entro | SOLUTION BRIEF

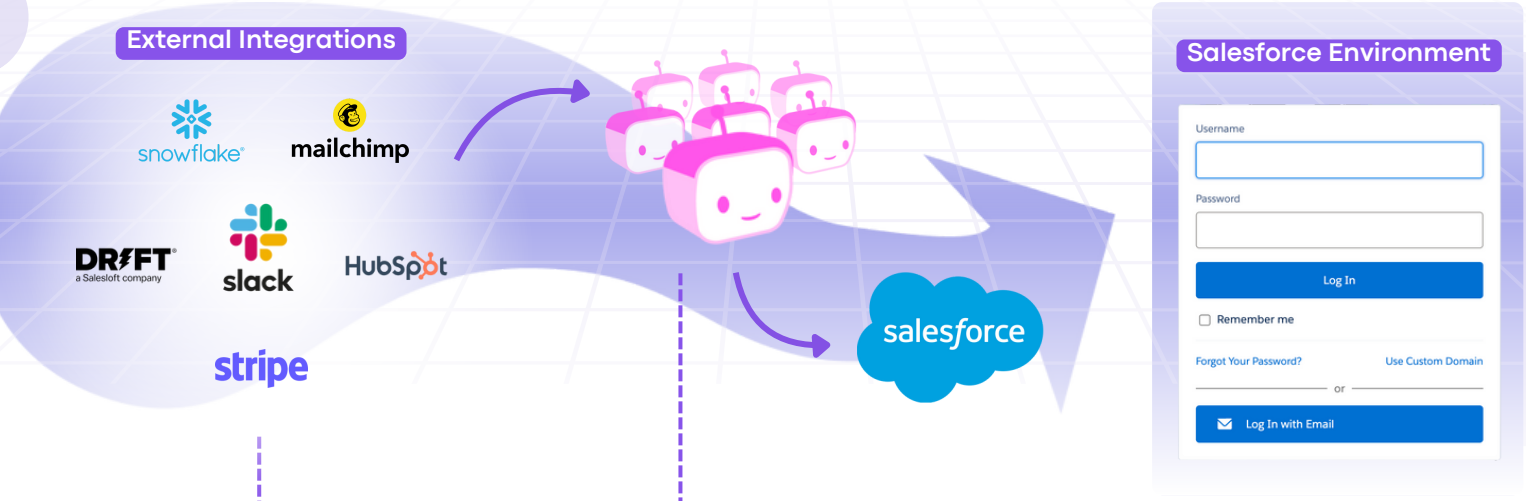
# Entro for Salesforce

Govern and Secure Connected and External Client Apps (NHIs) and Stop Secrets Leaking Through Your CRM


## Attackers Don't Break Salesforce, They Reuse Trusted App Access

### Salesforce is a high-trust hub. Your integrations are the shortcuts into it.

Recent Salesforce-related incidents (Salesloft Drift, Gainsight, etc) were non-human identities (NHIs) events. Attackers did not need to hack into Salesforce itself to compromise organizations. They abused trusted OAuth apps and issued tokens for third-party integrations in the Salesforce customers' environments. Once a vendor's app is compromised, its NHIs can be used to query, modify, and exfiltrate data at scale. Connected and External Client Apps sprawl across teams with broad scopes, long-lived OAuth tokens, and unclear ownership, creating durable compromise paths into CRM data. When a third-party app supply-chain incident hits, investigation and response often come down to stitching together logs, if you even have them*.




**Over 700** Salesforce customers were reported as impacted in the Salesloft Drift supply chain incident.

Source: Google Threat Intelligence Group

**Connected Apps**

Legacy Salesforce integration NHIs that define how external apps authenticate and what they can access via scopes and policies.

**External Client Apps**

Newer Salesforce NHIs for external integrations that are typically org-scoped by default but still define OAuth access, scopes, and permissions.

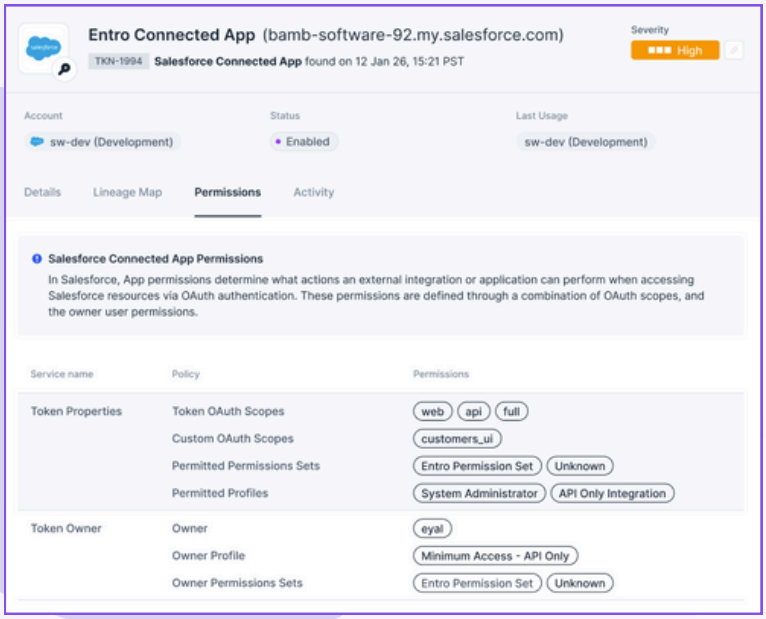
*log availability varies by Salesforce plan/add-ons

entro

## Make Your SFDC Integrated Apps a Governed NHI Surface

Entro integrates with your Salesforce to discover and monitor Connected Apps and External Client Apps as NHIs, giving security teams a live, unified view of which tools can access your CRM environment, what permissions they hold, how broadly they're scoped, and which human user or team owns each external integration.

Entro helps maintain your Salesforce security posture around the clock. Instead of hunting through scattered settings and logs when a third-party incident hits, you can quickly scope blast radius, identify relevant tokens and responsible owners, and respond or revoke risky access.




### Unified App NHI Inventory

See every Connected App and External Client App in one place, with status, environment, and usage context.

### Scope and Permission Risk Clarity

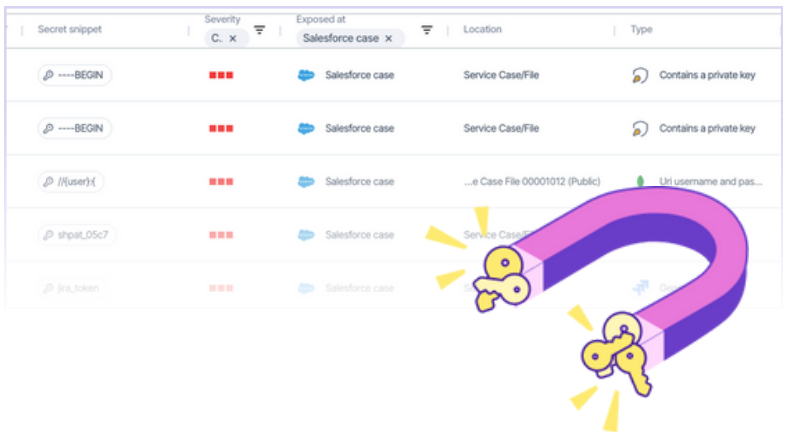
Understand what each app can do (OAuth scopes, permission sets, profiles) and flag over-privileged, stale or unowned access fast.

### Ownership and Rapid Response

Identify the human owner and the relevant tokens so you can route remediation, right-size access, or revoke quickly during an incident.

### Service Cases Secret Scanning

Entro scans Salesforce Service Cases to detect plaintext secrets and sensitive credentials exposed through day-to-day support workflows, including case descriptions, comments, and file attachments. Entro helps security teams find and remediate exposures, reducing the overall CRM blast radius.




## Ready to control your Salesforce NHIs?

Get a personalized demo to see how your organization can finally inventory, attribute, and govern Salesforce Connected Apps and External Client Apps.

entro

Get a Demo