

OcientAIQ for Lawful Disclosure and Compliance

Every record retained. Every response bounded. Every disclosure defensible.

The Problem

Lawful disclosure teams are asked to respond quickly and defensibly to warrants, subpoenas, court orders, emergency requests, and audits — but the records needed to answer them often span CDR, ICR/IPDR, signaling, messaging, location, subscriber identity, and case systems. When those records sit in fragmented stores with different retention windows and access paths, a tower dump or subscriber query can become a manual engineering event. The pressure shows up in three places:

Fragmented records

Disclosure data spans multiple systems, retention windows, and access paths.

Manual response

Tower dumps and subscriber queries become engineering tickets, not governed workflows.

Hard-to-prove outputs

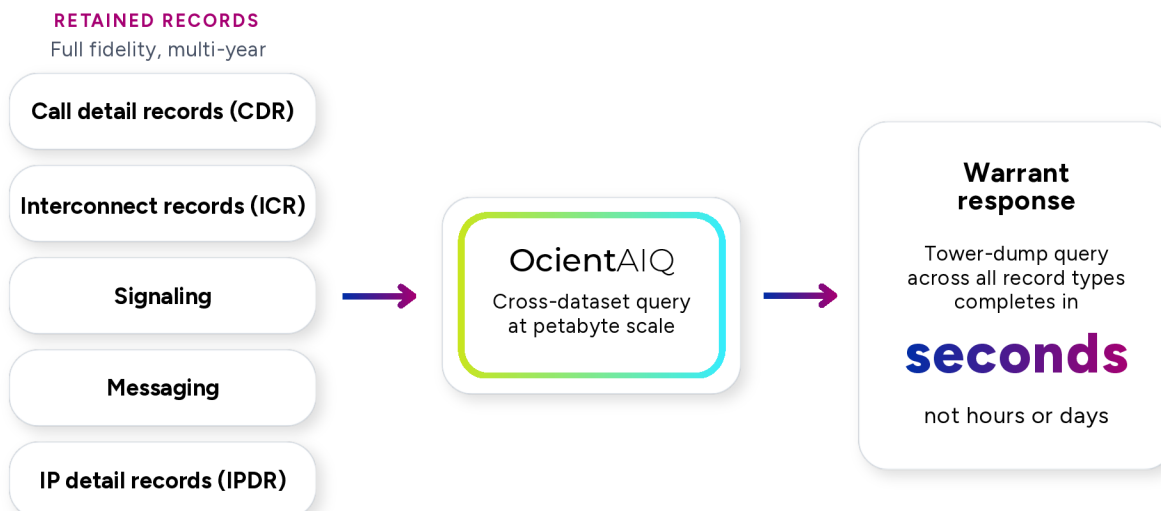
Sampling, cold-tier retrieval, and incomplete lineage make responses harder to defend.

The Solution

OcientAIQ™ gives lawful disclosure teams one place to retain, search, and produce disclosure-relevant records at carrier scale. CDR, ICR/IPDR, signaling, messaging, location, and subscriber context are retained at full fidelity, joined on demand, and returned only within the scope of the request.

The output is not just a faster result: it's a defensible response package that includes the records returned, the request parameters that bounded them, the query path that produced them, and lineage back to the source records.

From request to defensible response



How OcientAIQ Builds the Response Package

Retain every relevant record.

Keep CDR, ICR/IPDR, signaling, messaging, location, and subscriber context at full fidelity for the mandated window.

Bound every query to the request.

Search by authority, time window, geography, subscriber, device, tower, or identifier — and return only what the request allows.

Join across systems and identifiers.

Resolve records across fragmented network, subscriber, device, and case systems without a manual engineering project.

Trace every result to source.

Attach lineage from each disclosed record back to the retained source rows that produced it.

Audit every access and output.

Log who searched, what parameters were used, what records were returned, and when the response was produced.

Produce evidence-ready responses.

Deliver a package built for counsel, regulator review, internal audit, or downstream case-management workflows.

What Makes OcientAIQ Different

Disclosure-grade fidelity. OcientAIQ works from the retained full-fidelity record set, not sampled data, summarized extracts, or manually rebuilt histories.

Fits the lawful-disclosure estate. OcientAIQ supports existing administration, mediation, handover, and case-management systems; it does not replace them.

Retention economics that scale. Capacity pricing lets compliance teams search across the retained window without creating a new cost event every time a request arrives.

One foundation. Six solutions. CDR already retained for compliance or fraud? Revenue assurance lands at a fraction of the marginal cost.

Proof in Production

Reducing a tower dump query from minutes to seconds

A global CSP needed to respond to tower dump requests across its retained CDR record set without routing each request through a slow engineering process. With OcientAIQ™, the operator was able to query the full-population dataset directly and produce results in seconds — at lower cost than the prior CDR retention environment.

41 minutes → 16 seconds

Tower dump query time reduced on a full-population dataset.

~80% cost reduction

Lower cost versus the prior CDR retention infrastructure.

Ready to close the gaps?

✉ sales@ocient.com 🌐 ocient.com

© Ocient 2026