EXECUTIVE OVERVIEW

CUT SIEM COST, KEEP EVERY DETECTION

The SOC-aware security data pipeline.

Realm gives your SOC data it can trust, at a cost it can afford. It sits between your sources and your destinations, so your team decides what to keep, cut, enrich, and route, and proves coverage held on your own data. No data engineers required.

This is a short overview of who we are, how the platform works, and what teams find when they test it on their own data.

The challenges we solve

Log volume keeps climbing while budgets do not. The result is a constant tradeoff between visibility, cost, and control, and it shows up in four ways.

Rising costs.
SIEM ingest pricing penalizes data growth, forcing teams to choose between visibility and budget.

Data silos.
Security data is locked inside each tool, with no portability and no unified view across the stack.

Vendor lock-in.
Proprietary query languages and formats hand your SIEM vendor the leverage. Switching means rebuilding years of work.

SOC stagnation.
New tools need new data formats. Without control of your data, adopting new technology becomes impractical.

Who we are

Realm's founders have spent two decades building endpoint and detection products at enterprise scale, across Cisco, Carbon Black, Rapid7, and VMware. Pete Martin, Jeff Kraemer, and Sanket Choksey previously built Confer together, an event-stream processing platform that handled 50 million events per second before it was acquired by Carbon Black.

They started Realm because the same problem kept surfacing in every SOC they worked with: security data volume was outgrowing every team's ability to manage it, the bill was climbing with it, and the tools meant to help had been built for IT engineers rather than the security team that owns the outcome.

Realm has raised roughly $22M: a seed round co-led by Accomplice and Glasswing Ventures, a Series A led by Jump Capital, and a strategic investment from Presidio Ventures, the corporate venture arm of Sumitomo Corporation.

How we engage

SOC 2 Type II, with a live Trust Center at trust.realmsec.info

Open formats and no lock-in. Switch or consolidate tools without re-instrumenting

Fully managed. Realm runs the pipeline for you, with no professional-services engagement to buy and no data engineers to hire

What Realm does

The Realm Platform sits between your sources and your destinations and gives your SOC full control of its telemetry: what to keep, what context to add, what to mask, and what shape it arrives in. Connect any source, send to any destination, and control what happens to the data in between. The Platform reduces, enriches, redacts, and transforms your data on rules your team sets and approves, with the reasoning shown and the impact proven on your own data before anything ships.

Know what matters

See and understand your own data without being a log expert. Every recommendation from Realm Clarity AI shows its reasoning and a match rate, and it runs passively until your team approves it. Nothing changes in production that you did not sign off on.

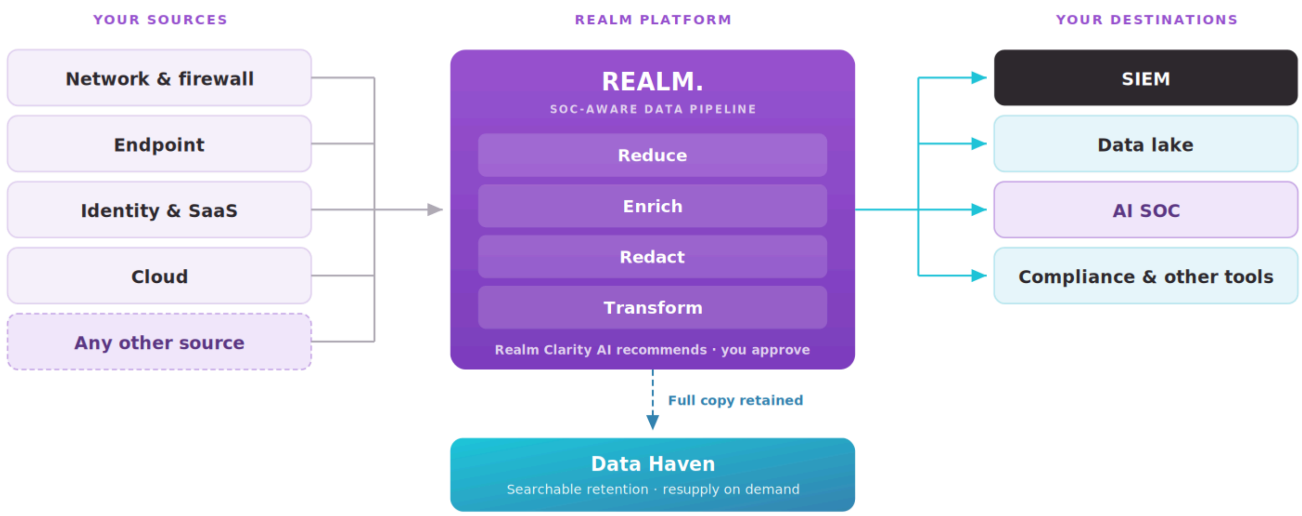
Control without complexity

Your SecOps team owns the pipeline end to end through a no-code interface. Re-routing a source is a change, not a rebuild. There are no dedicated data engineers to hire and no IT tickets to wait on.

SOC-ready data

The data reaching every tool is complete, enriched, normalized, and compliant, ready for a SIEM, a data lake, or agentic SOC tooling. Detection-aware reduction protects your coverage, while in-stream discovery and redaction keep sensitive data out of places it should not go. Cutting cost never costs you a detection.

Where Realm sits in your security stack



Realm Platform components

Three components in one pipeline: the Platform executes, Clarity AI understands and recommends, and Data Haven retains everything while keeping it searchable.

PLATFORM The pipeline itself

Ingests any source over any supported transport, fully managed, then applies four controls before data reaches a destination. **Reduce** strips noisy, low-value telemetry: junk events, DNS noise, duplicates, verbose fields, for 50 to 80% lower ingestion volume. **Enrich** injects geo, ISP, and ASN context in stream, so analysts skip manual lookups mid-incident. **Redact** masks sensitive data in transit, mapped to HIPAA, PCI-DSS, GDPR, and CCPA, without altering schema, so parsers and detections keep working. **Transform** normalizes vendor formats into one schema and shapes the same source per destination: lean for the SIEM, context-rich for the lake.

REALM CLARITY AI The intelligence layer

Clarity AI analyzes your live data and proposes the reduction, redaction, and routing rules. Every recommendation is evidence-based, arrives with its reasoning and a match rate, and runs passively in a Pending state until your team activates it. AI you can preview, audit, and approve, not a black box.

> **Detection Integrity.** How Realm proves that cutting your SIEM log volume never costs you a detection. Realm reads every detection you run across Sigma, KQL, and SPL, protects the exact fields each one depends on, and flags anything it cannot safely protect instead of cutting it. You get a report, on your own data, showing what was reduced, what was protected, and that your MITRE ATT&CK coverage held. Realm never writes your detections. It protects the ones you already run.

DATA HAVEN The searchable retention layer

Every connected source routes to Data Haven automatically, a complete immutable raw copy with OCSF observables attached, nothing to configure. Search your full history by time range, source, or observable through a graphical query builder with no query language to learn, and resupply the exact events to your SIEM, data lake, or MDR when an investigation or audit calls for them.

What an evaluation looks like

Realm proves its value on your data rather than in a pitch. A proof of value runs about a week and asks very little of your team. You pick one source, usually firewall logs, and Realm handles the rest.

DAY 0	DAYS 1–2	DAYS 3–5	DAYS 5–7
Kickoff	**Connect**	**Analyze**	**Report**
Goals set, success criteria agreed, and one source chosen together.	One source connected, with no code and no engineering on your side.	Clarity AI returns recommendations, each with projected impact and its reasoning.	Reduction, detection integrity, and ROI, measured on your own environment.

A one-week proof of value shows what Realm reduces, what it preserves, and what it returns, before you commit to anything.

What it takes to run

After you sign, a dedicated Technical Account Manager takes you from deployment to production value in **30 days**, through a structured four-week program with a 60-minute weekly cadence. By the end, your own SOC runs the platform day to day. There is no professional services engagement to buy and no standing data-engineering headcount to fund. The ongoing relationship is periodic check-ins and quarterly reviews, not a team you have to keep staffed.

Proof, in production

USE CASE: COST CONTROL

Vensure Employer Solutions, **a 10,000+ employee benefits and payroll provider protecting millions of users' highly sensitive financial data.**

83%
reduction in daily firewall logs

$254K
in annual downstream savings

Zero
detection gaps, signal fully preserved

> *"This is a game-changer for budget-constrained security teams."*
> **Dwayne Smith, Sr. VP InfoSec & Global CISO, Vensure Employer Solutions**

USE CASE: SOC MODERNIZATION

A global 36,000-employee enterprise **running one of the largest Microsoft Sentinel deployments, modernizing a heavy, rule-bound SOC.**

3x
return per $1 spent on Realm

1,000+
KQL rules and DCR logic replaced in 72 hours

~50%
further volume cut beyond their existing reduction

Two very different problems, cost control and SOC modernization, solved by the Realm Platform.

A detailed technical mapping, showing how Realm meets each category a security data pipeline is evaluated on, is available from your Realm contact on request.

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