DATASHEET | JUPITERONE CONTINUOUS CONTROLS MONITORING

Make compliance a queryable layer of your security stack.

Controls as code, evidence as data, compliance as a query on your graph.

THE PAIN

Most compliance tools were built for auditors, not architects. They ingest screenshots, store evidence in their own silo, and produce a separate posture model that doesn't map to anything else you run. Your team ends up rebuilding the same control logic three times — once in the GRC platform, once in the detection platform, once in your detection-as-code repo. When an auditor asks what was true on a given day, you stitch together exports. When the CISO asks what's drifting, you can't answer in the same place you answer everything else.

THE FIX

JupiterOne CCM runs your control program against the same security graph your architects already query — assets, identities, vulnerabilities, configurations, and relationships in one queryable data model. Controls are J1QL queries against the live graph, with a UI for the compliance team. JupiterOne AI translates plain-English requirements into J1QL with auditable reasoning. Lifecycle governance (Draft → Review → Live → Retired) keeps untested logic out of production posture. Every control run generates tamper-evident, time-indexed evidence — queryable, exportable, tied to the same entities your detections and dashboards already use.

01

Graph-native control model

Controls run against the same J1QL graph as your asset, vulnerability, and exposure data — no parallel data model, no separate ingestion, no reconciliation. The control that says "every prod workload encrypted with a CMK" is the same query your architects and engineers already write.

02

AI-assisted authoring, full J1QL power

JupiterOne AI generates control descriptions, severity, remediation steps, and J1QL from plain English — grounded in your linked requirements. UI for the compliance team, J1QL and Boolean composition for your architects. Author once, reuse across frameworks, version everything.

03

Closed-loop automation

Live control failures route to the owning team via Jira, ServiceNow, or Slack with AI-generated remediation steps tied to the specific control. Saved queries become alerts, dashboards, and controls — one definition of "what should be true," monitored continuously, wired into your existing stack.

200+ INTEGRATIONS · CLOUD, CODE, IDENTITY, ENDPOINTS, SAAS & SECURITY TOOLING

INFRA: AWS | Azure | GCP | Kubernetes | Okta | Entra | GitHub | GitLab | Snowflake | CrowdStrike | Wiz | Splunk | Jira | ServiceNow

FRAMEWORKS: CIS AWS | CIS M365 | CIS GitHub | CIS GCP | SOC 2 | ISO 27001 | NIST CSF 2.0 | DORA | HIPAA | PCI-DSS | Custom

EXAMPLE QUERY

```
FIND aws_s3_bucket WITH encrypted != true AND public = true THAT RELATES TO aws_account RETURN
bucket.name, bucket.region, account.name // powers a control, an alert, and a dashboard
```

One graph. One language. One source of truth.

JupiterOne CCM sits on the same security graph as your asset, vulnerability, and exposure programs — so your architects and engineers stop rebuilding and start reusing.

BUILT ON THE GRAPH YOUR ARCHITECTS ALREADY USE

One data model, every control

Controls evaluate J1QL against the same asset, identity, and vulnerability graph that powers your exposure programs. No duplicate ingestion, no parallel control DB.

J1QL native — with a UI on top

Author in plain English, the UI form builder, or J1QL directly. Reuse the same query as a control, an alert, and a dashboard. One source of truth.

Lifecycle governance: Draft → Review → Live

Only Live controls affect posture. Full audit trail on every state transition. Built-in review workflow before anything lands in production compliance.

Integration-aware control evaluation

Automatic detection of which integrations each control depends on. Ineligible tests hide by default. Non-effective controls flag the moment data goes missing.

FIG. CONTROL + QUERY · ONE GRAPH, TWO VIEWS

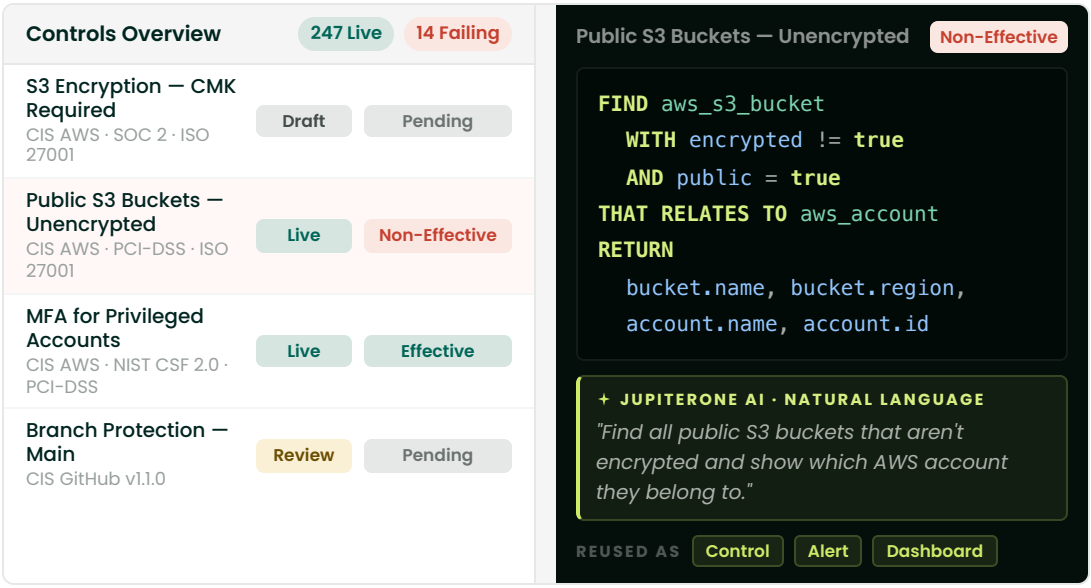

Fig. The same J1QL query powers your control, your alert, and your dashboard. Author once, monitor continuously, prove it on demand.

EVIDENCE, AUTOMATION, AND A CLOSED LOOP

Tamper-evident evidence as data, not screenshots

Every control run generates time-indexed, queryable evidence with 365-day retention. Answer "what was true on Aug 14" with a query. Pipe to your data lake via API or webhook.

Real-time framework rollups, exposed as API

Effectiveness at every level — test, control, requirement, framework — updated continuously. Pull posture into existing exec dashboards without a second login.

AI-generated remediation, routed to the owner

When a control fails, JupiterOne AI generates remediation steps tied to that control's objective. Tasks route via Jira, ServiceNow, or Slack automatically.

Pre-built libraries + custom frameworks

CIS AWS / M365 / GitHub / GCP, SOC 2, ISO 27001, NIST CSF 2.0, DORA, PCI-DSS — plus full UI and API support for proprietary frameworks.

ABOUT JUPITERONE

JupiterOne is the AI Risk Management Platform for security teams in highly regulated industries. Built on a graph-native data model with 200+ integrations, it continuously discovers assets, maps relationships, and monitors controls — so teams understand risk, blast radius, and what to prioritize in seconds, at enterprise scale.

WHAT CUSTOMERS SAY

"We stopped maintaining a separate GRC data model the day we moved CCM onto JupiterOne. Our compliance controls and our detections now share the same J1QL — one source of truth, one place to debug drift. The auditor gets a clean export; the team gets back its weekends."

— Principal Security Architect
Cloud-native enterprise SaaS

200+
integrations evaluated by your control library out of the box

365
days queryable, tamper-evident evidence — no screenshots, no spreadsheets

1 query
defines a control, an alert, and a dashboard in JupiterOne

jupiterone.com →