APPLICATION-USER ATTRIBUTION

Keep identity with the query.

A shared database account should not be the end of an investigation.



01

Application context

The user behind the request

02

Shared credential

The database account

03

Attributed activity

Context retained for review

Trace carries available user context with SQL. With Nanori Lens and Oversight, that context connects application activity to database evidence and risk findings. Trace can also work independently with compatible monitoring.

THE INVESTIGATION

Same account. Different explanations.

A customer portal uses app_svc for many people. Alex Morgan begins reading profile data linked to account records. What should an analyst establish?

SQL QUERY

```
SELECT p.full_name, p.email, a.account_number
FROM customer_profiles p
JOIN customer_accounts a
  ON a.customer_id = p.customer_id;
```

The SQL describes the data requested.
It does not, by itself, identify the application user or establish the business reason.

01 Separate the two identities.

Keep Alex Morgan as the available application identity and app_svc as the database credential. Trace supplies context; it does not independently authenticate the person.

02 Test the pattern, not just the query.

In Oversight, review repeated reads, measured rows or bytes, affected objects and available history. A scheduled report and gradual extraction may use similar statements.

03 Check missing context explicitly.

For a protected database account, missing application identity can generate an alert. Investigate direct access and instrumentation gaps; do not substitute a guessed user.

EXPECTED EXPLANATION

An authorized report with matching identity, scope and timing.

REASON TO ESCALATE

Unexplained accumulation or access that conflicts with the expected context.

FIT AND EVALUATION

Prove attribution on your application.

A useful evaluation shows both the context that is present and the gaps that remain.

WITH NANORI

Trace + Lens + Oversight

Trace adds application context. Lens captures database activity and sends it to Oversight for investigation. Lens and Oversight deploy together.

WITH OTHER MONITORING

Trace, independently

The monitoring product must preserve and interpret the annotations. Confirm its parsing and identity display on the intended connection path.

FOUR PROOFS TO REQUEST

EVALUATION	EVIDENCE TO INSPECT
Shared connection pool	Two application users produce distinguishable captured activity through one database account. Check isolation when requests overlap.
Missing context	A request without a resolved user remains visibly unattributed. In Oversight, test the protected-account policy separately.
Encrypted connection	Validate encryption metadata and readable SQL separately on your engine, driver and TLS path.
Investigation handoff	Follow the identity into scoped statements. With Oversight, inspect the finding, alert review outcome and a CSV or Parquet export.

Integration families: Java, Node.js, Python and .NET.
Available user, application, tenant, environment and client-IP context depends on the runtime, adapter and source supplied by the application.

Sammy supports the review: explain selected SQL or examine available risk context. The analyst retains the decision.

Plan an attribution evaluation at nanori.ai/request-demo