TransUnion | Cribl

CASE STUDY

TransUnion Teams Up with Cribl LogStream™ to Drive Greater Efficiency

CASE STUDY

TransUnion Teams Up with Cribl LogStream™ to Drive Greater Efficiency

TransUnion® is a global information and insights company that makes trust possible between businesses and consumers, by ensuring that each consumer is reliably and safely represented in the marketplace.

Big Data, Bigger Expectations

Ed Bailey and his colleagues in Enterprise Logging and Analytics at TransUnion are filling a tall order; with billions of logged events a day, the kind of scale they're working with is not commonly found in the enterprise data pipeline world. Along with scale and volume, they manage a wide, dynamic array of data sources, each of which can represent significant effort to onboard and maintain for their internal customers. The team works with Cribl to meet the challenge head on.

> *"We have a complex environment, challenging data, and a small team. Cribl helps us solve hard problems with greater ease."*
> *—Ed Bailey, Enterprise Monitoring and Operations Architect*

Unsurprisingly, when you're working at such a scale, efficiency is the word of the day — and with Cribl LogStream, there are many ways to say it at TransUnion:

Transform and Reroute Data on the Fly

The mission-critical job of keeping TransUnion's customers operating safely and smoothly means Ed's team collaborates with a lot of internal customers who use data from the same source, but in a unique way. For example, one team may need DNS metrics sent to InfluxDB, and another team needs the full DNS logs, but sent to Splunk, while another team needs data in a third format. With LogStream, each department gets what they need from the original data set, where they need it, without having to install additional agents or collectors.

> *"Anywhere to anywhere, in any format we choose, is massive."*
> *—David Olivas, Lead Advisor and Splunk Architect*

Typically, when altering a data source's format, you plan for some downtime while making the change, or at least a restart of agents and forwarders—but not at TransUnion:

> *"With LogStream, we can pivot on a data change in minutes, with no need to restart anything."*
> *—David Olivas, Lead Advisor and Splunk Architect*

HIGHLIGHTS

TransUnion onboards and processes hundreds of sources, billions of events with LogStream™.

The TransUnion team leverages greater speed and agility to transform and route critical data.

With LogStream, high-volume logging doesn't mean low-signal data.

"WE MADE A CHANGE THAT SAVED US A SIGNIFICANT AMOUNT IN LICENSING COSTS IN 30 MINUTES."

– ED BAILEY, ENTERPRISE MONITORING AND OPERATIONS ARCHITECT, TRANSUNION

Before deploying LogStream, the TransUnion team often set up individual data streams to achieve the desired results, and then maintained those additional streams on an ongoing basis.

"With Cribl, we can just divert existing streams to feed all the required destinations."
—David Olivas, Lead Advisor and Splunk Architect

Hot take: Not All Data is Beautiful ...or Valuable

The volume of data TransUnion engages with on a daily basis is staggering. Bailey's team uses LogStream to help ensure what's in that data is truly useful and valuable to the teams who work with it. Recently, they were able to massively reduce the scope of high-volume logging, such as DNS and Sysmon logs teams must examine from ~1TB a day to about 150GB – a near 20x reduction.

While simultaneously sending a full-fidelity set of the data to lower-cost, longer-term storage for potential future review, LogStream checks each external request against a vetted list of known trusted data in real time, enabling more than half of the requests to be filtered out as uninteresting. It then looks up the remaining traffic against known bad thread lists, this time reducing the data volume down to 150GB and providing better data.

"With Cribl, we're able to make our operational data strategy even more effective."
—Ed Bailey, Enterprise Monitoring and Operations Architect

Windows Event Logs are notoriously bulky, but with LogStream, Bailey's team is able to strip out useless event codes and unnecessary fields, cutting the clutter and speeding the work of their internal customers.

VPC Flow Logs are typically slow and expensive to deal with, but the TransUnion team runs them through LogStream to suppress uninteresting or repetitive content and serves up the cleaned results in near-real time to the requesting department at a much-reduced cost.

"We made a change that saved us a significant amount in licensing costs in 30 minutes."
—Ed Bailey, Enterprise Monitoring and Operations Architect

Is it Cheating if You Just Extract the Right Answers?

At TransUnion, analysts work around the clock to review and investigate potential issues. When a customer's business is at stake, speed is mission-critical. So when Bailey's team learned they could accelerate time to discovery and resolution by pre-extracting just the searched-for fields from the billions of firewall events they see a day, they didn't hesitate. They now use LogStream to extract and route only what's needed for immediate use, allowing their analysts to search for a single IP across days or weeks of firewall logs and get results in seconds rather than minutes or hours. When an interesting result is returned, the analyst can then review the full raw log for further intel. Analysts can rapidly assess and discard potential threats without needing to write a complex query to dig into the data.

"Not only does Cribl handle real-time matching on ingest, but it makes for a faster search time experience."
—Ed Bailey, Enterprise Monitoring and Operations Architect

Saying Yes— and Meaning It

The TransUnion team is excited to continue to leverage the many ways in which Cribl LogStream adds to the efficiency of their streaming data operations.

> *"We get to say 'yes' more often without diverting from our team's mission."*
> *— David Olivas, Lead Advisor and Splunk Architect*

Find out how your business can implement an observability pipeline to parse, restructure, and enrich data in flight, while cutting costs and simplifying operations.

Get Cribl, and take control of your data.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and machine data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.