REALM. SECURITY

SOLUTION BRIEF

REALM DETECTION INTEGRITY

Cut your SIEM volume. Keep every detection.

Detection Integrity is how Realm proves that cutting your SIEM log volume never costs you a detection. It reads every detection you run, protects the exact data each one depends on, and shows you, on your own data, that coverage held while volume and cost dropped.

The problem: cutting blind is a gamble

SIEM ingest costs keep climbing, and the obvious lever is cutting log volume. But the SOC owns the detections running on those logs, and a blind cut can silently break one. Nothing fails at the moment of the cut. You find out later, when a detection you counted on does not fire during a real incident.

The stakes keep rising. As the SOC leans harder on AI, there are more detections, more automation, and more dependence on data being complete and trusted. The team has to take out cost without gambling coverage, and prove coverage held rather than hope it did.

Proof, not faith

Every pipeline can cut volume. Only Realm proves the cut did not cost you a detection. Each reduction is checked against your live detections first, the exact fields they depend on are protected, and everything else is retained in Data Haven, searchable and ready to resupply. **You get a report, on your own data, showing what was reduced, what was protected, and that coverage held.**

How it works

01 READ

Realm parses every detection you run and maps each one to the sources, fields, and MITRE tactics it depends on. Any detection in text form: Sigma, SPL, KQL, CQL, Sumo Logic, SentinelOne, Cortex XDR.

02 PROTECT

Before a source is reduced, the cut is validated against your live detections and the exact fields they need are protected. Example:

```
T1078 Valid Accounts → 4 fields protected, 2 sources
```

03 PROVE

A report you can see and share: every detection mapped to its protection rule or finding, percent volume saved, percent of logs protected, and your MITRE tactic coverage.

When a detection cannot be safely protected, Realm flags it as a finding instead of cutting. Realm Clarity AI does the analysis. You see the reasoning and make the call.

WHERE DETECTION INTEGRITY ADDS VALUE

Cutting the SIEM bill
Take ingest cost out of the SIEM without gambling detection coverage.

Proving coverage held
Hand leadership or an auditor the report: what was reduced, what was protected, and your MITRE coverage.

Weighing what detections cost
See the log volume behind each detection, so you know which are cheap to keep and which carry real weight.

Keeping protection current
Detections change. Re-run the analysis and Realm rebuilds the protection rules from your current set.

What you get

Reduction without the gamble

- **Checked against your live detections first.** Before Realm reduces a source, it validates the cut against the detections you actually run and protects the exact fields each one depends on. You get the cost cut you came for without gambling coverage, so the team can act instead of stalling.

Coverage you can see

- **Your detections, mapped to MITRE and to the data feeding them.** See your tactic coverage, whether a change touches it, and how much log volume each detection actually depends on. You answer questions most teams cannot today, with the numbers in front of you.

Validation without the grind

- **The check most teams go without.** Validating detections against reduction by hand is too slow to keep up, so it gets skipped and the cut happens on faith. Realm does it automatically across any detection in text form, so the rules protecting your coverage are reliable, not best-effort.

83% of firewall log volume cut. Zero detections lost.

Vensure Employer Solutions reduced FortiGate log volume by 83% and saved roughly $254,000 a year with no loss of detection coverage.

Dwayne Smith, Sr. VP InfoSec and Global CISO, Vensure Employer Solutions

Cutting volume is not the same as cutting it safely

Every pipeline can reduce your SIEM ingest. They do it with configured rules, and the coverage gap shows up later, when a detection fails to fire during a real incident. **Only Realm checks the cut against the detections you actually run**, protects the fields they depend on, and proves coverage held on your own data. Realm sits upstream. It does not write your detections or decide what is malicious. Your SIEM stays your SIEM, your detection engineering stays yours, and nothing changes until your team approves it.

Prove it on your data

Pick one source and start a 7-Day Data Assessment. We show the reduction and the detection integrity, 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