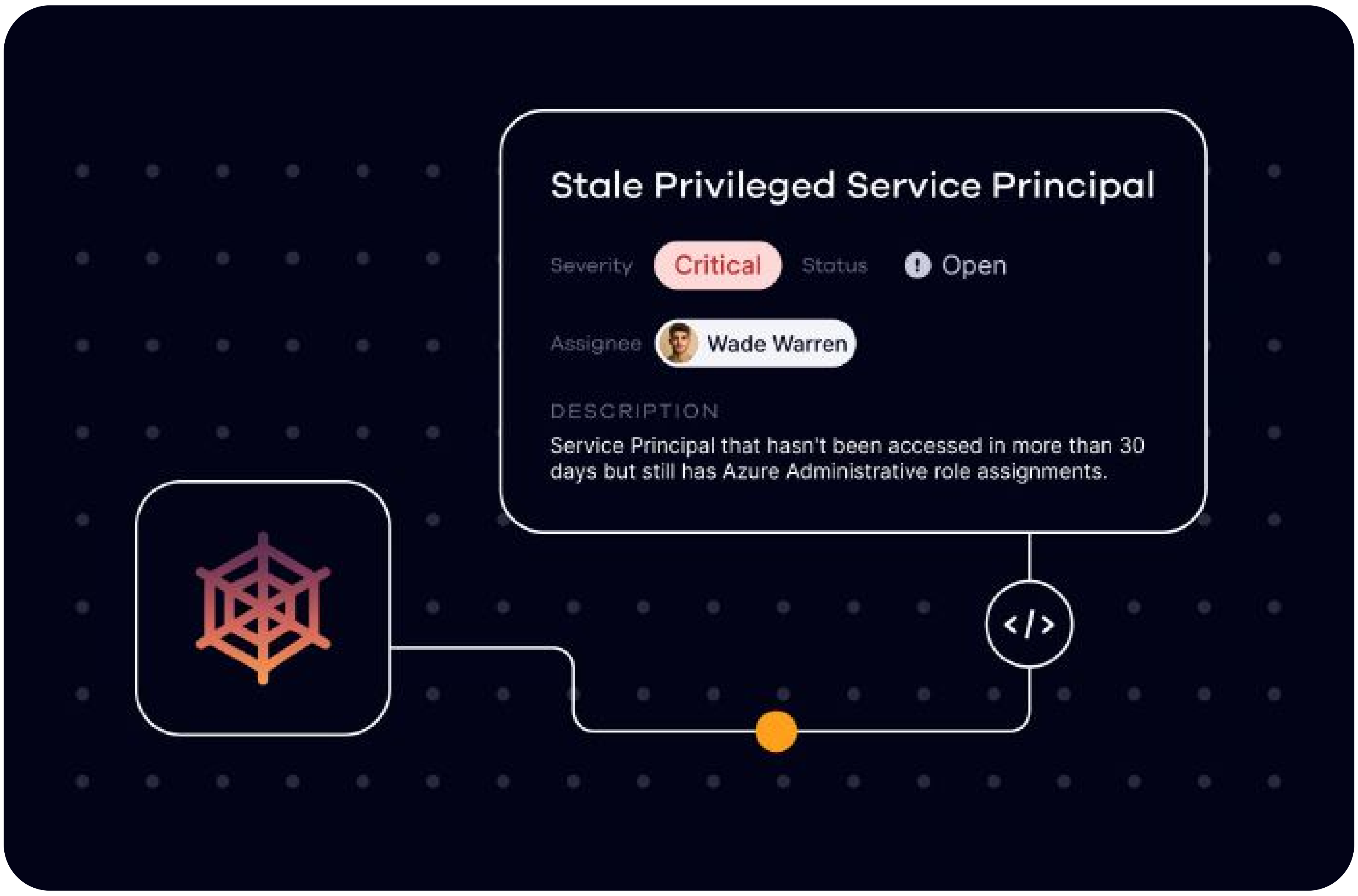
Unmanaged non-human identities (NHIs) pose a significant security risk in today's digital landscape. NHIs often operate outside traditional IT security reviews, making them vulnerable to exploitation. A common scenario we encounter during security assessments is the presence of stale or orphaned NHIs that should have been decommissioned but haven't.

An orphaned NHI is an NHI that is no longer in use but is still enabled and has active permissions. Stale or orphaned NHIs are typically the undesired outcome of changes in business operations, such as ceasing work with third-party vendors, changes in organizational structure, such as an employee leaving the company or transitioning to a new role, or technology changes, such as replacing an application. A common finding from our security assessment are stale NHIs from discontinued SaaS applications used for one-time tasks, such as data migration. Once the task is completed, these applications are often forgotten, left lingering in the environment without proper offboarding processes. From this simple example, it is easy to recognize how, in today's fast-paced business world, orphaned NHIs can become a common occurrence if an organization lacks good visibility and effective operational processes.

These NHIs represent a grave danger as they increase the attack surface and can serve as potential backdoors for extended periods without detection. For instance, cases similar to Cloudflare's recent breach have shown that exploited NHIs, which should have been decommissioned, served as entry points for unauthorized access.

The risk of inaction regarding unmanaged stale non-human identities extends even further. Over time, these dormant applications accumulate, needlessly expanding the attack surface. This situation parallels the risks seen in supply chain attacks, where adversaries exploit vulnerabilities in trusted third-party vendors or service providers to gain unauthorized access to networks and data.

Challenges With Decommissioning NHIs



Stale Privileged Service Principal

Severity: Critical   Status: Open

Assignee: Wade Warren

DESCRIPTION

Service Principal that hasn't been accessed in more than 30 days but still has Azure Administrative role assignments.

Offboarding non-human identities is a complex and error-prone process without the right tool for the job. The most common pain points we hear about before using Oasis are: #1 lack of visibility - "I don't know which NHIs are unused" - and #2 operational risk - "I don't know what an NHI is for, and I am afraid of breaking something". Insufficient understanding of security posture, rapidly evolving business needs, and ambiguous ownership are a few more.

A primary obstacle hindering the deletion of non-human identities is the difficulty in identifying and assessing their status accurately. Unlike human users, whose lifecycle within an organization is typically well-documented, non-human identities often operate in the background and are often excluded from the automated containment tools many detection offerings provide to stop identity-based attacks. This lack of visibility into whether these entities are still actively utilized complicates the offboarding process, leaving organizations susceptible to exploitation.

Moreover, the complexity of modern IT ecosystems further exacerbates the challenge of offboarding non-human identities. With the proliferation of interconnected systems, applications, and services, organizations struggle to maintain a comprehensive inventory of all non-human identities and their associated permissions. As a result, stale accounts and dormant identities accumulate over time, increasing the attack surface and presenting enticing targets for malicious actors.

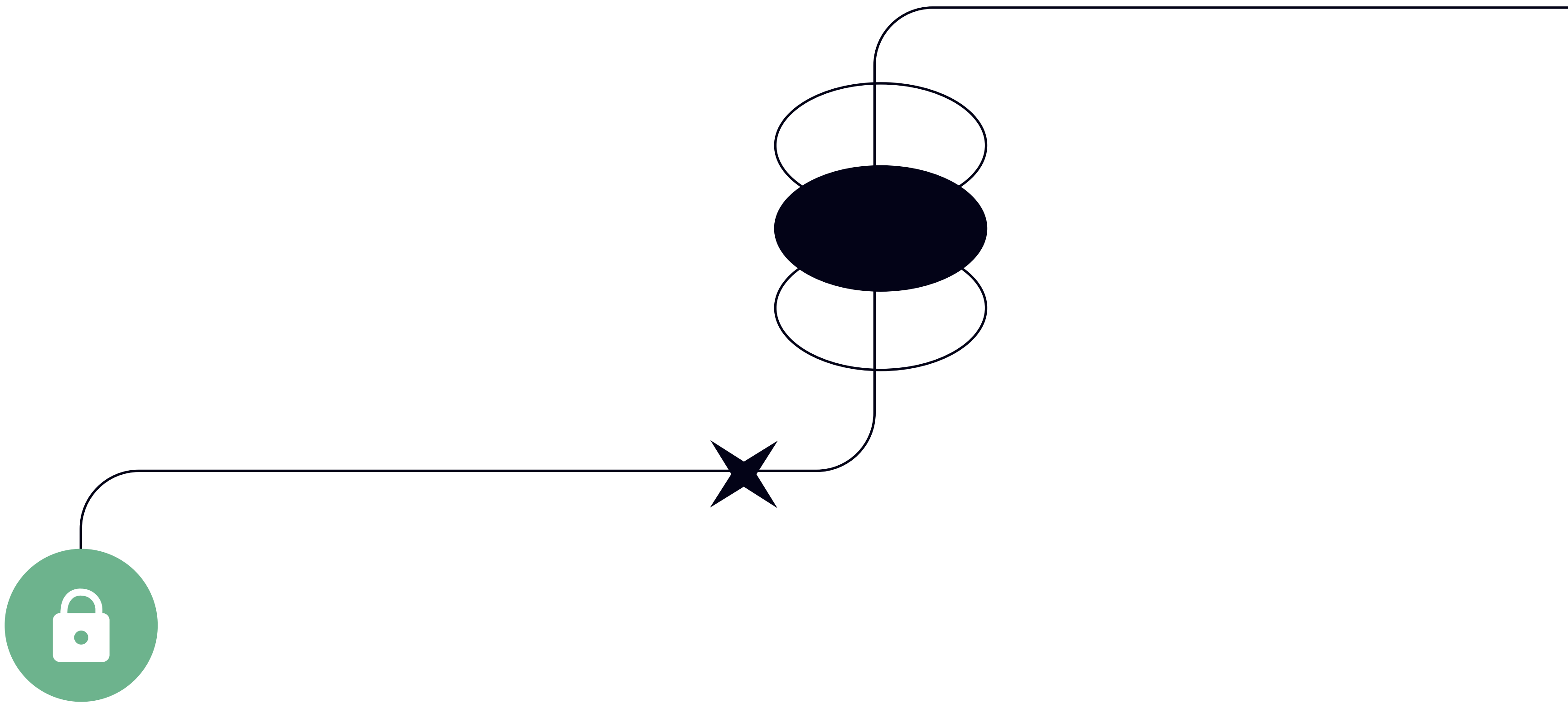
Because of the large scale and highly dynamic nature of NHIs, maintaining a reliable inventory is extremely challenging without automation. Recognizing if an NHI is orphaned or unused is even more complex because it requires critical contextual information on ownership and usage. Context and dependency mapping are also necessary to ensure that decommissioning operations won't impact business continuity. Prior to Oasis, for most organizations, managing operational risk involves manually tracking metadata and orchestrating cross-team triaging processes that can be laborious and prone to errors. In many cases, the complexity of manual operations becomes an insurmountable barrier that leads to inaction.

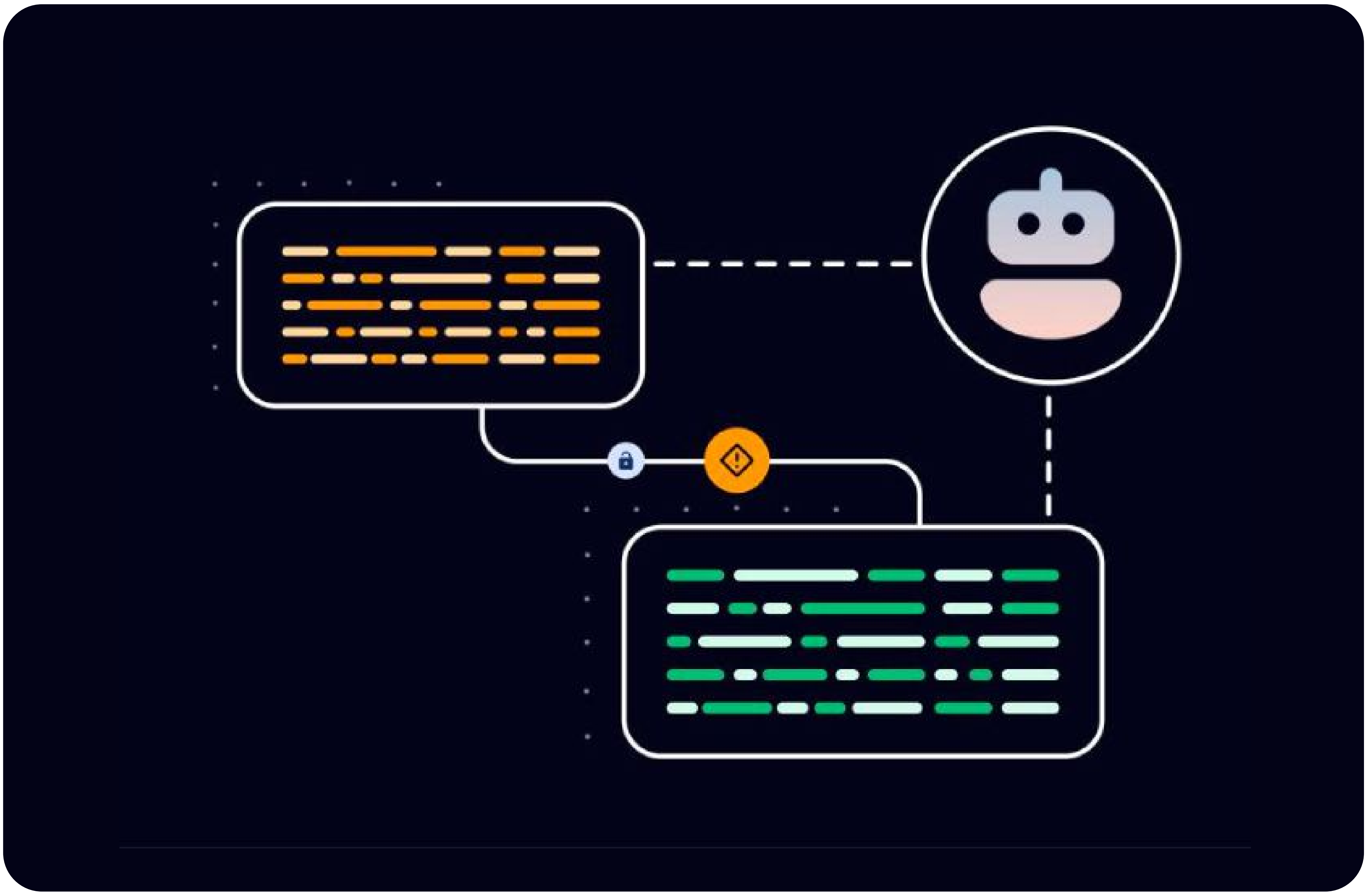
How To Decommission NHIs Without Operational Disruptions

To address these issues, organizations must adopt a proactive approach to non-human identity management. This includes implementing robust processes for regularly reviewing and revoking access permissions, establishing clear ownership and accountability for non-human identities, and leveraging advanced monitoring and analytics tools to detect and mitigate security risks promptly.

Leveraging a tool like Oasis, which automatically and continuously provides a holistic inventory of NHIs with rich contextual information, becomes paramount. Oasis ensures safe decommissioning that reduces the attack surface and also upholds the principle of least privilege access. Oasis incorporates risk-based prioritization principles that consider usage patterns to verify that an NHI is actually stale before recommending any action. By focusing on the most critical NHIs—such as those with privileged access, access to sensitive data, or external access—Oasis significantly alleviates any overhead and efficiently mitigates risks.

By investing in comprehensive non-human identity governance and management practices, organizations can mitigate the risks posed by these overlooked security holes. By doing so, they can strengthen their security posture, safeguard sensitive data, and ensure compliance with regulatory requirements in an increasingly complex and interconnected digital landscape.



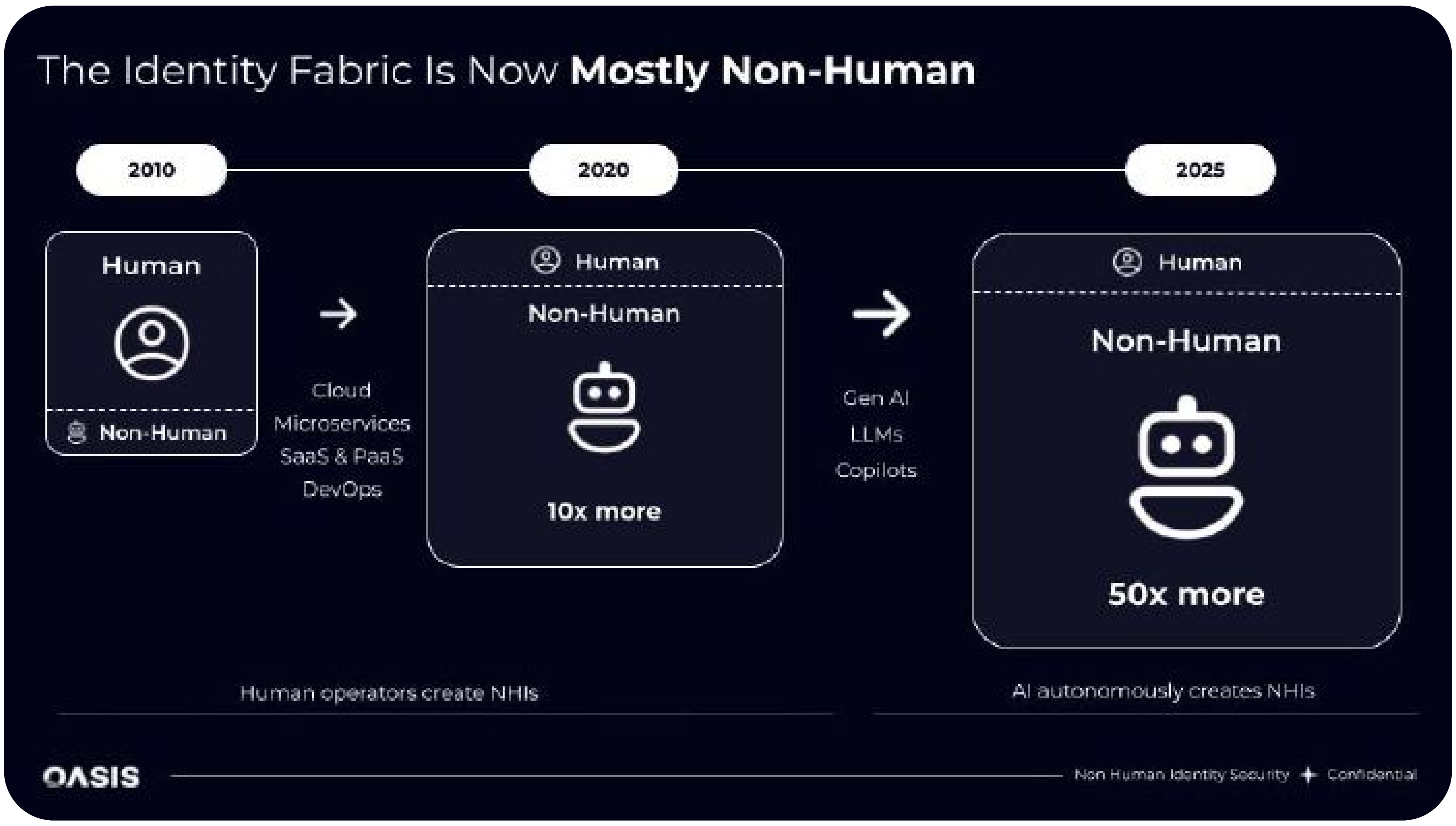


05

Securing Generative AI With Non-Human Identity Management And Governance

There are many inevitabilities in technology, among them is that rapid innovation will introduce unique risks and 3 letter acronyms will abide. Generative AI conversations have become top of mind, as business races to find the most value from a new technological arena, one that will transform our world in much the same way as other technological epochs like the emergence of the internet have. As we pursue the potential value of AI driven apps and automation, we will always need to consider the implications of the safe usage and implementation of such technologies. I will introduce some potentially new concepts and explain the need for proper non-human identity governance to ensure the privacy and integrity of data used in applications implemented under the RAG based architectural model.

What is retrieval augmented generation (RAG) architecture?
RAG is an agnostic architecture that allows the power of LLM's (large language models) like OpenAI's GPT (generative pre-trained transformer) to leverage "grounding data", data specific to a customer use case to power chat or Q&A based applications. The blending of the conversational power of LLM and local focused data sets make for a powerful tool to enable apps that drive more robust customer interactions and\or employee productivity. An example implementation would be leveraging a LLM of your choice tied to a local data store of product documentation to answer domain specific questions about your product. All the power of human-like articulation, powered by LLM with the relevance of your data, to drive a productive use case, and fully autonomous.



The Identity Fabric Is Now **Mostly Non-Human**

2010

Human

Non-Human

Cloud
Microservices
SaaS & PaaS
DevOps

2020

Human

Non-Human

10x more

Gen AI
LLMs
Copilots

2025

Human

Non-Human

50x more

Human operators create NHIs

AI autonomously creates NHIs

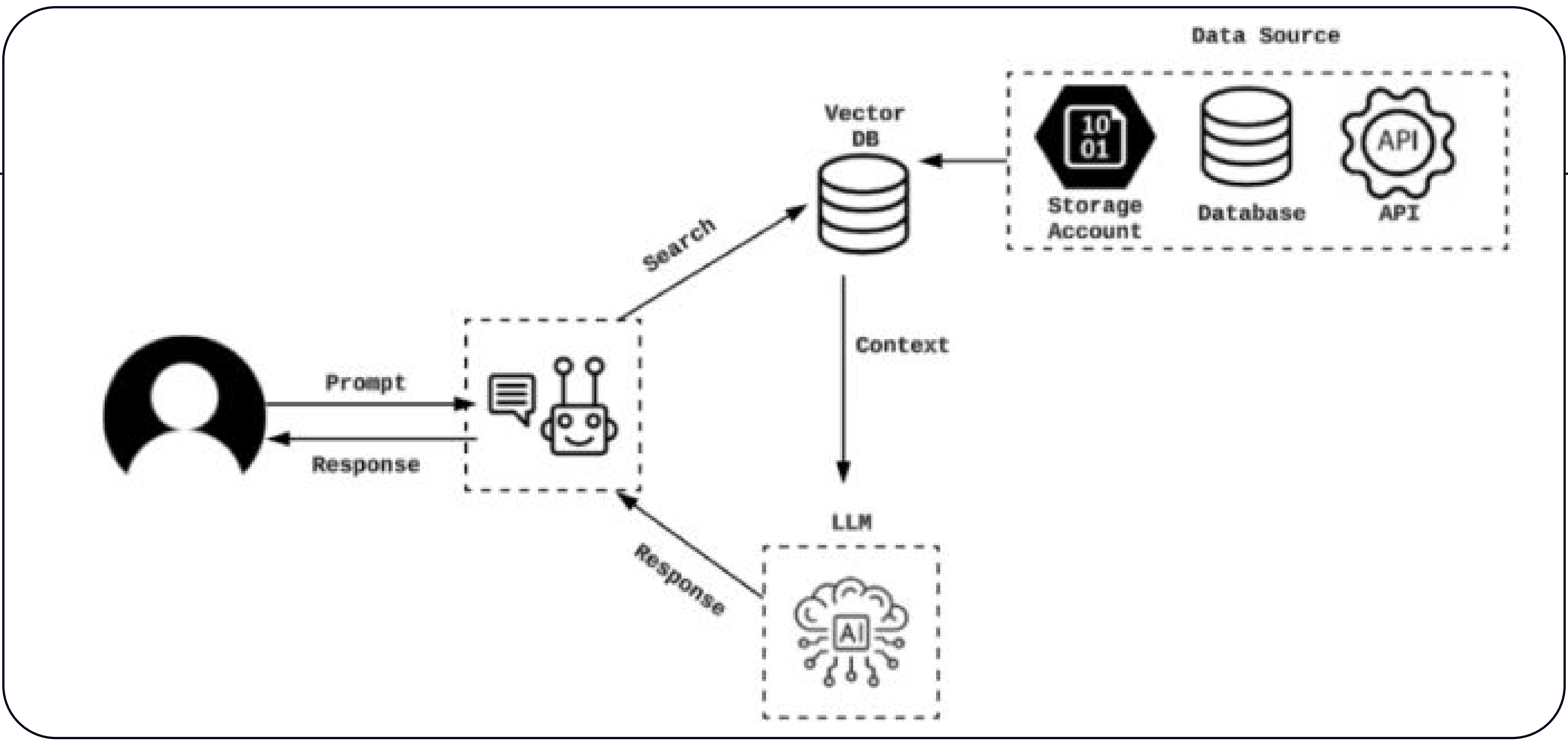
OASIS

Non Human Identity Security ✦ Confidential

AI will further increase the non-human identity attack surface

NHI is a digital construct that describes the credentialed access leveraged for machine to machine communication. These identities include service accounts, tokens, access keys, API keys, and countless others. NHI is the most rapidly expanding type of identity and the least governed attack surface for organizations today. The creation of NHI is democratized across dev, ops, and other teams, generally self governed and proliferates at the pace of digital innovation at an organization. NHI is more liberally leveraged in the cloud where the identity itself becomes the perimeter, or in other words the only form of access control. The combination of poor NHI governance and ubiquitous access has created a situation where the risk has become very pronounced. That risk is not going away and has expanded dramatically with the adoption of cloud and is on the precipice of further significant expansion with the advent of AI.

The intersection of NHI And RAG



In the diagram above I outline the basic flow of the RAG based architecture, and quickly we can see where NHI would drive the bridges of communication for backend machine to machine interaction. I will focus your attention on the data sources as I feel this is where implementation risk is most likely to live. One predominant implementation pattern observed online is the consistent use of storage accounts as a repository for unstructured data leveraged in the implementation of RAG architecture driven apps.

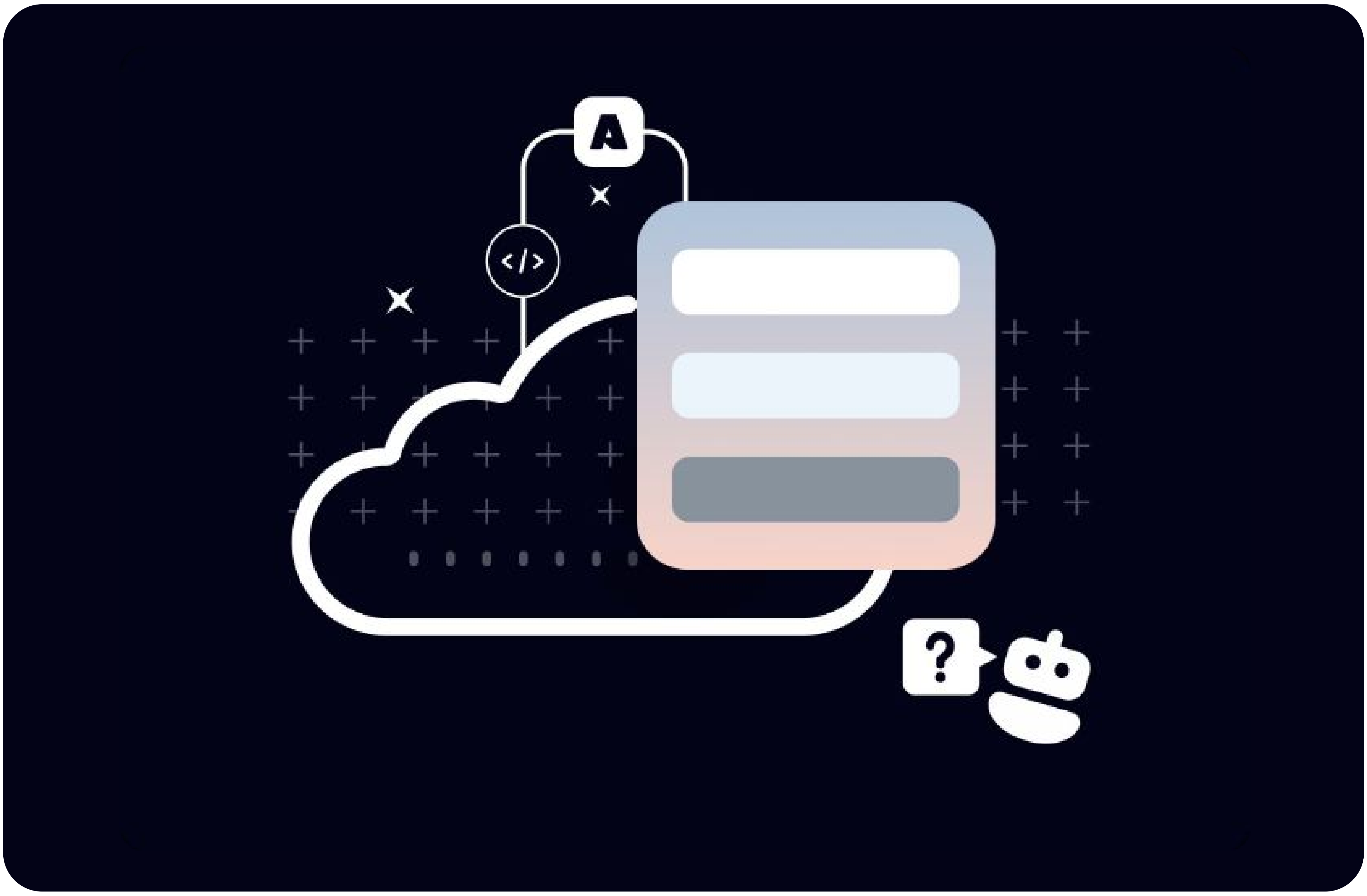
Exploring some of the access methods leveraged for storage accounts in cloud environments like Azure can help us understand some of the potential risks. Azure blob storage allows many forms of identity and access management, SAS tokens, service principals (Entra ID), and access keys among them. When configuring any of these access methods the utmost care should be taken to ensure least privilege and adherence to accepted best practices. It is unfortunately commonplace to see very old and unrotated (full access by default) access keys, SAS tokens with privileged access and very long TTL (time-to-live), or service principals whose usage is stale, secrets unrotated and not expiring any time soon. These examples are just some of the scope of the NHI that can introduce unwanted risk to a RAG based application.

Secrets used to assume non-human identities like those described above and others are stolen, accidentally exposed, and kept by former employees upon exit. The resulting risk to our app becomes multi pronged. Data privacy for any AI training data is a priority, sensitive data and the identities used to access should be locked down, monitored, and their lifecycle managed properly. Improper hygiene of NHI can lead to data leakage and if you think that's not likely in the context of the examples given above, review the recent Microsoft AI teams own data exposure incident involving SAS tokens.

Data poisoning also creates a very unique risk in RAG based architectures. Data sources in RAG architectures are likely cloud based and editable via NHI. The integrity of the training data and as a result of the responses we provide our customers\employees via our AI enabled chat bot should be protected from unauthorized additions of training material. The potential organizational risk from an incorrect or unpleasant response, as a result of the malicious pollution of training data sets via misconfigured or poorly maintained NHI, should be measured and accounted for.

Oasis provides the visibility and lifecycle management you need to safely deploy technologies in the era we live in.

- Inventory of NHI across diverse multi cloud\SaaS provider environments and on prem.
- Actionable insights into the most egregious NHI posture issues with guided or automated remediation
- Ongoing automation of lifecycle management for critical NHI tied to high value projects
- Complete context around NHI usage, from consumption to entitlements. Understand everything you need to know about NHI usage in your environment. This includes those elusive SAS tokens mentioned above!



06

What Are Storage Accounts And How To Secure Them?

Storage accounts are fundamental components within Azure's cloud infrastructure, serving as the cornerstone for storing and accessing data across various applications and services. While offering scalability and accessibility, ensuring the security of these accounts is paramount. In this article, we'll delve into the core concepts of storage accounts and outline practical strategies for safely managing them, minimizing risks, and protecting sensitive data.

Introducing Storage Accounts

Azure Storage accounts serve as repositories for various types of data, ranging from blobs and file shares, to queues and tables. They offer global access to stored data, allowing users and applications to retrieve and manipulate information from anywhere with an internet connection. While this accessibility facilitates collaboration and productivity, it also underscores the importance of implementing stringent security measures to safeguard against unauthorized access.

Non Human Identities In Storage Accounts

Non-human identities are crucial for accessing Azure storage accounts. Although service accounts and service principals, managed through RBAC, are commonly used to grant access, storage accounts feature two unique non-human identities specifically designed to facilitate access to these resources.

Access Keys: Access keys act as the primary access credentials for storage accounts, providing unrestricted access to all data within without granular controls. Unlike SAS tokens, access keys lack an inherent expiration date, requiring manual rotation to invalidate any potentially compromised keys. Each storage account is equipped with two access keys, known as "key1" and "key2", enabling seamless rotation.

SAS Tokens: Shared Access Signature (SAS) tokens offer precise access control over access to storage accounts, permitting users to specify permissions for particular actions (like reading, writing, or deleting) and resources (such as individual blobs or containers). Users can set custom expiration times for SAS tokens and apply additional security measures, such as IP restrictions or protocol limitations. These tokens are linked to a specific access key, making them invalid if that access key is rotated.

The Non Human Identity Risk Of Storage Accounts

Access Keys Leakage: When an access key is compromised, it poses a significant security threat as attackers gain unfettered access to the storage account. This scenario grants malicious actors full control over stored data, potentially resulting in data breaches and data manipulation.

Unmonitored SAS Tokens: The absence of robust monitoring mechanisms for SAS tokens introduces vulnerabilities akin to the Microsoft AI incident of 2023. Without adequate monitoring, detecting unauthorized access or misuse of SAS tokens becomes challenging. This lack of visibility can exacerbate security risks, particularly when combined with compromised access keys. In such cases, attackers may exploit leaked access keys to generate additional SAS tokens without detection, maintaining persistent access to the storage account and compromising data integrity.

Misconfiguration in SAS Tokens: SAS tokens configured with excessive permissions and extended expiration times can significantly increase security risks, similar to leaked access keys. Moreover, since SAS tokens are dynamically generated, they can potentially expand your attack surface far more than access keys, which are naturally limited in number.

How To Manage And Secure Storage Accounts:

Disable Shared Access and Embrace RBAC: Whenever possible, disable shared access to limit potential vulnerabilities and rely on Role-Based Access Control (RBAC) for fine-grained access management.

Prioritize SAS Tokens: Opt for SAS tokens as they offer more precise access control compared to access keys. Configure SAS tokens securely by:

- Granting minimal access permissions and scope necessary.
- Allowing only HTTPS requests to ensure secure communication.
- Setting a short expiration period, preferably not exceeding seven days, to minimize the vulnerability window.
- Restricting access based on IP addresses for an added layer of security.

Regularly Rotate Access Keys: Although challenging, regularly rotating access keys is essential for maintaining security. Oasis provides automated assistance for seamless key rotation and secure Non-Human Identity lifecycle management.

Minimize Service Accounts and Principals: Reduce the attack surface by minimizing the number of service accounts and service principals with access to storage accounts. This helps mitigate the risk of unauthorized access and potential data breaches.

Leverage Automation Tools: Consider leveraging automation tools like Oasis for secure automated Non-Human Identity lifecycle management to streamline access management processes and ensure compliance with security best practices.

Elevating Storage Account Security With Oasis Security's Lifecycle Management Solution:

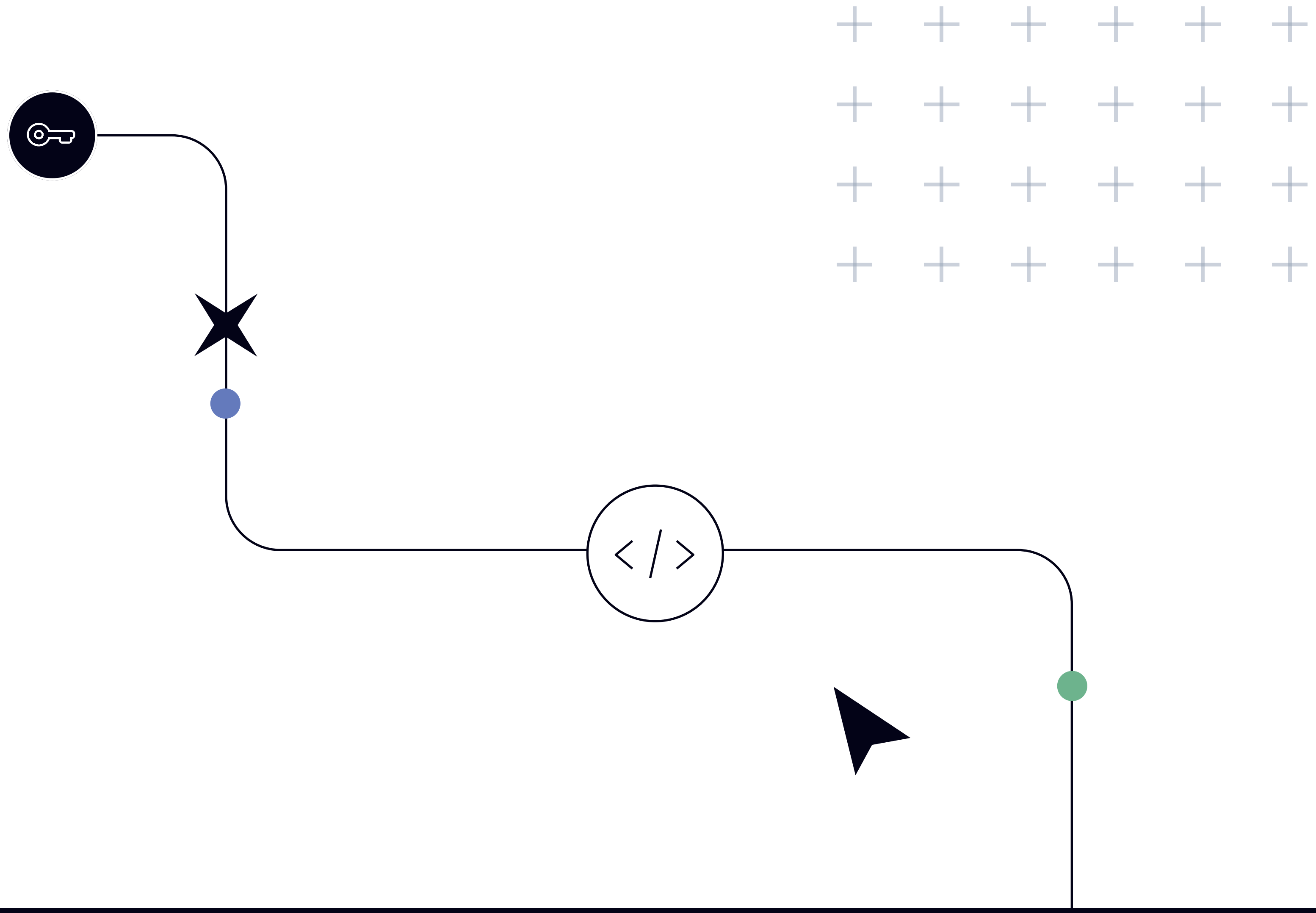
Oasis Security's platform effectively tackles the complexities of managing non-human identities like access keys and SAS tokens throughout the Azure Storage Account lifecycle. Here's how:

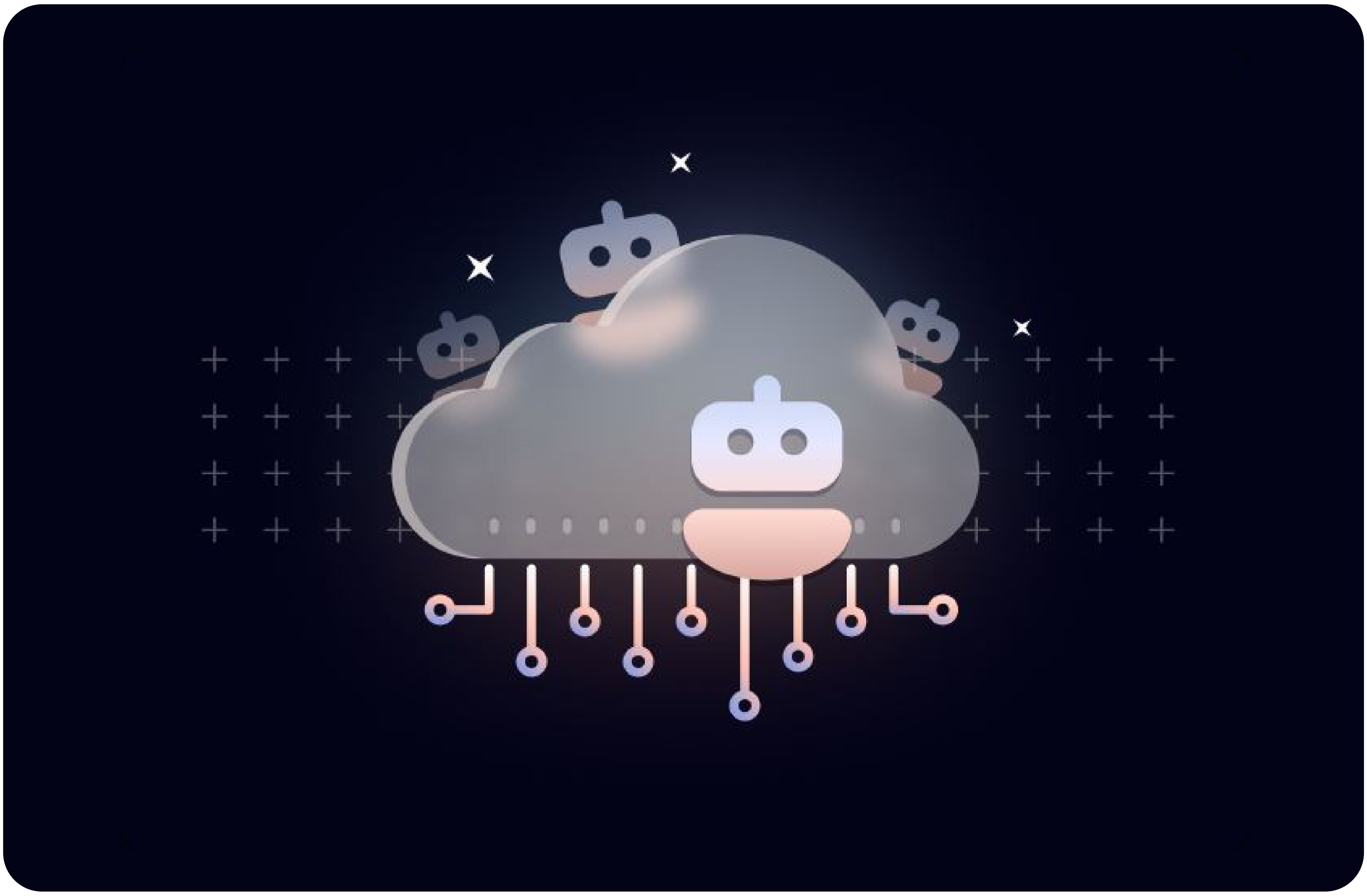
Contextual Mapping: Gain comprehensive insights into SAS tokens configurations, access controls, and usage patterns, ensuring a clear understanding of your storage environment.

Lifecycle Governance: Automate workflows for account provisioning, RBAC enforcement, and routine audits, streamlining management processes and ensuring consistency.

Security and Compliance: Enforce robust security policies and regulatory standards, guaranteeing adherence to industry best practices and safeguarding sensitive data.

In summary, while Azure Storage accounts are integral to modern cloud systems, managing them without dedicated tools can be challenging. Oasis Security's innovative platform offers a solution for automated management of Storage accounts and other non-human identities, reducing risks and bolstering security.





07

CSPM Vs. NHIM (Non-Human Identity Management)

TL;DR

CSPM and NHI Management serve distinct purposes and address different threat vectors, complementing each other to provide comprehensive security coverage.

CSPM focuses on fortifying cloud infrastructure security, identifying misconfigurations, and ensuring compliance with security policies. It is indispensable for organizations concerned with maintaining a secure cloud environment and adhering to industry standards.

NHI Management, on the other hand, addresses the unique challenges associated with managing and securing non-human identities. NHIs are responsible for governing the service-to-service connections. If cloud infrastructure are the islands where code lives, NHIs are the bridges that connect them. NHIM focuses on providing visibility, assessing security posture and automating the lifecycle of NHIs (provisioning, rotation, decommissioning)

In today's rapidly evolving digital landscape, the security of cloud environments stands as a paramount concern for organizations of all sizes. As businesses increasingly rely on cloud infrastructure and services, ensuring the protection of sensitive data and resources has become a top priority. Cloud Security Posture Management (CSPM) and Non-Human Identity (NHI) Management are two essential and complementary components of a robust cloud security strategy.

What Is CSPM?

Cloud Security Posture Management (CSPM) tools excel in assessing, managing, and enhancing the security of cloud environments. They focus on identifying and remedying infrastructure misconfigurations, ensuring compliance with security policies, and minimizing the risk of security breaches.

Key capabilities of CSPM Features:

- Continuous Monitoring: CSPM tools maintain a watch over cloud environments, detecting deviations from security best practices.
- Risk Assessment and Compliance: They conduct thorough risk assessments, ensuring compliance with industry standards and regulations.
- Remediation: CSPM solutions spring into action, automatically remedying security issues and enforcing policy compliance.
- Policy Enforcement: They automate the enforcement of security policies, maintaining a consistent security posture across the cloud ecosystem.

What Is NHI Management?

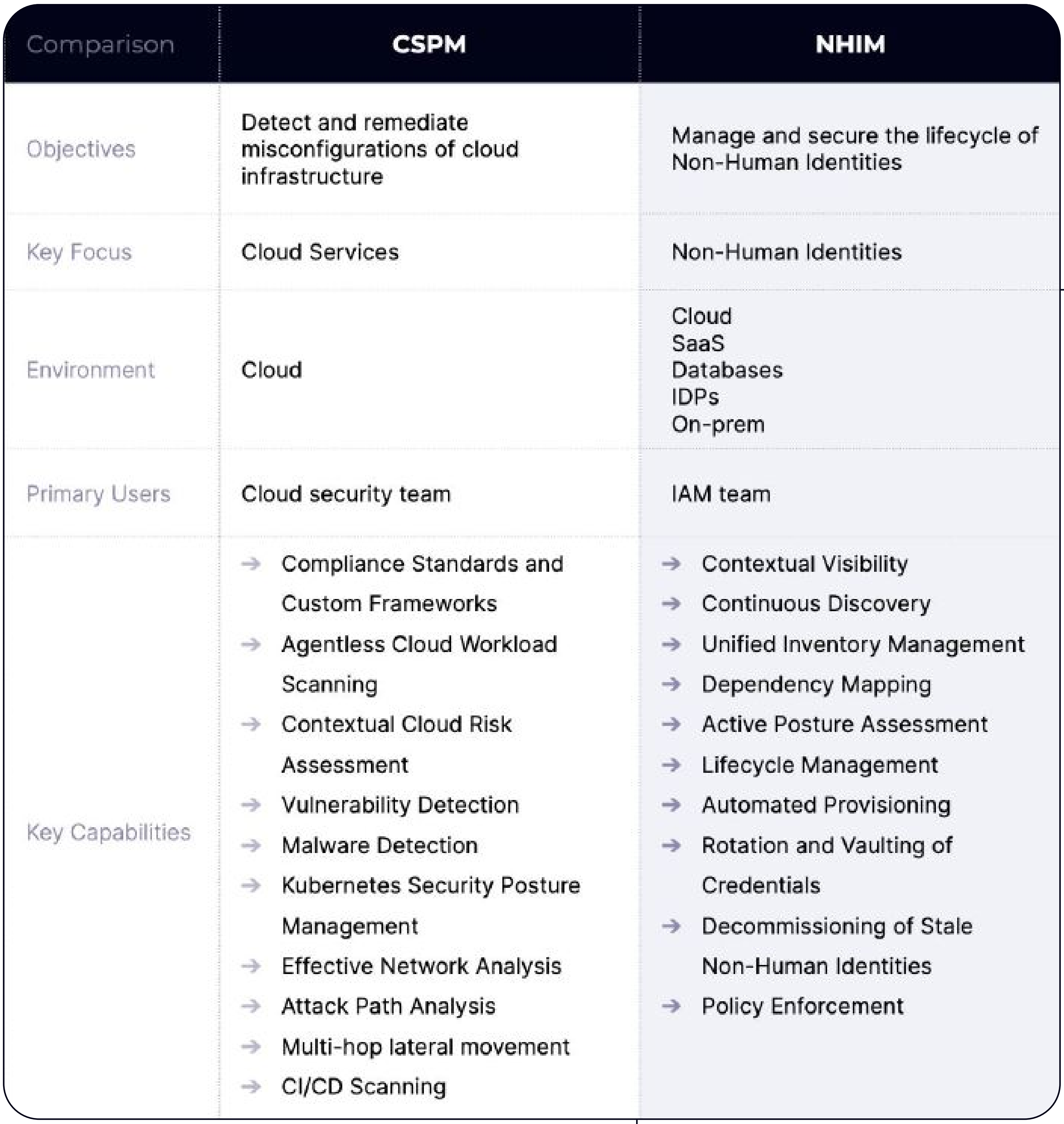
In cloud security, Non-Human Identities (NHIs) such as service accounts, IAM roles, and access keys, play a critical yet often overlooked role. NHI Management solutions provide a comprehensive approach to these entities, illuminating their presence within the network and overseeing their lifecycle from inception to retirement. This holistic management encapsulates visibility—offering a clear view of all NHIs in the environment, posture—assessing and enhancing their security configuration, and lifecycle management—ensuring their efficient operation and timely decommissioning. Through NHIM, organizations gain a balanced strategy that not only secures but also optimizes the use of NHIs in supporting cloud operations.

Key capabilities of NHI Management:

- **Continuous Discovery and Unified Inventory:** NHI Management solutions continuously discover and dynamically update a centralized inventory of all non-human identities across various platforms, including hybrid cloud environments (IaaS such as AWS, Azure, GCP; PaaS/SaaS; and on-prem systems like Active Directory and database local accounts). This capability ensures that all NHIs, whether previously known or newly instantiated, are consistently tracked and managed.
- **Holistic Contextual Visibility with Ownership and Dependency Mapping:** NHI Management tools provide deep insights into the usage patterns, operational dependencies, and ownership details of non-human identities. This comprehensive visibility, incorporating data from across the IT ecosystem, including interactions with infrastructure as code (IaC), IT service management (ITSM) systems, logs, and development tools. This enables informed decision-making and supports robust security and compliance strategies.
- **Active Posture Management with Automated Risk Assessment and Remediation:** NHI Management proactively assesses the security posture of non-human identities and automatically identifies vulnerabilities. It generates remediation plans based on these assessments, facilitating swift and effective responses to mitigate potential risks. This proactive stance helps maintain the integrity and security of the IT infrastructure continuously.
- **Lifecycle Automation for Secure Secret Management:** The management of secrets associated with non-human identities must be automated across their entire lifecycle. This includes the provisioning, policy definition, credential rotation, and decommissioning of secrets. Integration with various secret managers (e.g., HashiCorp Vault, Azure Key Vault, CyberArk, Delinea) is crucial to ensure that credential handling is secure and consistent across all environments. Automating these processes minimizes the risk of credential theft and misuse, supporting a robust security posture.

- **Developer-Ready, API-Driven Integration:** NHI Management solutions are designed to integrate seamlessly into the developer workflow and operational stack through robust, well-documented APIs. This ensures that non-human identity management can be effectively handled within existing development tools and paradigms, enhancing efficiency and reducing the likelihood of security gaps.

CSPM vs. NHIM (Non-Human Identity Management)



Comparison	CSPM	NHIM
Objectives	Detect and remediate misconfigurations of cloud infrastructure	Manage and secure the lifecycle of Non-Human Identities
Key Focus	Cloud Services	Non-Human Identities
Environment	Cloud	Cloud SaaS Databases IDPs On-prem
Primary Users	Cloud security team	IAM team
Key Capabilities	→ Compliance Standards and Custom Frameworks → Agentless Cloud Workload Scanning → Contextual Cloud Risk Assessment → Vulnerability Detection → Malware Detection → Kubernetes Security Posture Management → Effective Network Analysis → Attack Path Analysis → Multi-hop lateral movement → CI/CD Scanning	→ Contextual Visibility → Continuous Discovery → Unified Inventory Management → Dependency Mapping → Active Posture Assessment → Lifecycle Management → Automated Provisioning → Rotation and Vaulting of Credentials → Decommissioning of Stale Non-Human Identities → Policy Enforcement

Why Both CSPM And NHIM Are Essential For Enterprise Security

While CSPM and NHI management each address distinct facets of cloud security, their true power lies in collaboration:

Complementary: CSPM focuses on infrastructure security and compliance, while NHI management specializes in non-human identity management.

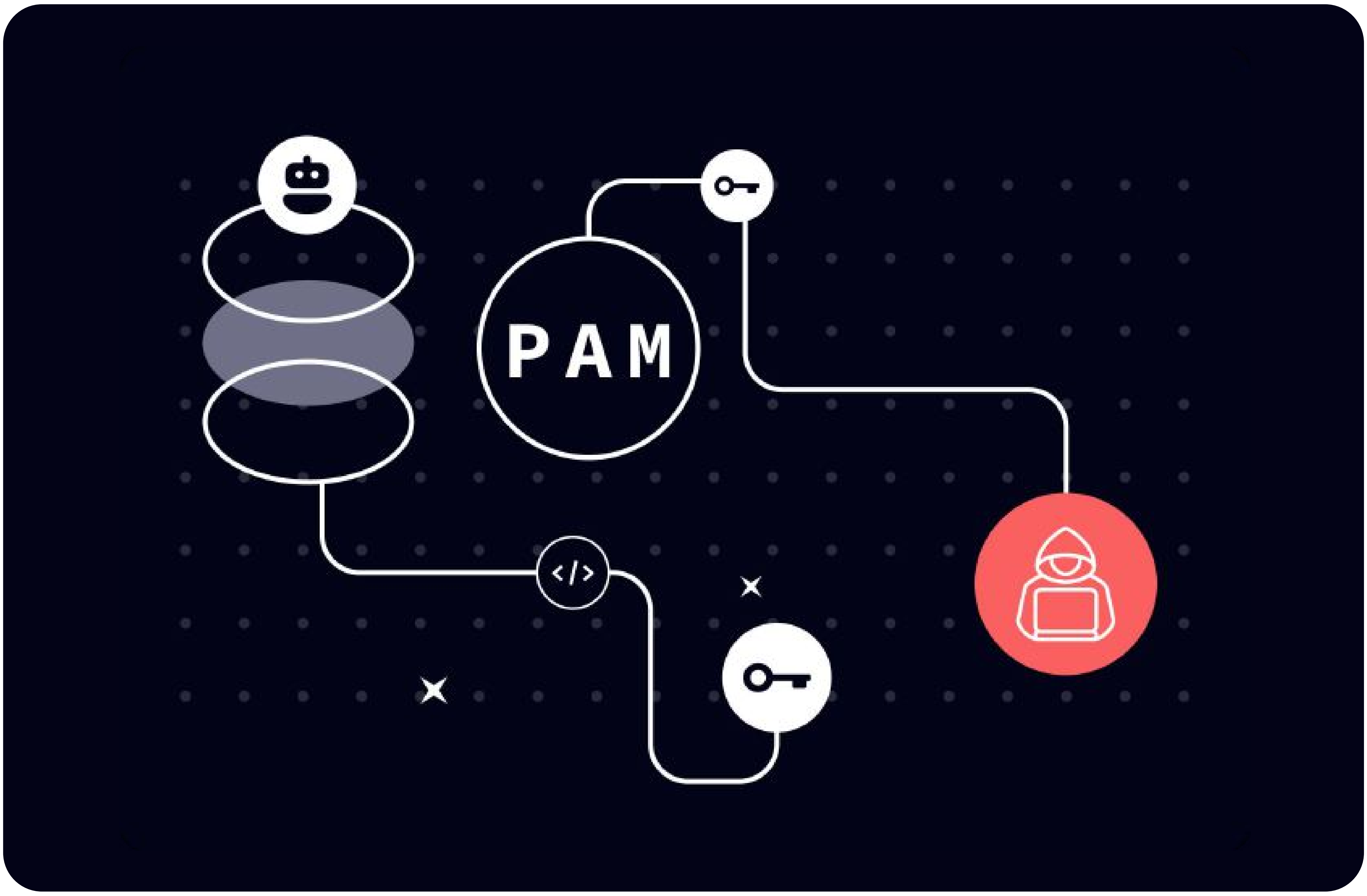
Comprehensive: By combining CSPM and NHI Management, organizations achieve a comprehensive security posture, effectively mitigating a wide range of threats By including both CSPM and NHI Management into their cloud security strategy, organizations can achieve comprehensive protection against a wide range of threats.

llustrating Their Significance

Consider the following scenarios that exemplify the pivotal role of CSPM and NHI Management:

CSPM in Action: Let’s consider a scenario of a cloud server that has been misconfigured during setup, inadvertently exposing it to public internet access. Additionally, this server is running an application vulnerable to the log4j exploit, significantly increasing the risk of unauthorized access. The CSPM tool alerts the security team to the misconfiguration and the vulnerability, recommends immediate actions to rectify the server's exposure, and suggests updating the application to patch the security vulnerability. By doing so, the CSPM ensures rapid mitigation of potential threats while reinforcing the organization's cloud security posture.

NHI management in Action: In this scenario, an organization makes extensive use of service accounts and API keys. These NHIs have been accumulating over time as the company digital transformation strategy progressed and developers increased their use of cloud and microservices. The organization is now faced with the challenge of identifying and decommissioning all the active, but unused non-human identities. These stale NHIs, which are often forgotten after project completion or personnel changes, pose significant security risks, potentially granting unauthorized access if exploited. In this case, an NHIM solution, like Oasis, drastically simplifies the process by automatically discovering, inventorying, and assessing which identities are stale, enabling timely decommissioning through automated remediation plans.



08

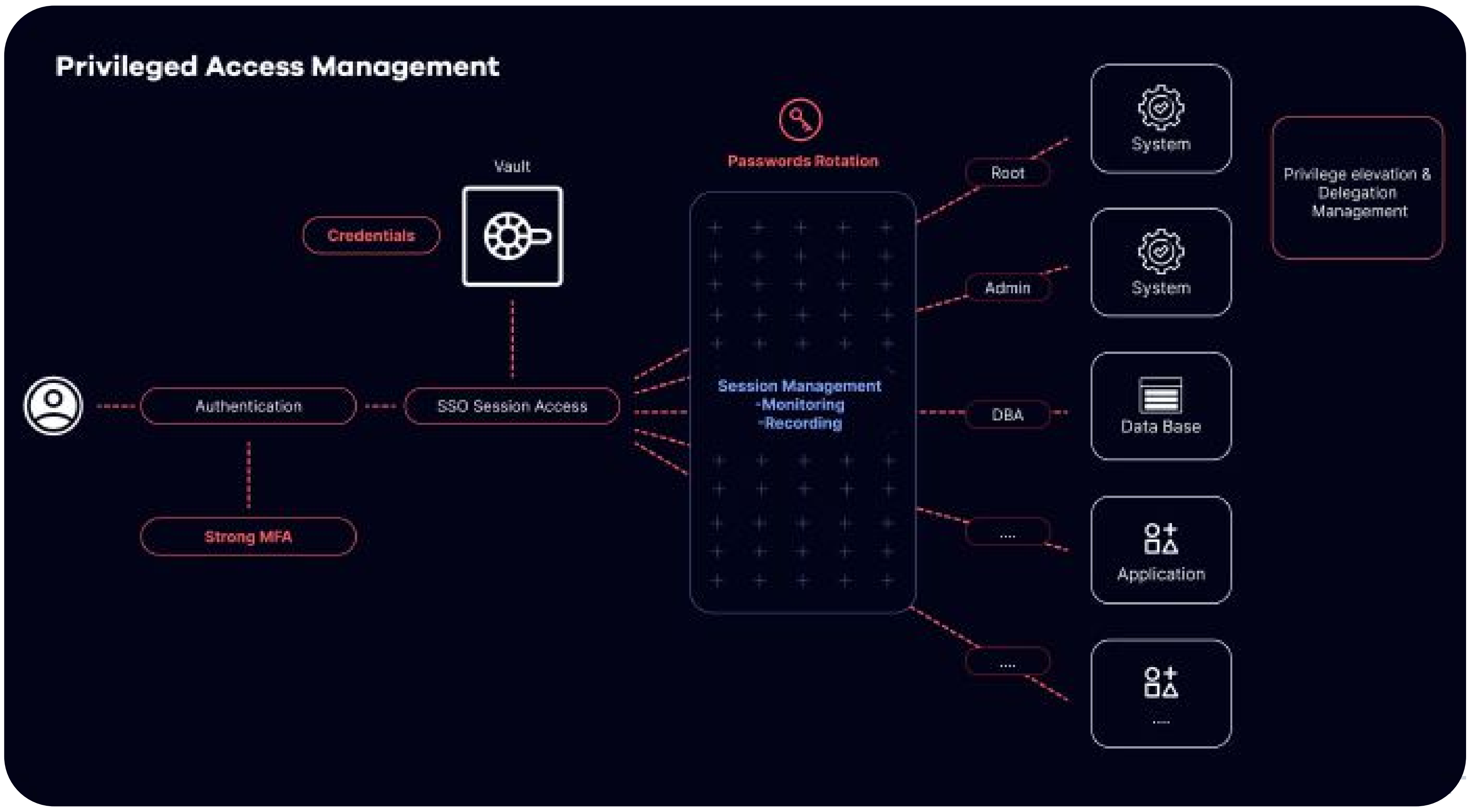
How Does Non-Human Identity Complement Privileged Access Management For 360-Degree Security?

As we engage with customers – across the board, from IAM professionals to CISOs —, a common question we come across is: "I use my Privileged Access Management (PAM) solution to manage administrator cloud accounts; why can't I use it for service accounts, too?". The short answer is that PAM solutions weren't originally designed with this dual purpose in mind. However, that oversimplifies things. The reality is more nuanced when considering the different requirements and use cases involved. Allow me to elaborate.

The Role Of PAM In The IAM Stack

Privileged Access Management (PAM) solutions, offered by vendors such as CyberArk, BeyondTrust, and Delinea, 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 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.



Privileged Access Management

Why Can't NHIs Be Managed Effectively By PAMs?

Now that we understand the core architectural principles of PAM, it will be easy to understand why they cannot effectively handle non-human identities (NHIs) like service accounts, API keys, secrets, etc. TLDR: NHIs have fundamentally different characteristics and lifecycle compared to human identities for which PAMs were designed.

With the shift towards cloud computing, the embrace of modern architectures, and the adoption of agile methodologies, the number of non-human identities has exploded, outpacing human identities by a factor of 10-50x. This exponential growth of NHIs has redrawn the boundaries of the identity perimeter, exposing a vast and rapidly expanding attack surface. The security implications are substantial. NHIs often possess privileged access yet lack robust authentication measures like multi-factor authentication (MFA), making them prime targets for adversaries seeking initial entry points and opportunities for lateral movement.

Unlike human users who are provisioned from an authoritative source such as HR databases or Active Directory, NHIs lack a centralized record system. They are 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 (developers) NHIs are created, fundamentally breaks the data model and governance frameworks upon which traditional PAM tools were built.

As a result, PAM solutions struggle to gain full visibility into the NHI landscape, track their lifecycle, and understand the rich context around them – such as their relationships to applications, data, and other resources they access. Without this contextual awareness, PAM tools cannot effectively manage and secure the rapidly growing number of NHIs.

Adding to the complexity is that NHIs often have multiple consumers, unlike human identities which are typically used by a single individual. Compounding the challenge is the lack of standardization of NHI types and formats across different cloud providers and technology stacks. AWS service accounts differ from Azure service principals, which differ from GCP service accounts, for example. PAM solutions designed around traditional data center resources struggle to natively understand and control this new cloud identity landscape. Furthermore, some NHIs function more like API keys—simple authentication mechanisms that may be used across a variety of platforms—adding another layer of diversity and complexity to their management.

Moreover, the ownership and relationships between NHIs and the business applications they access are often unknown or undocumented. An NHI may be bound to provide access to one microservice but then proliferate across teams to run batch jobs, utilities, and other processes. PAM solutions lack insight into these intricate dependencies and complex web of relationships that NHIs form across cloud infrastructure.

Ultimately, PAM platforms were built on the assumption of managing dedicated, long-lived privileged accounts mapped to individual human identities and following well-structured provisioning workflows. In contrast, most NHIs are ephemeral, infused throughout dynamic infrastructure, and born outside of legacy identity processes. Their privileged nature and lack of centralized control make them invisible to PAM solutions.

Complement Your PAM Tool With The Oasis Platform For NHI Management

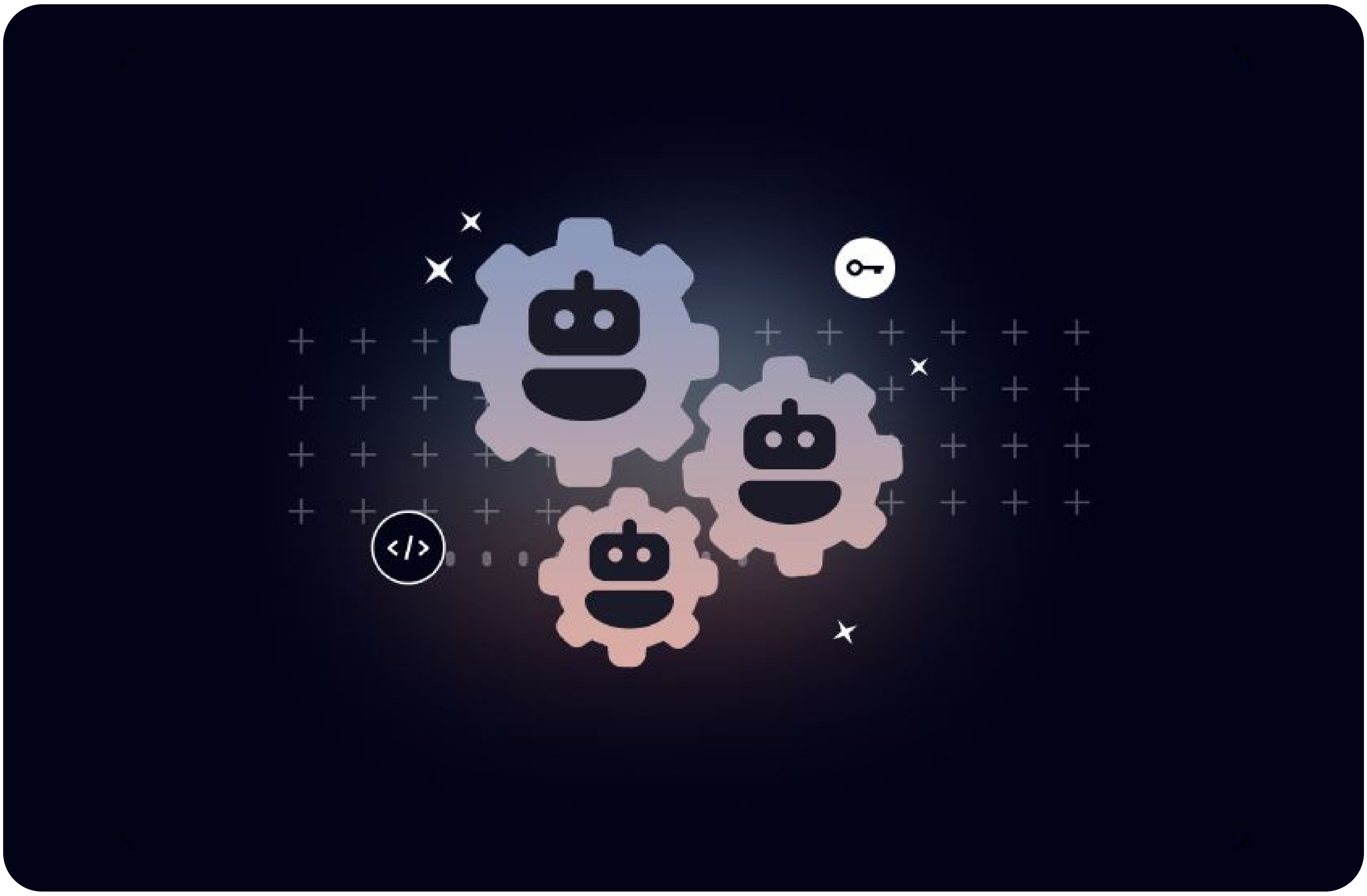
To truly secure your expanding identity perimeter, you need a new approach - one that complements existing PAM investments with a purpose-built solution for Non-Human Identity Management (NHIM) like Oasis.

Oasis is designed for NHIs from the ground up. In Oasis, NHIs are first class citizens, which results in drastically better visibility and more efficient operations. Because of the scale and dynamic nature of NHIs, Oasis has been built with powerful analytics that can process data from a wide range of systems (clouds, Paas, Saas, Secret managers, DSPM, ASPM...) to automatically discover all NHIs in your environment along with rich contextual metadata on consumers, resources, ownership, etc. To manage NHI efficiently at scale, automation is key. To make posture management actually possible, Oasis comes with a built-in Context Correlation Engine that automatically assesses and ranks issues according to configurable policies and provides tailored remediation plans that can be executed automatically.

The out-of-the-box automation coupled with the contextual visibility, allow to address complex use cases like secret rotation, stale accounts decommissioning and employee offboarding safely at scale without disrupting production availability.

Conclusion

NHIM platforms like Oasis are complementary to your PAM solutions. They address a new set of requirements and should become a core component of your IAM program and stack. By layering Oasis into your IAM stack alongside PAM, you achieve complete coverage across your entire identity footprint - both human and non-human.



09

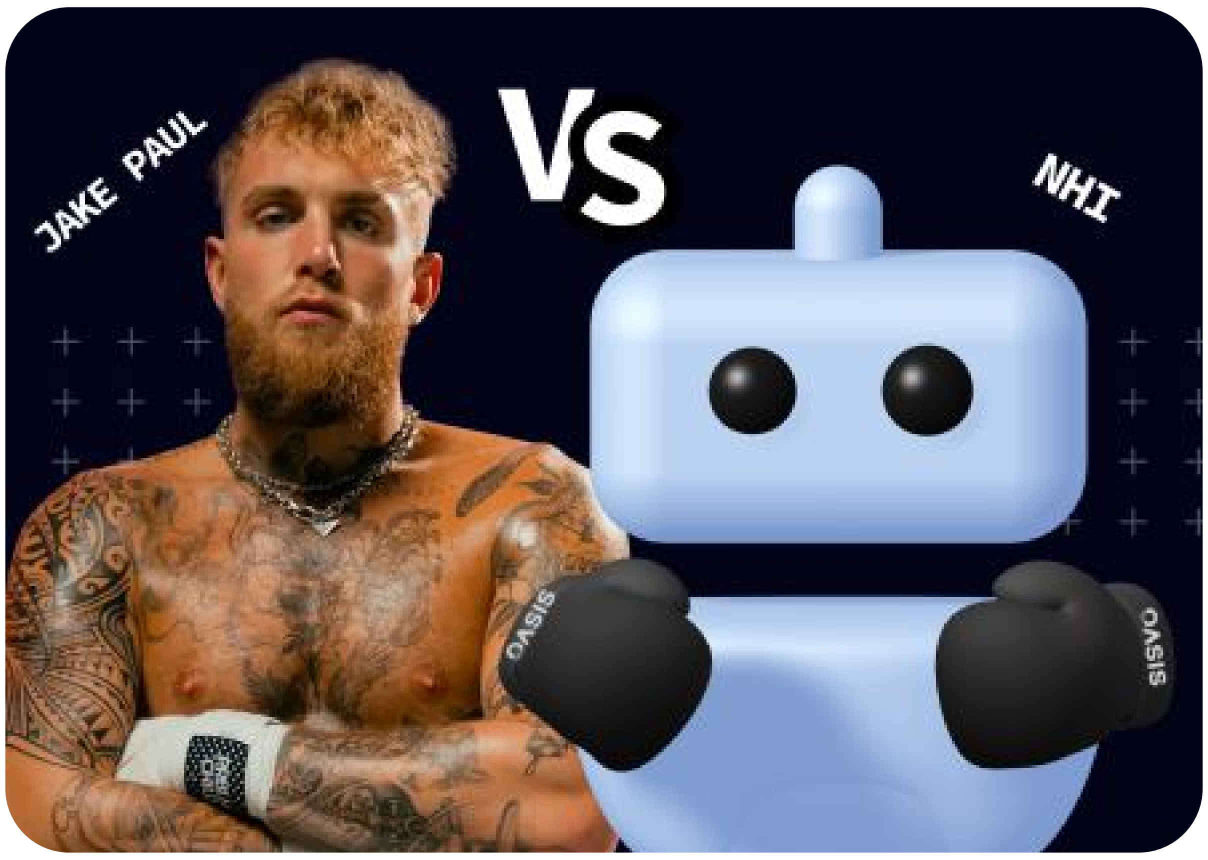
What Are Service Accounts And How Should You Secure Them?

Service accounts are non-human identities created by IT administrators for executing tasks on machines or specific processes, like software installations. Typically set up within Microsoft Active Directory (AD), these accounts are used by systems, applications, and administrators to interact with other systems, handling tasks such as file management or SQL server agent functions. They operate autonomously, performing automatic, repetitive, and scheduled actions in the background, often without human intervention. Tasks carried out by service accounts range from running applications on Windows operating systems to managing databases and conducting automated backups.

Similar to human users, microservices and workloads require access to networks, applications, and files, among other resources. Service accounts provide a means to assign identity and permissions to software programs or processes executing specialized tasks. Equipped with privileges granting extensive access to system resources, either locally or across clouds, service accounts are integral to system functionality.

A key difference between service accounts and user accounts lies in how they are managed and provisioned: user accounts are centrally managed, whereas service accounts are managed in a distributed manner.

The critical issue of centralized management versus distributed creation plays a pivotal role in understanding the distinction between service accounts and user accounts. While user accounts are meticulously managed and provisioned through Identity Governance and Administration (IGA) and Privileged Access Management (PAM) systems, service accounts follow a different trajectory. Typically, they are directly created by developers within the infrastructure. This decentralized approach often results in a lack of visibility and control, leaving most organizations uncertain about the exact number and functions of their service accounts. Consequently, they face challenges in effectively managing these accounts and understanding their roles within the system.



Non Human Identity vs. Jake Paul

Distinguishing service accounts from user accounts is far from a straightforward task, as it entails more than simply examining their purposes and naming conventions. Unlike user accounts, which are directly associated with individuals and commonly bear human names like "Jake Paul," service accounts are tailored for system functions and often possess descriptive names such as "NetworkService," or may even lack a name altogether. However, similar to user accounts, service accounts are assigned a name and a password. The password, being a secret credential, is crucial for authenticating the service account and granting access to system resources. Yet, their credentials must be widely known to the primary application and all associated programs. This emphasizes the importance of securely managing service account credentials to mitigate the risk of unauthorized access

Challenges In Service Account Management

As we explore the complexities of service account management, it's essential to explore specific hurdles encountered in legacy environments, as well as maintaining comprehensive NHI inventories and governance across cloud infrastructures.

Secret Rotation In Legacy Environments

While regular password rotation is standard practice for human accounts, it is often overlooked for service accounts. Concerns about potential disruptions to critical operations lead to the neglect of password rotation, allowing compromised service accounts to maintain prolonged access to an organization's network undetected.

Rotating passwords in outdated environments, especially those heavily dependent on Microsoft Active Directory (AD) service accounts, presents a significant challenge. An illustrative example of this challenge is the Cloudflare breach, where despite a rotation attempt of approximately 5000 accounts, four service accounts remained unrotated. This incident highlights the need for automation solutions to address this issue effectively. 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.

Furthermore, rotating secrets while ensuring uninterrupted business operations introduces another layer of complexity. Without a comprehensive understanding of how secrets are utilized, their rotation may inadvertently disrupt critical applications and workflows. This emphasizes the necessity for meticulous planning and coordination when implementing password rotation strategies, especially in legacy environments.

Maintaining A Holistic Up To Date Inventory Across Clouds

Service accounts operate within the depths of an organization's security infrastructure, rendering them elusive and challenging to monitor effectively. Their intricate dependencies spanning across various processes, programs, and applications create a veil of obscurity, leaving them susceptible to compromise without detection.

Managing service accounts presents a significant challenge due to the lack of centralized repositories or mechanisms for discovering, inventorying, and managing ownership of these accounts. As service accounts proliferate across various environments, including on-premises, cloud, SaaS applications, and databases, organizations struggle to maintain comprehensive visibility into their landscape of service accounts. With potentially hundreds or even thousands of service accounts in use, the task of tracking and identifying each one, along with its activity, becomes daunting. Without awareness of all service accounts, organizations cannot effectively secure them, highlighting the critical importance of comprehensive discovery and management processes.

Understanding Usage, Dependencies And Entitlement

The deficiency in comprehensive visibility into Non-Human Identities (NHIs) within organizational infrastructure extends beyond mere inventory to encompass crucial contextual aspects such as usage, dependencies, and entitlements. This lack of insight exacerbates several critical findings, including outdated privileged access rights, unattended secrets accessible to departed employees, stale storage accounts posing potential risks, and secrets with remarkably long expiration dates, some spanning over 50 years. Furthermore, the presence of inactive vaults with lingering access policies compounds security vulnerabilities. Without clarity on which services and applications rely on NHIs, the situation worsens, leading to both neglected and excessively empowered NHIs, ultimately heightening security risks for organizations.

Best Practices For Secure Management Of Service Accounts

Comprehensive Identity Governance

Instituting Comprehensive Identity Governance involves several key practices aimed at ensuring the security and integrity of service accounts within an organization. Central to this is the establishment of robust Identity Lifecycle Management processes, which leverage automation to maintain compliance with regulatory requirements throughout the entire lifecycle of identities.

Additionally, it's imperative to Define and Enforce Policies that govern various aspects of service account management, including passwords, rotation schedules, provisioning procedures, and rules surrounding credential sharing. Utilizing appropriate tools to enforce these policies effectively is crucial, striking a balance between operational efficiency and maintaining airtight security.

Secure Credential Management

Secure Credential Management is another critical aspect, necessitating the use of secure storage mechanisms like password vaults and key management systems. By centralizing and encrypting service account credentials, organizations can safeguard sensitive information from unauthorized access.

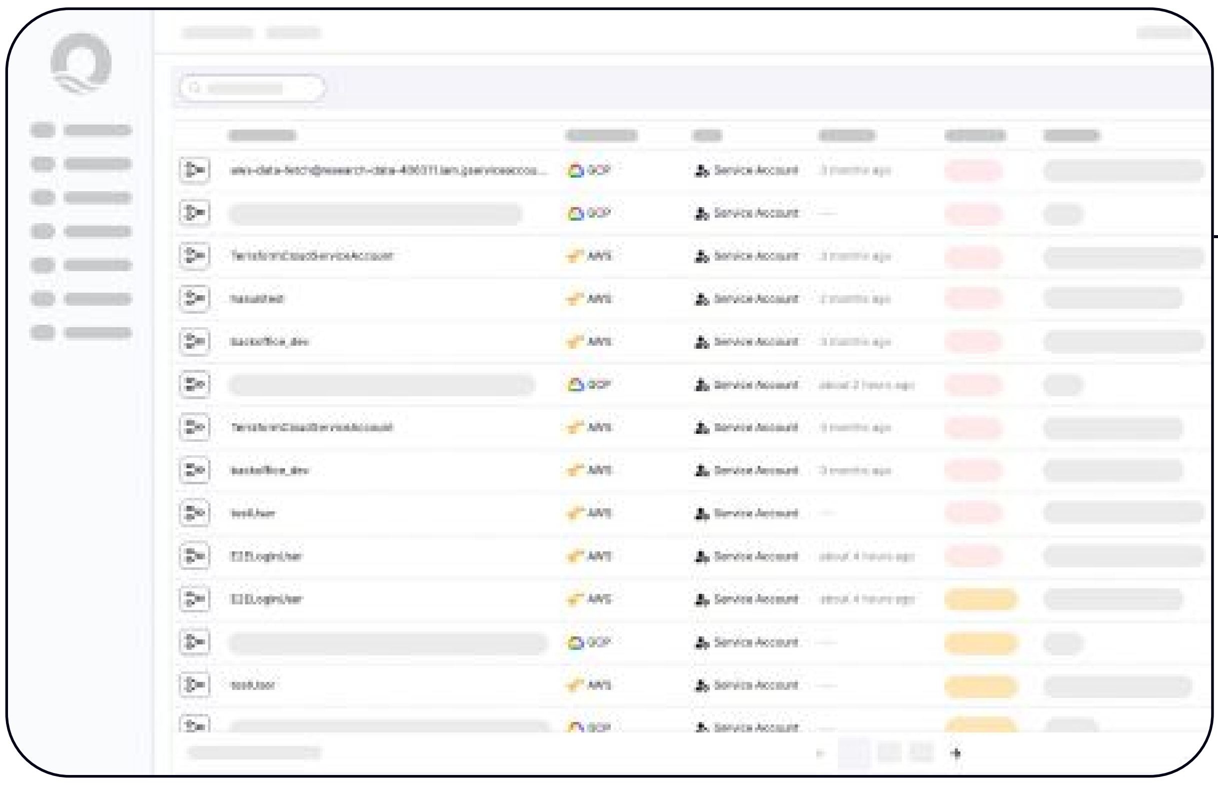
Automated Password Rotation policies further bolster security by regularly changing credentials, reducing the risk of compromise and unauthorized entry. This proactive approach helps mitigate potential threats without placing undue burden on administrators.

Continuous Monitoring And Auditing

Continuous Monitoring and Auditing play pivotal roles in maintaining a proactive security posture. Real-time monitoring capabilities enable the timely detection of suspicious activities and unauthorized access attempts, empowering swift response and mitigation. Regular audits and compliance checks serve to evaluate the effectiveness of security controls and ensure adherence to regulatory standards, fostering a culture of ongoing improvement and accountability

Securing Service Accounts With Oasis Security's Lifecycle Management Solution

Oasis Security's platform offers a comprehensive solution to effectively tackle the challenges associated with managing service accounts throughout their lifecycle, from creation, assignment, and governance to the rotation of credentials and decommissioning.



aws-data-fetch@research-data-406311.iam.gserviceacco...	GCP	Service Account	3 months ago
	GCP	Service Account	—
TerraformCloudServiceAccount	AWS	Service Account	3 months ago
hasudited	AWS	Service Account	2 months ago
backoffice_dev	AWS	Service Account	3 months ago
	GCP	Service Account	about 2 hours ago
TerraformCloudServiceAccount	AWS	Service Account	3 months ago
backoffice_dev	AWS	Service Account	3 months ago
testUser	AWS	Service Account	—
E2ELoginUser	AWS	Service Account	about 4 hours ago
E2ELoginUser	AWS	Service Account	about 4 hours ago
	GCP	Service Account	—
testUser	AWS	Service Account	—
	GCP	Service Account	—

Non Human Identity Management

Here's a closer look at how it accomplishes this:

Holistic Visibility: With Oasis you gain a complete view of your service account landscape. Oasis Security's platform provides holistic visibility, allowing you to identify all service accounts within your organization's infrastructure. This visibility extends to various aspects such as account usage, permissions, and associated resources, enabling administrators to track and manage service accounts efficiently.

Contextual Mapping: Without a comprehensive view of how non-human identities are being used within your systems, you may find it challenging to determine the appropriate course of action for rotation. Oasis gives you detailed insights into the context surrounding each service account. The platform offers contextual mapping capabilities, providing 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.

Automated Posture Assessment: Oasis automatically assesses the security posture of service accounts and other Non-Human Identities to identify and mitigate potential risks. Oasis Security's platform conducts automated posture assessments, evaluating factors such as secret rotation, access permissions, and compliance with security policies. This proactive approach helps organizations identify vulnerabilities and prioritize remediation efforts to enhance the overall security of service accounts.

Lifecycle Management Automation: Oasis streamline service account lifecycle management with automated workflows. The platform facilitates automated provisioning, role-based access control (RBAC) enforcement, and regular audits, ensuring that service accounts are managed consistently and in accordance with organizational policies. By automating these tasks, administrators can reduce manual effort and minimize the risk of errors or oversights during account management processes.

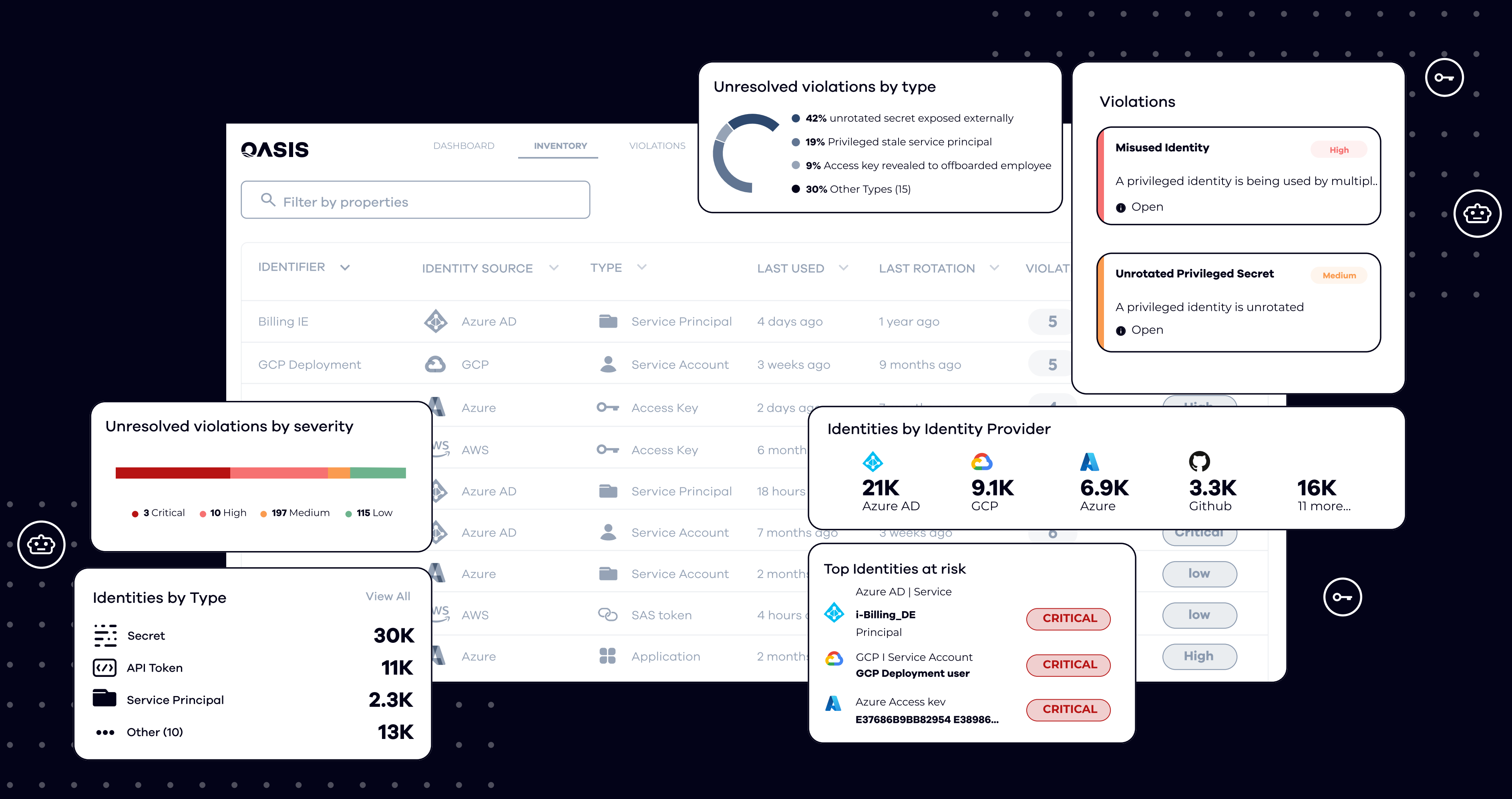
Security and Compliance Enforcement: With Oasis you can finally enforce robust security policies and regulatory standards for service accounts. Oasis Security's platform enables organizations to establish and enforce security policies tailored to their specific requirements. This includes enforcing password policies, access controls, and compliance with industry regulations such as GDPR or HIPAA. By ensuring adherence to security best practices and regulatory requirements, organizations can mitigate the risk of data breaches and maintain compliance with legal and regulatory mandates.

In conclusion, service accounts play a critical role in modern cloud systems, yet managing them effectively can be daunting without specialized tools. Oasis Security's innovative platform provides a solution for automating the management of service accounts and other non-human identities, thereby mitigating risks and enhancing security measures.

About Oasis Security

Oasis Security is the leading provider of Non-Human Identity Management (NHIM) solutions. NHI Management is a huge and unresolved security weakness that is constantly exploited by malicious cyber attackers.

By enabling control over Non-Human Identities, we bridge the gap between devops/R&D and security ensuring our customers elevate their security posture while maintaining highly efficient operations.



OASIS

IDENTIFIER	IDENTITY SOURCE	TYPE	LAST USED	LAST ROTATION	VIOLAT	
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 ag			
	AWS	Access Key	6 month			
	Azure AD	Service Principal	18 hours			
	Azure AD	Service Account	7 months ago	3 weeks ago	6	Critical
	Azure	Service Account	2 month			low
	AWS	SAS token	4 hours			low
	Azure	Application	2 month			High

Unresolved violations by type

- **42%** unrotated secret exposed externally
- **19%** Privileged stale service principal
- **9%** Access key revealed to offboarded employee
- **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

Unresolved violations by severity

- **3** Critical
- **10** High
- **197** Medium
- **115** Low

Identities by Identity Provider

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

Identities by Type — View All

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

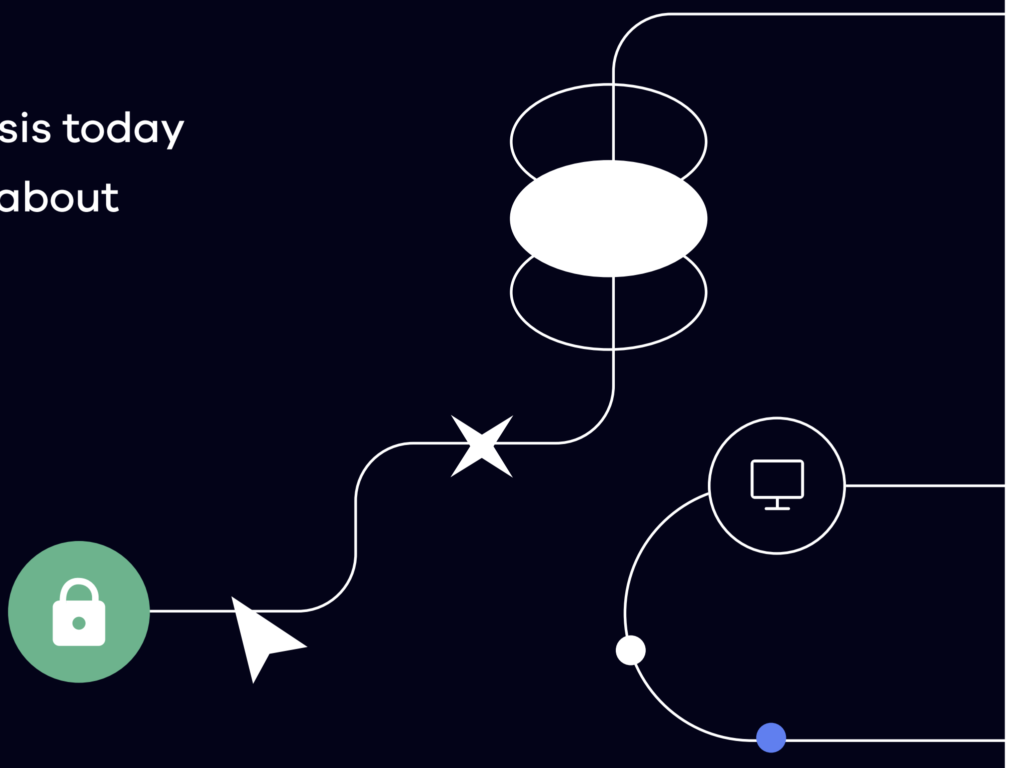
Top Identities at risk

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

Secure All Identities, NHIs First

Don't leave your business vulnerable. Contact Oasis today for a free security assessment and to learn more about how we can protect your assets and reputation

Get a Free Assessment



OASIS