# Seamless SIEM migrations

Gain choice, flexibility and control. Optimize your security telemetry for better value, insights and efficiency.

## WHY SIEM MIGRATIONS ARE SO DIFFICULT

### Increased Risk

Incompatible data formats make it easy to lose context during migration—creating blind spots and increasing security exposure.

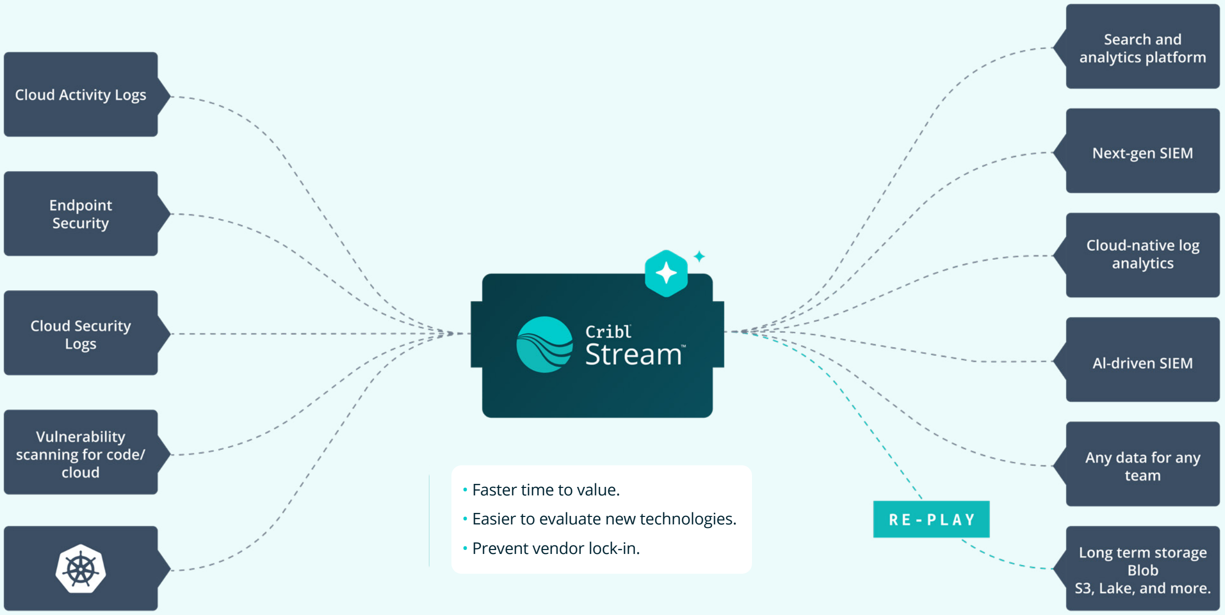
### Sky-High Costs

Running two SIEMs in parallel and managing duplicate alerts quickly drives up ingestion costs and operational overhead.

### Slow and Painful

Rebuilding pipelines, tools, and integrations from scratch leads to delays, burnout, and the risk of costly mistakes or data loss.

## A composable telemetry pipeline changes your migration game


Cloud Activity Logs
Endpoint Security
Cloud Security Logs
Vulnerability scanning for code/ cloud
Cribl Stream™
Search and analytics platform
Next-gen SIEM
Cloud-native log analytics
AI-driven SIEM
Any data for any team
RE-PLAY
Long term storage Blob S3, Lake, and more.

- Faster time to value.
- Easier to evaluate new technologies.
- Prevent vendor lock-in.

## CRIBL DELIVERS REAL-WORLD IMPACT TO ACHIEVE:

**30%+**

Reduction in data volume

**50%**

Reduction in data pipeline costs and complexity

**10x**

Increase in onboarding speed*

**0**

Vendor lock-in

**45%**

Faster queries and data routing

> “We were pretty much blind. We didn’t know the true value and true throughput of what we were receiving and ingesting into the SIEM platform. So when we brought Cribl in it was like turning on a switch and getting full visibility.”
>
> —**Dan Whittingham**, Security Solutions Architect, Rolls Royce

## Why Speak to Cribl:

### CUT COSTS:

- Slash infrastructure and licensing expenses by reducing log volume and eliminating duplicates.
- Route data to cost-effective storage like Amazon S3 or Cribl Lake—no more overpaying for hot storage.

### REDUCE RISK:

- Boost data quality and transformation efficiency while strengthening your SOC during migration.
- Capture and replay logs in real time to safely test migration scenarios — without touching production.
- Run two SIEMs in parallel, maintain operational continuity during migration, and enable safe testing without disrupting your live environment.

### MIGRATE FASTER:

- Ingest and route data from any source to any destination natively — no custom connectors needed.
- Transform and route telemetry with a click, streamlining workflows and accelerating your SecOps velocity.

## Cribl Stream optimizes your data sources across the board

**INGEST OPTIMIZATION INVOLVES REDUCING DATA VOLUMES BEFORE THEY ARE INGESTED INTO A SYSTEM OF ANALYSIS LIKE A SIEM.**

### Data optimization by source

| DATA SOURCE TYPE | AVERAGE DATA OPTIMIZATION |
|---|---|
| Syslog Collector | 39.0% |
| Cloud Activity Logging | 64.0% |
| Next-Generation Firewall / Network Security | 49.0% |
| Endpoint Detection and Response (EDR) | 49.0% |
| Windows Event Logs | 48.0% |
| Database Activity Monitoring Logs (SQL) | 74.0% |
| Secure Web Gateway | 71.0% |

### ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl’s vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl’s product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry’s leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry’s first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter