THEOM OVERVIEW

Theom for Airline Data Security and AI Governance

Data security posture, access governance, activity monitoring, and AI data-use control for airline environments

White paper for airline security, data, infrastructure, governance, AI, and leadership teams

Theom gives airline teams a live, evidence-based view of sensitive data: where it exists, who and what can reach it, how it is actually being used, and whether that use aligns with policy across passenger, loyalty, workforce, operational, partner, and AI workflows.

EXECUTIVE SUMMARY

Airlines need more than static inventories and periodic access reviews. Sensitive data now spans reservations and ticketing, loyalty platforms, payment flows, crew and workforce systems, operations and maintenance datasets, cloud warehouses, lakehouses, SaaS applications, analytics tools, notebooks, partner workflows, and AI-enabled applications. Theom helps airline security and data teams continuously understand their data risk surface and turn that understanding into practical control.

Theom combines data security posture management, data access governance, data activity monitoring, and AI-aware data-use monitoring. Together, these capabilities help airlines identify sensitive data, map entitlement paths, observe real usage, reduce unnecessary access and data sprawl, and prove that humans, service accounts, applications, partners, and AI systems are using data appropriately.

WHY THIS IS RELEVANT NOW

Airline data is live and distributed
Passenger, loyalty, reservation, payment, crew, maintenance, operations, and partner data move through booking channels, data platforms, SaaS tools, reports, exports, and shared workflows.

Access is increasingly non-human
Service accounts, data jobs, APIs, SaaS integrations, notebooks, analytics pipelines, and partner connections often touch sensitive airline data at scale.

AI expands the use surface
Copilots, agents, analytic assistants, retrieval workflows, and LLM-enabled tools can retrieve, join, summarize, or expose sensitive data faster than traditional reviews can track.

THEOM IN ONE SENTENCE

Theom continuously discovers sensitive airline data, maps access and entitlement paths, monitors actual activity, and tracks how AI systems use data - all from inside the customer's controlled environment, without requiring sensitive data to leave that boundary.

PRACTICAL USE CASES

Theom can start with focused, high-value airline data domains - such as passenger, loyalty, reservation, payment-adjacent, employee, crew, operational, maintenance, financial, and partner data - then expand coverage as evidence and policy maturity grow.

Use case	Core question	What Theom does	Airline value
DSPM Data Security Posture Management	Where is sensitive airline data, and what is exposed?	Discovers and classifies passenger, loyalty, payment-adjacent, employee, crew, operational, maintenance, and partner data; finds stale or risky copies; identifies	Prioritize real data risk across complex airline data estates instead of relying on static inventories, manual sampling, or fragmented platform views.

© Theom, June 2026. Public distribution.

Use case	Core question	What Theom does	Airline value
		excessive access; and highlights crown-jewel concentrations.	
DAG Data Access Governance	Who and what should have access, and why?	Maps users, groups, service accounts, jobs, APIs, partners, reports, and AI workflows to the sensitive data they can reach; compares entitlement to business purpose and actual use.	Support least privilege, access reviews, separation of duties, audit evidence, and defensible governance for airline business, operations, and data teams.
DAM Data Activity Monitoring	What is actually happening now?	Monitors queries, sessions, downloads, exports, joins, copies, and movement events with context from data sensitivity, identity, location, behavior, and business workflow.	Detect compromised identity misuse, insider risk, partner overreach, unusual exports, and risky joins before they become data incidents.
AI data-use monitoring	How are AI tools using sensitive data?	Tracks data touched by agents, copilots, notebooks, and retrieval workflows; connects prompts or tasks, tool calls, queries, identities, source data, and outputs where available.	Enable safe AI adoption for customer service, personalization, disruption management, revenue, operations, and maintenance use cases while controlling which data can be retrieved, joined, summarized, exported, or exposed.

WHAT AI-AWARE TRACKING ADDS

Traditional monitoring often sees a database query, API call, file download, notebook session, or SaaS event. AI-aware monitoring connects additional context: the human or service identity behind the task, the AI application or agent involved, the airline data sources queried, intermediate tool calls, and the final output or action where available.

- Prevent over-broad retrieval by AI assistants that should answer from approved policy, operational, maintenance, or knowledge-base data but not passenger PII, loyalty records, payment-adjacent data, employee records, crew data, or other restricted information.
- Detect AI-driven or notebook-driven joins that combine individually approved datasets into a higher-risk passenger, loyalty, employee, crew, financial, or operational profile.
- Show whether an AI workflow used stale, sensitive, or unauthorized data when producing a customer-service response, disruption report, forecast, audience, operational recommendation, or maintenance analysis.
- Create evidence for airline leadership that AI usage is governed by data sensitivity, identity, purpose, and policy - not just application-level controls.

A FOCUSED 30/60/90-DAY ADOPTION PATH

First 30 days

Map the airline data risk surface

Connect priority data environments and classify sensitive data. Identify crown-jewel domains, exposed datasets, unused access, risky service accounts, high-volume exports, and obvious governance drift.

Next 60 days

Govern access and AI use

Validate access paths for high-value passenger, loyalty, employee, crew, operational, and partner data. Establish policies for sensitive domains and add AI-aware controls for copilots, notebooks, retrieval workflows, agents, and analytics assistants.

By 90 days

Monitor, prove, and operationalize

Enable live activity monitoring for selected domains. Route high-fidelity findings into existing response workflows. Produce evidence packs for security leadership, data owners, audit, privacy, and compliance stakeholders.

© Theom, June 2026. Public distribution.

HOW THEOM COMPLEMENTS EXISTING CONTROLS

Existing control	What it does well	What Theom adds
Network micro-segmentation	Limits lateral movement and makes workload communication explicit.	Extends blast-radius thinking to sensitive data access, movement, usage, and AI retrieval across airline platforms.
IAM / PAM	Controls identity, roles, privilege, and access approvals.	Shows which sensitive passenger, loyalty, workforce, operational, and partner datasets those identities actually touch and whether use matches purpose.
DLP / CASB	Controls egress, endpoint movement, and SaaS usage patterns.	Adds data-native sensitivity, lineage, and live platform activity before sensitive data leaves controlled systems.
SIEM / SOAR	Correlates events and orchestrates response.	Feeds higher-fidelity alerts with evidence of the data, identity, action, policy, and risk involved.
Data catalog / governance	Documents assets, ownership, definitions, and lineage.	Turns inventory into live posture, access governance, activity monitoring, ROT reduction, and AI data-use evidence.
AI platform controls	Manage approved models, prompts, applications, and platform guardrails.	Connects AI behavior to governed data: what was retrieved, joined, summarized, exported, or exposed.

BOTTOM LINE

Theom helps airlines move from static data inventory to live data control: discover sensitive data, govern access, monitor activity, and prove how humans, services, partners, applications, and AI systems are using data. It complements the existing security and governance stack while adding the data-layer evidence needed for modern operations, analytics, customer experience, and AI workflows.

© Theom, June 2026. Public distribution.