Scaling Security for Non-Human Identities: A Zero Trust Approach

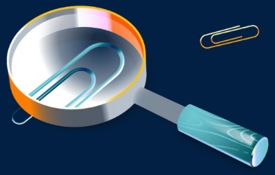
Sai Charan Goud Alligeri - Sr. Cybersecurity Engineer
Jacob Kilgore - Sr. Cybersecurity Engineer

Sep’18 2025

The Invisible Workforce

DEFINITION

Digital credentials that enable automated processes to access resources. Examples include Service Accounts, API Keys/Tokens, and Cloud Workload IDs.



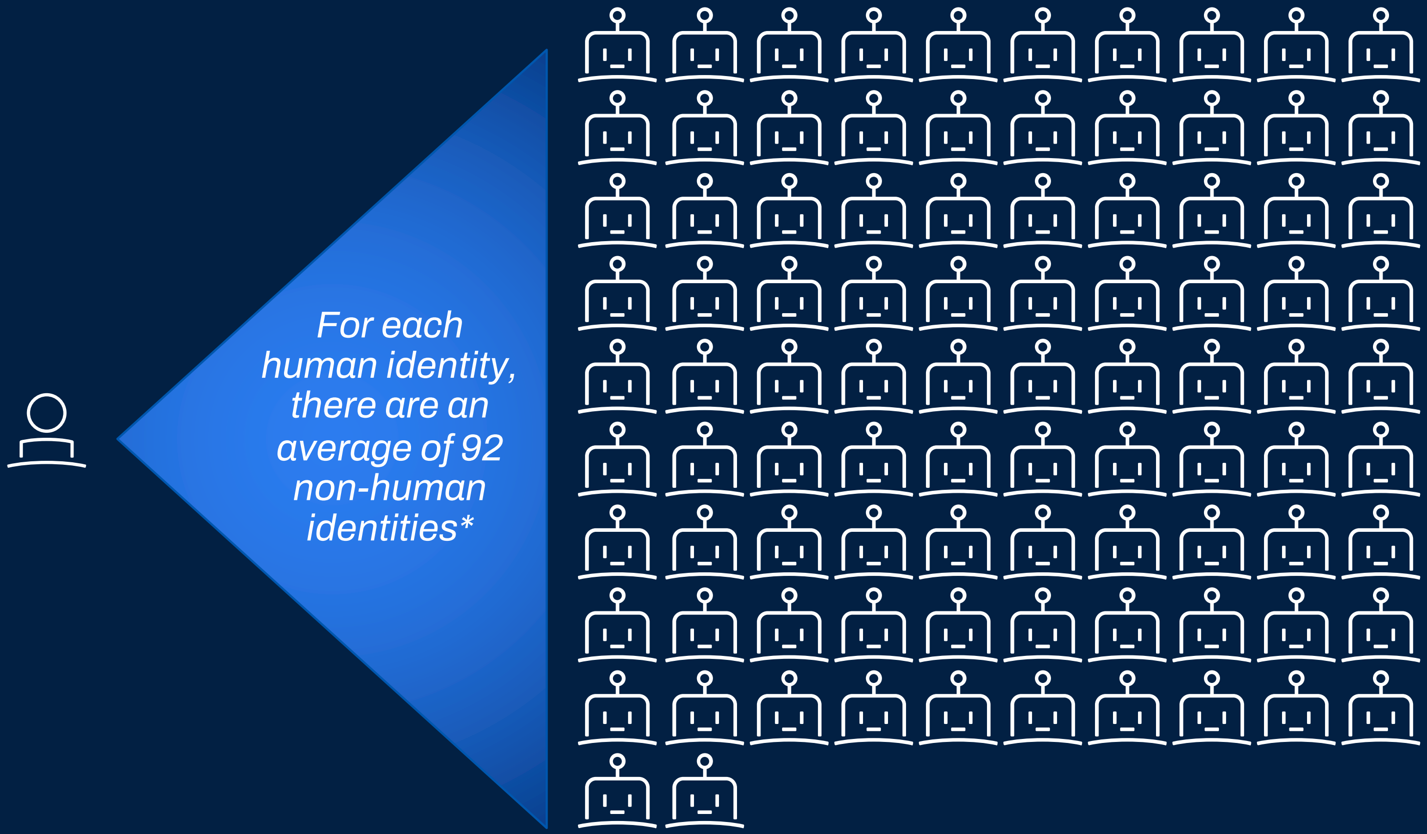
DISTINCTION

Unlike human identities (which use passwords and MFA), NHIs rely on keys, tokens, and certificates.

GROWTH

The rise of cloud, DevOps, CI/CD pipelines, and microservices has led to an explosion in NHIs.

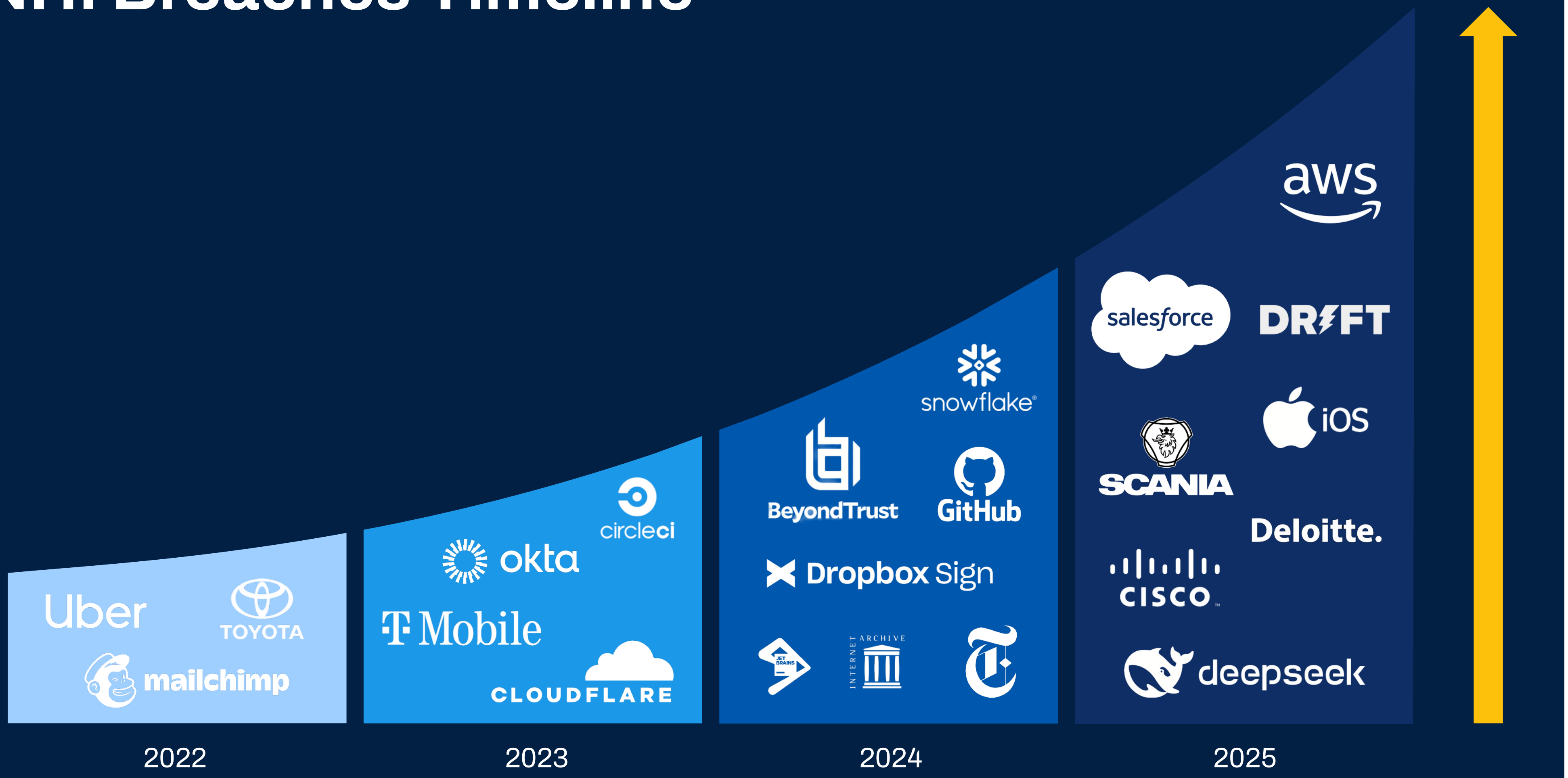
Proliferation of Non-Human Identities



*For each human identity, there are an average of 92 non-human identities**

*Entro Labs Research Report: Risks of Non–Human Identity, 2024

NHI Breaches Timeline

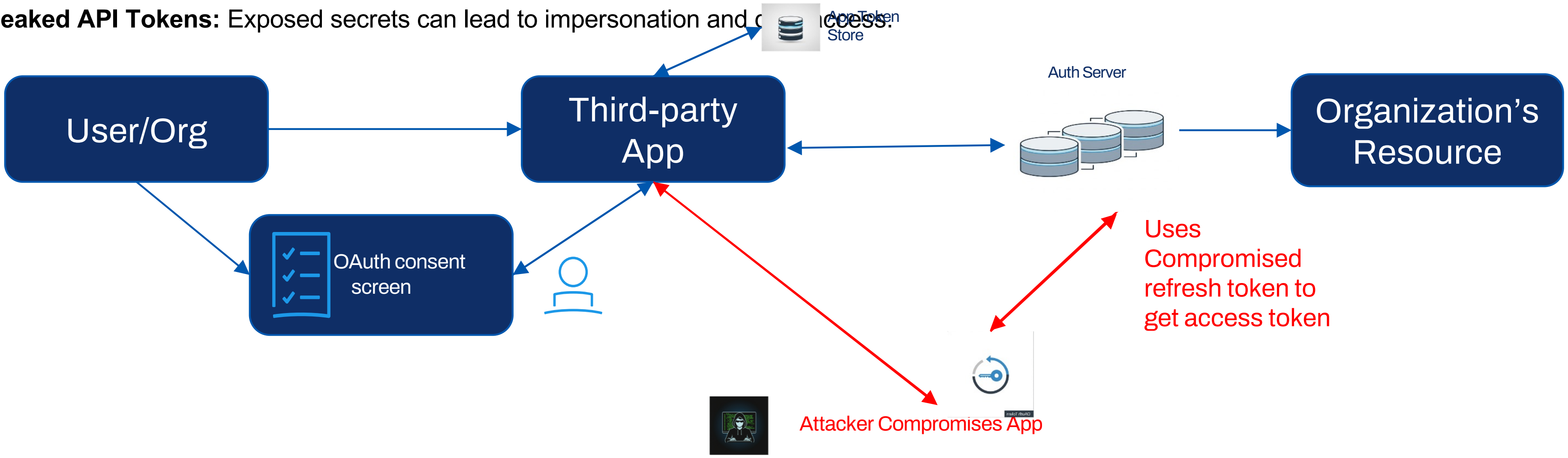


Why This Matters: The Supply Chain Attack

NHIs are a critical and an often-overlooked attack surface.

Common Attack Scenarios

- **Compromised OAuth Tokens:** A breached third-party app can lead to stolen tokens and access that appears legitimate.
- **Leaked API Tokens:** Exposed secrets can lead to impersonation and c[illegible] access.



It's Not a Vulnerability, It's an Identity Problem

The Salesloft Drift breach was a failure of non-human identity management.

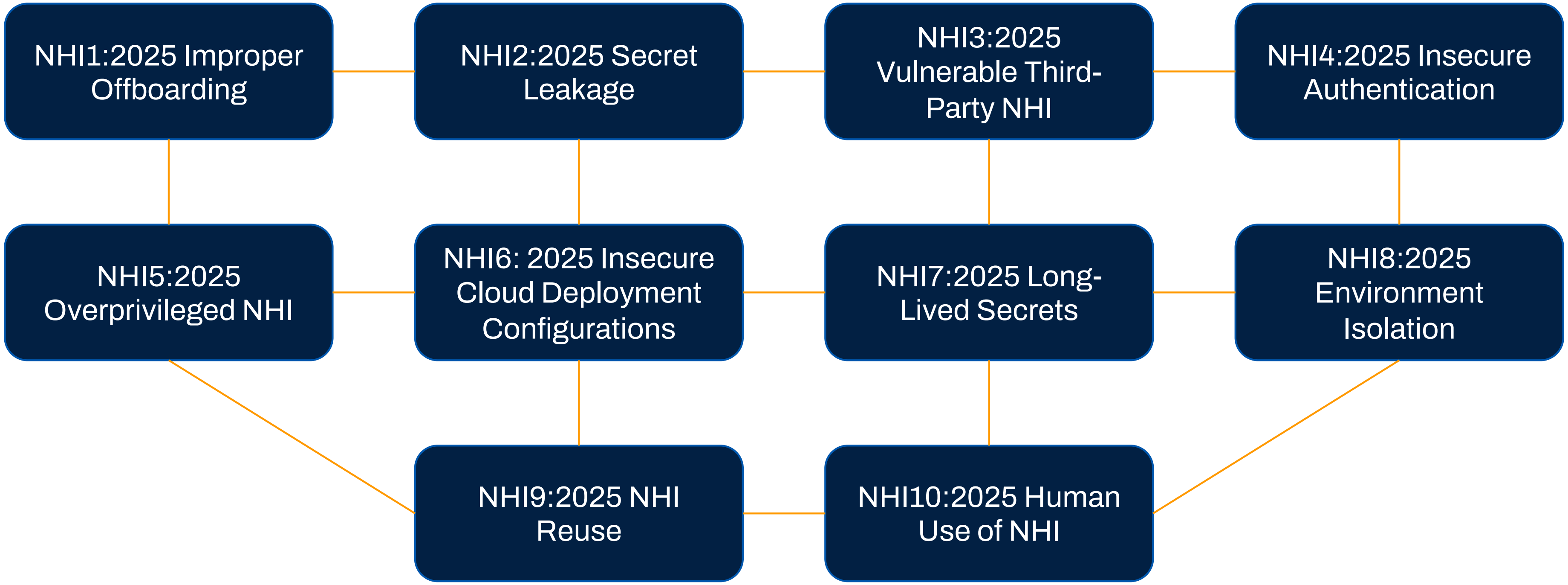
Core issues:

Lack of Visibility

Weak Security Configuration

Over-Permissive Access

Insufficient Monitoring



NHI1:2025 Improper Offboarding

NHI2:2025 Secret Leakage

NHI3:2025 Vulnerable Third-Party NHI

NHI4:2025 Insecure Authentication

NHI5:2025 Overprivileged NHI

NHI6: 2025 Insecure Cloud Deployment Configurations

NHI7:2025 Long-Lived Secrets

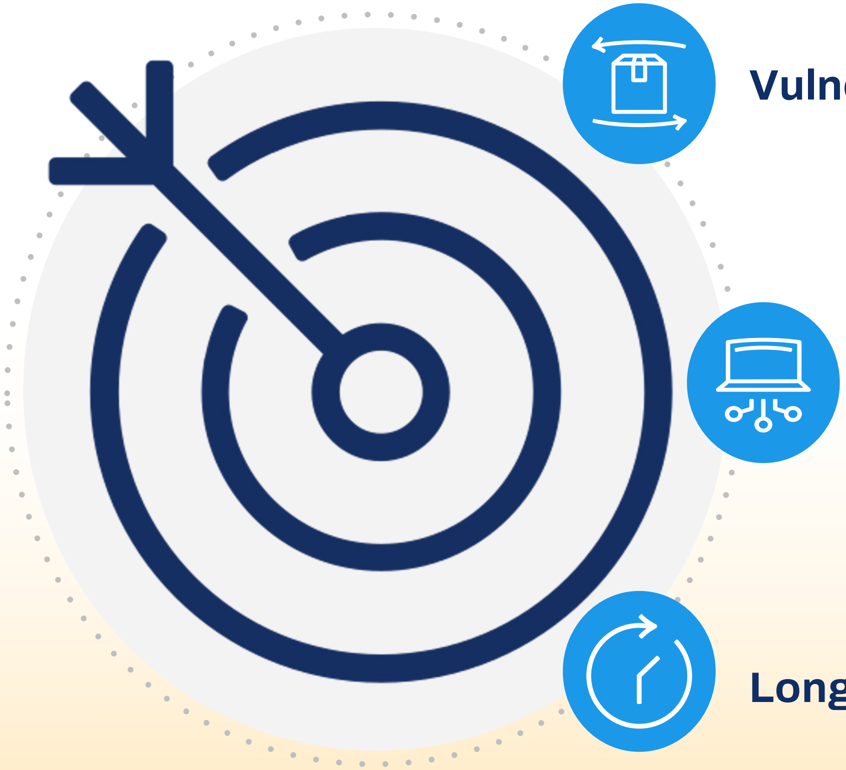
NHI8:2025 Environment Isolation

NHI9:2025 NHI Reuse

NHI10:2025 Human Use of NHI

OWASP NHI Top 10
The OWASP Non-Human Identity (NHI) Top 10 identifies and ranks the most critical risks associated with NHIs, providing a practical guide for developers and organizations.

Focus: OWASP NHI Top 10



Vulnerable Third-Party NHI (NHI3)

Compromised third-party extensions can steal credentials or misuse permissions.

Overprivileged NHI (NHI5)

A compromised, over-privileged NHI allows attackers to exploit its excessive permissions.

Long-Lived Secrets (NHI7)

A breached, long-lived secret gives attackers unlimited access to services.

Our Zero Trust Journey

Our strategy is built on three core pillars

Discovery & Classification

Real-Time Monitoring

Automated Governance

Discovery & Classification

Integrate

Identify and classify risks with integrated tools across our SaaS and IaaS environments.

Evaluate

Continuously re-evaluate and reclassify risk based on multiple factors, including permissions and usage patterns.

Empower

Grant owners full visibility to their platform, so they can directly identify and remediate security risks.

Real-Time Monitoring

Analyse

Incorporate behavioural analytics that go beyond static checks and are capable of identifying anomalies.

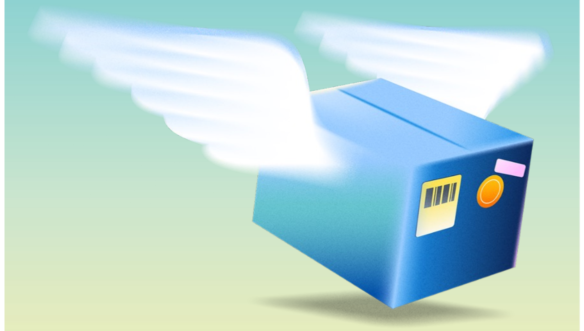
Notify

Immediate notification to the owner of high-risk identities to enable an instant visibility.

Escalate

Partner with other security teams and tooling to ensure rapid action and remediation of high-risk identities.

Automated Governance



Report

Highlight wins with proactive reports while pushing owners for continuous security improvement.

Review

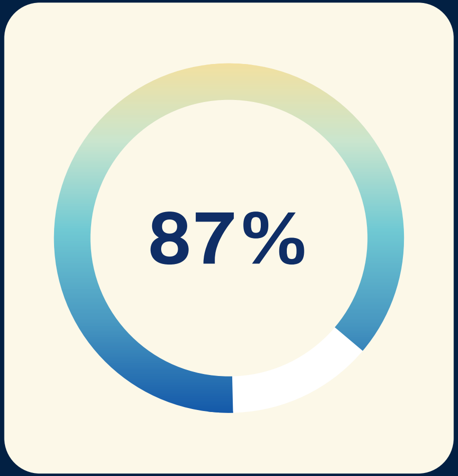
Conduct regular access reviews for identities in an automated way with a direct integration into Slack.

Assess

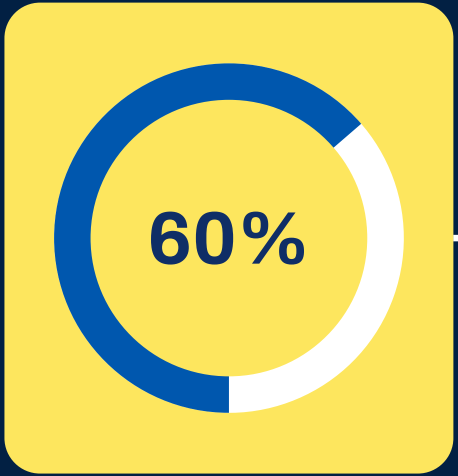
Automatically assess and categorize third-party risks using existing vendor assessments.

	Discovery & Classification	Real-Time Monitoring	Automated Governance
Vulnerable Third-Parties	Identifying what third-parties exist in the environment	Alerting based on public threat intelligence on compromised vendors	Automated third-party risk classification based on existing evaluations
Overprivileged Access	Classifying over privilege as high-risk	Alerting on anomaly detection	Automated NHI access reviews
Long-Lived Secrets	Classifying long-lived credentials as high-risk	Alerting on least usage patterns	Automated notification and proactive reporting as risks are identified

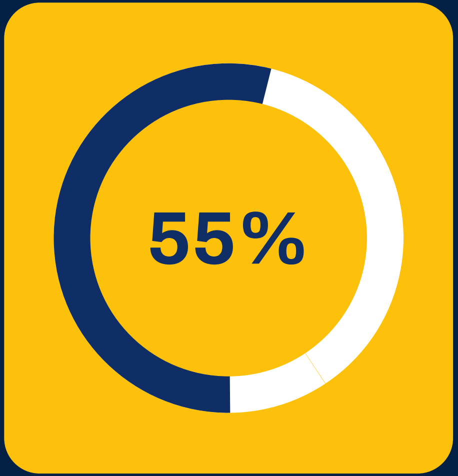
The Tangible Result



Reduction in High-Risk Identities



Existing Suppliers Offboarded



Classified Untrustworthy Suppliers

Our Shared Mission

- Identity Lifecycle Management
- Third-Party App Controls
- Architecture Safeguards
- Detection & Incident Response
- Empower Your Teams

Thank You

Q&A