Data and AI security that lives inside Snowflake

Theom runs natively inside your Snowflake account. It sees who and what touches your data, from people to apps to AI agents, and enforces your rules through Snowflake's own controls.

Your Data. Your AI. Used as Intended.

> Backed by **Snowflake Ventures**. Named **a Leader** in The Forrester Wave™: Sensitive Data Discovery And Classification Solutions, Q2 2026, and **a Leader and Outperformer** in the GigaOm Radar for Data Security Posture Management (DSPM) v3.

Why AI launches stall at the security review

Most Snowflake customers already have strong controls. Horizon classifies sensitive data, grants decide who can reach it, masking and row access policies protect it, and AI agents are getting identities of their own. What holds up the next Cortex or CoWork launch is a different question, and it lands on the security team: **who and what is actually using our sensitive data, and should they be?**

Grants and classifications describe what could happen. They won't tell you that a coding assistant has been querying the warehouse under an analyst's login for three weeks, or that a service account started reading payment tables it had never touched before. Today that answer comes from hand-written Access History queries and a spreadsheet, which gets you through one audit and little else.

How Theom and Snowflake work together

Theom works from inside the same Snowflake account and builds on what Snowflake already knows. Horizon knows which data is sensitive, and Snowflake keeps a record of every query. Theom connects the two with identity, so for each piece of sensitive data you can see who or what touched it, what they did with it, and whether that matched your policy. A list of grants becomes a picture of real behavior. Your teams can spot a service account acting like a person, an AI agent reaching customer records it was never meant to see, or a role holding access that nobody has used in a year.

For data leaders, the same record answers governance questions that used to take weeks: which copies of sensitive data have drifted from their source, which tables live outside the catalog, and who still reads the data you want to retire.

When something needs to change, Theom works through Snowflake's own controls. It labels the data, and Snowflake's masking and row access policies enforce on those labels, so protection follows sensitive data as new tables and schemas arrive, with nothing placed in the path of your queries. For AI agents and copilots, including those built on Cortex, Theom can also act on each request as it happens, allowing, masking, redacting, or blocking it, and it gives security a kill switch if an agent goes wrong.

For the business, that means AI projects on Snowflake reach production with the evidence security needs to approve them, and governance teams have a continuous record to show auditors and regulators. Your data and query text stay in your Snowflake account the whole time.

© Theom, 2026

WHERE THEOM RUNS

Inside Snowflake, next to your data

Theom runs inside your own Snowflake account, beside the data it protects, so your data and query text stay put and nothing sits between your people and the warehouse. For AI agents and copilots, Theom also sits inline on each request and can quarantine an agent before sensitive data reaches the model. Only findings leave, keyed by pseudo keys, and the mapping to your real names stays with you.



What Theom finds inside Snowflake

33,000+
AI agent sessions found running against one company's warehouse

130+
service accounts being used like human logins

2,200+
sensitive columns with no masking policy in place

75,000+
grants to data that nobody was using

~1,000
production objects shared into a development account

490+
data objects reached by AI services, 40+ of them sensitive

One platform to see, govern, and secure data and AI

MAP
Discover and classify sensitive data in place, and map every identity that touches it: people, service accounts, and AI agents.

DEFINE
Write policy in plain language, turn it into enforceable rules, and shrink over-broad access by comparing what's granted with what's used.

ENFORCE
Act inline on AI requests (allow, mask, redact, or block), and enforce for everyone else through Snowflake's native tags, masking, and row access.

KEEP CURRENT
Monitor every query continuously, prove it on demand for GDPR, HIPAA, PCI, and SOX, and send findings to Splunk, Sentinel, ServiceNow, Jira, and Slack.

See Theom on your own Snowflake data

A 30-minute conversation and live demo with the Theom team.

theom.ai/book-a-demo

Exposure figures are from Theom deployments; customer names are withheld. Forrester does not endorse any company, product, brand, or service included in its research publications and does not advise any person to select the products or services of any company or brand based on the ratings included in such publications. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. GigaOm Radar is a trademark of GigaOm. All rights reserved. Snowflake, Horizon, Cortex, and CoWork are trademarks of Snowflake Inc.