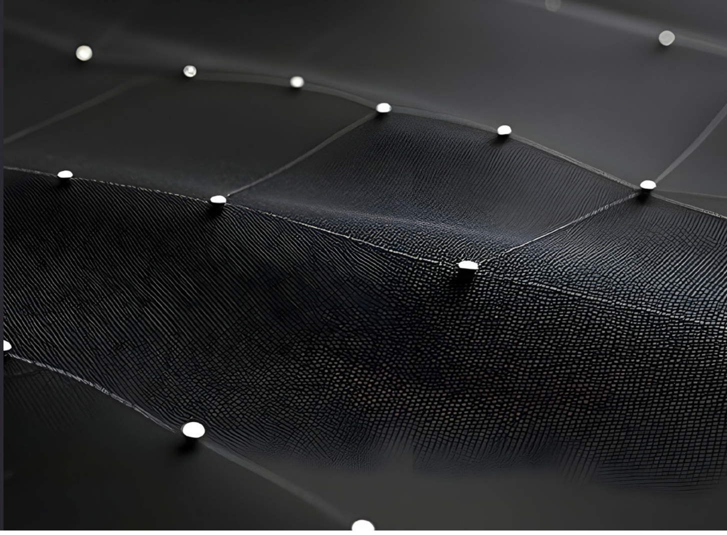
REALM.SECURITY



Customer Case Study

10,000+ Employee U.S.-Based Benefits & Payroll Provider

83% Log Reduction | $254k Annual Savings

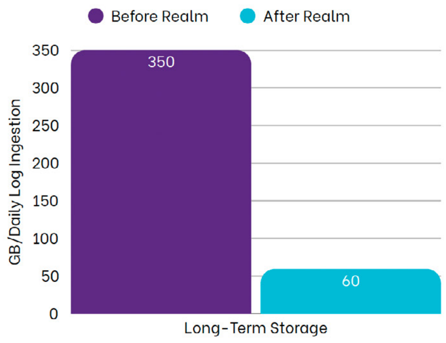
As a leading U.S.-based benefits and payroll provider, this organization operates a complex IT environment that protects millions of users' highly sensitive financial and personal data. Like many security programs, they faced the ongoing challenge of expanding their security telemetry footprint, adding firewall, network, endpoint, identity, and cloud log sources while adhering to the cost constraints of their SIEM.

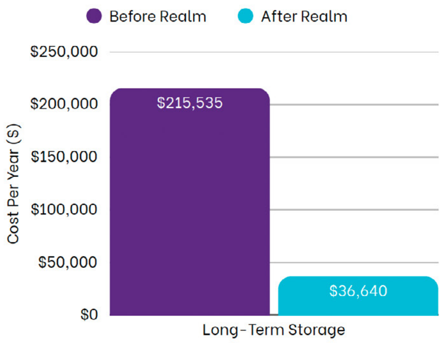
Not all logs deliver actionable security value. While the volume of raw telemetry grew, a large percentage of that data, routine firewall connection logs, redundant authentications, and benign system events, added minimal value to threat detection or investigations. Yet every byte of this non-relevant data was being ingested into their SIEM, driving up storage, compute, and licensing costs.

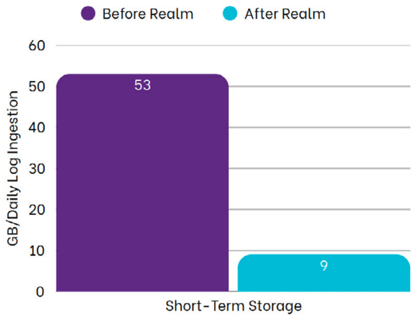
The security team recognized an opportunity: If they could intelligently filter non-security-relevant telemetry before ingesting it into their SIEM, they could control costs and free budget to invest in more strategic security priorities.

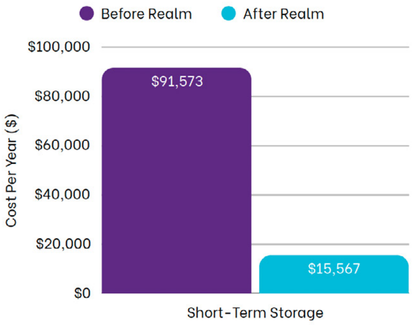
The Solution: AI-Native Security Data Pipeline Platform

The customer selected Realm.Security to directly address one of the most costly drivers of their SIEM spend: FortiGate firewall log volume.









Key Highlights

10,000+ Employees
Benefits & Payroll Provider

Source:
Fortigate Firewalls

Destination:
Sumo Logic

Key Results:
83% Log Reduction
$254k Annual Savings

"This is a game-changer for budget-constrained security teams."
- Global CISO

Web:
www.realm.security

Phone:
+1 (508) 314-1463

aws Google Cloud SOC 2 TYPE 2

Unlike legacy data pipelines, Realm.Security delivers security-specific filtering for Fortigate telemetry, enabling elimination of logs that provide no detection or investigative value, without risking visibility gaps.

- **Fortigate-Aware Filtering**: Realm's filtering algorithms are pre-tuned for Fortigate firewall logs, identifying routine connection events, permitted traffic logs, and redundant system messages that contribute heavily to SIEM storage costs but rarely support investigations.

- **Preserving High-Fidelity Signal**: Realm removes noise while ensuring critical threat indicators such as denied connections, unusual port activity, or policy violations remain fully ingested for correlation and response.

- **Easy to Deploy Filter Rules**: The security team easily pushed filtering rules into production using an intuitive no-code interface without involving complex engineering or risking pipeline errors.

- **Immediate Financial Impact**: Cost savings were realized as soon as Realm's filtering went live, eliminating waste before data reached the SIEM.

The Results: 83% Reduction in Daily Log Volume, $254K Annual Cost Savings

With Realm.Security deployed, the customer achieved immediate, quantifiable results, resulting in an annual cost savings of $254,901. By reducing daily Fortigate firewall logs by 83% while fully preserving relevant security signals, the customer unlocked significant ongoing budget relief, allowing the CISO to reinvest in higher-impact security initiatives.

> "Realm's Data Filtering module allows us to remove data that would never be needed for detection or an investigation. This saves us a significant amount of operational budget, which can be repurposed for other strategic priorities. This is a game-changer for budget-constrained security teams."
> - Global CISO at Leading U.S.-based Benefits and Payroll Provider

Looking Ahead: Building a Security Data Fabric for the Entire Telemetry Stack

Encouraged by the results of firewall log optimization, the customer plans to extend Realm.Security's filtering across additional log sources in their environment.

By centralizing control of its security telemetry, the customer is building a future-proof data architecture that eliminates telemetry waste, optimizes SIEM economics, and ensures complete, actionable visibility for its security operations team.