

**ent**ro



**Non Human Identity &  
Secrets Security for  
Travel Industry**

## Millions

potential to exploit millions of credit cards from an NHI attack

## Top 2

Secrets attacks are one of the top three frequent attack

## \$50 - \$90

The fine per customer for PCI DSS compromise

## The Need

Non-human identities are out of control. It's a huge challenge when organizations have 45X more non-human identities than human identities. Online travel agencies, with their constant expansion of cloud-native stack, find themselves challenged even more with scattered non-human identities across solutions without any oversight. In addition, many companies work with the PCI DSS Practices for a more trustworthy and secure payment program, but PCI DSS is difficult to implement and maintain.

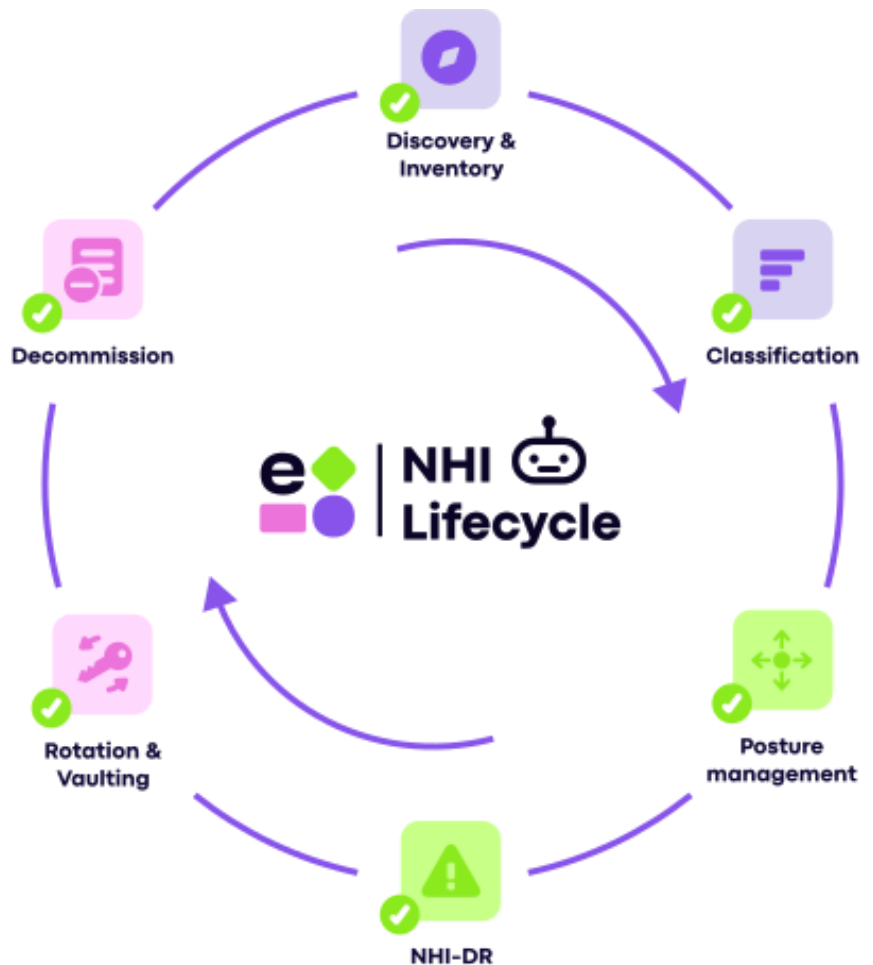
PCI Security Standards are technical and operational guidelines established by the PCI Security Standards Council (PCI SSC) to safeguard cardholder data. These standards are mandatory for all entities that store, process, or transmit cardholder data, including software developers and manufacturers of applications and devices used in these transactions. A data breach to a travel company would not only exploit the data of millions but cost even more in fines and reparations.

By reducing the overall risk of non-human identities and secrets exposure in the cloud, enterprises can maintain better compliance and management of PCI DSS standards, and stop potential threats before they happen.

\*"cost of a data breach report 2024", ibm security

# What is Entro?

Entro Security offers an agentless multi-cloud non-human identity lifecycle management and secrets security platform that discovers, classifies and protect your non-human identities from bad actors on all cloud services, including AWS, Azure, GCP, GitHub and more.



Leveraging full lifecycle management capabilities, Entro enables organizations to securely use non-human identities and secrets by creating non-human identity inventory, classification and enrichment, vaults misconfigurations, access anomalies, and preventing non-human identity vulnerabilities that increase the risk of a breach if not remediated.

Seamlessly integrating with your existing security solutions, Entro has full lifecycle management and control over all non-human identities and secrets.

# Features & Benefits

## Inventory

How many NHIs & secrets do you have?  
Where are all of your non-human identities & secrets?  
Remove exposure  
Vault all secrets

## Classification and enrichment

Visual lineage map  
Understand the secret owner  
Review NHIs Permissions  
See blast radius of each individual secret

## Manage NHI life cycles

Secure creation with policies  
Manage Rotation  
Vault them all  
Eliminate stale secrets & ensure NHIs are decommissioned

## Real-time behavioral alerts

Real time abnormal alerts for NHIs, secrets and vaults  
Monitor threat model changes and issues  
Remove misconfiguration and risks  
Seamlessly integrating with SOC solutions

## Save money and automate risk mitigation

Leverage automated flows to respond to breaches in real time

Cut communication cycle by alerting the owner directly using Slack, Teams, email, etc.

Save money by managing NHI lifecycle automatically

Cut vaults costs

# Non-human identity management & protection designed for security teams

[Start Now](#)

