REALM. SECURITY

SOLUTION BRIEF

REALM DATA HAVEN

Keep your entire security data history. Get the answers you need from it, fast.

Data Haven is the searchable retention layer of the Realm Platform. It keeps an immutable raw copy of all your security data, with OCSF-normalized observables attached to each event. When an investigation, incident, or audit calls for it, you search your full history directly and resupply the exact events you need to any destination.

The problem: stored is not the same as usable

Security data has outgrown SOC budgets. Because the SIEM commonly charges by ingest, teams offload the telemetry that is not detection-relevant into cheaper storage to keep SIEM noise and cost down. That move solves one problem and creates another: the offloaded data lands in mixed schemas, across separate tiers, and behind cross-team access requests, so it is hard to use in the moment that matters.

When an investigation needs older data, the team struggles to find it, so they pull back a wide, coarse range from their archive. They pay to bring back far more than they need, wait for it to land, then search the raw result by hand for the few records that count. Worse, some of the data they go looking for may have been filtered out to control cost and was never kept at all. As data volumes climb year over year, the gap between what is stored and what is usable only widens.

Direct search and targeted resupply

Data Haven keeps your entire security history and lets you search it directly on OCSF-normalized observables, then resupply only the exact events you need. **Years of retained data, ready to work for investigations, forensics, incident response, and compliance, without the coarse restore-and-dig step**.

How it works

01 STORE

All your sources (firewall, EDR, cloud + identity, custom apps) routed automatically. Data Haven keeps an immutable raw copy with OCSF observables on every event.

02 SEARCH

Search your full history in place, no rebuild. Example:

```
src_ip =
203.0.113.44 → 1,284
exact events in 0.4s
```

03 RESUPPLY

Only those events, to the SIEM or any destination. No coarse restore, no dig.

Every connected source is retained automatically. Search on the observables your SOC already works in, then resupply the exact events to the destination you choose.

WHERE DATA HAVEN ADDS VALUE

Security investigation

Chase an observable across months of history, no coarse restore, no manual dig.

Incident response

Pull the exact events in the moment, not after a rebuild, speeding up MTTR.

Forensic analysis

An immutable raw copy keeps the full event timeline intact and attestable.

Compliance and audit

Search for and export the exact records an auditor asks for, on demand.

What you get

Complete, automatic retention

- **Nothing dropped, nothing to configure.** Every connected source is retained automatically: your original logs, complete, with OCSF observables added for search. No per-source setup, no sampling, no cost-filtered gaps: a complete, audit-ready record in one place.

Direct search and targeted resupply

- **Find the exact events needed.** Search your full history in place with the observables your SOC already works in, no rebuild first. Pinpoint the exact events across sources and resupply only those, to any destination, not just back to the SIEM.

Control and ownership

- **Your data, open format, no limits.** Your data stays in an open, portable format with no storage cap, priced by ingest at a fraction of SIEM rates and never by use. Search as much as an investigation needs, keep history as long as you must, and run no infrastructure to do it.

Keeping your data is not the same as using it

A SIEM archive tier and a general-purpose data lake can both store your security data, but the data is difficult to access and expensive to search. **Only Data Haven keeps all of it and makes it usable the moment you need it**: captured automatically and complete, searchable directly in seconds, and yours to query and move freely without per-query charges. Detection, correlation, and alerting stay in your SIEM, and there is nothing to build or operate. When an investigation needs older data, it is already there and ready to retrieve.

Prove it on your data

Start with a 7-Day Data Assessment. We show the reduction and complete retention on your data.

Request a demo → realm.security

ABOUT REALM SECURITY

Realm Security gives security teams independent control over their telemetry before it reaches the SIEM, data lake, or AI agent. The platform understands what each source produces and what each downstream system needs, then guides teams on what to retain, cut, and route. Headquartered in Boston, Realm deploys in about a week and typically cuts SIEM ingestion costs by 50% or more.

REALM. SECURITY

The SOC-aware security data pipeline.

www.realm.security

LinkedIn: /company/realm-security

X: @Realm_Security

© 2026 Realm Security, Inc. All rights reserved.