REALM. SECURITY

CUSTOMER STORY

Vensure cuts 83% of its log volume and keeps every detection intact

KEY CHALLENGE

Like many security programs, Vensure faced the ongoing challenge of expanding their security data footprint while adhering to the cost constraints of their SIEM.

KEY RESULT

83% Log Reduction. $254k Annual Savings. Critical threat indicators remain fully ingested for correlation and response.

VensureHR

Size: 10,000+ Employees

SIEM: Sumo Logic

Source: Fortigate Firewalls

Focus: Benefits & Payroll Provider

Not all logs deliver actionable security value.

As a leading U.S.-based benefits and payroll provider, Vensure Employer Solutions 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 data footprint, adding firewall, network, endpoint, identity, and cloud log sources while adhering to the cost constraints of their SIEM.

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.

OUTCOMES

83%
Log Reduction

$254k
Annual Savings

The security team recognized an opportunity: If they could intelligently reduce 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: The SOC-aware security data pipeline

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

Unlike legacy data pipelines, Realm understands what Fortigate logs contain. Realm Clarity AI reads the source, recommends what to reduce, and shows the projected impact, so logs that provide no detection or investigative value come out without risking visibility gaps.

Reduced data is not dropped. What Realm reduces out of the SIEM is retained as a complete, searchable copy, so the SOC can search its full history and resupply the exact events an investigation or audit needs. Realm calls this Data Haven.

"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."

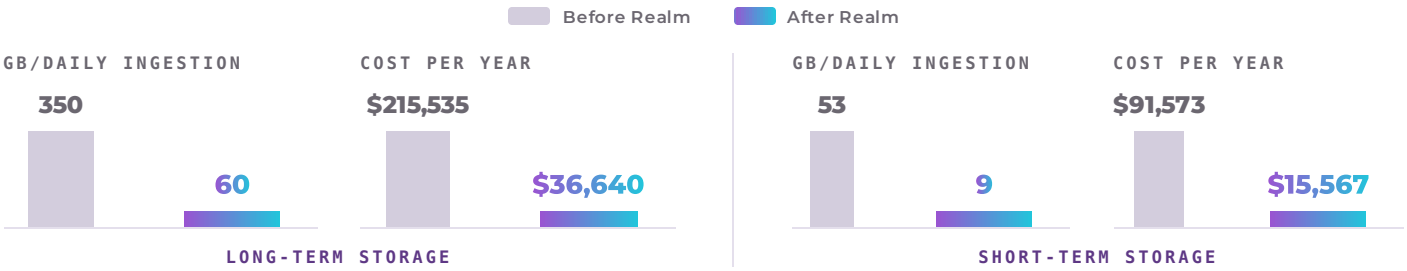
Dwayne Smith
Sr. VP Information Security & Global CISO, Vensure Employer Solutions

- **Trained on Fortigate**
  Clarity AI is trained on Fortigate, so Vensure had tailored reduction recommendations from day one: routine connection events, permitted traffic logs, and redundant system messages that contribute heavily to SIEM storage costs but rarely support investigations.
- **Recommended, Then Approved**
  Clarity AI analyzed their logs and detections, then recommended the rules. Each ran in a pending state against live data, so nothing changed until Vensure approved it.
- **Checked Against Their Detections**
  Before reducing the source, Realm checked the cut against the detections Vensure runs and protected the exact fields each one depends on. Denied connections, unusual port activity, and policy violations kept reaching the SIEM in full.
- **Immediate Financial Impact**
  Once the approved rules went live, cost savings were realized immediately, because reduction happens before data reached the SIEM.

The Results: 83% Log Reduction, $254K Annual Savings

With Realm deployed, Vensure achieved immediate, quantifiable results, resulting in an annual cost savings of $254,901. By reducing daily Fortigate firewall logs by 83% with coverage held, Vensure unlocked significant ongoing budget relief, allowing the CISO to reinvest in higher-impact security initiatives.

By the numbers



Looking Ahead: Full Control of Its Security Data, Source to Destination

Encouraged by the results of firewall log reduction, Vensure plans to apply the same approach to additional log sources across its environment.

By centralizing control of its security data, Vensure is building an architecture that cuts waste, keeps SIEM economics predictable, and gives its SOC complete, actionable visibility.

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.

Start an assessment → 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, route. Headquartered in Boston, Realm deploys in about a week and typically cuts SIEM ingestion costs by 50% or more.

REALM. SECURITY

www.realm.security
LinkedIn: /company/realm-security
X: @Realm_Security

© 2026 Realm Security, Inc. All rights reserved. All other brand names, product names, or trademarks belong to their respective owners.