



Unified Logs and Metrics

Turn Raw Machine Data into Continuous Intelligence for Modern Applications

Machine data, in the form of logs and time-series metrics, contains the raw information which can be collected, analyzed and visualized to deliver continuous intelligence. By unifying logs and metrics in a single analytics platform, Sumo Logic provides real-time visibility into the health and viability of your modern applications.

Digital Transformation

Businesses today are embracing digital transformation, using software as a primary driver for innovation and growth. Modern applications, typically cloud-based and revenue generating, are at the heart of this digital transformation driving new sources of innovation and competitive differentiation.

Over the next three to five years, the percentage of enterprises with advanced DX (digital transformation) strategies and implementations will more than double.* Digital transformation is also fueling organizational changes. Organizational silos are adopting collaborative approaches such as DevOps and agile development to accelerate application delivery cycles and innovation.

To keep pace with market shifts and customer needs, application teams are re-thinking how they build, run and secure modern applications. They are adopting new technologies such as microservices, containerization, IaaS, and PaaS designed to accelerate innovation and code delivery. However, with speed comes risk, complexity and lack of visibility.

The Need for Machine Data Analytics

Legacy, siloed tools designed for monolithic, three-tier applications struggle to provide the real-time operational, security and business insights needed to support modern applications. Their relevance is diminishing as more and more application developers and operators are favoring new toolsets that provide real-time, end-to-end visibility across on-premises, hybrid and cloud architectures.

What makes these new toolsets unique is their reliance on machine data. Machine data, in the form of logs and time-series metrics,

contains the raw information, which can be collected, visualized and analyzed to deliver real-time [continuous intelligence](#). Analyzing machine data represents its own set of challenges, however, due to the volume, velocity and variety of the data.

Metrics are structured measurements of behavior over time like application performance (i.e. database latency), infrastructure performance (i.e. CPU utilization) or user KPIs (i.e. # of visits to a web page).

Logs, on the other hand, are semi-structured and unstructured records of activities that have occurred at some point in time.

Unifying Logs and Metrics

Until now, machine data analytics tools were designed either for logs or siloed, time-series metrics. Businesses typically rolled out multiple tools and switched between multiple screens in an attempt to correlate data for monitoring, troubleshooting and insights into usage patterns.

In the interests of combining metrics data with log files, many tool providers often take the route of extending existing capabilities to address new data types instead of re-architecting their tool to handle different data types natively. The former approach sacrifices speed and sub-optimizes compute cycles. For example, queries, burdened with architectural limitations, slow down dramatically. And more hardware and compute cycles are required to support the analytics environment, negatively impacting the cost/value equation. In the interests of containing costs, IT organizations may restrict the number of metrics only to find themselves at a loss when problems occur and the needed metrics for troubleshooting are not at their fingertips.



“Gone are the days where we require separate tools in order to ingest and analyze metrics and log data. With Sumo Logic’s new capability unifying both logs and metrics, we have everything we need within a single platform.”

Jon Dokulil, VP of Engineering, Hudl

Architecting a tool that can support ingestion and real-time analytics for application performance metrics, infrastructure metrics, custom metrics and log events is not trivial. In addition, custom metrics are often difficult and costly to incorporate as they are not inherently supported by legacy tools.

Modern applications need a machine data analytics platform that encompasses the capabilities of multiple tools to flexibly address operational, security and business needs. This means optimizing not only for performance and new technologies such as containerization and automation, but also for cost models.

Modern Application Health and Viability

Digital businesses are not only disrupting existing markets, but are unearthing new sources of competitive advantage in how they proactively and reactively address the health and viability of their modern applications.

Proactively, DevOps, Operations teams and line-of-business owners focus on continuous monitoring using real-time dashboards to gain visibility into what is happening within their modern applications. They want flexible views to take advantage of a diversity of information, such as business KPIs, application services, clusters, nodes or even containers. They are seeking to understand modern application usage patterns, and gain operational, security and business insights. Using dashboards and alerts, IT teams monitor for SLA compliance, identify anomalies and issues and compare current to past behaviors to identify issues before customers are impacted.

Reactively, the focus shifts to correlating and understanding what is going on in real-time to quickly identify and remediate issues. Correlation and contextual visualization of multiple metrics and multiple sources of log data are critical as DevOps, Operations and line of business owners analyze problems across multiple log sources

and multiple metrics. The goal is to overlay performance metrics on log file data to surface patterns and identify failures and timelines of changes in real time to quickly resolve the issue at hand.

In addition, root-cause analysis processes improve as multiple metrics and multiple log file sources are unified and overlaid contextually. It becomes easier and faster to perform historical analysis, correlate behaviors and uncover long-term fixes.

The Sumo Logic Difference

In order to provide real-time search and analytics, Sumo Logic has invested in a new architectural platform, one that provides the same level of capabilities to structured time-series metrics as semi-structured and unstructured logs. This new architecture delivers real-time, side-by-side and contextual insight into machine data for:

- **Top-to-bottom visibility** through real-time dashboards that integrate custom metrics, AWS CloudWatch and infrastructure metrics and display them in histograms, pie charts and real-time dashboards
- **Team collaboration** by providing richer and real-time insights based on a shared version of the truth to support DevOps and continuous delivery
- **Accelerating and simplifying troubleshooting** by applying advanced analytics and machine-learning algorithms to your logs and time-series metrics

About Sumo Logic

Sumo Logic is a secure, cloud-native, machine data analytics service, delivering real-time, continuous intelligence from structured, semi-structured and unstructured data across the entire application lifecycle and stack. More than 1,000 customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a multi-tenant, service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth.

Learn more about Sumo Logic’s unified log and metric capabilities in this [five-minute demo](#). For more information, visit www.sumologic.com/unified-logs-metrics

**IDC FutureScape: Worldwide Digital Transformation 2016 Predictions, Doc # 259616, November 2015*



Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 9460
www.sumologic.com

© Copyright 2016 Sumo Logic, Inc. All rights reserved. Sumo Logic, Elastic Log Processing, LogReduce, Push Analytics and Big Data for Real-Time IT are trademarks of Sumo Logic, Inc. All other company and product names mentioned herein may be trademarks of their respective owners. SB-U/LM-0516. Updated 05/22/2016