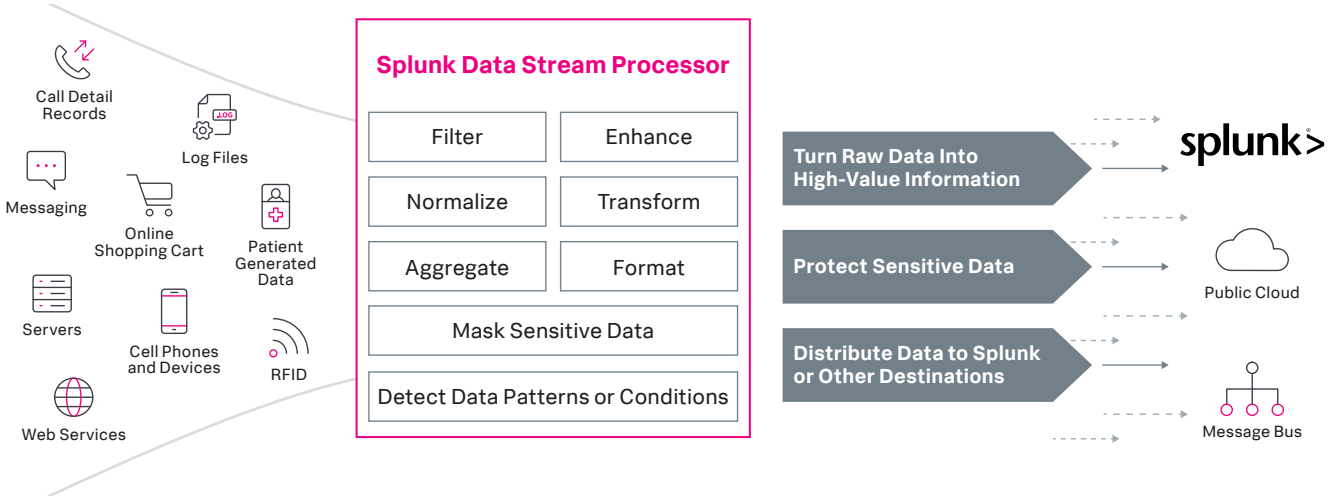
Splunk Data Stream Processor

A real-time stream processing solution that collects, processes and delivers data to Splunk and other destinations in milliseconds

- **Quickly turn raw data into high-value information** before data is sent to Splunk or another destination
- **Take action on data in motion** by quickly identifying abnormal data patterns or specific conditions that occur on the stream
- **Protect sensitive information** by masking sensitive data before it reaches downstream consumers
- **Distribute data across the enterprise** to Splunk and other third-party destinations



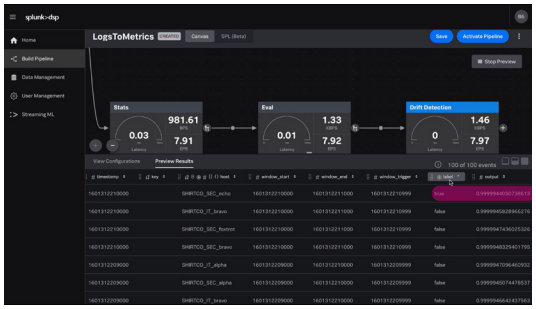
As the data and technology landscape continues to evolve at unprecedented levels of scale, new types of devices and more data sources, organizations need a robust solution that guarantees efficient data delivery across the enterprise.

Splunk® Data Stream Processor (DSP) is a scalable stream processing solution that collects data from diverse sources and distributes insights to multiple destinations across the enterprise. As events occur, DSP continuously collects, transforms and aggregates high-velocity, high-volume data based on specified conditions, masks sensitive or private information, detects abnormal data patterns, and then distributes results to Splunk or other destinations in milliseconds.

DSP is a complete stream processing solution built on the Splunk platform to complement our entire portfolio of products that solve IT, security, IOT and business analytics use cases. Further, DSP not only is an extensible solution, but also can help centralize multi cloud sprawl as well, providing integrations with platforms like Apache Kafka®, Amazon S3 and Kinesis, Azure Event Hub, GCP Pub/Sub and more.

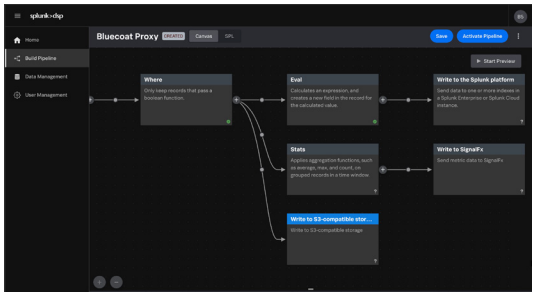
What is Stream Processing?

Stream processing is a technology that lets users optimize data flow to get faster, more immediate data insights. Unlike batch processing which first collects large batches of data then processes that data, stream processing is designed to instantly process and analyze continuous streams of data, which reduces latency and lets organizations immediately respond to critical events.



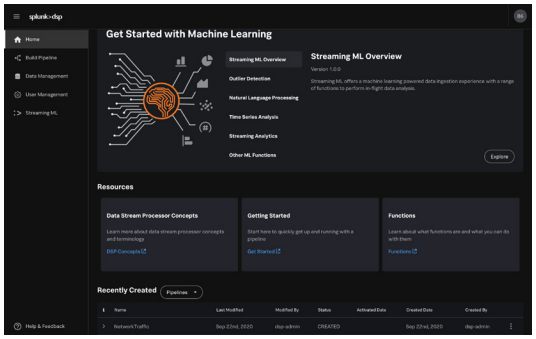
Take action on data in motion

- Aggregate noisy events on the stream, pulling out critical insights like distinct counts that can be enriched with anomaly scores, then route to SOC teams for further investigation
- Uncover Personal Identifiable information (PII) in-stream and mask, reducing security and compliance risks



Centralize enterprise data collection and deliver to multiple destinations

- Increase visibility with unified data collection in sprawling multicloud environments
- Distribute subsets of data to various teams and destinations, such as critical data with security implications for your SOC team
- Use a robust streaming solution built on top of Apache Pulsar that guarantees data delivery and scales as your organization experiences growth



Stream at enterprise scale with a graphical UI and embedded machine learning

- Use a drag and drop UI to design data pipelines
- Leverage pre-built pipelines by creating templates for future use
- Set up rules to format, filter and send subsets of data downstream based on predefined conditions
- Identify anomalous behavior, such as malicious threats, in streams of data with embedded ML and eliminate hours of manual work

---

Technical Requirements

- Minimum Node Requirement
  - CPU: 8 core (16 recommended)
  - Memory: 64GB (128GB recommended)
  - Network: 10Gbps
  - Storage: 1TB
- Minimum 3 Node Cluster

Supported Data Sources: Apache Pulsar, REST APIs, Splunk (Universal Forwarder, Heavy Weight Forwarder), GCP Pub/Sub, Azure Event Hub, Amazon S3, AWS Metadata, Azure Monitor Metrics, Syslog (via Splunk Connect for Syslog), Splunk HTTP Event Collector (HEC), Amazon CloudWatch Metrics, Microsoft 365, Google Cloud Monitoring Metrics

Supported Destinations: Splunk, SignalFx Metric + Trace, Apache Kafka®, Amazon Kinesis, Amazon S3, Azure Events Hub

Think **Splunk Data Stream Processo**r is a good fit for your organization? Learn more about Data Stream Processor pricing. Contact our sales experts.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

20-15677-SPLK-Splunk Data Stream Processor-105-PB