token

2025

THE TOKEN SECURITY

NON-HUMAN IDENTITY SECURITY (NHI) BUYER'S GUIDE

The Token Security: Non-Human Identity Security (NHI) Buyer's Guide

Table of Contents

WELCOME

With the rapid evolution and adoption of AI, we're at the beginning of a new era in identity security that requires a mindset shift as profound as the move to the cloud.

The rise of machine identities, service accounts, ephemeral workloads, agentic AI, and automation pipelines has introduced a new class of security risk: **Non-Human Identities (NHIs)**. These identities now outnumber human ones by orders of magnitude. They operate at machine speed, across distributed systems, and often without the same governance or visibility as their human counterparts.

Yet despite this growing risk, most organizations are still trying to secure NHIs with tools and frameworks built for people.

We believe it's time to reframe the conversation. NHI security isn't a niche concern or a subset of IAM. It's now a foundational layer of enterprise security. If left unaddressed, it becomes a silent enabler of privilege sprawl, shadow access, secret leakage, and AI-based threat vectors.

But this challenge also presents a unique opportunity: to get ahead of the next generation of identity risk by building proactive, machine-first defenses that are ready to be effective at massive scale.

Many security leaders are left confused and unsure how to evaluate and build an NHI program, and how to assess a solution. This document aims to clarify the different elements you should consider in order to have a successful NHI program.

At Token Security, we're committed to helping security teams regain control over this fast-moving, high-risk identity layer while accelerating innovation.

Let's take the next step together.

token

Itamar Apelblat
Co-Founder and CEO
Token Security

Introduction

This guide was created to help you understand, evaluate, and build a strategy around NHI Security. Whether you're a CISO, leading an IAM program, running cloud security, or navigating the risks of AI adoption, you'll find actionable insights to help you navigate this emerging landscape and answer the questions that matter:

- **How many NHIs do I have, and where are they?**
- **What are they doing, and who can access them?**
- **Are they overprivileged, orphaned, or exposed?**
- **Can I detect NHI threats in real time, and respond fast enough to stop a breach?**

We believe the answers to these questions can't be found by stitching together legacy, human-centric tools. They require a new approach: **AI-native, machine-first, and purpose-built for NHIs.**

NHIs, such as service accounts, machine roles, CI/CD artifacts, containers, and AI agents, are now the dominant form of identity in most enterprise environments. They are rapidly created, dynamically provisioned, and often operate with elevated privileges and limited oversight. As a result, they represent one of the fastest-growing sources of identity-based risk. Yet most security programs remain focused on human users, leaving critical NHI gaps in discovery, governance, visibility, and response.

NHIs, such as service accounts, machine roles, CI/CD artifacts, containers, and AI agents, are now the dominant form of identity in most enterprise environments. They are rapidly created, dynamically provisioned, and often operate with elevated privileges and limited oversight. As a result, they represent one of the fastest-growing sources of identity-based risk. Yet most security programs remain focused on human users, leaving critical NHI gaps in discovery, governance, visibility, and response.

This guide will help you:

Assess your exposure:
Understand how NHIs are used across your environments and what makes them a unique security risk.

Identify what matters:
Learn the key capabilities required to secure NHIs effectively, from visibility and lifecycle management to threat detection and remediation.

Evaluate solutions:
Get a side-by-side comparison of NHI security approaches to help you determine what's essential, what's optional, and what aligns with your infrastructure and priorities.

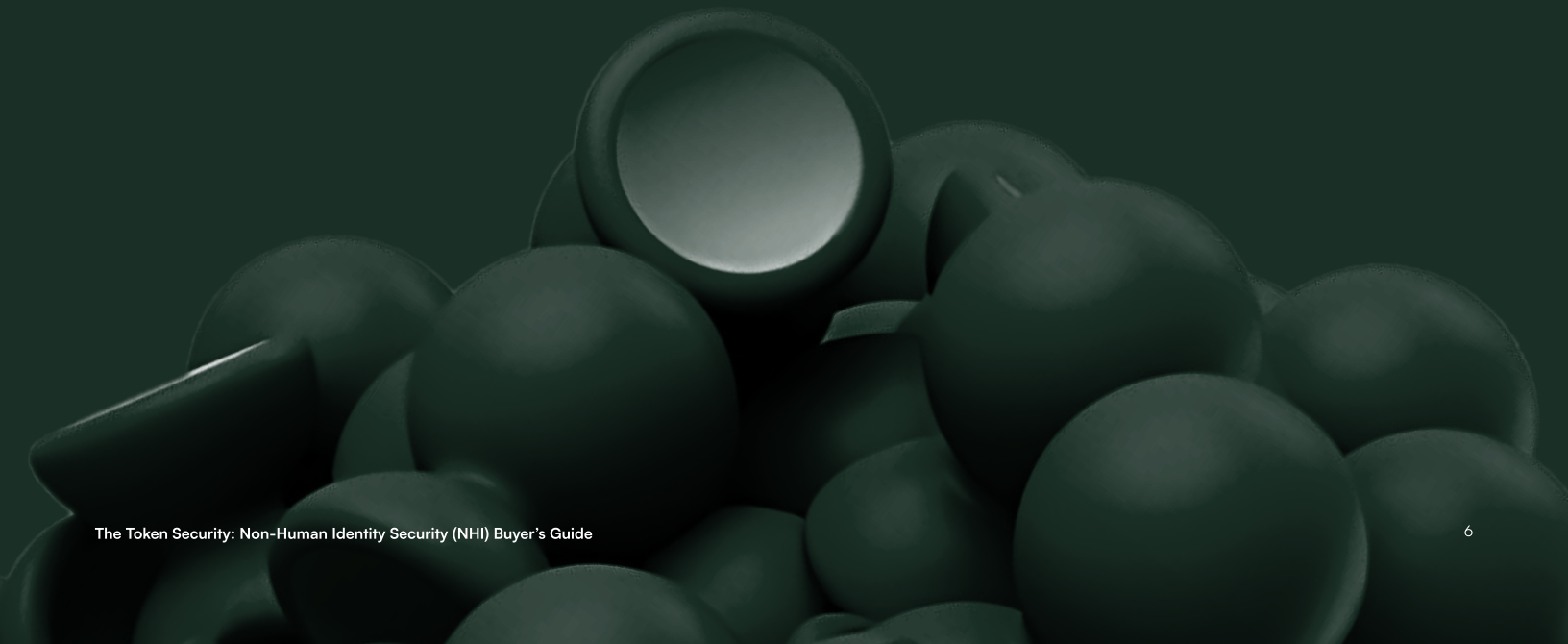
Plan your approach:
Use practical criteria and use cases to shape your NHI security roadmap, whether you're just starting or looking to mature an existing program.

Throughout the guide, we've included capability matrices, definitions, and real-world context to help you make informed decisions. Our goal is to equip you with the clarity and structure needed to move confidently from understanding to execution so you can build a scalable, future-ready NHI security program that aligns with your broader security strategy.

token

06

THE NATURE OF THE THREAT



98% of the identities in your organization aren't human, including many of the most privileged.

Today's enterprises run on a vast web of services, APIs, containers, bots, and automation tools, all powered by Non-Human Identities (NHIs). These identities:

- **Authenticate with secrets such as access keys, tokens, and certificates**
- **Often operate autonomously and are increasingly generated dynamically by code or AI**
- **Are everywhere: in your cloud workloads, CI/CD pipelines, SaaS integrations, and LLM-powered applications**

The result? NHIs have exploded in both volume and importance, and so has their risk.

A Growing, Largely Unseen Attack Surface

Most organizations can't say how many NHIs they have, where they are, who owns them, or what they're doing. Many are not managed, overprivileged, hardcoded into infrastructure, left unrotated for months or years, or worse, never decommissioned. This lack of visibility and control has created an ideal environment for attackers.

Malicious actors are no longer just targeting users. They're going after service accounts, cloud roles, API keys, and embedded secrets. These credentials often provide persistent, elevated access to critical systems without triggering traditional detection mechanisms. In fact, recent breaches have shown that once inside, attackers increasingly move laterally using compromised NHIs.

AI and Automation Are Accelerating the Risk

As part of AI transformations, many security leaders are asked to support chatbots, LLMs, MCP servers, and AI Agents across their organizations. This creates a new level of urgency to gain visibility into new types of NHIs and manage and secure them while they are rapidly evolving.

The rise of agentic AI introduces an entirely new class of NHIs. These identities are spun up dynamically by AI agents, autonomously perform actions on behalf of users or code, and interact with APIs and services across your tech stack. Their behavior is unpredictable, their lifespans are short, and their access levels can be dangerously high.

Legacy identity tools weren't built for this reality. They focus on human logins, role hierarchies, and user governance, not fast-moving, code-generated, privilege-bearing NHIs.

What Makes the NHI Threat Unique?

Scale

NHIs now outnumber human identities by orders of magnitude

Speed

NHIs are created and used at machine speed

Sprawl

They exist across cloud, on-prem, SaaS, and third-party environments

Fragmentation

Different individuals and teams are responsible for different elements of the identity

Invisibility

Many are unmonitored, untracked, or embedded in code

Privilege

They often have broad or poorly-scoped permissions

Longevity

Orphaned NHIs can persist indefinitely without detection

Complexity

NHI dependencies introduce security risks and service outages

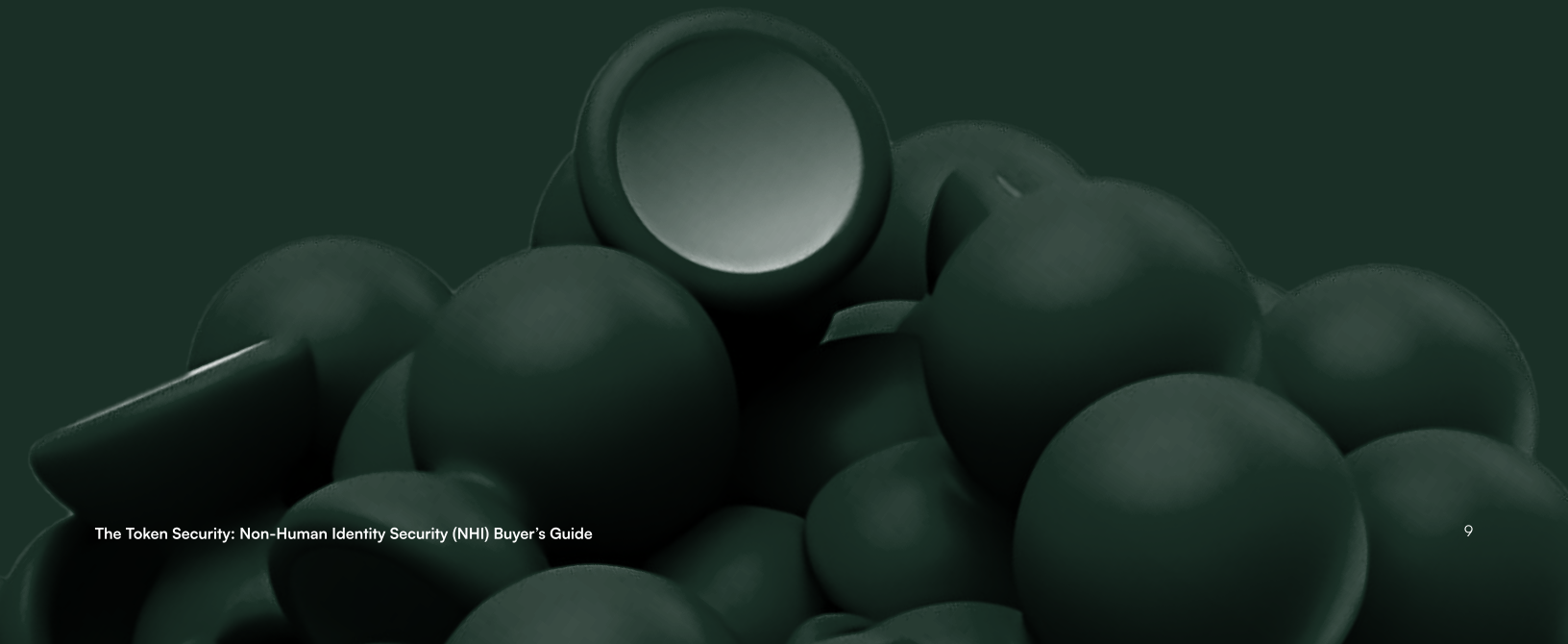
In short, NHIs have become the soft underbelly of modern infrastructure: highly privileged, lightly governed, and increasingly targeted.

The path forward requires a new mindset: machine-first, AI-native, and built to secure NHIs with the same rigor once reserved for human users. The rest of this guide will walk you through how to evaluate and select the right NHI security solution to implement this approach.

token

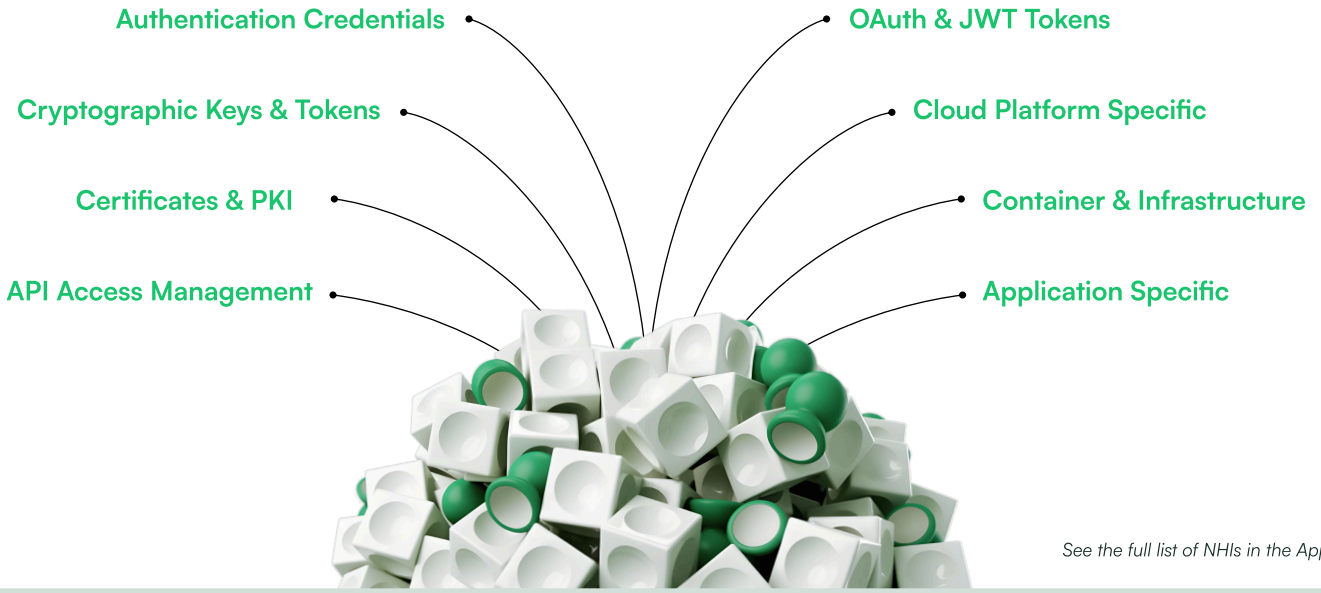
09

THE SCOPE AND COMPLEXITY OF NHIS



Non-Human Identities (NHIs) are not a single category of entity; they are a sprawling, diverse ecosystem of credentials, tokens, keys, certificates, and machine accounts used across every layer of modern infrastructure. What makes NHIs so complex, and so dangerous, is their variety, volume, and velocity. They are created dynamically by code, tools, and services; they authenticate in dozens of different ways; and they often operate autonomously, without human oversight. Many are embedded in automation scripts, infrastructure-as-code files, cloud-native workflows, or even AI agents. And because they lack standardized governance, they are prone to being overprivileged, forgotten, or misused.

The list below illustrates the wide range of NHIs in typical cloud-native, DevOps, and SaaS-driven environments. This fragmentation makes NHIs incredibly difficult to inventory, monitor, and control.
Yet each one, if compromised, can serve as a direct path to your most sensitive systems and data. Securing NHIs requires more than just vaulting secrets or rotating keys. It demands full visibility, contextual understanding, and machine-speed controls across all identity types.

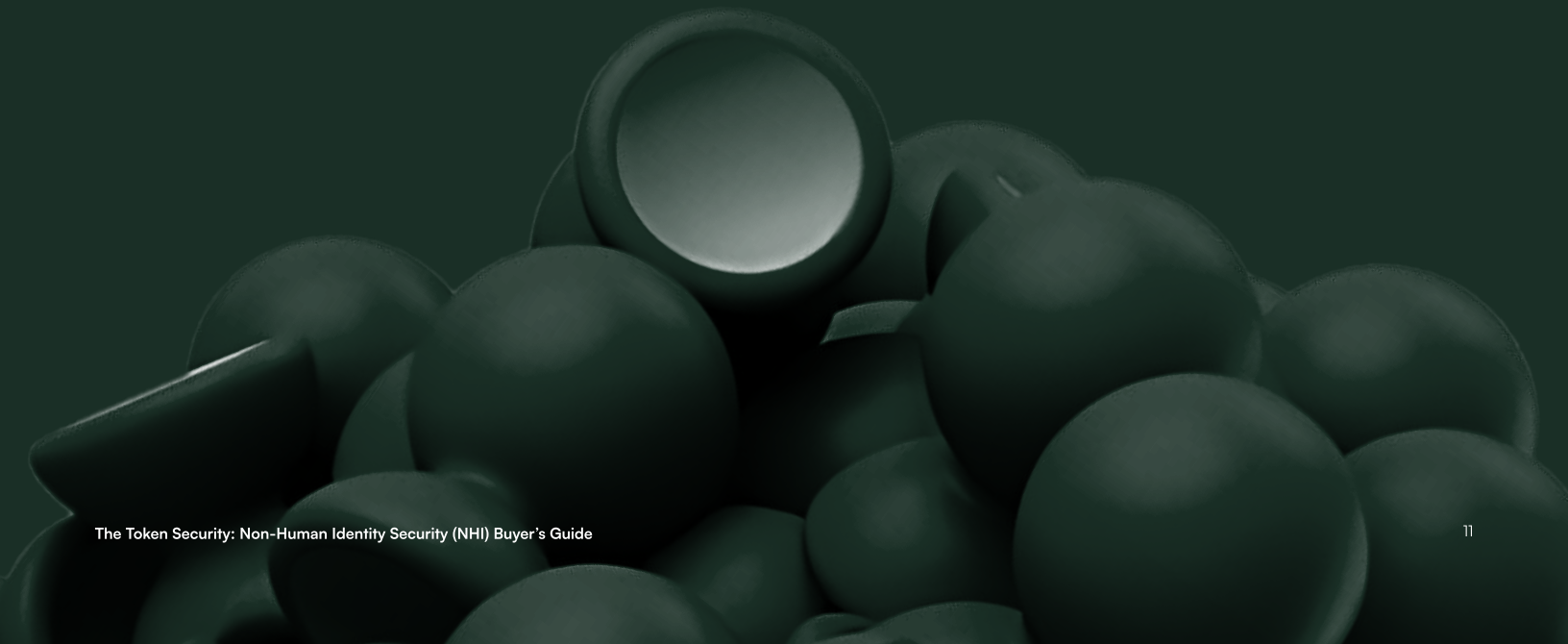


See the full list of NHIs in the Appendix.

> Current machine IAM practices are fragmented, inadequate and rife with security and compliance issues. Security and risk management leaders must modernize their machine IAM practices with all stakeholders and focus on just-in-time credentialing, technology debt management and continuous monitoring to protect assets.
>
> **Gartner**
>
> Strategic Roadmap for Modern Machine IAM, Gartner Inc, Felix Gaehtgens, Erik Wahlstrom, Steve Wessels, 2 June 2025

11

WHY LEGACY HUMAN IAM FALLS SHORT IN A MACHINE-FIRST WORLD



Identity and Access Management (IAM) has been a cornerstone of enterprise security. It is designed to ensure that the right people have the right access to the right resources at the right time. But today, most identities in your environment aren't people. They're machines. From service accounts and APIs to containers, workloads, bots, and autonomous AI agents, NHIs now outnumber human identities by a wide margin. And, they must be understood and secured very differently.

While traditional IAM platforms excel at governing user logins, enforcing MFA, and managing role-based access for employees, contractors, and customers, they were never built to manage the **speed, sprawl, and invisibility** of NHIs. As a result, most organizations are left with major blind spots that attackers have already begun to exploit.

Because identities are interconnected, the legacy centralized approach does not work!

Human IAM Limitation	Description
Static Access Models for Dynamic Identities	Human IAM systems assume identity access is relatively stable and granted based on department, role, or title. NHIs don't follow that pattern. They are: • **Ephemeral**, short-lived containers and serverless functions or AI agents that instantiate new tasks on demand • **Frequently automated**, without human oversight Static policy enforcement simply can't keep up.
Lack of Contextual Visibility	Human IAM tools focus on login events, directory structure, and user group affiliations. But NHIs don't log in like humans, and often aren't tied to user accounts. Instead, they use: • API tokens • Secrets • Embedded credentials • Certificates and keys Traditional IAM lacks visibility into how these credentials are used, by what system, and for what purpose.

Human IAM Limitation	Description
Misalignment with DevOps and AI Workflows	NHIs are created and used by developers, DevOps engineers, and even AI systems, often outside centralized IAM or IT controls. They can be provisioned in seconds via code, CI/CD pipelines, or third-party SaaS tools. Human IAM systems are not integrated into these workflows, making it easy for: • NHIs to be overprovisioned, • Secrets to be hardcoded, and • Expired or orphaned identities to persist unnoticed.
No Support for Machine-Native Threat Detection	Human IAM alerts are built around human behavior, such as failed logins, credential misuse, and suspicious locations. NHIs don't behave like users. Their misuse signals are subtle: changes in API call patterns, lateral movement between services, or anomalous system-to-system communication. Legacy tools simply aren't built to detect these patterns.

Legacy IAM is built for a different era.

Human-centric IAM was designed for a world where people were the primary users of systems. But today, the most privileged, most scalable, and most invisible users in your environment aren't people.

Securing NHIs requires a fundamentally different approach:

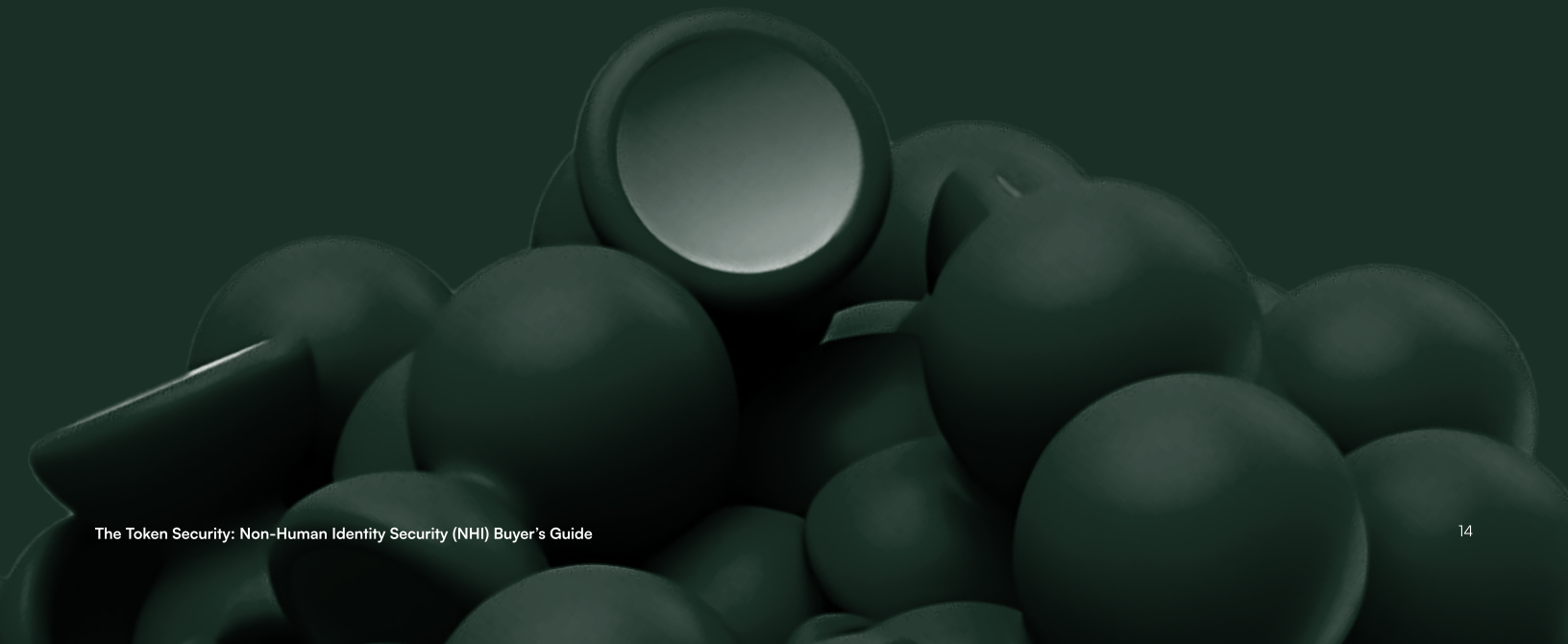
- One that treats machine identities as first-class citizens
- One that operates at speed and scale
- One that is built from the ground up for decentralized environments, automation, and AI

That's why NHI Security can't be an afterthought or an IAM feature. It must be a core capability of your modern security strategy.

token

14

APPROACHES TO NHI SECURITY



As the ecosystem of Non-Human Identities (NHIs) continues to grow, so too does the market for NHI security solutions. Organizations face a rapidly diversifying landscape of vendors, each offering a distinct methodology for securing NHIs. Understanding these approaches is essential to choosing the right fit for your infrastructure, development practices, and risk posture. Broadly, NHI security vendors fall into four major categories:

Category

Context-Driven Platforms

Description

These platforms offer a holistic and context-aware view of NHI security. Rather than zeroing in on a single vulnerability type or environment, they aggregate data across identity posture, runtime behavior, infrastructure ownership, and lifecycle state.

Key Capabilities

- Rich identity graphs and access analytics
- Integration with Infrastructure-as-Code for ownership attribution
- Continuous inventory of NHIs across cloud, SaaS, and on-prem
- Detection of permission drift and posture anomalies
- Full lifecycle controls for provisioning, use, and decommissioning

Best Suited For

Enterprises with hybrid environments, where ownership clarity, risk prioritization, and unified policy enforcement are critical.

Category

Secrets Scanning & NHIDR-Focused Vendors

Description

These vendors specialize in discovery and monitoring of secrets within the development pipeline. Their goal is to detect leaked or misused credentials early, and support Non-Human Identity Detection and Response (NHIDR) workflows.

Key Capabilities

- Secrets detection in code, config, and collaboration platforms
- Alerting on use of long-lived, unvaulted, or exposed secrets
- Automated rotation and secrets hygiene enforcement
- Monitoring for credential misuse or policy violations

Best Suited For

Dev-heavy organizations where CI/CD velocity and secrets sprawl are major challenges.

Category

Vault and Rotation-Centric Solutions

Description

These solutions prioritize automation of credential rotation, typically assuming secrets are already housed in a secure vault. They offer strong compliance alignment, especially in regulated sectors.

Key Capabilities

- Central inventory of vaulted secrets
- Policy-based rotation scheduling and triggers
- Enforcement of expiry rules and audit logging
- Integration with secret managers and vaults

Best Suited For

Organizations where secrets are decoupled from application code (but often struggles with tightly coupled legacy systems or opaque third-party integrations)

Category

SaaS-Oriented NHI Vendors

Description

Focused on SaaS-to-SaaS integrations, these vendors address API and OAuth-based non-human access across business platforms like Salesforce, Slack, and GitHub. They're well-suited to high-SaaS environments with unmanaged integrations.

Key Capabilities

- Discovery of unsanctioned or unmanaged SaaS apps
- Mapping and monitoring OAuth scopes and app usage
- Risk-based prioritization of app permissions
- Detection of suspicious API key activity or misuse

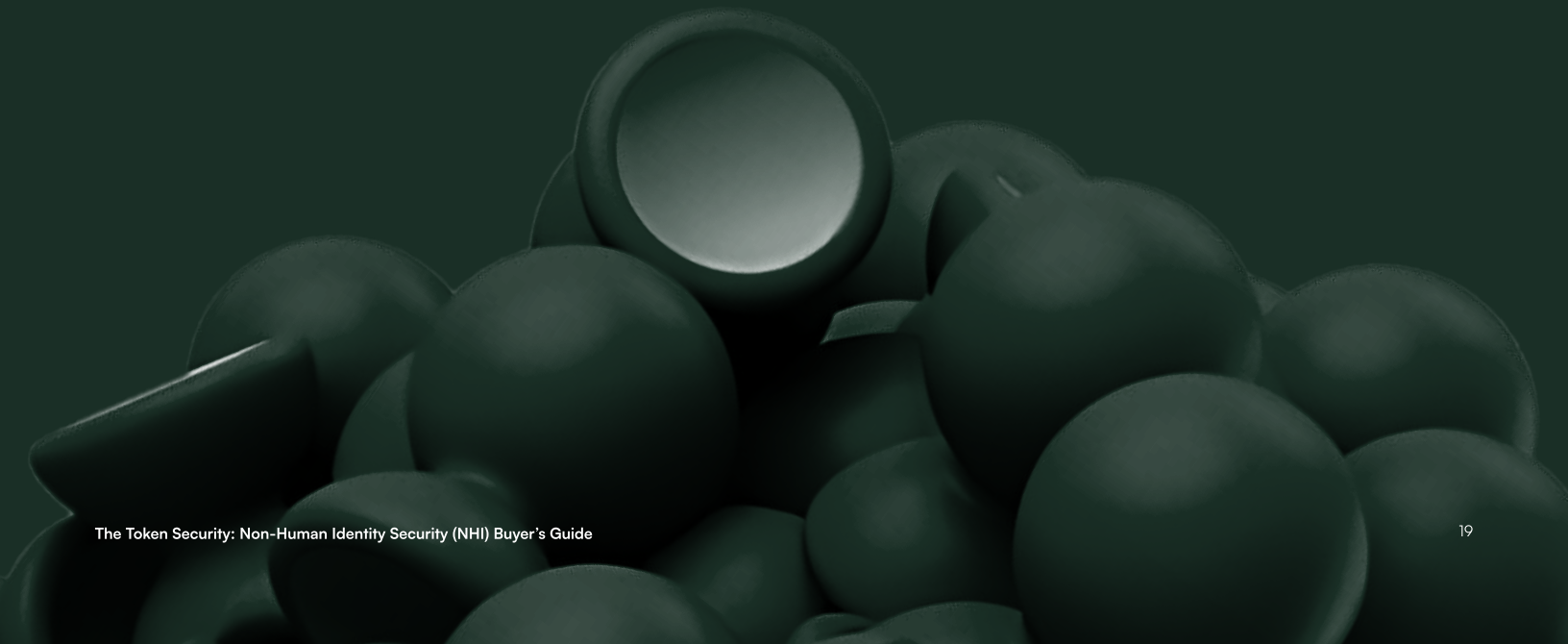
Best Suited For

Organizations where shadow IT and cross-SaaS workflows pose major access and compliance risks.

token

19

NHI SECURITY SELECTION CRITERIA



When selecting an NHI Security platform, there are critical requirements that must be met to enable an effective defense against machine-based identity threats.

NHI Security Platform Capability Areas

Ensure your NHI Security vendor meets requirements across several key areas:

Discover & Understand	Govern & Secure		Detect & Respond	
NHI Discovery & Visibility	NHI Security Posture Management	NHI Lifecycle Management	NHI Threat Detection & Response	Automation & Remediation
Enterprise Management				
Environment Coverage				

Discovery & Understand

The first step in securing Non-Human Identities is knowing what exists and how they behave. NHIs are often created outside of standard IT processes and are difficult to track with legacy tools. Effective security starts with comprehensive discovery, deep context, and real-time visibility across all environments. This category focuses on capabilities that help you identify, classify, and monitor every NHI in your ecosystem so you can move from blind spots to full awareness.

NHI Discovery & Visibility

You can't secure what you can't see. NHIs are often created outside of centralized IT processes, hidden within infrastructure-as-code, CI/CD pipelines, cloud consoles, or AI agents. An effective NHI Security solution must continuously discover and inventory all machine identities, including shadow accounts, privileged credentials, and federated/unfederated identities. It must then add context so that informed decisions can be made. This includes AI Observability: the ability to monitor, attribute, and contextualize NHIs generated by AI systems, such as agentic processes, LLM integrations, or AI-based automation pipelines. These AI-driven identities often act autonomously, generate access dynamically, and disappear quickly. Without observability into their creation, behavior, and associated risk, they become invisible entry points for attackers. Deep, contextual visibility is the foundation of all downstream NHI governance, risk assessment, and threat detection.

Functionality	Description	Token Security	Others
NHI Discovery & Visibility			
Continuous and updated NHI inventory	Build and maintain an updated inventory of NHIs, authentication methods, and entitlements across systems, environments, and accounts.	✔	
Identity type classification and identity prioritization	Identify and distinguish human users from non-humans, categorizing NHIs based on their function, criticality, and level of access to sensitive systems or data.	✔	
Visibility to local and unfederated accounts (Okta bypass authentication using local users in cloud accounts)	Gain visibility into and discover accounts that are not connected to your IdP or SSO.	✔	
Visibility to external users (3rd party, contractors, etc.	Gain visibility into any non-employee accounts that have access to your organization, including contractors, partners, and more.	✔	
Identity access graph	Visibility into the permission level, usage, dependencies, and activity.	✔	
Visibility into cross-account / product access	Gain visibility into data sharing, interactions, or processes that occur between different products or platforms, as well as across different accounts within the same product or platform.	✔	

Functionality	Description	Token Security	Others
NHI Discovery & Visibility			
Auto-discovery of new and known services	Discover and identify unfederated, shadow NHIs, and existing types of NHIs.	✔	
Discovery of new privileged keys, credentials, accounts, services, and permissions	Gain visibility into any type of privileged keys, accounts, environments, and their permission levels.	✔	
Discovery of privilege escalation paths and role-chaining	Discover role-chaining, which can create complex permission structures that are difficult to manage and audit, potentially leading to unintended privilege escalation.	✔	
Discovery of new admins and privileged identities	Discover new admins and accounts that have been granted permissions that effectively make them admins, even though they are not explicitly defined as administrators within the organization or account.	✔	
Alert upon newly created credentials	Example: New access keys/API keys/secrets.	✔	

Functionality	Description	Token Security	Others
NHI Discovery & Visibility			
Identify human owner to each non-human identity	Identify who created the identity or service and who currently owns it.	✔	
NHIs usage tracking	Identify who uses each NHI, track the usage patterns, and associate each source IP with a concrete service, workload, global service, or human.	✔	
IaC ownership	Identify Terraform ownership and associate it back to the human who created or maintained the code.	✔	
Dependencies and associations	Identify the actual workloads (VMs, K8s, Serverless) using the identities.	✔	
Analyze permission utilization	Identify and alert on overly permissive access, based on usage utilization.	✔	

Govern & Secure

Once NHIs are visible, they must be governed with the same precision and control as human identities, if not more. This category includes capabilities that help enforce least privilege, assign ownership, rotate secrets, and ensure continuous compliance. From lifecycle management to posture monitoring, these tools ensure NHIs don't become a silent source of risk, drift, or over-privilege as your infrastructure evolves.

NHI Security Posture Management

Managing NHI security posture requires analysis of activity, entitlement usage, secrets exposure, and compliance risk across all environments. A strong posture management capability provides actionable insights, highlights risk concentrations, flags misconfigurations, and identifies overprivileged or unmonitored identities before they're exploited.

Functionality	Description	Token Security	Others
NHI Security Posture Management			
Risk management dashboard	Present an overview of identity security posture compared to an industry benchmark, highlighting total identities across all environments, risk levels, key rotation overview across all authentication types, top risky identities, and critical security insights across all environments, cloud and on-prem.	✔	
Mitigate risks based on their criticality and potential blast radius	Have the ability to prioritize risks based on potential blast radius or other metrics for immediate attention.	✔	
Active vs. non-active identities	Identify all active and inactive identities across all environments.	✔	
Detect unrotated keys and the time since they were last rotated	Identify the last time each key was rotated, who consumed it, and from where (IP/ Service/workload).	✔	

Functionality	Description	Token Security	Others
NHI Security Posture Management			
Detect multiple access keys	Detect identities with multiple access keys and/or multiple personal access tokens (PAT) to avoid potential abuse.	✔	
Detect inactive access keys	Detect forgotten access keys that are no longer used.	✔	
Detect unfederated identities	Detect local users of the database, bypassing cloud federation, detect unfederated users, and detect local users bypassing IDPs.	✔	
Detect shared roles and accounts	Detect roles shared by many applications and having extensive permissions, as opposed to more granular permissions tied to a specific application.	✔	
Detect access token embedded in a code repository	Detect secrets, SSH keys, API keys, access keys, and OAuth tokens embedded in code repositories.	✔	
Detect IdP bypass	Detect local users bypassing the SSO facilitated by the identity provider.	✔	
Detect missing network policies on service accounts	Detect service accounts that work from a closed set of IPs and ports with missing network restrictions to avoid leaked permissions used by malicious actors.	✔	

Functionality	Description	Token Security	Others
NHI Security Posture Management			
Detect credentials created by offboarded employees	When an employee leaves an organization, their access should be revoked across all systems. Credentials such as API keys, service accounts, or SSH keys may have been created before offboarding and remain active, posing a security threat.	✔	
Detect permanent tokens with no expiration date	Detecting permanent tokens with no expiration date is critical for reducing security risks, as these tokens can provide indefinite access if compromised.	✔	
Detect secrets referenced in K8s pods	Detecting secrets referenced in Kubernetes pods helps prevent credential exposure and unauthorized access. Organizations should monitor pod configurations to identify secrets stored in ConfigMaps, environment variables, or mounted volumes, ensuring they are securely managed using Kubernetes Secrets, encryption, and RBAC controls to reduce security risks.	✔	
Alert on permissions drift	Alerting on permissions drift helps prevent unauthorized privilege escalation and security gaps by detecting unintended or unapproved changes to identity permissions over time. Permissions drift occurs when IAM roles, policies, or access controls deviate from their intended configurations due to manual modifications, misconfigurations, or overly permissive changes.	✔	

Functionality	Description	Token Security	Others
NHI Security Posture Management			
Alert on secrets not stored in vaults	Cross-correlate secrets generated in the source environments with secrets stored in secrets managers and values to identify long-term credentials not stored in vaults such as HashiCorp Vault, Akeyless, or other vaults.	✔	
Discovery of over-privileged accounts and services	Discovery of permissive access of service accounts and users, by comparing permissions scopes and actual usage across the different environments, technologies, and authorization schemes.	✔	
Discovery of actions on non-rotated keys/ over-privileged	Identify activity performed with long-term unrotated secrets, identify relevant consumers, such as workloads, cloud services, or humans, in order to enable safe rotation and avoid service downtime.	✔	
Ability to ensure compliance with industry regulations.	Ensure identity posture controls in a variety of regulatory frameworks such as: GDPR, HIPAA, SOC2, PCI DSS, CCPA, FINRA, FISMA, HITRUST, NIST and others.	✔	
Have the ability to store and track audit trails	Generation and retention of comprehensive audit trails that document all actions and events related to NHIs, including access attempts, modifications, and usage.	✔	

NHI Lifecycle Management

Unlike human users, NHIs don't onboard with HR or offboard through IT tickets. They're spun up by people across the organization or even code and can persist indefinitely if unmanaged. That's why lifecycle management is essential. From ownership assignment and least privilege enforcement to safe credential storage, rotation, and deprovisioning, your platform must provide automation and accountability throughout the NHI lifecycle, preventing orphaned access, sprawl, and drift.

Functionality	Description	Token Security	Others
NHI Lifecycle Management			
Auto-assignment of ownership	Automatically identify human owners of any service account and detect involved infrastructures as code (IaC), to ensure clear accountability. This improves visibility and operational efficiency and reduces time to mitigate security posture findings.	✔	
Help maintain least privilege	Suggest a minimized scope of permissions, based on actual usage. This minimizes the risk of privilege escalation and unauthorized access.	✔	
Help storing in the vault when needed	Ensure safe migration of secrets such as API keys, access keys, SSH keys to a vault, by providing extensive context of relevant consumers and actual activity.	✔	
Help with key rotation and transition to short-term credentials	Automate the rotation of keys and credentials at predefined intervals or based on security triggers, when consumed from vaults. Reduces the risk of long-lived secrets being compromised or misused.	✔	

Functionality	Description	Token Security	Others
NHI Lifecycle Management			
De-provisioning of an NHI	Ensures proper offboarding of NHIs by revoking permissions, deleting unused accounts, and cleaning up associated credentials. Prevents security risks from lingering or abandoned identities.	✔	
Share alerts with the NHI owner	Send real-time security alerts and notifications directly to the assigned NHI owner. Helps in quick remediation of security issues and policy violations.	✔	
Search NHI by the owner and help in off-boarding	Enables security teams to quickly find NHIs linked to specific owners for audit and offboarding. Ensures proper lifecycle management and prevents orphaned identities.	✔	

Detect & Respond

NHIs are increasingly targeted by attackers because they're often unmonitored, over-permissioned, and hard to detect in action. This category highlights capabilities that enable real-time threat detection and scalable, automated response. Whether it's identifying anomalous behavior, intercepting dark web credential leaks, or orchestrating remediation via SOAR or IaC pipelines, the ability to detect and respond at machine speed is essential for minimizing damage and ensuring resilience.

NHI Threat Detection & Response

NHIs behave differently than humans, and so do the threats targeting them. Detection engines must be machine-native, tuned to identify behavioral anomalies, privilege escalation attempts, misuse of secrets, or access from suspicious IPs. Response must be equally fast, with real-time alerting and integrations into existing SIEM, SOAR, or XDR workflows. The ability to detect and respond to NHI threats at machine speed is non-negotiable.

Functionality	Description	Token Security	Others
NHI Threat Detection & Response			
Detect unusual or abnormal behavior patterns of NHIs	Continuously monitor NHIs for deviations from normal usage patterns, such as unexpected API calls, data access, excessive privilege requests, or requests from unusual source IPs or geo locations. Behavioral analytics help identify potential threats, compromised credentials, or misuse.	✔	
Real-time monitoring of access attempts and activities associated with NHIs	Tracks authentication attempts, permission changes, and rejected API calls to detect unauthorized or suspicious activity. Provides visibility into NHI interactions across cloud and on-premises environments.	✔	
Alerting and notifying security teams or administrators of detected threats or suspicious activities involving NHIs	Generates real-time alerts when anomalous or high-risk activities are detected, ensuring security teams can respond quickly. Integrates with SIEM, SOAR, or XDR platforms for automated incident response.	✔	
Detect authentication from suspicious IPs	Identifies NHIs authenticating from high-risk or blacklisted IP addresses, such as TOR nodes, foreign locations, or known attacker infrastructure.	✔	

Functionality	Description	Token Security	Others
NHI Threat Detection & Response			
Detect attempts to escalate privileges	Monitors for unauthorized role changes, permission modifications, or privilege escalation attempts by NHIs.	✔	
Alert on used keys found on the dark web	Continuously scans dark web sources and threat intelligence repositories for exposed API keys, service credentials, or secrets linked to NHIs. Sends alerts and initiates automated remediation, such as key revocation or rotation	✔	
Detect service account used and authenticated by an employee	Identifies instances where an employee manually authenticates from their own endpoint, using service account credentials, which may indicate misuse or a security gap.	✔	

Automation & Remediation

The scale of NHIs makes manual triage and remediation impossible. An NHI Security platform must automate common tasks: routing alerts to owners, correlating findings with IaC artifacts, and generating AI-driven remediation instructions. Ideally, it should integrate with cloud-native automation and SOAR systems to orchestrate resolution at scale, without disrupting services or introducing operational drag.

Functionality	Description	Token Security	Others
Automation & Remediation			
Route alerts with prescriptive instructions to the appropriate person	Automatically direct actionable alerts, including clear remediation guidance, to the responsible stakeholder for resolution	✔	
Automatically identify the relevant Infrastructure as Code artifact involved with identity provisioning	Detect and surface the specific Infrastructure-as-Code artifact responsible for provisioning a given identity.	✔	
Use an advanced AI Solution to generate remediation instructions, involving Infrastructure as Code technologies	Leverage AI to generate precise remediation steps aligned with Infrastructure-as-Code configurations and best practices.	✔	
Trigger predefined remediation workflows	Integrate with SOAR and Cloud Automation solutions.	✔	

Functionality	Description	Token Security	Others
Automation & Remediation			
Manage ongoing remediation programs according to pre-defined project scope	Track and coordinate remediation efforts as structured campaigns aligned to defined timelines, scopes, and accountability.	✔	
Conduct access reviews for service accounts	Facilitate periodic access reviews for service accounts to validate necessity, scope, and compliance with least-privilege principles.	✔	

Enterprise Management

As your NHI footprint grows, your security platform must be able to grow with it. Enterprise readiness means flexible APIs, seamless integrations with ITSM, collaboration tools, and cloud-native workflows, and the ability to create custom policies and reporting for different stakeholders. Managing NHIs at enterprise scale requires agility, extensibility, and alignment to your operational model.

Functionality	Description	Token Security	Others
Enterprise Management			
MCP Server	MCP server that integrates with external LLMs to answer questions and provide environment-specific remediation guidance.	✔	
AI Chat Interface	In-platform AI-powered chat.	✔	

Functionality	Description	Token Security	Others
Enterprise Management			
SIEM Integration	Integration with SIEM tools for alerts.	✔	
SOAR Integration	Build automated workflows based on alerts and enrich security incidents.	✔	
Configure policies and adjust risk to fit my organization's needs.	Ability to build custom policies based on specific security needs.	✔	
Restful API and Webhook	Ability to push, pull, and prioritize alerts to be consumed by the customer's security tools.	✔	
Integration with collaboration, ITSM tools	Integrating with ServiceNow, Slack, Teams, PagerDuty, etc.	✔	
Scalability	Scalable with the growing capacities of hybrid cloud, critical SaaS apps, and other integrations.	✔	
Reporting	Provide different levels of reporting from the executive level to the technical level to fulfill their respective needs.	✔	

Environment Coverage

Before solving the NHI challenge, you need full awareness of where NHIs exist across your environment. This means covering more than just cloud service accounts or IAM roles. A modern NHI Security platform must support a wide spectrum of identity types, from ephemeral workloads and API keys to AI agents and SaaS integrations. The broader your coverage, the deeper your visibility, and the lower your risk.

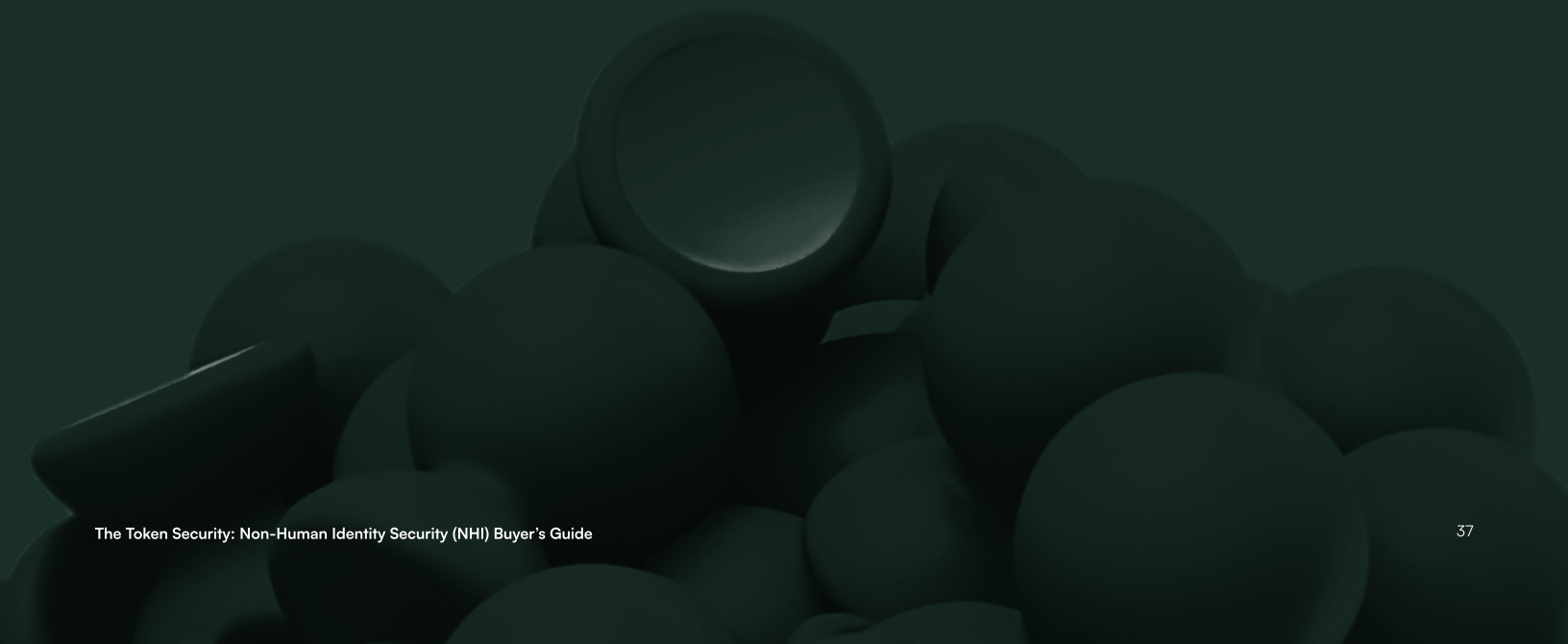
Functionality	Description	Token Security	Others
Environment Coverage			
NHI Types and Authentication Methods	Usernamed and passwords, service accounts, access keys, storage accounts, Kubernetes, service principles, RDS users, EC2/VM roles, OIDC, SSH keys, API keys, OAuth 2.0 tokens, SAML	✔	
All Major IaaS apps	AWS, Microsoft Azure, GCP	✔	
Workloads	Kubernetes, Docker, EC2, VMs, ECS, GKE, AKS, Lambda, etc.	✔	
Databases and Data Warehouses	Snowflake, MySQL, Databricks, PostgreSQL, Redis, MongoDB, etc.	✔	
SaaS apps	Salesforce, Workday, NetSuite, Jira, Microsoft Teams, etc.	✔	
CI/CD, Dev pipeline tools	GitHub, GitLab, CircleCI, Jenkins, Terraform, etc.	✔	

Functionality	Description	Token Security	Others
Environment Coverage			
IdPs and SSOs	Okta, Ping, JumpCloud, OneLogin, Google Workspace, Entra ID, etc.	✔	
Vaults and Secret Managers	Azure Key Vault, GCP and AWS Secret Managers, HashiCorp Vault, etc.	✔	
Gen AI and LLM App Identities	AI Agent Identities, LLM Roles, API/Access Keys, User/Pwd, MCP Servers, OpenAI, Anthropic, etc.	✔	

token

37

THE TOKEN SECURITY ADVANTAGE



Addressing NHI challenges requires a machine-first, AI-native approach. From on-premises infrastructure to the cloud and Agentic AI systems, The Token Security platform helps organizations reduce risk and accelerate AI adoption. Token Security enables security teams to discover, understand, govern, and protect NHIs, while detecting and responding to emerging threats. With deep, actionable insights and comprehensive NHI coverage across your entire environment, Token Security empowers innovation while keeping you in control.

The Token Security Approach

Token Security provides a Data and Context-Driven platform by design, offering a unified view of Non-Human Identities across infrastructure, code, and runtime environments. By linking NHIs to their source, whether through Infrastructure-as-Code, deployment metadata, or cloud resource ownership, Token delivers unprecedented clarity into who created an identity, who owns it, and how it's being used. This contextual model enables proactive risk management, fine-grained access control, and comprehensive lifecycle governance. In contrast to narrower approaches focused solely on secrets or vaults, Token Security empowers security and identity teams with continuous insight across every phase of the NHI lifecycle, making it the most complete and future-proof strategy for securing machine and non-human identities in complex, hybrid, and fast-moving environments.

Business Outcomes

- **Reduce exposure to breaches involving machine identities**
- **Accelerate innovation, including secure AI adoption**
- **Improve efficiency and simplify compliance while securing complex, distributed environments**

Capabilities

NHI Discovery & Visibility	**“See What Others Miss”** Stay ahead of the oncoming wave by securely enabling business use of Agentic AI.
NHI Security Posture Management	**“Strengthen Your Core”** Reduce your attack surface by mitigating identity-based risks while aligning with security and regulatory requirements.
NHI Lifecycle Management	**“Orchestrate and Govern”** Simplify the management of machine identities while closing governance gaps, eliminating blind spots like offboarded identities with active access and permission drift.
NHI Threat Detection & Response	**“Detect and Disarm NHI Threats in Real-Time”** Catch behavioral anomalies and suspicious activities as they happen.
Automation & Remediation	**“Beep. Boop”** Playbooks, campaigns, webhooks, AI-generated, auto-rotation etc. Rules engine. Automated response to identities where the risk threshold has been passed. Autonomously interacting with your ecosystem and taking actions on your behalf.

Use Cases

Agentic AI Security	**“Every AI Agent has an Identity”** Ensure intelligent agents operate within defined boundaries, with visibility, controls, and response mechanisms in place.
Third-Party NHI Security	**“Every Vendor Expands Your Attack Surface”** Gain visibility and control over supplier access to your data, identities, and privileges.
Zero Trust NHI Security	**“Don’t Trust Anyone … or AnyTHING”** Continuously validate every non-human identity, action, and access path. No assumptions, no exceptions.

Use Cases

Compliance	**Compliance Doesn't End With Human IAM** Simplify audits and NHI access review to demonstrate compliance by continuously monitoring, governing, and remediating non-human identities.
Mergers & Acquisitions	**"Accelerate Secure Integration During M&A"** Quickly assess and secure non-human identities across merging environments to reduce risk and streamline consolidation. When you integrate an environment, where are all the accounts? Who has the knowledge? Do we want to keep the employee? You need to know how to integrate, what to integrate, which • Divestitures as well. Leave a backdoor for offboarded employees? • Migrations: Moving from AWS to GCP, how do I do that? What are the accounts? Lift and shift or build new? Who are the identity owners and consumers?

Key Differentiators

Deepest, Most Actionable Insights	Analyzes the relationships between all types of NHIs and their complete context.
Machine-Centric	Takes a decentralized approach to discovering and securing NHIs.
AI-Native	Discovers and secures AI agents while providing a natural language interface via an MCP server and embedded AI chat interface..
Scalable	Never in-line, Token Security will not impact your operations.
The Most Coverage	Analyzes data from on-premises to cloud to AI.

Types of NHIs

Location	NHI	Description
Authentication Credentials	Service Accounts	Non-human users created to run applications, services, or automated tasks.
	Machine Passwords	Static passwords assigned to services or automated systems for authentication.
	Database Credentials	Usernames and passwords used by applications or services to access databases.
	SQL Authentication Credentials	Credentials used to authenticate against SQL-based databases.
	Git Credentials (GitHub, GitLab, CodeCommit)	Used to authenticate Git operations from CI/CD pipelines or developer systems.
	CodeCommit Git Credentials	AWS credentials used to access CodeCommit repositories.
	Git Credential	Credentials that allow read/write access to source code repositories.
	Amazon Keyspace Credentials	Credentials to access Amazon Keyspaces (for Apache Cassandra).
	Transfer Server Credentials	Used to authenticate SFTP/FTPS users in AWS Transfer Family.
	SMTP Credentials	Used to send emails from applications through SMTP servers.

Location	NHI	Description
Authentication Credentials	Active MQ Broker Passwords	Credentials for authenticating to message brokers like Apache ActiveMQ.
	AUTH Strings	Base64-encoded credentials used in HTTP basic authentication headers.
API Access Management	API Keys	Used by applications or services to access APIs.
	Access Keys	Typically refers to cloud provider access keys (e.g., AWS Access Keys) for programmatic access.
	Subscription Keys	Used to authenticate and authorize API usage under a subscription model.
	Personal Access Tokens (PATs)	Token-based authentication for accessing APIs or developer tools (e.g., GitHub, Azure DevOps).
	Access Tokens	Temporary tokens used to access resources via APIs, often in OAuth flows.
	Client Secrets	Secrets used by applications to prove identity when calling APIs.
	App Keys	Keys used to authorize applications accessing cloud services or internal APIs.
	Web API Keys	Keys used by frontend or backend apps to call web APIs.
	Resource Tokens	Tokens tied to specific API resources or scopes.

Location	NHI	Description
API Access Management	Apigee App Credentials	Keys and secrets used to access APIs managed through Google Apigee.
	User Pools Client	OAuth clients defined in user pools (e.g., Amazon Cognito) to authenticate apps.
	Federated Identity Tokens	Tokens used to authenticate external services via SAML, OIDC, etc.
Certificates & PKI	Certificates	Digital certificates with public/private key pairs used for encrypting communications and validating identity.
	Private/Public Certificates	Certificates issued by a public or private certificate authority for SSL/TLS and mutual authentication use cases.
	X.509 Signing Certificates	Certificates used to sign and verify software, messages, or identities.
	Web Push Certificates	Certificates used for authenticating web push notifications.
Cryptographic Keys & Tokens	SSH Key Pairs and Certificates	Used to authenticate access to servers, CI/CD pipelines, or developer environments.
	Service Account Keys	Key files that allow authentication on behalf of service accounts (e.g., GCP, AWS).
	HMAC Keys	Keys used to perform message authentication in APIs or internal protocols.

Location	NHI	Description
Cryptographic Keys & Tokens	URL Signing Keys	Used to generate signed URLs for restricted access to resources (e.g., media, downloads).
	URL Signing Secrets	Secrets that act as the cryptographic seed for signed URLs.
	IAM Roles and Policies	Permissions containers assigned to NHIs in cloud platforms like AWS or GCP.
OAuth & JWT Tokens	JWTs	JSON Web Tokens used to authenticate and authorize access across distributed systems.
	OAuth2 Access Tokens	Bearer tokens used to grant scoped access to APIs and applications.
	Authorization Keys	Keys or tokens that authorize access to protected resources.
Cloud Platform Specific	Shared Access Signatures (SAS)	Azure tokens that grant limited access to storage resources for a defined period.
	Shared Access Policies	Policies defining conditions under which access is granted via SAS tokens.
	ElastiCache Auth Tokens	Used to authenticate clients to AWS ElastiCache clusters.
	Origin Access Identity	CloudFront-specific identity used to securely serve private content from S3
	Secrets in Environment Variables	Secrets passed to apps at runtime; often hard to track and secure.

Location	NHI	Description
Container & Infrastructure	Kubeconfig Credentials	Credentials used to authenticate and configure access to Kubernetes clusters.
	CI/CD Build Secrets	Tokens/secrets used during build and deployment (e.g., to fetch code, publish artifacts).
Application Specific	App Access Tokens	General-purpose tokens used for application-level authentication or session control.
	SDK Meeting Tokens	Tokens issued by SDKs (e.g., Zoom, Twilio) to join or host meetings programmatically.
	Application Secrets	Any sensitive value (e.g., keys, passwords) stored and used by applications or services.
	Package Manager Tokens	API keys for publishing to or pulling from package registries (e.g., npm, PyPI).