



CYTEX™

CYBERSECURITY | COMPLIANCE | GRC



**AI-Powered
Anomaly Detection**



**Automated NHI
Discovery & Risk
Scoring**



**Compliance-Ready
Reporting &
Remediation**

Technical Brief

Cybersecurity Risks Posed by Non-Human Identities



hello@cytex.io

cytex.io





Addressing the Non-Human Identity Security Gap

As organizations increasingly adopt cloud-native architectures, DevOps practices, and automation, non-human identities (NHIs) have become a critical attack vector in cybersecurity. Unlike human users, NHIs—such as service accounts, API keys, bots, and IoT devices—often operate with elevated privileges and minimal oversight, making them prime targets for exploitation.

This technical brief explores the risks associated with NHIs and how Cytex, a SaaS-based unified security platform, helps organizations mitigate these threats through continuous monitoring, least-privilege enforcement, and automated remediation.

What Are Non-Human Identities?

Non-human identities (NHIs) are digital entities that interact with systems, applications, and data without direct human intervention. They include:

- Service Accounts (e.g., database access, backup services)
- API Keys & Tokens used for machine-to-machine communication
- Cloud Workload Identities (AWS IAM roles, Azure Managed Identities)
- DevOps & CI/CD Pipelines (automated deployment scripts, containers)
- IoT & Edge Devices (sensors, embedded systems)
- Bots & RPA Agents (automated workflows, chatbots)

NHIs often have persistent, high-level permissions and are rarely rotated or audited, creating significant security gaps.



Key Cybersecurity Risks Posed by NHIs

Credential Theft & Misuse »

- Hardcoded Secrets: API keys and credentials embedded in code or config files are easily exfiltrated.
- Lack of Rotation: Long-lived credentials increase exposure to brute-force and phishing attacks.
- Shadow IT NHIs: Unmanaged service accounts created without security oversight.

Excessive Privilege Escalation »

- Many NHIs are granted unnecessary permissions due to poor IAM policies.
- Attackers exploit overprivileged NHIs for lateral movement and data exfiltration.

Lack of Visibility & Monitoring »

- Traditional IAM tools focus on human identities, leaving NHIs unlogged and unaudited.
- Security teams struggle to detect anomalous NHI behavior (e.g., unusual API calls, unexpected data access).

Supply Chain Attacks via NHIs »

- Compromised CI/CD pipelines or third-party integrations can inject malware via NHIs.
- Attackers abuse DevOps toolchains (e.g., GitHub Actions, Jenkins) to deploy malicious code.

Insider Threats & Misconfigurations »

- Developers may accidentally expose NHIs in public repositories (e.g., GitHub leaks).
- Malicious insiders can abuse NHIs to bypass access controls.



UNIFIED RESILIENCE PLATFORM



Preventative Methods for Securing NHIs

Continuous Discovery & Inventory »



Cytex Solution: Automatically discovers and catalogs all NHIs across cloud, hybrid, and on-prem environments.

Benefit: Eliminates shadow IT NHIs and ensures complete visibility.

Least-Privilege Access Enforcement »



Cytex Solution: Dynamically adjusts permissions based on usage patterns, enforcing just-in-time (JIT) access.

Benefit: Reduces attack surface by removing unnecessary privileges.

Automated Credential Rotation & Secret Management »



Cytex Solution: Integrates with vaults (HashiCorp, AWS Secrets Manager) to enforce regular credential rotation.

Benefit: Reduces attack surface by removing unnecessary privileges.

Behavioral Anomaly Detection »



Cytex Solution: Uses AI-driven analytics to detect unusual NHI activity (e.g., abnormal API traffic, privilege escalation attempts).

Benefit: Enables real-time threat response.

Secure DevOps & CI/CD Pipeline Governance »



Cytex Solution: Scans IaC (Terraform, CloudFormation) for misconfigured NHIs and enforces security policies.

Benefit: Prevents supply chain attacks via compromised automation workflows.

Audit & Compliance Reporting »



Cytex Solution: Provides detailed audit logs and compliance reports for NHIs (SOC 2, ISO 27001, NIST 800-53, NIST 800-171, PCI, HIPAA, CMMC).

Benefit: Simplifies regulatory adherence and forensic investigations.



Why Cytex?

Cytex is a next-generation identity security platform designed specifically to address the growing risks of non-human identities. Unlike traditional IAM solutions, Cytex offers >>

- ✔ Automated NHI Discovery & Risk Scoring
- ✔ Dynamic Least-Privilege Access Controls
- ✔ AI-Powered Anomaly Detection
- ✔ Seamless Integration with Cloud & DevOps Tools
- ✔ Compliance-Ready Reporting & Remediation

Non-human identities represent one of the most overlooked yet dangerous attack surfaces in modern cybersecurity. Traditional IAM solutions fail to address NHI risks, leaving organizations vulnerable to credential theft, privilege escalation, and supply chain attacks. By securing NHIs, Cytex helps organizations prevent breaches, reduce insider threats, and maintain compliance—all without disrupting operational workflows.



Cytex provides a proactive, automated approach to NHI security, ensuring that every machine identity is monitored, controlled, and protected.



Cytex – Identity Security for the Machine Era
Discover. Secure. Automate.



<https://cytex.io>



msp@cytex.io



[@cytextsmb](https://twitter.com/cytextsmb)



[@cytexsecure](https://www.youtube.com/channel/UC...)