entro | DATASHEET

CrowdStrike EDR + Entro Integration

Endpoint-powered discovery and inventory for **AI agents** and **MCP connections**, **secrets**, and on-prem **non-human identities.**

entro × CROWDSTRIKE

AI Agent, MCP Server and an Exposed Secret Walk Into a Laptop

Agentic AI adoption is moving faster than security.

Devs (but not only) are using AI clients and local MCP servers running on their machines to connect models to SaaS tools, code repos, cloud, and enterprise infrastructure. Those connections are powered by non-human access: API keys, tokens, service accounts, and secrets that often land in locally stored files. That makes endpoints an old/new control gap of the AI-native organization. You can lock down cloud and vaults in your NHI security program, but it only takes one laptop, one local MCP, or a legacy Active Directory user to create an untracked access path with devastating blast radius.

Agentic adoption accelerates without visibility

AI clients and MCP servers proliferate on endpoints, security and IAM teams have no viable way to build inventory, ownership and policies around them.

Authentication is everywhere to everything

MCP and agentic workflows rely heavily on NHI tokens and secrets to access and invoke resources on SaaS, cloud, CI/CD and internal apps.

Endpoints are a goldmine of plaintext secrets

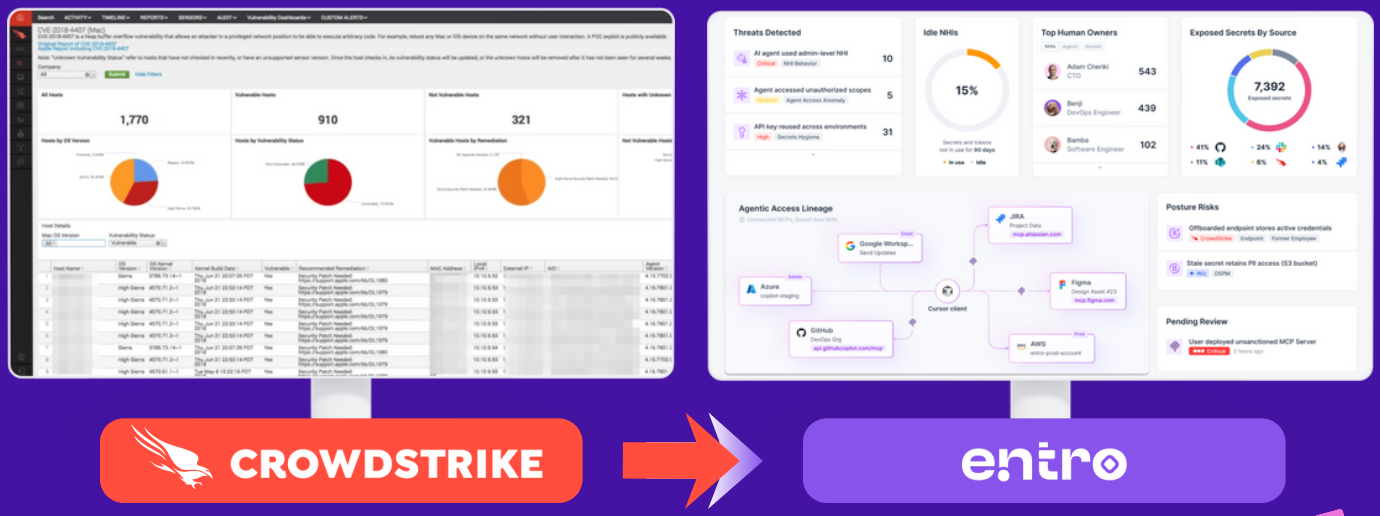
Config files, scripts, environment files, and tool settings become a default, unsafe secrets storage on devs' laptops.

Cloud and SaaS are only half of the NHI picture

Cloud-only visibility misses most local and legacy NHIs, especially on-prem service accounts that remain widely used and over-scoped.

Introducing Entro + CrowdStrike Falcon integration

Entro integrates with CrowdStrike Falcon to extend Agentic and NHI visibility to the endpoint layer. Using Falcon's endpoint reach, telemetry and response capabilities, Entro collects targeted signals from workstations, then correlates them with identity context to build an actionable inventory of AI agent clients, exposed secrets, and on-prem non-human identities.



AI Agents Discovery on End-Users' Machines

Entro's AI access discovery & inventory give security teams the ability to identify which AI clients and agents are being deployed, where they run in the organization, how they connect to tools and services, and which NHIs or human credentials power them. By analyzing network telemetry and correlating it with device signals and identity context. Entro turns scattered and local agentic activity into an actionable, governed inventory. It's built for the messy reality of "vibe coding" and shadow AI, where new AI apps and tools show up on laptops and quietly connect to mission-critical data and sensitive systems.

Centralize agent management and governance

Get AI services, MCP servers, and their NHIs into one inventory to enforce guardrails, track changes, and drive remediation.

See shadow AI and vibe-coding access paths

Detect unauthorized AI clients and local MCP configs running on your organizations' endpoints to identify agentic access.

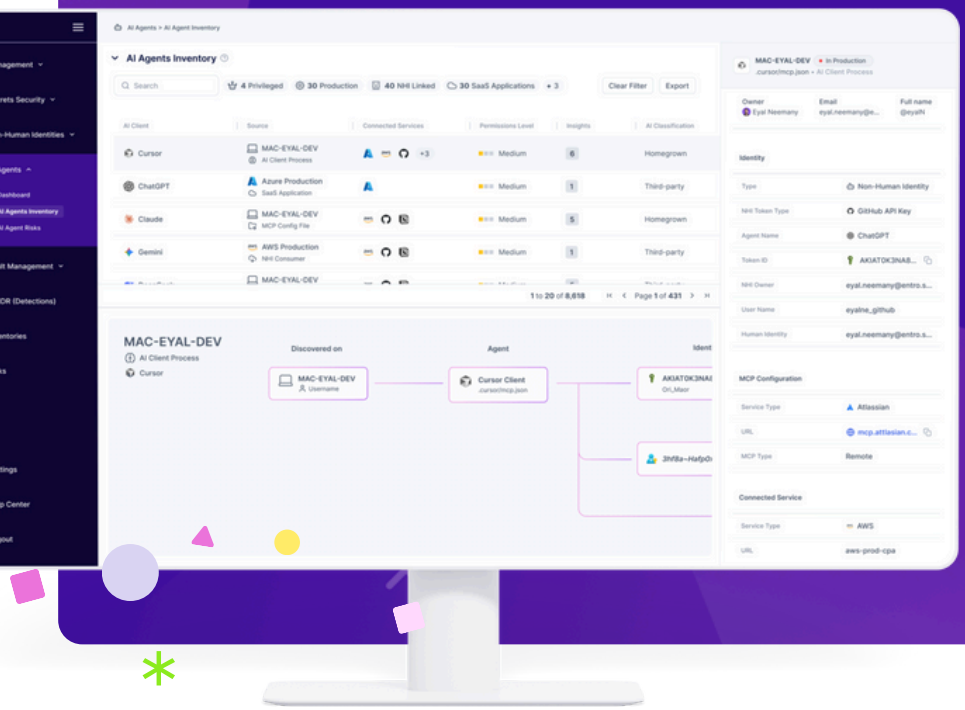
Add context: ownership, permissions, and risk

Correlate EDR signals with identity context to understand who owns the agents, what it can reach, and which paths are at risk.

entro CROWDSTRIKE

A Multi-layered AI Access Coverage

With CrowdStrike Falcon providing endpoint reach and telemetry, Entro's platform maps AI access across three connected layers:



Cloud Layer

Discover AI-related keys, tokens, and usage signals across cloud and SaaS.

NHI Layer

Control the identities that power AI agents, with context, lifecycle, and risk.

Device Layer

Correlate AI usage and MCP evidence directly from the users' endpoints.

Secrets Scanning on Local Endpoints

With or without AI tooling, endpoints are where developers' secrets tend to accumulate: staging credentials, test keys, one-off POC tokens, and "temporary" configs that quietly stay valid long after the project is done. Entro uses CrowdStrike Falcon's Real Time Response (RTR) to discover exposed secrets on workstations and servers, then turns raw findings into contextual risks with clear ownership, and automated remediation workflows.

Catch the "temporary" creds that never expire

Find staging, test, and POC credentials lingering on laptops before they become long-lived access paths into production.

Reduce blast radius from endpoint sprawl

Uncover plaintext secrets in configs and scripts, then centralize them into one inventory you can prioritize and clean up.

Make remediation practical, not disruptive

Add context (where, what it's for, likely owner/team) so rotation and replacement can happen without breaking workflows.

entro CROWDSTRIKE

On-Prem AD Service Accounts (Legacy NHIs)

Entro brings on-premise Active Directory service accounts into your NHI security program and enriches them with CrowdStrike endpoint context and identity activity signals, so you can understand where they run, how they are used, and what to fix first.

Unify AD service accounts with your NHI inventory

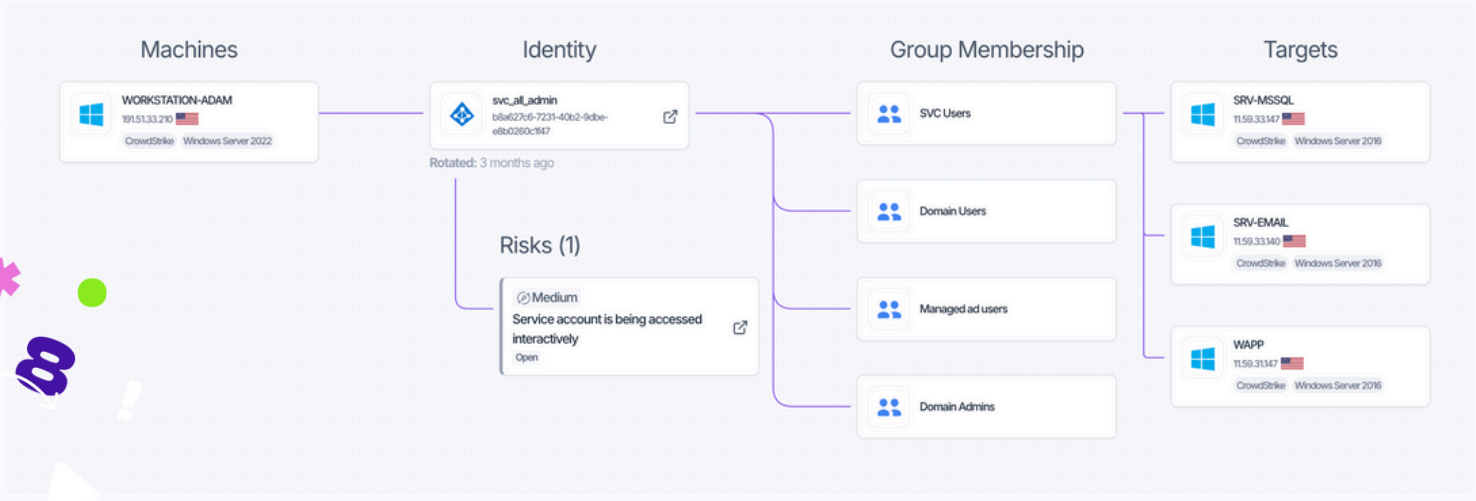
Get a single view of on-prem service accounts alongside cloud NHIs and secrets, including ownership and operational context.

Detect risks faster with device and identity context

Spot suspicious patterns like interactive logons, unusual hosts, and behavior that may indicate credential theft or compromise.

Visualize lineage and attack paths across devices and identities

Map how NHIs are used across hosts, services, groups, and permissions to understand blast radius and likely attack paths.



CrowdStrike + Entro: Endpoint Reach, NHI Context

Get a personalized Entro demo to discover AI agent and MCP access, exposed endpoint secrets, and AD service account risk.

entro

Get a Demo