

NON-HUMAN IDENTITY & MACHINE-TO-MACHINE AUTH.



Every API key, service account, and workload identity is a credential nobody logs into — **non-human identity governance treats machine credentials with the same rigor as human ones, because attackers already do.**

- SERVICE ACCOUNT SPRAWL
- API KEY LIFECYCLE
- WORKLOAD IDENTITY
- SECRET ROTATION

01 THE MECHANISM

Service Account & API Key Sprawl

Every integration, pipeline, and automated process gets its own credential, and **those credentials accumulate far faster than human accounts do**, often with no clear owner.

Workload Identity

Modern platforms issue narrowly-scoped, automatically-expiring identities to workloads instead of long-lived static keys, **shrinking the window a stolen credential is useful.**

Secret Rotation & Vaulting

Centralized secret management stores, rotates, and audits access to credentials **instead of leaving them hardcoded** in config files or source code.

02 THE FLOW

The Scoped Workload Identity SCOPED

1

A workload requests a short-lived credential from the identity platform at runtime instead of storing a static key.

2

The credential is scoped to exactly the permissions that workload needs and expires automatically within minutes to hours.

3

If the credential is ever exposed, **the exposure window and blast radius are both minimal by design.**

The Static Service Account EXPOSED

1

A long-lived API key is generated once and hardcoded into a config file, script, or repository.

2

The key is never rotated because no one owns it, and it carries broad, un-scoped permissions granted at creation.

3

Once the key leaks, **it remains valid and exploitable indefinitely**, with access far beyond what any single task requires.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Non-Human Identity Inventory	Discovers and catalogs every service account, API key, and workload identity across environments, not just the ones formally provisioned.
Least-Privilege Scoping	Grants each machine credential only the specific permissions its function requires, independent of convenience.
Automated Rotation & Expiration	Replaces static, long-lived secrets with short-lived or automatically rotated credentials wherever the platform supports it.
Ownership & Lifecycle Accountability	Assigns a responsible owner to every non-human identity and deprovisions it when the workload it served is retired.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Human IAM Policies Applied to Service Accounts	No	Assumes a login pattern and review cadence that machine credentials never follow, missing how they're actually used.
Static API Keys Without Rotation	No	Remains valid indefinitely once issued, regardless of whether the workload or its need still exists.
Secrets Stored in Code or Config Files	No	Exposes credentials to anyone with repository or filesystem access, including in version history.
Manual Credential Audits	No	Can't keep pace with how quickly automated pipelines and integrations create new machine identities.
Centralized Vaulting + Short-Lived Credentials + Ownership Tracking	Yes	Scopes, rotates, and attributes every machine credential automatically, at the speed they're created.

NON-HUMAN IDENTITY MANAGEMENT.

ISSUE · SCOPE · ROTATE

05 PROGRAM OPERATIONS

Non-human identities already outnumber human ones in most environments.

Every service, pipeline, and integration adds accounts that traditional IAM programs were never built to track.

A credential with no owner is a credential no one is rotating.

Ownership gaps are the single biggest predictor of a stale, over-privileged service account.

Short-lived credentials aren't just more secure, they're self-cleaning.

An expired credential can't be the thing an attacker finds six months after a breach.

Non-human identity governance depends on platform support, not policy alone.

You can't rotate what your infrastructure doesn't support rotating.

06 CONTROL MAPPING

NIST SP 800-207 (ZERO TRUST)

Extends zero trust principles to non-human and workload identities, not just human users.

CSA NHI SECURITY GUIDANCE

Cloud Security Alliance guidance specifically addressing service account and machine credential risk.

OWASP SECRETS CHEAT SHEET

Practical guidance for storing, rotating, and vaulting application secrets and credentials.

SOC 2 (COMMON CRITERIA)

Requires logical access controls and credential management practices that extend to system and service accounts.

07 WHAT THIS DOES NOT SOLVE

Vulnerabilities in the Workload Itself

Scoped, rotated credentials don't fix a vulnerable application that a valid credential can still be used to exploit.

Legitimate-Looking Automated Abuse

A compromised but properly-scoped credential can still be misused for anything within its legitimate permission set.

Third-Party & SaaS-to-SaaS Credentials

Machine credentials issued to and managed by external vendors often sit outside an organization's own vaulting controls.

Human Error in Initial Scoping

A workload identity granted overly broad permissions at creation stays overly broad no matter how well it's rotated afterward.

08 MYTHS VS. REALITY

MYTH "Service accounts are lower risk because no human is using them."	REALITY Machine credentials are frequently more valuable to attackers, since they're monitored less and often carry broader, standing access.
MYTH "Rotating keys occasionally is basically the same as short-lived credentials."	REALITY A key rotated quarterly still leaves a months-long exploitation window; short-lived credentials measure that window in minutes or hours.
MYTH "If it's in a private repository, a hardcoded secret is safe."	REALITY Private repos are still exposed to every contributor and CI/CD system, plus the secret persists in git history.
MYTH "Non-human identity is a cloud-only problem."	REALITY On-premises service accounts, scheduled tasks, and legacy integrations carry the same risk and are often even less monitored.
MYTH "One inventory sweep is enough to get this under control."	REALITY Automated pipelines create new machine identities continuously; without ongoing discovery, the inventory is stale within weeks.

09 SPEAK THE PROGRAM — KEY TERMS

NON-HUMAN IDENTITY (NHI)

Any credential or identity used by software, a service, or a device rather than a human user to authenticate.

WORKLOAD IDENTITY

An identity issued directly to an application at runtime, **typically short-lived and automatically scoped**.

SECRET SPRAWL

The uncontrolled proliferation of API keys, tokens, and credentials across code and pipelines **with no central tracking**.

CREDENTIAL VAULTING

Centrally storing and controlling access to secrets so they're **never hardcoded or exposed in plaintext**.

SERVICE ACCOUNT

A non-human account created for an application or automated process **to authenticate and perform actions**.

LEAST PRIVILEGE (MACHINE CONTEXT)

Granting a machine credential **only the specific permissions its function requires**, nothing broader.