token SVCI Silicon Valley CISO Investments

2025

WHY WE INVESTED

SVCI / TOKEN

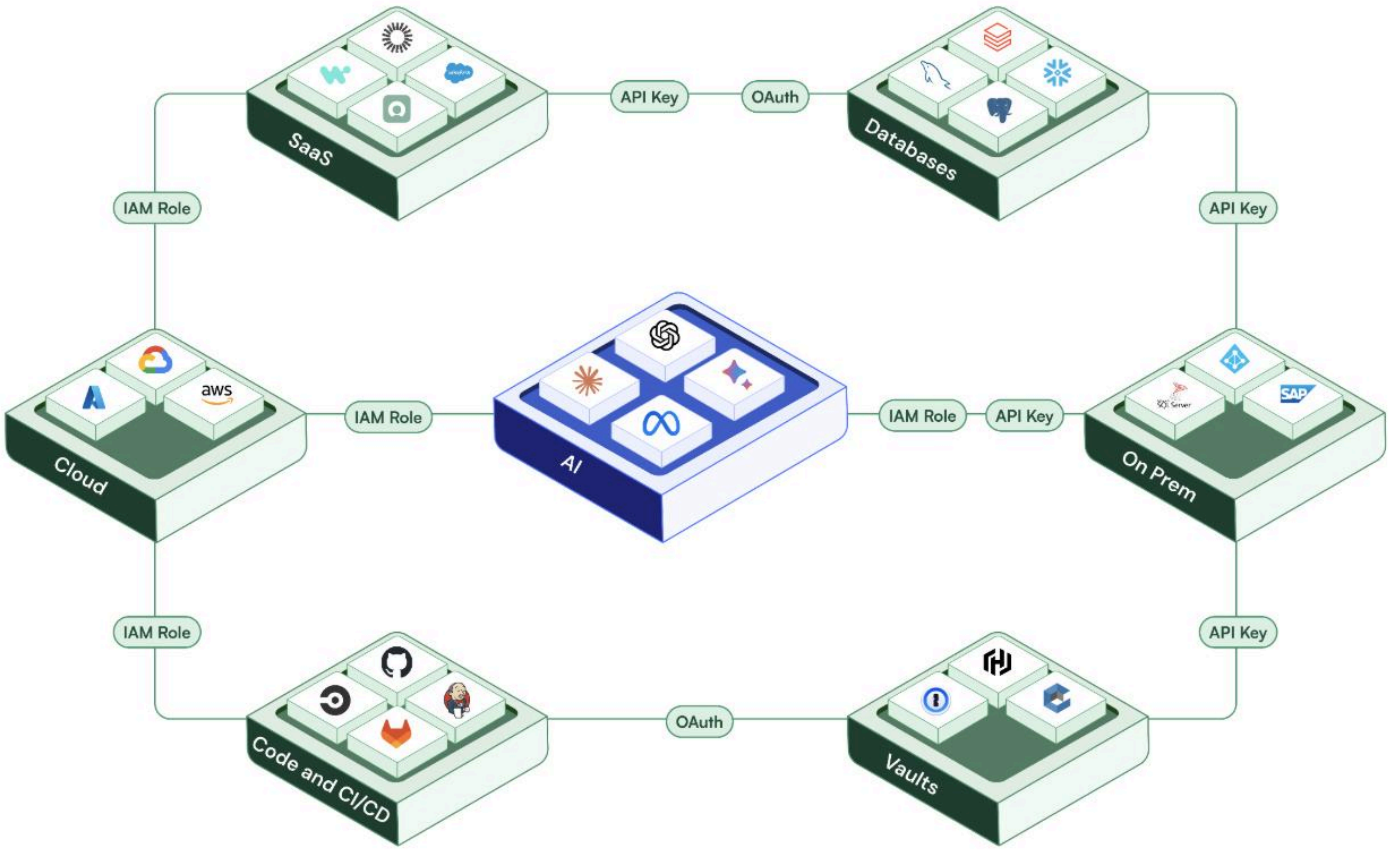
Why We Invested : SVCI / Token

Table of Contents

SVCI /Token

As enterprises embrace AI and cloud at scale, Non-Human Identities (NHIs), like service accounts, APIs, and AI agents, are exploding in number, creating serious security and compliance gaps. Traditional IAM tools can't keep up. That's why SVCI invested in Token Security: an AI-native platform purpose-built to discover, govern, and secure NHIs across the enterprise.

Token stood out in SVCI's rigorous, founder-led diligence process for its deep visibility, automated controls, and real-time threat response. It helps security teams tackle shadow identities, privilege sprawl, and orphaned accounts—making it essential for modern, cloud-driven orgs navigating the NHI security challenge.

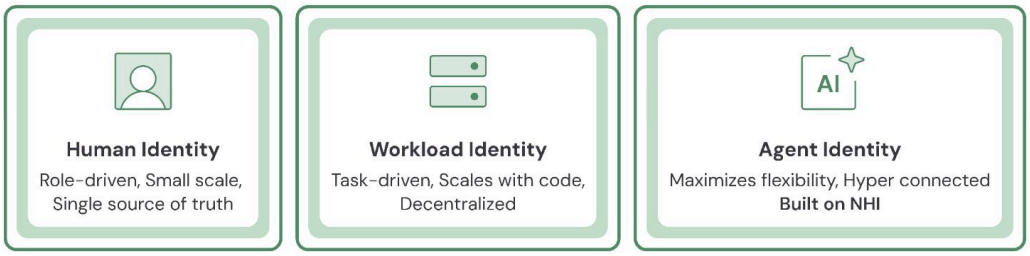


The SVCI group has a unique ability to understand current cybersecurity challenges across industries, and one trend stands out: the rise of NHIs and adoption of AI is reshaping enterprise risk. Traditional Identity and Access Management (IAM) solutions excel at governing human logins and access, but fall short at managing machine and non-human identities, which often do not have multi-factor authentication, clear ownership, and lifecycle management. These gaps enable attackers to exploit excessive privileges, move laterally, and escalate privileges undetected.

Key challenges highlighted by SVCI's CISO community include:

Exponential Growth and Visibility Gaps	The rise of machine and non-human identities (service accounts, ephemeral workloads, agentic AI, APIs, and automation pipelines) has introduced a new class of security risk. NHIs now outnumber human identities by as much as 45:1 or even greater, operating at machine speed across distributed systems, often without the same governance or visibility as their human counterparts. The rapid adoption of cloud services, microservices architectures, DevOps practices, and agentic AI has only accelerated this trend, leading to an explosion of NHIs that are invisible to centralized IT and Security processes. These identities are frequently created dynamically, span environments, and persist beyond their intended lifecycle. Unlike human identities, managing and securing NHIs is a significant challenge due to insufficient oversight and no clearly defined ownership. This creates critical gaps in accountability and makes it increasingly difficult to monitor, manage, or remediate risks effectively.
Security Risks and Privilege Sprawl	NHIs frequently operate with elevated privileges and without the safeguards typically applied to human users, such as multi-factor authentication (MFA). NHIs are also often created in a decentralized manner making excess entitlements the norm and not the exception. The risk isn't just theoretical: compromised NHIs have been linked to significant breaches. An example of such a breach includes the OAuth attack against Microsoft by Midnight Blizzard. By exploiting this weakness, the threat actor took advantage of an unused, deprecated OAuth application with the full_access_as_app role to access a production Office 365 Exchange server containing data from a number of high-profile customers, including government agencies. Similar NHI related incidents have occurred across companies like Snowflake, Uber, and Okta.
Lifecycle Management and Governance Challenges	Managing the lifecycle of NHIs, from creation to decommissioning, is complex. Many NHIs are created without clear ownership or expiration policies, leading to "orphaned" identities that persist indefinitely and pose security risks. Because of complex infrastructures and no understanding of context and dependencies, NHIs will outlive their lifecycles so that critical business systems are not impacted which often sacrifices security controls.

Emergence of Autonomous AI Agents	The rise of AI-powered agents introduces new scale and complexities. These agents can operate autonomously, making decisions and taking actions without human intervention. Securing their identities and ensuring appropriate access controls are in place is a growing concern. Additionally, the rapid adoption of agentic AI is creating serious security blind spots as many organizations do not have proper visibility and/or organizational policies for ensuring security and compliance. SVCI established that an NHI security solution is now an essential tool for modern IT and engineering environments and a crucial part of every company's security program.



The Challenges Enterprises are Facing Today

	Cloud Centric Tech Companies:	Regulated Financial and Health Services
Characteristics	Organizations with extensive deployments on cloud services, leveraging data warehouses and AI	Organizations with hybrid compute environments that must satisfy regulatory mandates to ensure security and compliance
CISOs and Identity Leaders	Decision makers responsible for reducing risk, especially during AI agent adoption while enabling business	Decision makers who are facing increasing regulatory pressure and increased digital transformation initiatives to automate identity governance
Use Cases	Those seeking to enhance their ability to detect and respond to threats associated with NHIs	Those looking to mitigate heightened risk management needs, close access and offboarding gaps and maintain audit readiness

Silicon Valley CISO Investments (SVCI) is a highly curated, operator-led syndicate composed of security executives from some of the world's most forward-leaning technology companies. Each quarter, the group executes a structured investment evaluation cycle, beginning with broad market scans and culminating in deeply collaborative investment decisions. The process is intentionally rigorous - designed to reflect both the technical scrutiny and strategic foresight expected of world-class CISOs.

Key challenges highlighted by SVCI's CISO community include:

Theme-Based Exploration: The Case of NHI Security

While most SVCI cycles are opportunistic, driven by standout companies, the review of the NHI (Non-Human Identity) security space represented a rare shift toward a thematic diligence approach. Members recognized that this domain was rapidly gaining relevance, particularly as enterprise architectures evolve toward machine-centric models. Generative AI, M2M automation, ephemeral services, and decentralized cloud workloads all rely on NHI frameworks that are increasingly targeted and progressively more brittle.

Given this confluence of macro shifts, SVCI declared "NHI Security" a priority theme for the quarter.

Landscape Mapping and Initial Filtering

Over a 4—6 week period, the team evaluated more than a dozen early-stage companies with solutions focused on securing machine identities, API/service accounts, workload identities, agentic runtimes, and robotic process automation (RPA) access patterns.

This stage involved:

- Asynchronous founder questionnaires, co-developed by members with operational expertise
- Comparative feature and architecture reviews
- Technical teardown of open-source repos (where applicable)
- Initial 1:1 founder calls to probe depth of thinking, product vision, and strategic flexibility

From this pool, three companies emerged as front-runners - Token Security, focused on machine-first identity security, along with two others whose respective strengths lay in workload policy enforcement and cloud-native service mesh integration.

Deep Diligence and Collaborative Review

Each finalist entered a structured diligence phase. This phase involved:

- **Team Interviews:** Multi-member panels met with founders, CTOs, and GTM leaders to assess founder chemistry, credibility, and execution orientation
- **Product Validation:** Members conducted guided product demos with specific use-case walkthroughs (e.g. workload identity injection across multiple cloud runtimes; delegated privilege in zero-trust NHI topologies)
- **Customer References**: SVCI conducted blind and founder-facilitated calls with early design partners, paying customers, and pilot participants to validate problem fit, user experience, and post-sales support posture
- **Market Traction and Roadmap Alignment:** The companies' sales pipelines, pricing models, and roadmap prioritization were reviewed against enterprise adoption patterns and procurement dynamics observed firsthand by SVCI members in their operating roles

SVCI also conducted competitive SWOT analysis, peer benchmarking against legacy players and newer entrants, and assessed where each startup's approach either differentiated or overlapped with incumbents and emerging adjacent plays.

Following the diligence phase, a dedicated write-up team compiled a detailed internal Investment Diligence Memo.

This memo included:

- A structured decision matrix (problem criticality, TAM/SAM, timing, most potential, founder strength, execution risk, etc.)
- Customer testimonial transcripts
- Pricing strategy assessments
- Security and compliance review of the platform architecture

Ultimately, the group voted to invest in and partner with Token Security, based on its strong founder-market fit, clarity of vision in a chaotic identity landscape, early customer traction, and the extensibility of its platform into multiple layers of machine and workload identity control.

Token Security's solution aligned tightly with SVCI members' lived pain points—bridging the gap between ephemeral identity lifecycles and enterprise policy enforcement in AI/ML and containerized environments.

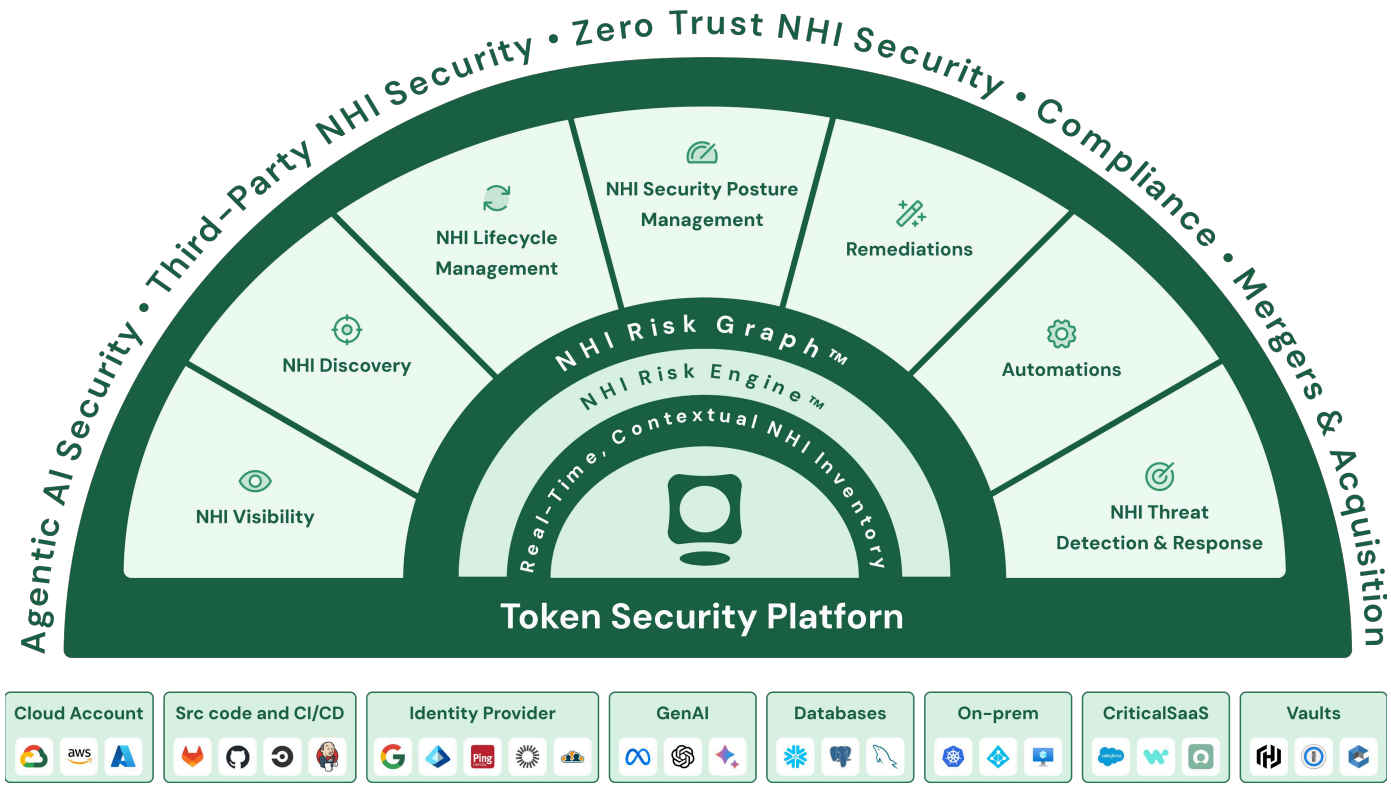
This investment decision was not just about potential return—it was also about conviction. SVCI invests only when a material number of members are not just believers, but potential future customers and evangelists. In Token's case, that bar was met and exceeded.

SVCI's diligence process is not outsourced. It's not delegated. It's member-led, operationally grounded, and community-driven. Over a dozen security leaders, from Fortune 500 CISOs to high-growth SaaS operators, contributed directly to this investment evaluation. The result is not just a capital investment, but a high-conviction partnership that brings product feedback, reference customers, and deep GTM insight.

Token Security, and others like it, don't just get funding, they get a tactical advisory bench composed of some of the sharpest minds in enterprise security.

Token Security addresses the core challenges CISOs face today, enabling them to:

- Gain a complete and contextual inventory of NHIs to understand and reduce risk
- Achieve centralized control over the entire NHI lifecycle for efficient management and governance
- Generate compliance data and reports to meet security regulations and standards.



Token Security provides a NHI Security platform, from on-prem and cloud to agentic AI. Token Security's NHI platform helps teams to reduce risk while accelerating AI adoption by discovering, understanding context, governing entitlements, and securing NHIs plus detecting and responding to emerging and active threats. With an AI-native, machine-first platform that secures NHIs across your entire organization, Token Security delivers the deepest, most actionable insights while enabling business innovation and growth, while ensuring security and compliance.

Discover and Understand

You can't secure what you can't see. NHIs are often created outside of centralized IT processes, hidden within infrastructure-as-code (IaC), CI/CD pipelines, or cloud consoles. The Token Security solution continuously discovers and takes inventory of all machine and non-human identities, including shadow accounts, privileged credentials, and federated/unfederated identities. The resulting identity graph that is created and maintained by the Token Security platform adds valuable context, such as the human owner of each identity traced back to the source code, so that informed decisions can be made.

Govern and Secure

The Token Security team understands that NHIs are not managed like human users. Rather, they are spun up by code and can persist indefinitely if left unmanaged. That is why robust lifecycle management, including ownership assignment, least privilege enforcement and automated deprovisioning are a core part of the platform.

Detect and Respond

Token Security delivers machine-native threat detection and automated response tailored for NHIs because traditional, human-centric security tools fall short. The Token Security platform uses behavioral analytics tuned specifically for NHIs to identify privilege escalation, misuse of secrets, anomalous access patterns, and suspicious IP activity in real time. Token Security integrates with SIEM, SOAR, XDR, and IaC pipelines to ensure rapid response without disrupting operations. The Token Security platform focuses on automating critical workflows like routing alerts to asset owners, correlating threats with IaC artifacts and generating AI-powered remediation steps.

Differentiation

In a crowded market of legacy IAM tools, Token Security's machine-centric, AI-native approach to NHI Security sets it apart. By treating NHIs as first-class citizens—discovering, governing, and securing them with context-aware intelligence—Token Security enables organizations to innovate fearlessly and securely accelerate cloud and AI adoption.

SVCI anticipates Token Security will define the NHI security category and drive industry best practices for the next decade because it:

- Provides deep, actionable insights by analyzing NHIs and their complete context by analyzing data from across the entire IT ecosystem
- Takes a decentralized approach to discovering and securing NHIs
- Discovers and secures AI agents while providing a natural language interface
- Will never impact operations
- Rapidly ideates and deploys new features to their platform, driving swift innovation and real-world impact for their customer

As enterprises embrace AI and cloud at scale, Non-Human Identities (NHIs), like service accounts, APIs, and AI agents, are exploding in number, creating serious security and compliance gaps. Traditional IAM tools can't keep up. That's why SVCI invested in Token Security: an AI-native platform purpose-built to discover, govern, and secure NHIs across the enterprise.

Token stood out in SVCI's rigorous, founder-led diligence process for its deep visibility, automated controls, and real-time threat response. It helps security teams tackle shadow identities, privilege sprawl, and orphaned accounts—making it essential for modern, cloud-driven orgs navigating the NHI security challenge.