TOKEN SECURITY

Messaging and Positioning

Token Security Messaging Framework

Final Copy

Level 1 Messaging

Context-Driven NHI Security

Go from invisibility to visibility. Protect your most valuable assets with machine-first identity security.

Take back control of your cloud systems from invaders you can't even see. Trust in Token.

Approach / Tagline / USP

Level 2 Messaging

The Problem We Solve

Visibility Gap

NHIs operate without proper monitoring or governance

Management Mismatch

Human-centric IAM tools can't handle machine-speed operations

Attack Surface Expansion

NHIs embedded everywhere represent ideal entry points

Legacy Security Debt

Unrotated secrets, orphaned credentials persisting for years

Modern Attack Vectors

Attackers targeting cloud service roles, exposed tokens

Additional Challenges: AI Complexity creating autonomous authentication needs • Architectural Misalignment between machine-native attacks vs. human-first defenses

Level 3
Messaging

Context-Driven NHI Security Solution Set — Token is the only provider that secures access from the threat of scalable NHI attacks.

Offering

Complete NHI Lifecycle Mapping

Token maps who created a non-human identity, who owns it, how it's used, what permissions it has, and how it behaves over time.

Infrastructure-as-Code Linkage

We link NHIs to their Infrastructure-as-Code origins, providing full traceability from creation to deployment.

Cross-Platform Usage Tracing

We trace NHI usage across cloud, SaaS, CI/CD, and AI workflows, giving you visibility everywhere.

Drift, Risk & Anomaly Detection

We detect drift, risk, and anomalies in real-time, identifying when NHIs deviate from intended behavior.

Level 4 Messaging

Benefits

Cover all identities. All the time.

Token Security is deeply connected to all levels of your cloud environment so it never misses a thing – and neither do you.

Focus on what's critical.

Risk prioritization makes sure you stay focused on remediating the exposures that actually affect your organization.

Act fast when action's needed.

With Token embedded into your workflows, proactively securing all types of identities is easier than it sounds.

Robust support for the enterprise. Token is designed to support the scale of operations and strict security standards of the world's most competitive enterprises.

Level 5 Messaging

Reasons to Believe - how it's possible

Discover

Reveal all identities in your cloud environment.

From cloud-native identities to Kubernetes, databases, applications, workloads, and servers. Token deeply analyzes all levels using agentless scanning and log analysis.

Context

Uncover who owns and who uses each identity.

Token collects attribution data about human owners, machine dependencies, and usage patterns including entitlements and pathways.

Exposure

Prioritize risks with richly detailed information.

Token shows your attack surface with rich details – including where identities are exposed, over-privileged, or misconfigured.

Remediation

Secure your accounts without breaking anything.

Token supports remediation by directing the right people with contextualized information, playbooks, and impact analysis.

Level 6 Messaging

Key Features

Discovery Engine

- Agentless Multi-Cloud Scanning
- Log Analysis Integration
- Kubernetes Identity Mapping
- Database & Application Identity Detection

Contextual Attribution System

- Infrastructure-as-Code Tracing
- Ownership Graph
- Usage Pattern Analysis
- Entitlement Mapping

Risk Intelligence Platform

- Dynamic Risk Scoring
- Privilege Drift Detection
- Anomaly Detection Engine
- Attack Path Visualization

Remediation Orchestration

- Workflow Integration
- Contextualized Playbooks
- Safe Remediation Engine
- Automated Policy Enforcement

Token Security

Overview

Token Security provides the only machine-first identity security platform that protects enterprises from the explosion of non-human identities (NHIs).

Customer pain points

Why organizations need Token Security:

- **Visibility Crisis:** 87% of organizations can't see all their machine identities
- **Security Breaches:** 61% of breaches involve

Key differentiators

	Token	Oasis	Astrix
Approach	Machine-first	NHI-Focused	AI-Enhanced
Discovery	★★★★★	★★★★	★★★★
Context	★★★★★	★★★	★★★★
AI Readiness	★★★★★	★★	★★★
IaC Integration	★★★★★	★★★	★★★★★

Why we win

- **45:1 Machine-to-Human Identity Ratio:** We're the only platform designed specifically for the machine-first era where NHIs vastly outnumber humans.
- **Complete Visibility:** Our agentless scanning reveals ALL identities across cloud, Kubernetes, databases, applications, and AI workflows.
- **Infrastructure-as-Code Traceability:** Unique ability to link NHIs back to their IaC origins for complete lifecycle management.
- **AI-Native Security:** Purpose-built to secure AI agents and autonomous systems that competitors can't handle.

Handling objections

- **Objection:** *"We already have Okta/CyberArk for identity management"*
- **Response:** "Those are human-centric tools. Your machine identities outnumber humans 45:1 - they simply can't scale to handle machine-speed operations and AI-generated identities."

<table>
<tr>
<td>compromised machine identities
- **Compliance Gaps:** Inability to audit and govern non-human access
- **Operational Chaos:** Orphaned credentials, unrotated secrets, over-privileged access
- **AI Complexity:** New AI agents creating identities faster than humans can track
- **Legacy Tool Limitations:** Human-centric IAM tools break at machine scale</td>
<td></td>
<td>- **Objection:** *"Our cloud provider handles machine identities"*
- **Response:** "Cloud providers only see their own environment. We provide cross-platform visibility across AWS, Azure, GCP, Kubernetes, SaaS, and CI/CD - giving you the complete picture."
- **Objection:** *"This seems like a nice-to-have, not critical"*
- **Response:** "Machine identity breaches cost $4.45M on average. Companies like Microsoft, Toyota, and GitHub have all been breached through machine identities. It's not if, but when."</td>
</tr>
<tr>
<td>**Key features**</td>
<td>**Questions to ask**</td>
<td>**Pricing**</td>
</tr>
<tr>
<td>- **Complete NHI Lifecycle Mapping:** Maps who created identities, ownership, permissions, and behavior patterns across all environments
- **Infrastructure-as-Code Linkage:** Traces NHIs</td>
<td>- **Discovery:** *"How many machine identities do you think you have across all your cloud environments?"* (Answer is usually 10-50x more than they think)
- **Pain Point:** *"When was the last time you audited all your service account permissions and secrets?"* (Most can't answer or it was months/years ago)
- **Urgency:** *"How quickly could you detect if a compromised API key was being used to access your most sensitive data?"* (Usually can't detect it at all)</td>
<td>
<table>
<tr><th></th><th>Monthly</th><th>Annually</th></tr>
<tr><td>Token</td><td>$3-5</td><td>$30-50</td></tr>
<tr><td>Oasis</td><td>$4-6</td><td>$40-60</td></tr>
<tr><td>Astrix</td><td>$5-8</td><td>$50-80</td></tr>
</table>
Per identity pricing. Competitive + superior capabilities.</td>
</tr>
</table>

back to their IaC origins for complete lifecycle visibility and governance ● **Cross-Platform Usage Tracing:** Monitors NHI usage across cloud, SaaS, CI/CD, and AI workflows for complete visibility ● **Real-Time Risk Detection:** Detects drift, anomalies, and policy violations when NHIs deviate from intended behavior ● **Contextualized Remediation:** Provides safe remediation with impact analysis and workflow integration ● **AI Agent Security:** Purpose-built to secure AI agents and autonomous systems	● **AI Readiness:** "How do you plan to secure the identities created by your AI agents and autonomous systems?" (Most haven't considered this)	
Quick tips	**Third-party validation**	**Relevant customers**
Discovery Call: Start by asking about their cloud environments	● **Funding:** $27M total funding from top-tier investors	**FinTech (heavy API usage)** **SaaS providers (multi-tenant)**

and recent security incidents. Most have machine identity blind spots. **Demo Focus:** Show the IaC linkage and AI agent discovery - these are unique differentiators competitors can't match. **Urgency Creation:** Reference recent breaches (Microsoft, Toyota, GitHub) that involved machine identities. **Technical Validation:** Offer a quick scan to show them identities they didn't know they had.	including TLV Partners and Shlomo Kramer ● **Team Credentials:** Founded by Unit 8200 veterans with 15+ years of cybersecurity experience ● **Market Recognition:** Featured in TechCrunch, SecurityWeek, and industry reports as a leader in machine identity security ● **Customer Results:** "Reduced machine identity attack surface by 80% in 30 days" - Fortune 500 FinTech customer ● **Industry Validation:** Gartner identifies machine identity management as a top security priority for 2024-2025	**E-commerce (high scale)** **Healthcare (compliance)** **AI/ML companies (agents)** **Size:** 500+ employees, $50M+ revenue

Additional resources
● ***ROI Calculator:*** *Machine Identity Risk Assessment Tool* ● ***Competitive Comparison:*** *Token Security vs. Oasis vs. Astrix detailed analysis* ● ***Case Studies:*** *FinTech, SaaS, and E-commerce success stories* ● ***Technical Deep Dive:*** *Architecture and integration documentation* ● ***Security Assessment:*** *Free 30-day trial with identity discovery report*