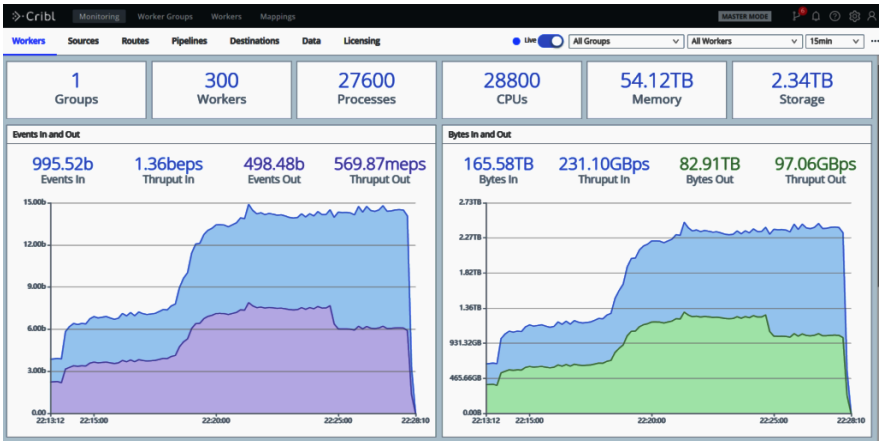
Cribl LogStream

What is Cribl LogStream?

Cribl LogStream processes log data before you pay to analyze it. LogStream helps you discern which data you need to send to an analytics tool to analyze now; which logs can be aggregated into metrics; which data should be stored and analyzed later if needed; and which elements of data should be dropped altogether. LogStream allows you to implement an observability pipeline which helps you parse, restructure, and enrich data in flight. Get the right data, where you want, in the formats you need.



UI showing reduced output volumes

The Benefits of Cribl LogStream

Deployment of LogStream allows you realize some or all the following:

- **Save Costs:** As you route data to Log Management Systems (LMS) - such as Splunk – the LMS will typically be licenced on a per GB per day ingest rate. As your data volumes increase, this becomes increasingly expensive and licence fees can be several million dollars per year. Larger installations run from Terabytes to Petabytes of ingest per day. Cribl LogStream allows you to filter and reduce ingestion volumes prior to the data hitting the LMS. This can be very useful for firewall and/or Windows environments which generate a lot of data with may redundant and empty fields that can be stripped.

  In addition, the LMS will index ingested data in primary, expensive storage so that it is immediately available for search. But if your use case allows, Cribl LogStream will allow you to filter data that may not be needed to low cost S3 storage, and then replay it back to the LMS at a later date should an incident require the data to be queried.

  On mid to large deployments, using Cribl to trim Splunk data by >10% results in significant savings that more than covers the cost of the Cribl license.

For Further Information:
Email: sales@xiaa.co.uk
Telephone +44 (0)208 412 7107

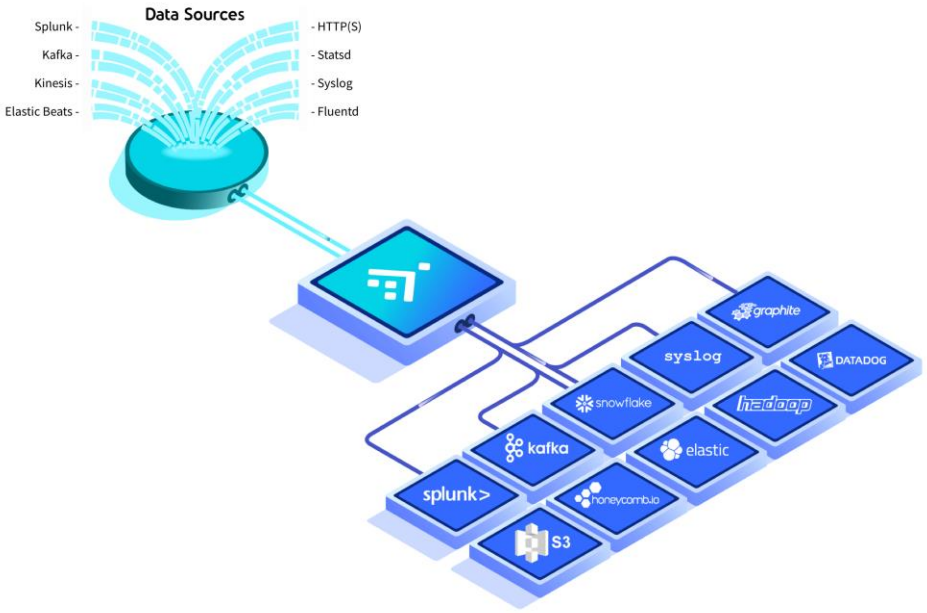
- **Control Budgets:** On a larger LMS deployment you may be at your ingest volume limit and any increase will require you to negotiate a larger licence with the Supplier. A department has an urgent business case to ingest and analyse additional data which will push you over the limit. You can use Cribl LogStream to filter out unneeded data from the current ingest, or maybe minimize the new data volume, thereby avoiding the need for renegotiation and remain inside your current budget.

- **Simplify Architecture:** Cribl LogStream acts as a Universal Receiver (Splunk Forwarder, Elastic Beats, Syslog, Kafka, S3) and a Universal Collector (S3, Filesystem, APIs, Scripts) for log data, enabling you to simplify the collection architecture in complex environments. When there are multiple collection points, an instance of Cribl LogStream becomes a Master Controller enabling configuration to be defined centrally through the UI in one place, and then automatically push changes to the Worker nodes. Not only does this simplify the overhead of managing the configuration for data collection, but it may also result in less infrastructure to manage the processing of input data.

Cribl LogStream Functionality

Routing

LogStream makes it easy to route data to multiple destinations, delivering the right data to the right tools while putting full fidelity data in the most cost-effective destination.



For Further Information:
Email: sales@xiaa.co.uk
Telephone +44 (0)208 412 7107

Data Reduction
As much as 50% of log and metric data goes unused – null fields, duplicate data and fields that offer zero analytical value. With LogStream, you can trim wasted data streams and analyze only what you need.

Universal Receiver
Log systems require a lot of ancillary software: Syslog-ng, Splunk Heavy Forwarders, AWS & Kafka Connectors. LogStream consolidates receiving Splunk HEC, AWS, Kafka, and other sources all in one tool.

Parse and Structure Data
Parse and shape events in the stream, no matter how ugly the original log, and add context through enrichment before sending onto your destination system.

Process Log Data
LogStream can aggregate logs into metrics for analysis by a wide array of tools, suppress duplicate events, or sample to keep a statistically significant subset of the full stream.

Intuitive Management Interface
Reduce management overhead, with a robust and easy-to-use GUI-based configuration and testing interface. Capture live data and monitor your observability pipeline in real-time.

Customer Success

Financial services firm lowers Splunk costs with Cribl LogStream
Challenge: The company wanted to use Splunk to analyze DNS logs for the first time but adding a terabyte of data per day to their existing license was deemed prohibitively expensive.

Solution: They use Cribl LogStream to enrich log data with a top internet domains list. This allowed them to filter and drop uninteresting logs from trusted domains. DNS log volume was reduced from 1 terabyte a day to about 50GB a day – well within their budget.

MSP delivers value for multiple customers with Cribl LogStream
Challenge: A Security Managed Service Provider manages log data for several customers. They needed to simplify how to get data from agents in multiple customer environments to separate Splunk instances.

Solution: They use Cribl LogStream to centralize data ingest from multiple forwarders. Data is filtered, enriched, and transformed by LogStream in real-time, without comingling data across customers. LogStream routes data to each customer's instance of Splunk, allowing the MSP to manage all of this from a single console without adding staff as they add customers.

Please call us if you need further information.

For Further Information:
Email: sales@xiaa.co.uk
Telephone +44 (0)208 412 7107