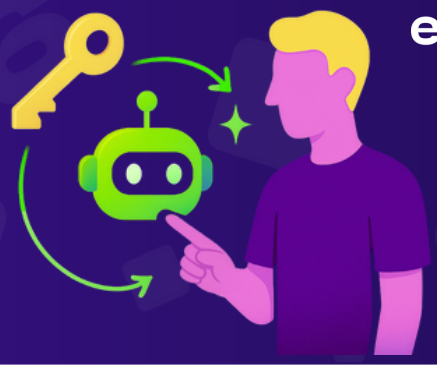
SOLUTION BRIEF

NHI Ownership Attribution

Bringing Human Accountability to Secrets & Non-Human Identities



THE CHALLENGE

Secrets don't operate in silos. Neither do the workloads, service accounts and bots that use them. But when something goes wrong, like a hardcoded secret leaking or an API key being compromised, security teams are left asking: **Who can fix this?**

But most organizations today can't really answer that.
NHI and secrets ownership data is scattered across the stack and without clear ownership, remediation stalls, risks live longer and compliance becomes harder - especially during M&As, mass layoffs and other critical organizational changes.

THE SOLUTION

Entro's **Ownership Attribution Model** brings clear, contextual ownership to secrets and non-human identities in your organization. The model ingests and analyzes data from across the stack including: IdPs, secrets exposure locations, cloud IAM policies, logs and historical activity, and more.

The model applies structured attribution logic to map each exposed secret or NHI to a human owner, while simultaneously mapping a complete hierarchy across team, project, and organization levels. Entro identifies the **Primary Owner**, and depending on the source, assigns additional employees with the sufficient permissions to handle the risk, like repository admins, Space owners and organization admins, ensuring accountability, quick remediation and escalation paths.

CAPABILITIES & KEY BENEFITS

1

Owner Assigned Per Secret or NHI

Automatically enriched with ownership details (name, email, Slack ID, etc.) to ensure accountability from the moment of detection.

2

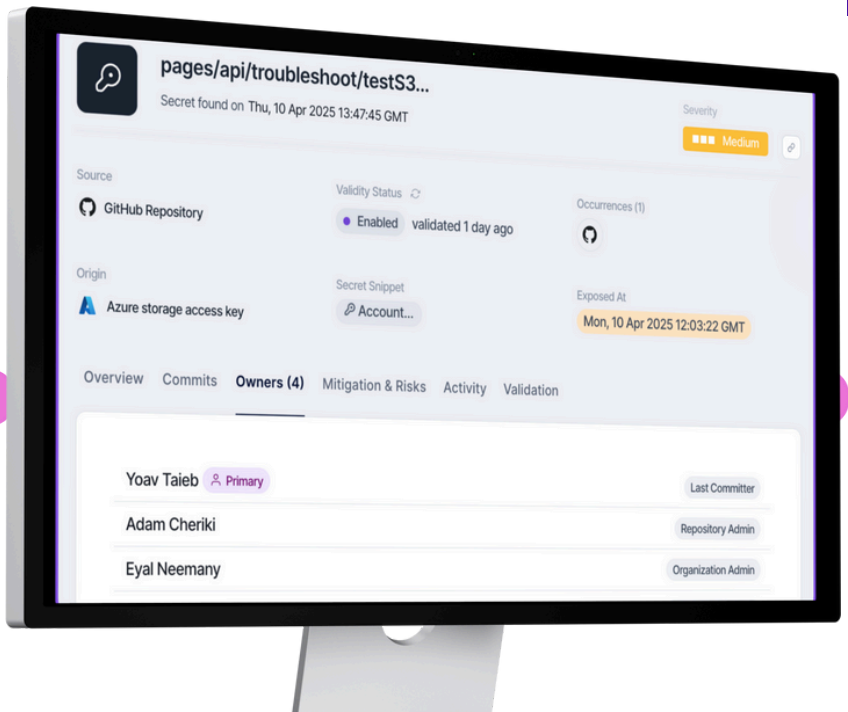
Escalation Path Context

A Primary Owner + two fallback layers mapped and labeled for smarter, faster triage of exposed secrets and NHI threats.

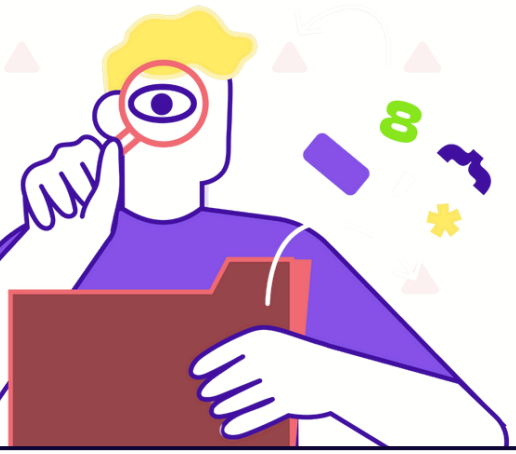
3

Risk Assignment, Remediation Workflows

NHI risks detected by NHIDR™ are tied back to a human user and pushed into Slack, SOAR, ticketing systems, etc., via OOTB integrations.



DETECTION → OWNERSHIP → RESOLUTION

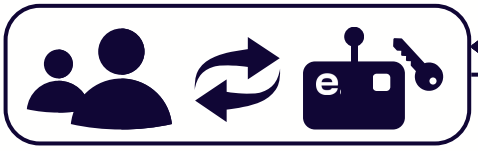


Identity Providers

Exposure Locations

IAM Policies

Logs & Vaults



Secret/NHI linked to human owner

Risk Assignment with ownership

Escalation-aware context

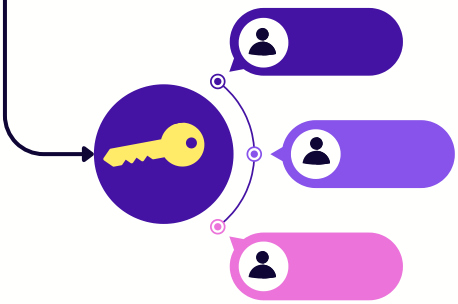
Workflow-integrated remediation

NHI OWNERSHIP NOW ENRICHED WITH HIERARCHY CONTEXT

Entro automatically maps and displays the full human ownership chain for exposed secrets and NHIs at risk, ensuring accountability and clear escalation paths at every level.

For example, if a secret is exposed on a **Jira** comment, Entro attributes ownership not just to the employee who posted the comment (Primary Owner), but also to the project lead and workspace admin.

Similarly, when a leaked token is detected in **GitHub**, ownership can be escalated from the commit author to the repo admin and also to the organization owner.



REMEDIATION STARTS IN TOOLS YOUR TEAM ALREADY USES

Entro assigns ownership and pushes risk alerts directly into Slack, Teams, SOAR, SOC automation tools, and ticketing systems, so the people who can fix the issue are notified and can act fast.

servicenow torq

Ready to **Own** Your Secrets & Non-Human Identities?

Entro closes the security-dev gap other tools leave open.
Visit entro.security to see how we connect secrets & NHIs at risk to the humans who can fix it.

Book a Demo

entro