How Revolution Medicines cut daily SIEM ingest 60% while its logs grew 700%

Revolution Medicines' logs were outgrowing its SIEM budget. Now Realm cuts what the SIEM doesn't need before ingest, without breaking a detection, and keeps the data clean for its SOC agents.

Key challenge

Log volume grew 700% in two years, and renewing the SIEM would have meant buying up to triple the capacity.

Key result

Realm cut daily SIEM ingest 60%, keeping a complete copy in Data Haven and freeing budget for other tools.

The company

Revolution Medicines

Biotechnology

SIEM: CrowdStrike Next-Gen SIEM

Sources: Zscaler, Microsoft Entra ID, and more

Focus: SIEM cost reduction

Pay for a bigger SIEM, or start dropping data.

Alec Lessard, Senior Security Engineer at Revolution Medicines, works hands-on across the security stack and helps run the SOC team. Log volume grew 700% in two years. Zscaler and Microsoft Entra ID were the sources he watched most closely.

When its CrowdStrike Next-Gen SIEM came up for renewal, it was at capacity, and AI was pushing volume higher still. "AI is generating more data than it ever has," Alec says.

> **"Without some kind of log optimization, we were looking at doubling, if not tripling, our SIEM capacity."**
>
> **Alec Lessard**, Senior Security Engineer, Revolution Medicines

The obvious way out was to stop sending whole sources. "Most people's first reaction is to drop a source completely, but you lose all of that telemetry, and that becomes dangerous," Alec says.

Outcomes

60%
less data ingested into the SIEM each day

2-3x
SIEM capacity increase avoided at renewal

15 minutes
from data flowing to the first Realm reduction rule in production

1 year
of complete, searchable log history retained in Data Haven

Cutting ingest without losing a source or breaking a detection

Revolution Medicines chose Realm over its SIEM vendor's option for its flexibility. "The real golden nugget with Realm is that it does the legwork to show you which types of logs are your highest ingesters."

Knowing what drives the volume only helps if the team knows what's safe to cut. Realm Clarity AI recommends each reduction rule, and Detection Integrity checks it against the team's detections, protecting the fields each one depends on. Alec calls it "a silent but very effective feature."

A reduction rule live 15 minutes after the data arrived

What surprised Alec most was how quickly Realm was running. The team connected its first source within the first hour of the proof of concept. Alec started with a known problem in the Zscaler firewall, where every macOS update wrote the same log once for every Mac, so a single update meant a flood of identical entries. Realm's engineers walked him through a reduction rule for it, and 15 minutes after the data was flowing, the rule was live in production. "It was a product we'd never evaluated before, so we were nervous going in," Alec says. "Once we got our hands on the controls, we got comfortable very fast."

From over 200 GB a day to under 80, with budget back for other tools

Daily ingest into Next-Gen SIEM fell from 200-220 GB to 65-80 GB, a number Alec watches closely. The highest-volume sources are down 60% to 80%, even as overall log volume keeps growing. With Realm cutting ingest, Revolution Medicines didn't need the extra capacity, and the money it expected to spend went to other tools in its security stack. "It's a triple win," Alec says. "You optimize your logs, you make your SIEM better, and you make your CFO happy."

> **"Realm is the unsung hero. It saves us time, and in a real incident, it would let us react faster and help the business."**
>
> **Alec Lessard**, Senior Security Engineer, Revolution Medicines

Everything cut from the SIEM is still in Data Haven

Data Haven, Realm's searchable retention layer, holds a complete copy of everything Realm keeps out of the SIEM, and Revolution Medicines retains a year of it. If an investigation needs events the SIEM doesn't have, the team searches Data Haven and resupplies the exact ones. "If we ever got a little too aggressive optimizing our logs, knowing Data Haven is there is very reassuring," Alec says. "And if there were ever a breach where it wasn't clear which endpoints and sources were involved, Data Haven is one of the first places I'd start."

Getting the data ready for SOC agents

For Alec, a smaller SIEM bill is only part of the value. The rest is what stays in the data: clean enough for the SOC agents he already runs. "We're getting into an agentic SOC," he says. "We need to respond at machine speed, and if your data lake is a mess, your response time degrades with it."

AI is adding volume at the same time. Vendors are turning on AI features in tools the team already runs, and employees' AI agents write logs every time they call another tool. Alec expects endpoint logs alone to grow 300% to 400% over the next few years. "It won't just be the employee. It'll be the employee's agents doing tasks while they're away from their computer," he says. Realm keeps those logs to what an investigation needs: the tool, the machine, the source and the destination. Next, Revolution Medicines is looking at routing data through Realm to S3 or Azure storage close to its agents, so they can act during an incident without waiting on the SIEM.

Find out which logs are driving your SIEM ingest.

Pick one source and start a 7-Day Data Assessment. We'll show what you can cut and what stays protected, on your own 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, or 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.