

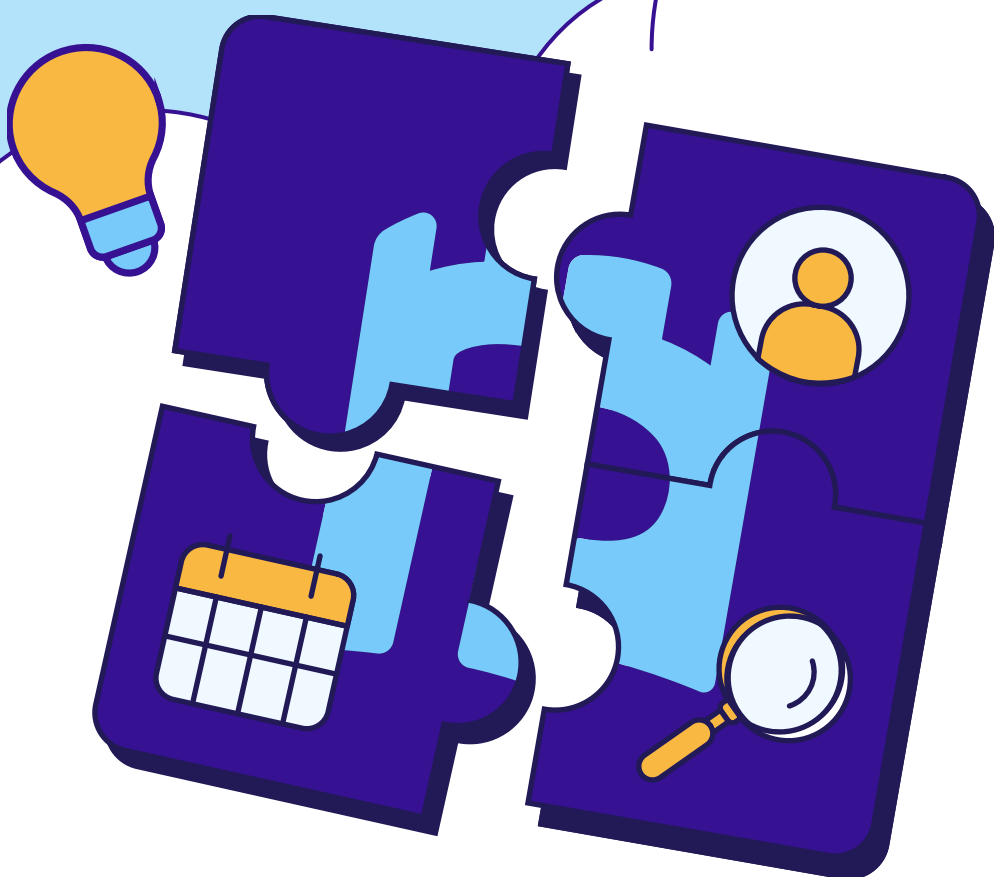


CASE STUDY

How a Cloud Comms & IT Enterprise Unified 1M+ Identities Across 20+ Integrations

A global enterprise operating across multiple cloud tenants and an extensive SaaS footprint needed clear, fast answers to **who did what, when, and where**, and a way to connect fragmented identities back to a single source of truth. Investigations were slowed by identity sprawl, and blind spots left teams uncertain about the real scope of incidents.

By deploying the **Permiso Identity Security Platform**, powered by the **Universal Identity Graph (UIG)**, the customer unified fragmented identities, accelerated investigations, and established a repeatable, risk-based approach to reducing exposure. What was once a fragmented view of activity across clouds and apps became a consolidated identity picture that enabled the team to **investigate faster, remediate smarter, and reduce risk at scale**.





The Challenge

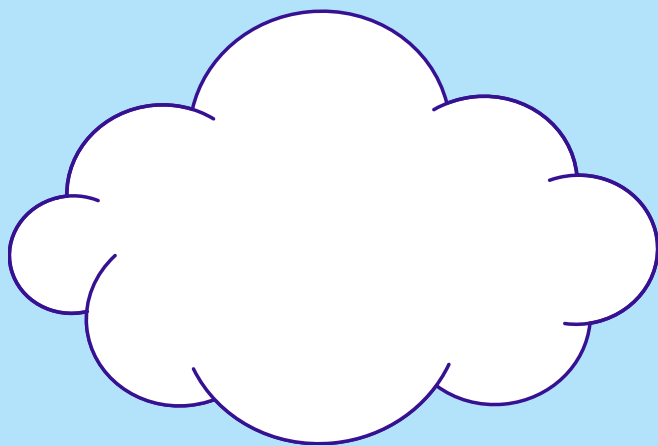
The enterprise operated in a complex, distributed environment spanning multiple cloud providers, numerous tenants, and a wide range of SaaS applications.

Identity sprawl had become one of their biggest pain points. Incident investigations often stalled because activity could not be easily tied back to a single identity or session. Logs were siloed, tools weren't designed to stitch together human and non-human identities, and critical questions like “*who initiated this action, from where, and what else did they touch?*” required hours of manual correlation.

Traditional tools could not reliably handle the volume, variety, and complexity of identity data in their environment, leaving them with blind spots especially around non-human identities like API keys, tokens, and service accounts that often carried excessive privileges.

“We were looking for something to give us an edge in the cloud identity space. We are integrated into multiple cloud environments spanning multiple tenants as well as having a large suite of SaaS tools and platforms.

We wanted to answer the questions of who, what, when, where during an incident across multiple domains in a large corporate footprint as well as tie all distributed identities back to a single source.”



Objectives

The customer set out with clear priorities:

- Centralize identity visibility** across multi-cloud and SaaS.
- Accelerate incident response** with precise attribution (who/what/when/where).
- Reduce blind spots** around non-human identities, including service accounts, tokens, and keys.
- Prioritize risk reduction** by surfacing and fixing the highest-impact exposures first.
- Simplify investigations** with a consistent, authoritative source of identity truth.





The Solution: Permiso Identity Security Platform

The customer implemented the **Permiso Identity Security Platform** to unify their distributed identity landscape and power identity-centric detection, investigation, and response across their enterprise.

How the Universal Identity Graph Powers the Platform

At the core of the platform is the Universal Identity Graph (UIG), which transforms scattered signals into a coherent, actionable view of identity activity. The UIG:

Unifies identities (human and machine) from multiple clouds, tenants, and SaaS into a single canonical identity.

Stitches activity into sessions, correlating events across domains to accurately attribute actions.

Maps relationships and permissions, surfacing potential attack paths and blast radius.

Prioritizes risky identities and access paths, ensuring remediation efforts are focused where they matter most.

Today, Permiso manages **1M+ identities across 20+ integrations** in the customer's environment, giving them the scale and confidence to tackle identity challenges across one of the largest distributed cloud and SaaS estates in their industry.

Permiso

Search for entity names and IP addresses

Alerts > Multi-Plane Alert: LUCR3 - Multiple TTPs

Multi-Plane Alert Details

Signature

LUCR3 - Multiple TTPs

PO_LUCR3_MULTIPLE_TTPS

Time

02:21:14
23-11-09

Severity

9.0

Critical

Environments

Description

Multiple TTPs related to LUCR-3 have been found in your environment, sourcing from two (2) identities ([jean-luc picard](#), [harry](#)):

- MFA Default Method Downgraded
- Weak Authentication Method Registered
- Sensitive Search Query Performed
- Cloudtrail Trail Stopped
- EC2 SSH with Root
- SecretsManger Harvesting
- AWS Accesskey Created
- S3 Browser usage
- Github Bulk Repository Download

Who Is LUCR-3

LUCR-3 (Scattered Spider) is a financially motivated threat actor specializing in leveraging Identity Providers (IDPs) for initial access, with the goal of stealing Intellectual Property (IP) for extortion purposes. [Read more about the group](#)

10 Alerts triggered

11h 5m 19s Duration

3 Identities involved

2 Credentials used

1 Secrets used

1 Resources affected

3 Environments affected

18 Sessions recorded

Inventory

Entities related to this multi-plane alert

NAME	ENVIRONMENTS	STATUS
jean-luc picard Entra ID User	Permiso Demo 14a96ed4-7b33-451...	Active
william riker Entra ID User	Permiso Demo 14a96ed4-7b33-451...	Active
Harry AWS IAM User	Permiso Demo 687406467988	Active
Death-Star-Schematics GitHub Cloud Repository	PM-Empire-of-Co... 150068507	Active
AKIA2ADE6JOKARRFQ... AWS Access Key	Permiso Demo 687406467988	Active

By bringing together fragmented identity data into a consolidated graph, the platform eliminated investigative guesswork and gave teams a **trustworthy, end-to-end view of identity activity across their environment.**

Case Study: How a Global Enterprise Unified 1M+ Identities Across 20+ Integrations with Permiso

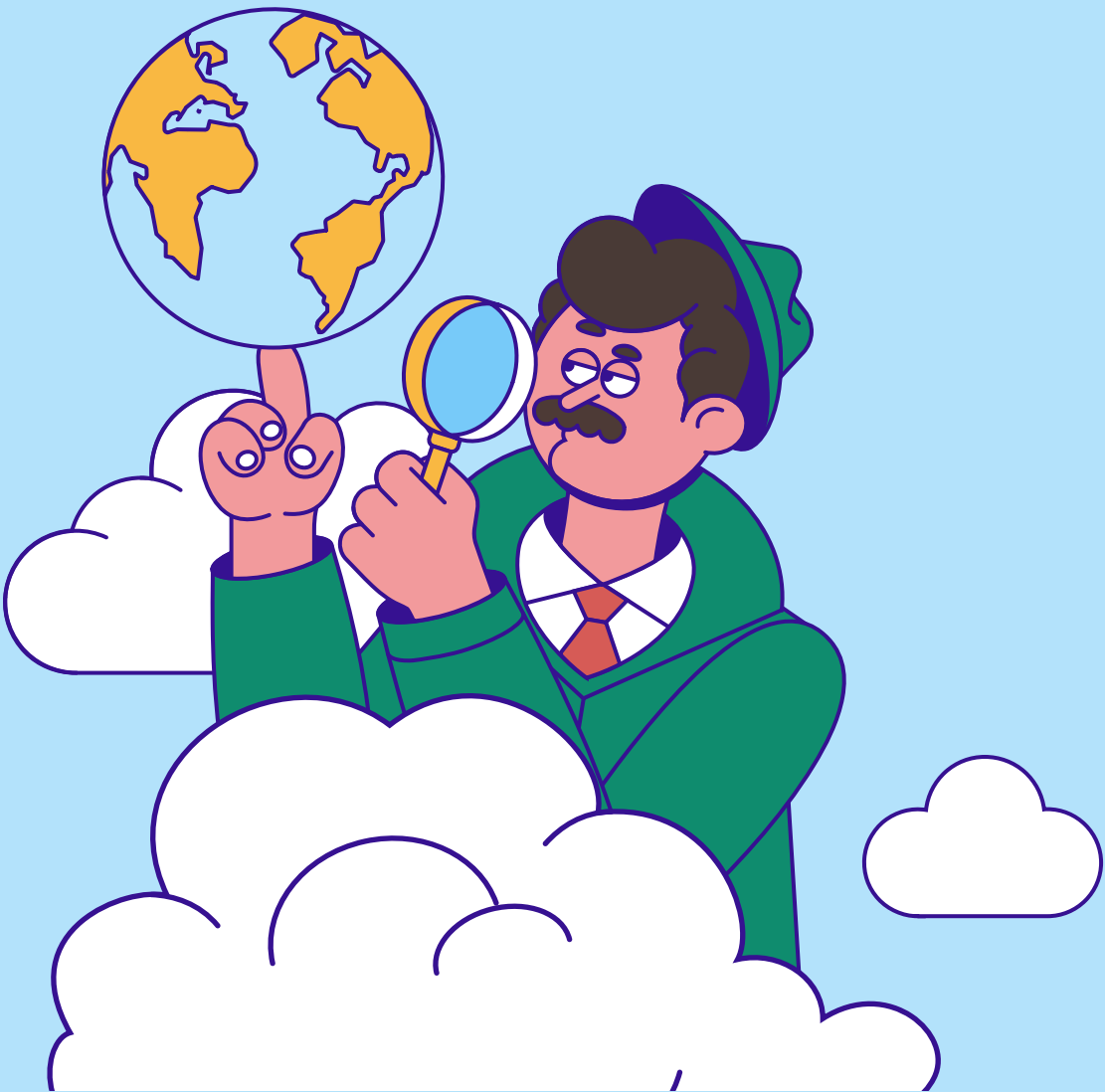
3



Implementation Highlights

Within weeks, the customer moved from fragmented visibility to a unified, risk-prioritized identity view:

- ✓ **Integrated identity providers**, cloud accounts, tenants, and key SaaS platforms into the Permiso platform.
- ✓ **Ingested and normalized identity activity** (including machine credentials) into UIG for consistent, searchable context.
- ✓ **Enabled threat-informed detections** and investigation workflows aligned with the customer's incident response playbooks.
- ✓ **Established a repeatable, risk-based prioritization process**, guiding remediation to the most critical identities and access paths first.
- ✓ **Improved cross-team workflows**, allowing SecOps, IAM, and cloud platform teams to collaborate around a single source of identity truth.



Results

With Permiso, the enterprise moved from fragmented signals to confident, end-to-end identity visibility and response.

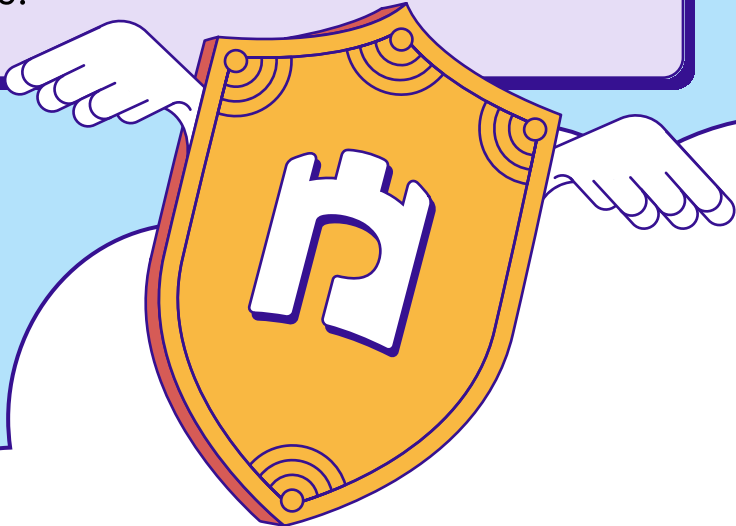
Clear Attribution (Who/What/When/Where)
Investigations now start from a unified identity, eliminating hours of log hunting and guesswork.

Confidence at Scale
A single source of truth for identity activity across clouds and SaaS improved collaboration, alignment, and decision-making.

Faster Incident Response
Full sequences of actions across tenants and apps are visible in minutes, accelerating scoping and containment.

Operational Efficiency
By automating identity stitching and risk prioritization, the team reduced manual effort and focused resources where they added the most value.

Prioritized Risk Reduction
High-risk identities and overprivileged access paths are surfaced early, allowing the team to fix what matters most first.





PERMISO

Why Permiso

- ✓ **Platform first**
End-to-end identity detection, investigation, and response in one solution.
- ✓ **UIG advantage**
Deep identity stitching and relationship mapping that other tools simply can't deliver.
- ✓ **Actionable risk focus**
Transforms sprawling identity data into prioritized, measurable risk reduction.
- ✓ **Scale proven**
Managing **1M+ identities across 20+ integrations** with consistent accuracy and context.
- ✓ **Team alignment**
Provides a common language and consistent context across security, cloud, and IAM functions

By choosing the **Permiso Identity Security Platform**, the enterprise replaced fragmented visibility with a unified, risk-prioritized defense. They can now answer who, what, when, and where with confidence, while proactively reducing risk across one of the largest and most distributed identity footprints in their industry.

Clear the Clouds of Confusion

TRY PERMISO NOW

www.permiso.io