

SPICEDB ENTERPRISE

Five things the engine does not give you.

SpiceDB open source is a production-grade authorization engine, and plenty of teams run it successfully. These five capabilities are what a commercial licence adds around it — what gets recorded, who is told first, what each service may do, how often, and who you call.

1**Audit logging****2****Security embargo****3****Restricted API
access****4****Rate limiting****5****A support
relationship**

Who checked what, and what you told them

Every API operation published to a log sink you own, with the request, the response and the credential that made the call.

WHAT IS CAPTURED

Request and response

Token hash, method, request body, request IP, response body and any errors — including the permission decision itself.

WHERE IT GOES

A sink you control

AWS Kinesis, Kinesis Firehose or GCP Pub/Sub, in your own account. Configured by flags on the binary you already run.

BUILT FOR THE HOT PATH

Buffered and batched

Asynchronous buffer, batched delivery, worker pool and jittered retry backoff, so logging cannot become its own outage.

IN OPEN SOURCE

No audit logging of any kind. Metrics, traces and the Watch API exist, but none records who asked a question or what they were told — and a denied request leaves no trace at all.

WHAT IT MEANS IN PRACTICE

“Who could reach this record last quarter?” has an answer you can query, rather than a report somebody reconstructs and hopes is right.

You hear before the world does

A defined process under which issues are privately reported, analysed, notified and resolved — before anything is published.

PRIVATE NOTICE

Told once verified

Notice comes after a report is confirmed and a timeline agreed, not when the advisory appears in a public feed.

A WINDOW

Time to act deliberately

Assess applicability, plan the upgrade, test it, brief your security team — or accept the risk on the record.

INFLUENCE

Publication waits on participants

Absent a strict reporter deadline, an issue goes public once affected customers have resolved it or accepted the risk.

IN OPEN SOURCE

Advisories are published openly to GitHub, NVD and the MITRE CVE list, and the fix is available to everyone. That publication is also the first notice open-source users receive.

WHAT IT MEANS IN PRACTICE

The same vulnerability is an upgrade ticket on a Tuesday afternoon, or an incident read from a public feed at the same moment attackers read it.

Least privilege for the services that call you

Service accounts, tokens, roles and policies — the IAM model your team already uses, applied to SpiceDB itself.

DEFAULT DENY

No access until granted

A new service account can do nothing until a role is bound to it. Access is deliberately granted, not remembered to be removed.

REQUEST-TIME RULES

Method plus a condition

A role grants named API methods, optionally narrowed by a CEL expression evaluated against the actual request payload.

SAFE ROTATION

Many tokens per account

Deploy a new token before deprovisioning the old one, so credential rotation stops being a cutover with a window of risk.

IN OPEN SOURCE

One bearer token with full authority. A credential that can run CheckPermission can equally run WriteSchema and DeleteRelationships. Narrowing it means building a proxy.

WHAT IT MEANS IN PRACTICE

A reporting service that can genuinely never write, an importer limited to one resource type, and an integration that can add access but never remove it.

One service's bad day stays its own

Distributed rate limiting with flexible matching and custom bucketing, configured in YAML rather than in code.

MATCHING

Which requests a rule covers

By endpoint, service account, role, header, or a custom CEL expression — so a rule can be broad or very specific.

BUCKETING

Whose budget it draws from

Per service account, per token, per header or custom logic, so each workload gets an independent allowance.

COORDINATION

The limit holds as you scale

Coordinated across replicas, so 500 means 500 whether you run six replicas or sixty — with graceful degradation if coordination drops.

IN OPEN SOURCE

No rate limiting. A retry storm, a batch job that grew, or a loop shipped on a Friday raises latency for every service sharing the deployment.

WHAT IT MEANS IN PRACTICE

A misbehaving caller hits its own limit and gets a ticket, instead of degrading the one dependency every other service shares.

The team that builds it, on your side of the table

A commercial licence establishes a working relationship with the people who design and maintain SpiceDB.

EXPERTISE

People who know the model

Help from people who understand SpiceDB, relationship-based access control, and the decisions that shape production systems.

TIMING

Guidance before it is expensive

Schema design, permission models, consistency requirements and deployment architecture — while those choices are still cheap to change.

COMMITMENT

A defined escalation path

Contracted support, escalation routes and response-time commitments appropriate to your agreement.

IN OPEN SOURCE

Community troubleshooting, and whatever expertise you build and retain internally. Workable for many teams — and entirely yours to resource.

WHAT IT MEANS IN PRACTICE

A permission model that fits your first product rarely survives the second unchanged. Expertise is most valuable before that complexity compounds.

IN SUMMARY

The engine is the same. What surrounds it is not.

Each of these is a question a security review, an auditor or an incident will eventually ask. Enterprise is where the answers come from.

- | | | |
|---|-------------------------------|--|
| 1 | Audit logging | What did we decide, for whom, and when? |
| 2 | Security embargo | When do we find out about a vulnerability? |
| 3 | Restricted API access | What is each service actually permitted to do? |
| 4 | Rate limiting | What happens when one caller misbehaves? |
| 5 | A support relationship | Who do we call, and how fast do they answer? |