THEOM OVERVIEW

Theom for Banking: Data Governance, Security and AI

A shared data, identity and evidence layer for trusted banking operations and governed AI

White paper for data governance, security, risk, compliance, AI, data-platform and leadership teams

Theom gives banks a live, evidence-based view of sensitive data: where it exists, how it moves, who and what can reach it, how it is used, and whether that use aligns with policy and regulatory expectations.

EXECUTIVE SUMMARY

Banking data moves across core systems, warehouses, cloud stores, files, SaaS applications, dashboards, notebooks, service accounts, partners and AI-enabled workflows. Catalogs, entitlement records and periodic reviews describe intended controls, but they do not always show where regulated data has propagated or how it is being used now.

Theom connects data discovery, classification, lineage, identity, effective authorization and observed activity across User-to-Data, Application-to-Data and AI-to-Data. This shared context helps governance teams reconcile policy with datastore reality, security teams prioritize evidence-backed risk, and AI teams trace and control how models and agents consume banking data—while keeping processing and sensitive operational context inside the bank's controlled environment.

WHY THIS IS RELEVANT NOW

Intent and reality diverge

Sensitive fields, downstream copies, catalog entries, tags and masking controls can drift as data is transformed and reused.

Consumers are fragmented

Employees, roles, service accounts, BI tools, applications, partners and pipelines create access paths that are difficult to assess in isolation.

AI expands the use surface

Copilots and agents can retrieve, join, summarize or expose banking data faster than application-only controls and manual reviews can track.

ONE FOUNDATION, THREE STAKEHOLDER OUTCOMES

Governance

Discover and classify assets; reconcile catalogs; track lineage, copies, ownership, freshness and control drift.

Security

Assess exposure and access; detect first-seen or abnormal behavior; investigate with sensitivity, identity and lineage context.

AI

Trace user or service → agent → tool/query → data → result; validate retrieval and apply bounded policy controls where needed.

PRACTICAL BANKING USE CASES

Theom can begin with a focused production domain—such as customer PII, accounts, transactions, lending, payments, treasury, fraud, KYC/AML, employee or operational data—and expand coverage as evidence and policy maturity grow.

Shared evidence model: data inventory + classification + lineage + identity + authorization + observed activity + AI context

Use case	Core question	What Theom does	Banking outcome
Data discovery, catalog assurance & lineage	What data exists, how sensitive is it, where did it come from and where has it propagated?	Discovers and classifies structured, semi-structured and supported unstructured assets; compares catalog intent with datastore reality; maps upstream sources, downstream derivatives and copies; and surfaces missing ownership, classifications or tags.	A current, owner-ready inventory; stronger catalog coverage; traceable data products; and consistent governance as banking data changes form.
Data security posture & risk assessment	Which sensitive-data concentrations, exposures and behavior patterns require attention first?	Combines sensitivity, permissions, observed use, lineage and business context to highlight exposed or stale copies, excessive or unused access, risky service accounts, unusual joins, bulk extracts and first-seen consumers.	Prioritized, evidence-based risk for security and data owners instead of long lists of disconnected misconfigurations or events.

© Theom, July 2026. Public Distribution.

Use case	Core question	What Theom does	Banking outcome
Data access governance	Who and what can reach regulated data, who actually uses it and does that access still match purpose?	Maps employees, groups, roles, service accounts, jobs, applications and partners to effective authorization and actual use; compares source and derivative permissions, row-level controls and masking where supported.	More defensible least privilege, access reviews, separation of duties, exceptions and data-owner decisions.
User/Application-to-Data monitoring	What is happening with sensitive data across people, tools and applications?	Connects direct users and non-human consumers to queries, sessions, downloads, exports, copies and movement events; fingerprints recurring tools and identifies novel or abnormal patterns with supporting evidence.	Faster investigation of identity misuse, insider risk, partner overreach, shadow integrations and activity that differs from established behavior.
AI-to-Data governance	How are copilots, agents and AI-enabled applications using sensitive banking data?	Connects the initiating identity, AI application or agent, tool calls, generated queries, source data and response or action where telemetry is available; tests policy and can use native data controls or bounded retrieval enforcement where required.	Governed AI adoption with clearer accountability, safer retrieval and evidence that controls operate at the data layer—not only in the application.

WHAT AI-AWARE GOVERNANCE ADDS

Traditional controls may see a database query, API call, file download or notebook session. AI-aware governance connects the human or service identity behind the task to the application or agent, tools, retrieved data, generated query and resulting output or action where available.

- Prevent over-broad retrieval from customer PII, account records, loan files, KYC/AML materials, payment data or employee information.
- Detect AI-driven joins that combine individually approved datasets into a higher-risk customer, household, credit, fraud or operational profile.
- Show when an AI workflow relies on stale, sensitive or unauthorized data, and surface approved versus unapproved AI access paths using available datastore and agent telemetry.
- Give data owners, security teams, model-risk stakeholders and auditors a common trace from request to source evidence and response.

A CONTINUOUS BANKING CONTROL LOOP

1. Discover	2. Connect	3. Assess	4. Act
Inventory and classify sensitive assets across connected banking platforms.	Relate data to lineage, copies, identities, roles, applications and agents.	Compare intended controls with permissions, actual use, anomalies and policy drift.	Route evidence to owners and workflows; apply approved native or bounded controls.

A FOCUSED 30/60/90-DAY ADOPTION PATH

First 30 days
Map the data reality

Connect a priority production platform. Validate known sensitive data, identify unknown assets, compare catalog coverage, and establish access and activity baselines.

Next 60 days
Prioritize and govern

Review lineage, copies, permissions, actual consumers and control drift. Test one non-production AI workflow in observe mode with representative identities and policies.

By 90 days
Operationalize evidence

Route findings to owners and existing workflows. Apply approved native controls or bounded enforcement, and produce evidence for leadership, risk, compliance and audit.

HOW THEOM COMPLEMENTS EXISTING CONTROLS

Existing control	What it does well	What Theom adds
Data catalog / governance	Documents assets, owners, definitions and intended controls.	Reconciles intent with observed assets, contents, lineage, access and use; surfaces drift and evidence for owner action.
IAM / PAM	Controls identities, roles, privilege and approvals.	Shows which sensitive data identities can reach and actually use, including service, application and agent paths.
DLP / CASB	Controls egress and SaaS usage patterns.	Adds sensitivity, lineage and in-platform activity context before data leaves controlled systems.
SIEM / SOAR	Correlates events and orchestrates response.	Provides enriched findings with the data, identity, consumer, action, lineage and policy evidence needed to investigate.
AI platform controls	Manage models, prompts, applications and guardrails.	Connects AI behavior to the enterprise data retrieved, joined, summarized, exported or exposed.

BOTTOM LINE: Theom gives governance, security and AI teams a shared, live view of banking data, identity, access and use—strengthening ownership and lineage, prioritizing activity risk, and governing how sensitive data is retrieved by applications and AI.

© Theom, July 2026. Public Distribution.