The Axonius → JupiterOne switching kit

Exactly what a migration involves, how long it takes, and how to run both platforms side by side — so the decision is based on your data, not our slides.

Who this is for. Security teams running Axonius for asset management who are re-evaluating — at renewal, after a pricing conversation about separate exposure management, or because they need answers an inventory can't give.

THE SHORT VERSION

- **It's integration reconfiguration, not data migration.** Your asset data lives in your tools — cloud providers, identity, EDR, scanners. JupiterOne connects to the same sources via API. Nothing gets exported from Axonius.
- **Most integrations connect in hours.** A typical enterprise runs a 30-day parallel period and cuts over inside a quarter. A recent enterprise replacement went from first conversation to enterprise-wide cutover in under five months, with a 4-week evaluation.
- **You don't lose your queries — you upgrade them.** Anything you ask Axonius, you can ask JupiterOne. The reverse isn't true: blast radius, attack paths, and privileged access to sensitive data require a graph.

PHASE 1 · WEEK 0–1

Map your integrations

Inventory your Axonius adapters and map them to JupiterOne's 200+ native integrations. Common mappings:

YOUR SOURCE	AXONIUS ADAPTER	JUPITERONE INTEGRATION
AWS / Azure / GCP	Cloud adapters	Native — full resource graph, not just instances
Okta / Entra ID	Identity adapters	Native — users, groups, apps, MFA state as graph nodes
CrowdStrike / SentinelOne / Defender	EDR adapters	Native — agent coverage mapped to hosts
Jamf / Intune	MDM adapters	Native
Tenable / Qualys / Rapid7	VA adapters	Native — findings land in Unified Vulnerability Management
GitHub / GitLab / Bitbucket	Limited	Native — repos, PRs, code scanning as first-class assets
ServiceNow / Jira	CMDB / ITSM adapters	Native — bi-directional (tickets out, context in)
Custom / homegrown	CSV / custom adapters	Custom integrations via SDK + API

Gap check: if an adapter has no J1 equivalent, flag it in week 0 — not month 3. Ask us directly; the integration catalog is public at jupiterone.com/integrations.

PHASE 2 · DAYS 1–30

Parallel run

Connect your top 5–8 sources to JupiterOne while Axonius keeps running. Nothing changes in production; this is read-only API access.

WEEK 1 **Coverage parity.** Compare total asset counts and dedup quality side by side. Expect counts to differ — the review question is *why* (J1 models relationships and ephemeral cloud resources that inventories flatten).

WEEK 2 **Run your real questions.** Take your top 10 Axonius saved queries and run the equivalents in J1QL or plain English via JupiterOne AI. Then run the four queries an inventory can't do:

1. Which cloud workloads have privileged access to our most sensitive data?
2. If this identity is compromised, what's the blast radius?
3. Which internet-facing assets are missing EDR?
4. Which controls are passing against live data right now?

WEEK 3 **Workflows.** Wire one alert rule, one dashboard, and one ticket-routing workflow to prove operational fit for the SOC.

WEEK 4 **Decision review.** Score against your success criteria (template below). Bring your internal audit or compliance team in this week — controls-as-code is usually the tiebreaker.

PHASE 3 · DAYS 30–90

Cutover

1. Recreate remaining saved queries, alert rules, and reports. A query translation working session is part of onboarding.
2. Repoint downstream consumers — ticketing, SIEM enrichment, compliance reporting — to JupiterOne.
3. Freeze Axonius changes; run one final side-by-side validation week.
4. Decommission at your renewal date. Timing the cutover to renewal is the norm; your TAM's guided cutover plan covers the sequencing.

Success criteria template

CRITERION	TARGET	RESULT
Source coverage vs. incumbent	≥ parity on shared sources	
Dedup / unification quality on devices	Spot-check 25 devices, ≥95% correctly unified	
Top-10 saved queries reproduced	10/10	
Relationship queries (the four above)	All answerable in seconds	
Time-to-answer, ad-hoc investigation	Minutes, not hours	
One compliance framework mapped with live evidence	Yes / No	
SOC workflow (alert → ticket with context)	Working end-to-end	

What to expect commercially

One platform, one contract: asset management, Vulnerability & Exposure Management, and Continuous Controls Monitoring included — exposure management is not a separate SKU. Enterprise agreements include a fair asset-growth buffer, so discovery finding more assets doesn't trigger surprise true-ups. Ask about first-year opt-out terms if you need to de-risk a multi-year commitment.

FAQs

Do we need to export anything from Axonius?

No. JupiterOne connects to your original sources directly.

Will we lose history?

Historical trending starts at connection. Most teams run the 30-day overlap precisely so reporting continuity is unbroken at cutover.

Do we need agents?

No — API-based, agent-free.

What about our custom adapters?

The JupiterOne SDK and API support custom integrations; scope these in Phase 1.

Who runs the migration?

Your team, guided. Enterprise onboarding includes a named TAM, integration working sessions, and a cutover plan.