Corsha

The Non-Human **Identity Landscape**

What are Non-Human Identities (NHIs)?

A Machine Identity is a spectrum of attributes that make up the definition of a digital system. These machine identities are used in securing systems, managing machine-to-machine access, and ensuring the integrity of digital environments.

NHIs come in the form of:

- API keys
- OAuth tokens
- JWTs
- Service accounts
- PKI certificates (X.509, SPIFFE, SPIRE)
- IP addresses
- MAC addresses
- Cloud provider app secrets
- Passwords

Where do NHIs show up?

- Cloud Workloads
- Microservices
- OT Equipment
- Third Party Apps and Integrations
- AI LLMs
- Sensors
- CI/CD Pipelines
- IOT devices
- Robotic Process Automation (RPA)
- Data Warehouses/Data Lakes

How many NHIs are out there?

Statistics on Machine Identity Growth and Risk

90% of traffic is generated by machines.[1]

45:1 Non-Human Identities outweigh human identities by a factor of 45 to 1 across enterprises.[2]

80% Attacks against APIs exploded by 400% of which 80% were authenticated.[3]

6.8B Enterprise Container Instances by 2028.[4]

57M IoT Devices by 2027.[5]

1B Applications by 2028.[6]

Where are the blindspots and challenges?

The rise of the Internet of Things (IoT), cloud computing, automation, connected devices, and microservices architecture has significantly increased the number of machine identities. This rapid increase highlights some key risks and challenges that must be specifically addressed to maintain identity security, prevent unauthorized access, and ensure the integrity of communications.

Challenges

Lack of Visibility
NHIs don't involve humans, so their requests and actions can easily go unnoticed and unmonitored.

Uncontrolled Access and Over Privileged
Elevated privileges of NHIs are less scrutinized. Once a secret is provisioned, machine access is often unregulated and not easy to turn off/on.

Little or no lifecycle management
NHI lifecycle stages, from initial deployment to active use to decommissioning, are often undefined or unmanaged. Secrets alone are a weak proxy for identity.

Secrets Sprawl
The scale and breadth of NHIs leads to an explosion of secrets, spread across hybrid clouds, third-party systems, and both East-West and North-South API traffic.

Best Practices to reclaim control of your Non-Human Identities

Continuous Discovery
You don't know what you can't see. Real-time discovery of NHIs and their actions is essential.

Least Privilege
Regular review of NHI privileges should occur to apply least privileges necessary for the machine's role.

Deny Risky Access
Detect and prevent access using risky identities, shared credentials, and other anomalous behavior through real-time IAM analytics.

Scheduled Access
NHI access that is only required during specific hours or days of the week should be turned off outside of those hours.

Lifecycle Management
Have policies around rotation and expiration and a way to automatically check that the policies are being enforced.

Discover how Corsha can help your team move beyond static secrets with dynamic machine identities. Learn about innovations like automated, single-use MFA credentials, scheduled access, and deep discovery for secure machine-to-machine communications.

www.corsha.com

Corsha

Corsha is a Identity Provider for Machines that allows enterprises to securely connect, move data, and automate with confidence from anywhere to anywhere. Corsha builds dynamic identities for trusted machines and brings innovation like automated, single-use MFA credentials to APIs. This ensures automated communication across clouds, data centers, or shop floors is pinned to only trusted machines and helps organizations move past outdated, costly secrets management and reimagine identity and access for machines.

1. Akamai 2019 State of the Internet. 2. Cyberark 2023 Identity Report. 3. Salt Security Q1 2023 State of API Security Report
4. IDC x86 Container Forecast, September 2024. 5. IDC IoT Installed Base Forecast, 2023-2027. 6. IDC's 1 Billion Logical Apps: More Background