SOLUTION BRIEF

Entro + Wiz

Unifying NHI Security and DSPM to Secure Cloud Assets

THE CHALLENGE

Modern enterprises are flooded with non-human identities: tokens, API keys, service accounts, and secrets.
Without proper governance, they become silent threats, especially when they can grant access to sensitive cloud data like PII, PHI, proprietary code and financial records.

As cloud adoption grows, so does the gap between identity security and data protection. Security teams often can't answer: **Which NHIs can access what data** and **what happens if it's exposed**?

Sensitive data is the **target**.

NHIs are the **entry point**.

THE SOLUTION

Entro and Wiz join forces to bridge the gap between data and identity security. The integration correlates Wiz's Data Security Posture Management (DSPM) insights with Entro's non-human identity (NHI) intelligence and risks, so security teams can instantly understand which machine identities and secrets can access sensitive data, where it lives and whether those identities pose a threat.

WIZ tells you what data is sensitive & where it is.

entro shows you who can access it & what to do next.

CAPABILITIES & KEY BENEFITS

1 Correlate NHIs & Secrets with DSPM

Enrich every identity and secret with Wiz's data classification to understand what sensitive assets are truly at risk.

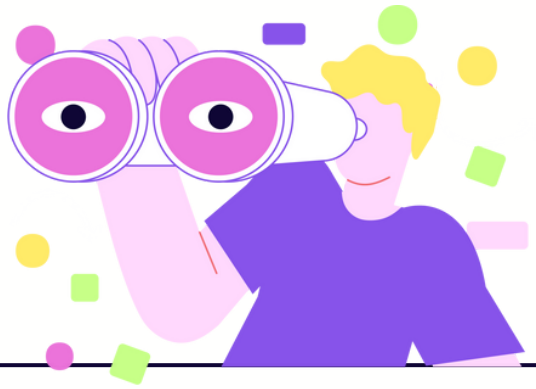
2 Visualize Identity-to-Data Attack Paths

Map how NHIs interact with sensitive data and cloud services - so you can detect, disrupt, and respond before threats spread.

3 Prioritize Remediation with Full Context

Focus response on the most critical issues by combining identity risk signals with data sensitivity labels.

NHI RISK REMEDIATION WITH DSPM CONTEXT



Entro is Now Officially Part of Wiz Integration Network (WIN)

Entro brings deep expertise in securing non-human identities and secrets, an area that complements our focus on data security in the cloud, by combining Entro's identity intelligence with Wiz's DSPM, we're giving customers a new level of context to uncover and remediate complex, data-centric risks

Oron Noah, VP of Product & Partnerships at Wiz

Enriching NHI Context with Wiz Data Sensitivity

Entro enriches NHIs with Wiz's data labels (type + sensitivity), so you know:

- Which machines have access
- What kind of data they reach
- How risky that access is

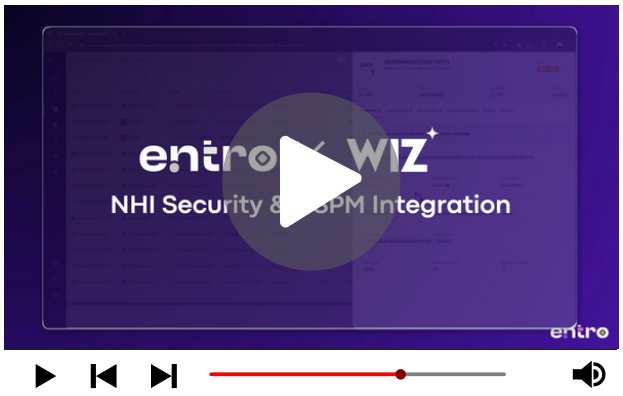
Example 1: Minimize Blast Radius from Exposed Secrets

Entro detects an exposed AWS access key in **Slack**. Wiz reveals that it accesses sensitive financial data in an S3 bucket. Entro maps the path and triggers remediation: rotating the token or adjusting its scope before damage spreads.

Example 2: Map NHI Permissions to Data Risk

Wiz classifies PII in RDS and PCI in S3. Entro correlates which IAM roles and tokens can access that data. Lineage mapping reveals over-permissioned or orphaned NHIs, helping teams close attack paths before they're exploited.

Watch the Demo (YouTube)



Ready to **Unify** Your NHI & Cloud Data Security?

Wiz & Entro customers get full visibility into which identities can access sensitive data and what to do about it. Visit **entro.security** to see how we turn NHI and secrets risks into actionable data-aware remediation.

Book a Demo

entro