

To err is non-human too

# Securing the Unseen: Non-human Identity protection for a machine-first world

Non-human identities (NHIs)-service accounts, API keys, tokens-now outnumber humans by as much as 80:1. They're the silent operators powering your cloud, pipelines, and automation. But with hardcoded secrets, excessive permissions, and zero lifecycle control, they've become prime targets for breaches.

<p><b>80:1</b></p> <p><b>Machine to Human Ratio</b></p> <p>Traditional IAM cannot scale to meet machine-driven volume.</p>	<p><b>27M+</b></p> <p><b>Secrets Leaked Annually</b></p> <p>Scattered across GitHub, CI/CD pipelines, and stale branches.</p>	<p><b>46%</b></p> <p><b>Hit by NHI Incidents</b></p> <p>Visibility, risk reduction, and governance are mission-critical.</p>
--	---	--

## The problem

RISK VECTOR	DESCRIPTION
<b>Machine Mayhem</b>	For every human identity, there are at least 80 non-human identities. Traditional IAM just can't keep up.
<b>No lifecycle management</b>	NHIs lack human-like governance. They experience little or no rotation, revocation, or review, let alone proper onboarding and off boarding.
<b>The eyes have it</b>	You can't secure what you can't see. Most organizations lack a true NHI inventory.
<b>Overprivileged access</b>	NHIs are often granted more access than they need. It's a blast radius waiting to happen.
<b>Zombie NHIs</b>	NHIs are often created fast and forgotten faster. Many are long-lived identities with no ownership or purpose, yet still are active.
<b>Secret spillage</b>	With unsecured and unmanaged NHIs, your enterprise secrets are sitting ducks for breaches.
<b>Agentic AI security</b>	Without dedicated safeguards, intelligent autonomous AI agents can gain unauthorized access and act independently. Traditional IAM can handle identities, not intent.

## Why StackGuard

### Remediation First Solution

Resolve vulnerabilities using Agentic AI and execution ready scripts. Seamless integration with Native CI/CD tools.

### Deep Contextual Visibility

Maps scope, ownership, permissions and expiry. Extracts secrets even from stale & deprecated branches.

### Local Deployment

Zero sensitive information leaves your infrastructure. Architected for strict compliance environments.

## How StackGuard can help

### 01 Continuous discovery

**Extensive scanning** of NHIs across cloud, AD, CI/CD, SaaS, Storage & Chat Apps

**Real-time visibility** and mapping of secret sprawls, trust relationships, and ownership structures.

**Automatic scanning** of Pull Requests (PRs), commit histories and legacy code.

**Real-time flagging** of dormant, over-permissive and misconfigured Service Accounts.

### 02 Precision risk remediation

**Blast radius analysis** exposes potential access helping in implementing right-sized access.

**Context-aware remediation** using usage patterns in cloud infrastructure.

**AI/ML-powered virtual patching** with one-click remediation to securely store and rotate the NHIs in a Vault.

**Scenario-based remediation** using custom scripts for service accounts.

### 03 Audit-ready governance

**Auto-blocking of PRs** containing hardcoded secrets, Anonymize chats with NHIs.

**Attack path analysis** for comprehensive risk analysis and AppSec triaging.

**Proactive scanning** at regular intervals for continuous, verifiable compliance.

**Audit-ready reports** that decode NHI behavior for security and compliance teams.

## Use cases: where StackGuard can help



#### Comprehensive Discovery

Monitor and govern secrets across infrastructure (Code Repos, Cloud Infra, Directory Services, Chat Apps & SaaS Apps).



#### Eliminate Privilege Escalation

Secure Directory Services against Shadow Admins, Stale Accounts, Password Never Expires, Disabled & Privileged Service Accounts.



#### Frictionless AI Remediation

Agentic AI automatically generates validated PRs, thereby ensuring developers release velocity is minimally impacted.



#### Compliant Cloud Infrastructure

Remediate Misconfigured IAM roles using execution-ready scripts and ensure adherence to PCIDSS, SOC 2, ISO 27001, and other standards.



#### NHI Governance

Secure PRs by auto blocking, Anonymize NHIs in real time and provide Just in Time (JIT) access for Chat Apps.



#### NHI Lifecycle Automation

Establish unified ownership-tracked inventory, enforce rotation via vault integrations, and maintain immutable versioned audit histories.



#### Crest Infosolutions

 [info@crestsolution.com](mailto:info@crestsolution.com)

 [www.crestsolution.com](http://www.crestsolution.com)

**REQUEST SECURITY  
ASSESSMENT**

