Introduction

Not all log data is created equal. While some logs are critical for real-time debugging and incident response, most are often passed directly into storage for compliance purposes. However, many organizations are funneling all of that data through Splunk, and are paying a premium for every gigabyte ingested. The complicated nature of data configuration in Splunk makes it difficult to implement intelligent routing to reduce costs. This inevitably leads to tradeoffs that result in blocking the ingestion of large chunks of data (or even direct data sources) from Splunk, effectively leaving security and development teams at risk of not having access to essential data for resolving incidents, responding to threats, or even the knowledge that something is happening in their environment.

LogDNA Observability Pipeline

The Observability Pipeline is a platform that allows SREs, ITOps, and DevSecOps to easily and intelligently control data outside of Splunk and gain greater value. The platform enables teams to use custom rules to more intelligently ingest, classify, and route log data, resulting in more relevant insights entering Splunk and a dramatically reduced Splunk bill. Security teams specifically can drive down “Dwell Time” by leveraging Splunk for high-level analysis and when needed for storage for threat hunting.

By removing Splunk as the single control point, Operations can effectively break the chokehold that it has on their budget and breathe a sigh of relief knowing that they are protecting their license quota by only indexing actionable data without limiting their access to all log data insights.

How It Works

Ingestion

With a number of ingestion options (Agent, Syslog, Code Libraries, etc.), along with support for a number of platforms (Kubernetes, Heroku, CloudWatch, Palo Alto Networks as well as an ingest API), our broad support ensures that you can get your data in one place. And with the scale to handle petabytes of data, LogDNA can grow with your data needs on demand.
**Exclusion**

Powerful exclusion rules allow you to only store what you need. Send the most relevant data types to Splunk for threat detection and response and avoid additional costs associated with sending noisy logs to a single pane of glass.

**Streaming**

LogDNA Observability Pipeline gives you the flexibility to easily send data wherever it is most valuable, allowing you to control both data destination and cost. Stream enriched data to Splunk for analysis and visualizations or route it to storage for compliance.

**Try Observability Pipeline**

We are excited to share this new solution with our customers who are struggling with their Splunk Bill. Current LogDNA users can access Observability Pipeline as part of a limited-time private beta program. Try out our newest technology, work with members of our product team, provide feedback to help shape the future of Observability Pipeline, and ultimately save money on your Splunk bill! And the best part? The private beta is completely free to join.

Contact your Customer Success Manager for more information or request access by emailing outreach@logdna.com.