token

2025

REIMAGINING NON-HUMAN IDENTITY DISCOVERY AND VISIBILITY IN THE AGE OF AI

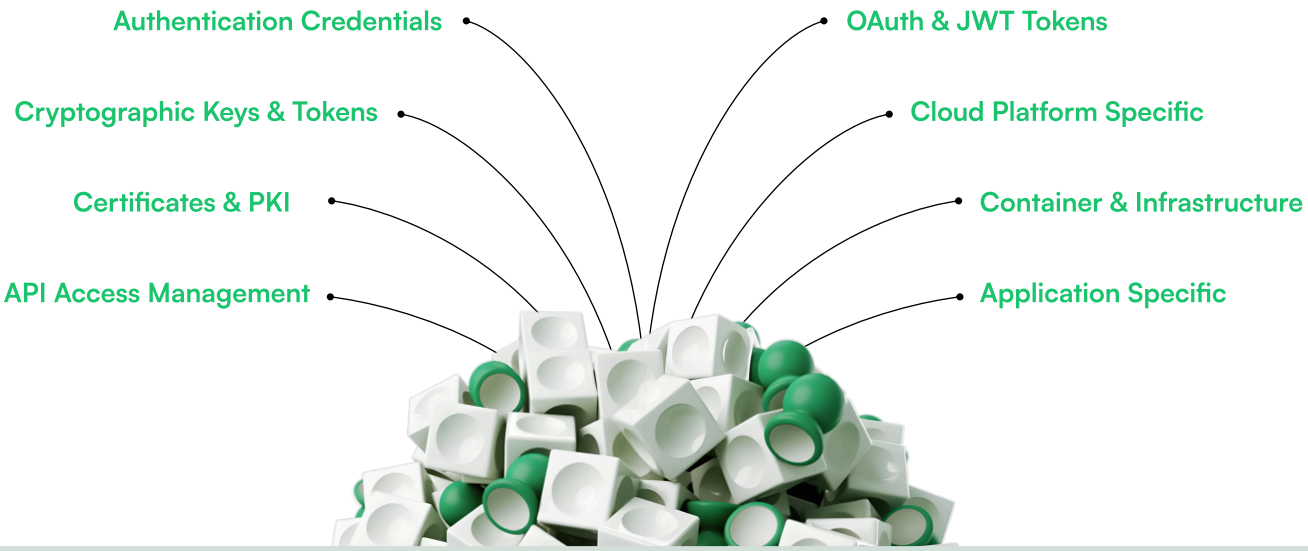
HOW TOKEN SECURITY DELIVERS THE CONTEXT YOU NEED TO CONTROL YOUR FASTEST-GROWING ATTACK SURFACE

Table of Contents

Executive Summary

You can't manage and secure what you can't see. And in the modern enterprise, there is far more in the shadows than most security teams realize.

Beneath every cloud deployment, CI/CD pipeline, microservice, and AI-driven process lies a vast and ever-changing layer of non-human identities (NHIs), which includes service accounts, workload identities, API keys, tokens, secrets, and autonomous agents. These identities authenticate, authorize, and automate the systems that keep your business running.



Today, they outnumber human identities by a staggering 45 to 1. Yet few organizations can answer the simplest questions about them: How many exist? Where are they? What can they do? And, who is responsible for them?

The visibility gap isn't just a technical inconvenience. It's an identity and access management (IAM) and security crisis. Unseen NHIs can act as hidden backdoors into production systems, expand the blast radius of an attack, and undermine the very principles of Zero Trust. Token Security aims to help organizations to close this gap.

With a machine-first, AI-native platform, Token Security continuously discovers every NHI across on-premises, hybrid, multi-cloud, and AI-driven environments. But, discovery is just the start. Token Security goes deeper to enrich each identity with metadata, actionable context (permissions, entitlements, ownership, dependencies, etc.), and even runtime behavior. This gives you the intelligence to remediate, govern and secure NHIs effectively and efficiently.

The Hidden Layer of Modern Infrastructure

The scale and complexity of NHIs didn't emerge overnight. It is the product of innovation and converging trends that continue to reshape the enterprise IT landscape.

First, hybrid and multi-cloud architectures have spread identity data across cloud platforms (AWS, Azure, GCP), and on-premises systems, each with its own formats, controls, and permission models.

Second, ephemeral infrastructure has become the norm, with containers, serverless workloads, and microservices spinning up new identities on demand and often discarding them just as quickly.

Finally, the rise of agentic AI has added a new layer of complexity with autonomous agents that create and consume credentials at machine speed, often without human oversight.

This sprawling ecosystem is largely invisible to traditional identity management approaches. Many identities are unfederated, existing outside of centralized directories or SSO systems. Others are abandoned service accounts that still hold permissions to sensitive systems. And some are active connections from third parties which have been long forgotten, but still present and silently expanding your attack surface.

For attackers, this is fertile ground. Every undiscovered NHI is a potential point of attack. Every poorly understood credential is an opportunity for escalation and lateral movement.

Why Discovery Alone Isn't Enough

The first step toward securing NHIs is to find them. But a raw list of identities, without context, is of limited value. Security and identity teams need more than an NHI count. They need to understand the full story of each identity.

What kind of identity is it?

Who owns it?

Where does it live?

What systems or workloads depend on it?

What permissions and entitlements does it have?

And, most importantly, how is it behaving in real time?

Without these answers, any attempt to remediate risk becomes a gamble. Removing an identity without knowing what it supports can break mission-critical services. Leaving it untouched can leave a door wide open for attackers.

True NHI visibility means having the context to take action with confidence.

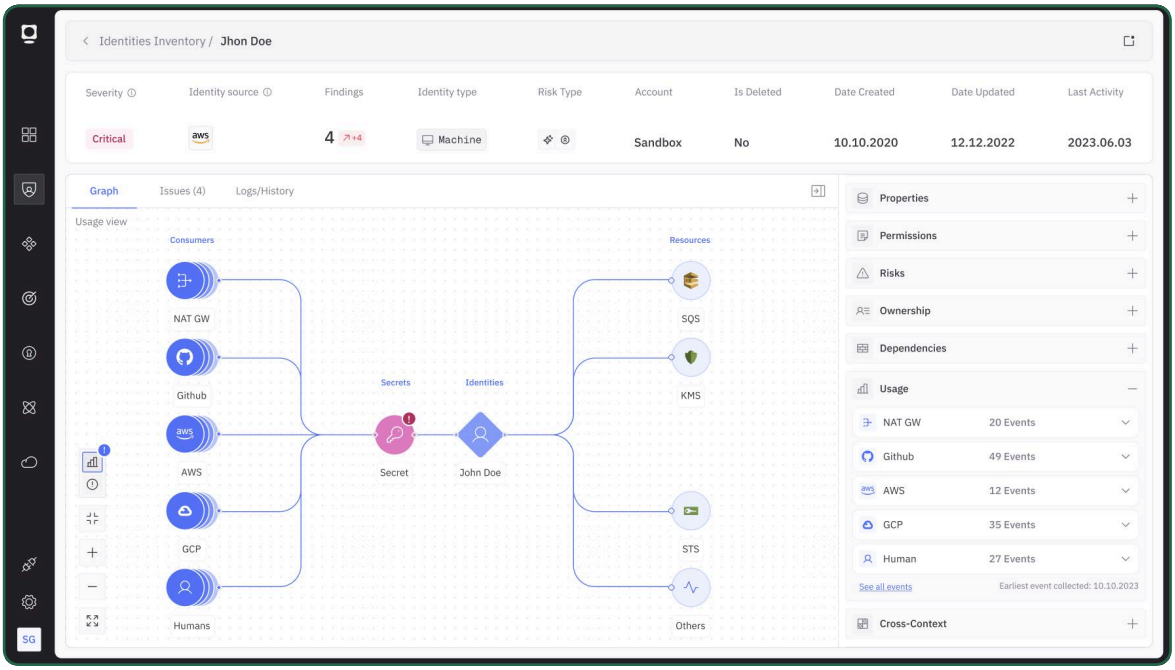
How Token Security Sees What Others Miss

The Token Security platform is purpose built to discover the complex NHI landscape and provide comprehensive visibility. By connecting directly to cloud platforms, SaaS applications, on-premises infrastructure, CI/CD pipelines, databases, vaults, and AI systems, it automatically discovers every machine identity in your environment.

But it doesn't stop there. Each identity is enriched with intelligence that includes entitlements, ownership details, and mapped dependencies. Token Security builds NHI Risk Graphs™ that show exactly how each NHI interacts with the rest of your environment, what it can access, and what depends on it. This contextual awareness allows you to prioritize identities based on their sensitivity, exposure, and operational importance.

The Token Security platform also uncovers accounts that are typically invisible to other tools, such as local and unfederated accounts outside of IdP control, or forgotten vendor integrations that still have access to critical systems. Even third-party NHIs are brought into view, giving you a complete picture of supply chain risk.

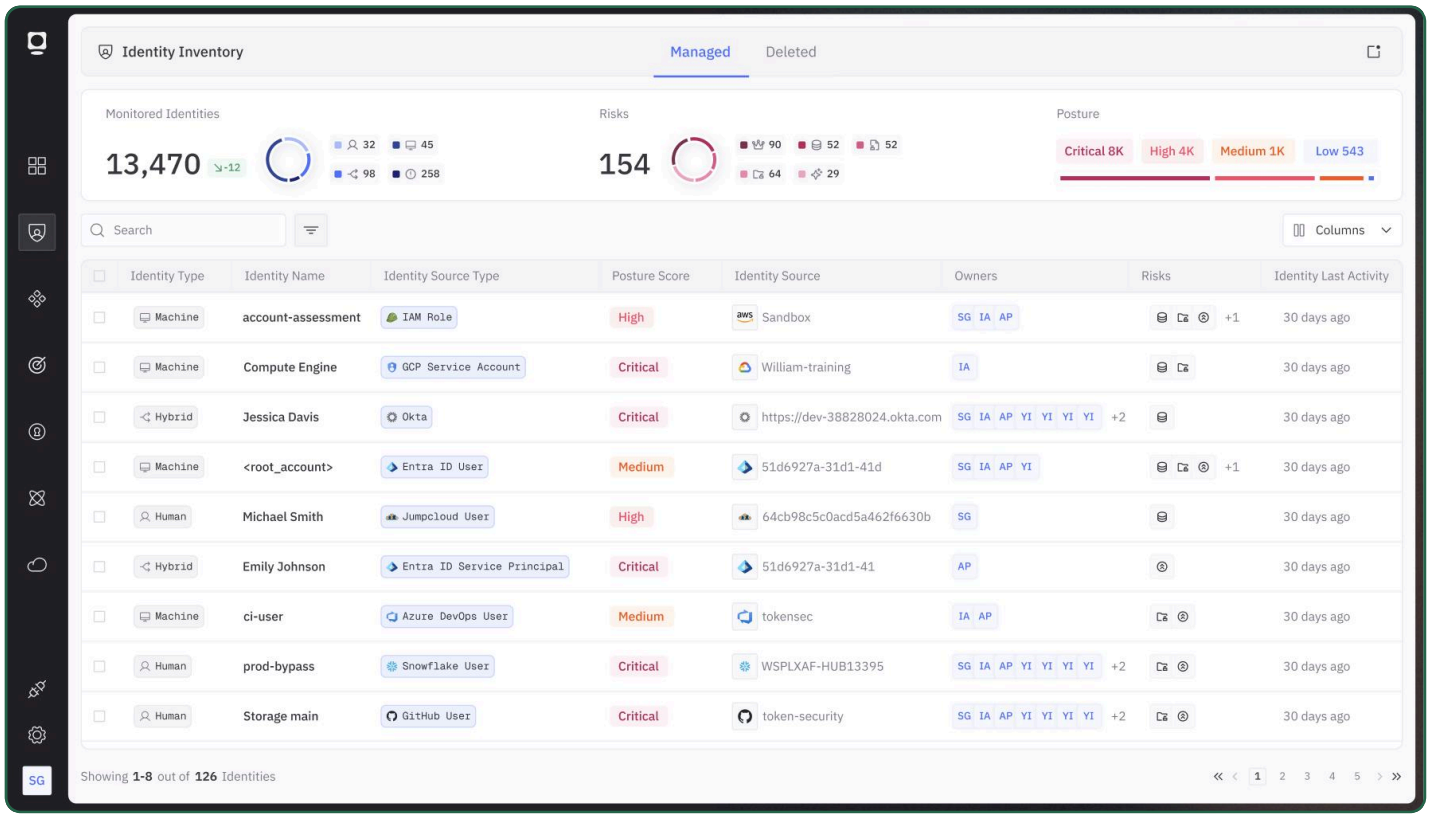
At the core of this capability is the NHI Risk Graph™, a continuously updated model that correlates configuration data, logs, and runtime telemetry to reveal the true state of your machine identity ecosystem.



From Snapshots to a Dynamic Inventory

Traditional discovery tools and audits give you a moment-in-time view of your identities. Token Security gives you a dynamic inventory. As new identities are created, permissions change, or accounts are removed, the platform updates in real time. You are never working from stale information.

This continuous discovery and visibility not only shows you what identities exist, but also detects when something changes that increases risk such as an account that becomes orphaned, a key that remains unrotated past its policy deadline, or an identity that suddenly gains overly broad permissions. These insights allow you to intervene before a vulnerability becomes an incident or a compliance issue.



The Strategic Advantage of Complete Discovery and Visibility

With deep NHI discovery and full visibility, security and identity teams can move from reactive problem-solving to proactive risk management. They can assess posture with precision, uncover compliance gaps before auditors do, and align security and identity governance with the principles of least privilege. They can also move quickly to mitigate threats, knowing exactly what is at stake and who is responsible.

Most importantly, complete discovery and visibility empowers organizations to innovate without fear and hesitation. When you trust your understanding of the machine and non-human identities in your environment, you can confidently adopt new automation, AI capabilities, and cloud services with the intelligence and context to secure and control these identities.

Discovery and Visibility Is the Foundation for NHI Security

The non-human identity problem is a critical blind spot for most organizations regardless of their size. The path to solving this problem begins with discovery and visibility. But basic discovery is not enough, you need a continuous, all-encompassing view that reveals not just what identities exist, but what they mean for your overall security posture. Token Security delivers that view. By combining comprehensive discovery with deep, real-time context, the Token Security platform enables security and identity teams to see what others miss, understand their true risk, and lay the foundation for safe automation, remediation, governance, and compliance.

To learn more about the discovery and visibility capabilities of the Token Security platform, request a demo today: https://www.token.security/book-a-demo