DATABASE ACTIVITY. IDENTITY. RISK.

From a database statement to an informed decision.

Nanori combines captured activity, available application identity and risk context in a single investigation environment.



Trace adds application-user context. Lens captures at the database.
Oversight connects users, applications, database accounts and tables in Flow.

ATTRIBUTE

Trace

Available application identity carried with SQL. Optional with Nanori.

CAPTURE

Lens

Database-host capture. Sends observed activity to Oversight.

INVESTIGATE

Oversight

Events, Flow, risk, sensitive data, audit policy and Sammy.

01 / RISK AND IDENTITY

What deserves a closer look?

Risk combines observable behavior with identity, history and policy. Findings guide review; they are not a verdict of compromise.

SIGNAL FAMILY	REPRESENTATIVE BEHAVIOR	CONTEXT TO CHECK
Identity and access	Interactive use of a service account; unexpected source; protected account without an application user.	Identity source, attribution coverage, database credential and application tier.
Extraction	Hourly or gradual extraction; sensitive-data extraction; bulk dump patterns.	Measured rows or bytes, analysis window, affected tables and available history.
New behavior	First sensitive-data access; new database, host, tool or operation; unusual hours.	Whether the profile has learned enough activity to make a useful comparison.
Volume and peers	Activity above usual or peer ranges; gradual increase; unusually broad table access.	User baseline, peer context and the scope of observed activity.
Critical sequences	Privilege grant followed by sensitive access; dormant account active on sensitive data; audit tampering.	Linked statements, ordering, access context and legitimate change activity.
Errors and authentication	Failed-login or statement-error spikes; failed logins followed by success.	Protocol visibility and the events actually captured on the connection path.

THREE ALERT PATHS

Corroborated behavior

Score-based alerts use evidence across behavior families.

Policy violation

A protected account without application identity has its own alert path.

Critical sequence

Defined tripwire behavior has a direct alert path.

Review control. New, Acknowledged, In review and Closed states support investigation; closure records a confirmed or benign outcome. Eligible normal behavior can be approved temporarily and later revoked.

02 / EVIDENCE AND POLICY

What can an investigation retain?

Capture coverage and policy determine which questions can be answered later.

EVIDENCE	AVAILABLE CONTEXT / INTERPRETATION
Statement and access	SQL, operation, database, tables, time, duration and captured errors. Parsed fields depend on the engine and capture path.
Identity and connection	Application identity when supplied; original database account, source, client and available encryption context. Declared identity is distinct from authentication.
Volume and response	Measured rows and bytes. Row counts can be available without full response capture when the protocol provides an unambiguous count. Unmeasured counts remain unknown.

AUDIT ACTIONS

ACTION	WHAT REMAINS	INVESTIGATION CONSEQUENCE
Keep full	Statement text and captured detail.	Supports statement-level review.
Summary	Counts, identity and duration.	No statement text to reconstruct.
Ignore	Activity is counted, not stored.	No retained event detail to inspect.

Rule selection: criteria include database, table, operation, who, sensitive data and where. The most specific matching rule selects the action; equal specificity favors retaining more.

Retention: 1-3650 days per rule, or inherit the default. Full-detail events can be held until manually purged. The longest applicable retention wins; the fallback covers unmatched activity.

Sensitive data and egress

Classify from observed column names and values; review certainty and readers. Confirm or dismiss classifications. This reflects observed traffic, not a scan of every stored value.

Examine returned data by database user, application user, application or confirmed data class. Export scoped Events as CSV or typed, compressed Parquet; export timestamps use UTC.

03 / ANALYST ASSISTANCE

Sammy. On your side. The decision stays with you.

An AI companion in Oversight that helps reduce navigation and query-review work while keeping actions under analyst control.

Ask a question. Review the proposal. Choose the next action.

FIND THE ACTIVITY

“Show me activity for this user.”

Sammy proposes Events filters. Review the filter chips and choose Search; it does not run the search on its own.

UNDERSTAND THE STATEMENT

“What does this query do?”

Explain selected SQL, including recorded truncation. Sammy does not execute the statement or inspect its returned results.

EXAMINE IDENTITY RISK

“Why does this identity need review?”

Use the risk context and linked findings available in Oversight. Check them against scoped activity and baseline readiness.

REFINE AUDIT POLICY

“Help me draft a rule.”

Load a proposed change into the editor and preview its impact. An administrator saves the change; that save is audited.

Operational control. Sammy runs on the appliance and can be disabled by an administrator. How-to answers reference product help. Example questions above describe supported tasks, not captured conversation output.

04 / DATABASE COVERAGE

Database engines and connection coverage.

Lens captures at the database host. Support varies by engine, version and encryption path; these distinctions matter when evaluating a deployment.

DATABASE	VERSIONS	UNENCRYPTED	ENCRYPTED
PostgreSQL	13, 14, 15, 16, 17, 18	Supported	Supported
Citus	13	Supported	Supported
MySQL	5.7, 8.0, 8.4	Supported	8.0 / 8.4 supported; 5.7 not supported
MariaDB	10.6, 10.11, 11.8	Supported	Supported
Percona Server for MySQL	8.0, 8.4	Supported	Supported
SQL Server on Linux	2017, 2019, 2022	Supported	Supported
CockroachDB	25.2	Supported	Not supported
TiDB	8.5	Supported	Not supported
AlloyDB Omni	16	Supported	Not supported
Oracle Database	19c, 23ai / 26ai	Supported	Limited
MongoDB	6.0, 7.0, 8.0	Limited	Limited

Oracle encryption: NNE/TCPS statement capture uses optional in-process capture, off by default. Database identity, reply-derived fields and bound values are limited. This capability requires separate evaluation and legal review.

MongoDB: limited coverage; validate command completeness and field visibility on the intended workload. **Other versions:** do not infer coverage from protocol compatibility. YugabyteDB is not yet validated.

Legacy versions: PostgreSQL 13, MySQL 5.7/8.0 and MariaDB 10.6 are listed by the product guide as best-effort versions. Confirm the applicable release matrix and support terms before deployment.

05 / INTEGRATION AND EVALUATION

Start at the application. Verify the complete path.

Trace adds application context. Lens and Oversight operate together for capture and investigation. Trace can also work independently with compatible monitoring.

TRACE RUNTIME	INTEGRATION APPROACH	REPRESENTATIVE DRIVERS
Java	JVM agent, JDBC and supported request contexts.	pgjdbc, MySQL, MariaDB, Microsoft JDBC, Oracle JDBC.
Node.js	Process bootstrap and request-context capture.	pg, mysql2, mariadb, mssql, oracledb.
Python	Auto-attach or library integration; supported WSGI/ASGI paths.	psycopg, asyncpg, PyMySQL, mariadb, pyodbc, oracledb.
.NET	CLR profiler; .NET Framework and modern .NET.	Provider-specific; confirm the release matrix.

DEFINE THE EVALUATION

Identity continuity

Check the identity source, runtime, driver and request isolation. A shared database account must not collapse distinct application users into one identity.

Capture and encryption

Verify the database-host OS and architecture, engine/version, TLS path and required fields. Encryption metadata and readable statement text are separate checks.

Evidence and capacity

Choose response detail and retention for the investigation you need. Measure field completeness, host overhead and storage on the intended workload.

Transport to Oversight

Strict ingest requires an appliance-issued client certificate by default. Assess any permissive configuration against the network trust boundary.

Define your evaluation at nanori.ai/request-demo