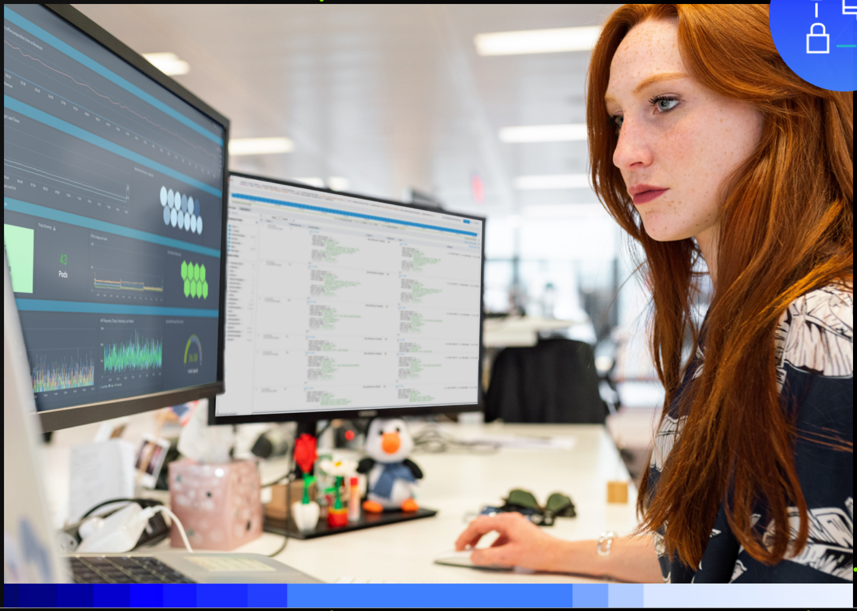
Log analytics at scale

The best way to keep your apps and infrastructure reliable and secure



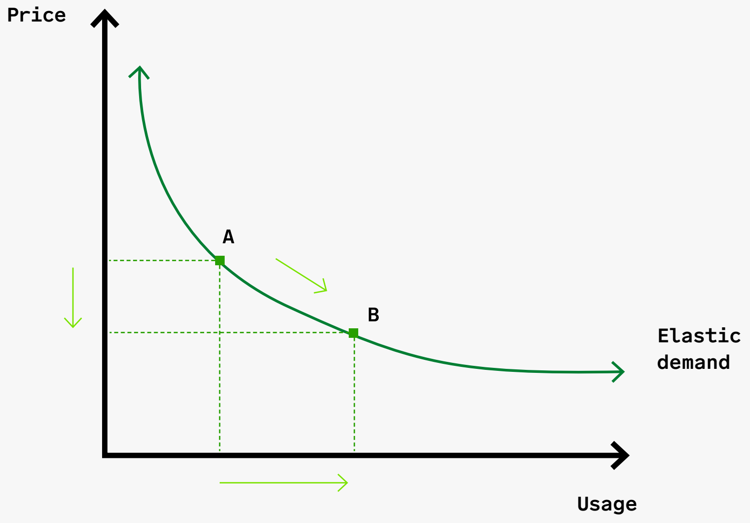
sumo logic

Log analytics guide

Few things are as powerful, as frightening, as overwhelming and as important as data.

Every day, more companies move to cloud solutions for their critical business applications. This shift causes an exponential explosion of data from various sources across cloud environments. While sound log management practices help tame that data, organizations rely on real-time time analytics and actionable insights to ensure the reliability and security of digital experiences.

According to Gartner research, more than half of enterprise IT spending is shifting to cloud-based platforms and products. When it comes to vital business operations, log management — and log analytics — play essential roles. As Gartner puts it: Technology and service providers that fail to adapt to the pace of cloud face an increased risk of becoming obsolete or, at best, being relegated to low-growth markets.



■

Jevons Paradox

A visualization of how falling prices (greater efficiencies) generally lead to more usage vs. less. The lower the cost, the more applications people will find for a good. As cloud compute becomes less expensive, people find more ways to use it, making it more prevalent — increasing demand. Its “elastic demand” is a reflection of more efficient pricing.

This guide addresses how to use log analytics to take advantage of growing data vs. being drowned by it. Because when you master logs, you master your business. Here’s what you need to know to get started.

DEFINING

Logs, log management & log analytics

Businesses generate data at a rapid pace and from several distinct sources.

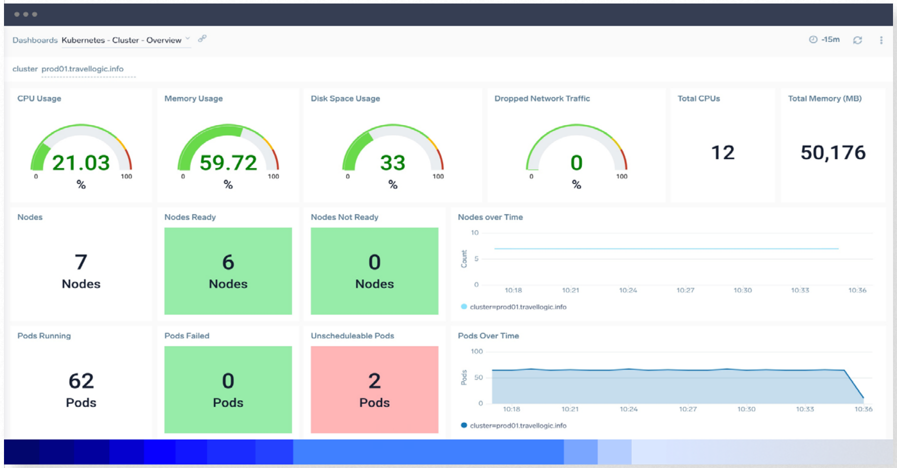
In this context, a log or log file is a computer-generated data file that contains information about usage patterns, activities, and operations within an operating system, application, server or another device. These time-stamped digital records document actions or events and materialize from a number of sources.

Solid log management and analytics provides valuable insights for effectively monitoring these components.

Machine data comes from many sources

- Applications
- Application infrastructure
- Cloud infrastructure
- Containers
- Load balancers
- Networks
- Servers

Log management and log analytics are closely related but not identical concepts.



■

Ongoing monitoring and proactive analysis are hallmarks of well-developed log management and analytics.

Log management

refers to a set of processes for collecting, managing, storing and archiving large sets of log data. Within the context of site reliability and a larger DevOps framework, log management involves gathering — and analyzing — log data from relevant systems to monitor and improve performance, identify issues and bugs and improve security.

Log analysis

refers to reviewing, interpreting and understanding computer-generated records (or logs). Logs are essential for application performance and security and provide the basis for proactive DevSecOps practices.

So, what exactly is a log analytics solution?

A log analytics solution may refer to a particular tool, platform or framework that outlines an organization's log management and analytics priorities. The absence of a modern log management and analytics platform, leaves organizations with challenges in need of solutions — challenges like:

Siloed data

between development, site reliability engineering (SRE), Ops and security teams and tools.

An extremely high volume of log data

making it difficult to get the right visibility or actionable insights out of any of it.

Mean time to resolution (MTTR)

suffers due to the excessive time it takes for logs to rehydrate, slowing teams' ability to troubleshoot.

A comprehensive log management and analytics platform unites these objectives and provides a single source of truth for understanding any trends or disruptions to system performance and output.

What are examples of log analysis functions and methods?

Log analysis involves the manipulation of complex, often separate data sources and types — and extends to the extraction of specific information from those logs. There are several popular methodologies for data organization, processing and interpretation, including:

Normalization

indexes, standardizes and translates log data into a common format for easier comparison and analysis.

Pattern recognition

compares real-time data with historical patterns to highlight abnormalities, anomalies or errors (enabling quicker diagnosis and remedies).

Classification and tagging

groups similar log entries by type to identify and address specific error types or locations.

Correlation analysis

brings logs from various sources together to identify connections and potential correlations between systems and events.

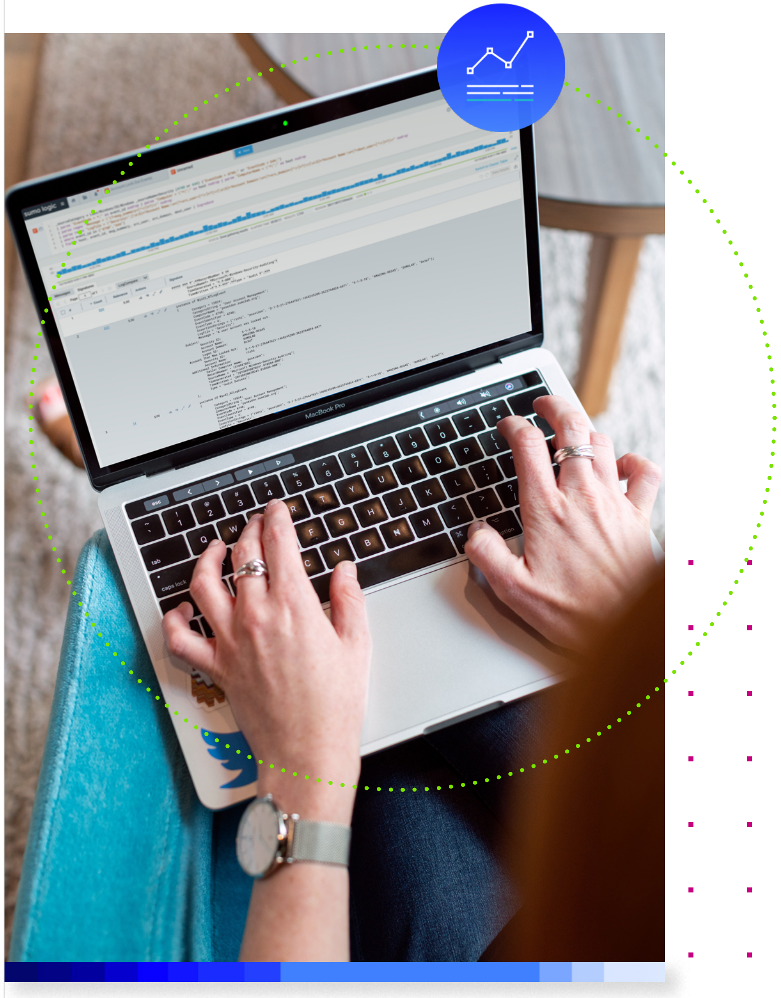
DEEP DIVE

Log analytics use cases

System logs provide a treasure trove of information, including whether resources are performing properly and optimally. Log management and analysis provide the foundation for observability and security use cases (or the evaluation and investigation of a system's behaviors, actions, outputs and security posture).

Even in the recent past, collecting and evaluating logs required tedious, manual effort, which is susceptible to human error. DevOps and security teams are at a disadvantage when they can't access and process accurate, up-to-date information.

Four primary, high-level use cases for log analytics are proactive monitoring, troubleshooting, digital forensics investigation and data analysis and reporting.



FOUR PRIMARY LOG ANALYTICS USE CASES

Proactive monitoring

By monitoring application performance and security, organizations can take a timely and direct approach to understanding and improving performance and system behavior. This includes the identification of unusual or anomalous activity, as well as investigating security events. The goal is to detect and remedy performance issues or security threats quickly before they wreak havoc. Sumo Logic offers a variety of tools for proactive monitoring, including infrastructure monitoring, real user monitoring, application observability and cloud security monitoring and more.

Troubleshooting

With proactive monitoring in place, troubleshooting capabilities improve. Once an anomaly is detected, log analytics should provide accessible insights into what may have occurred before, after or even concurrently with the problem or suspicious behavior.

Forensics investigation

This refers to the process of analyzing log data to identify when a security incident occurred, who initiated it, the sequence of actions involved, and the impact it had on the business. It also helps to identify the data affected by an attack and pinpoint the attack techniques used.

Data analysis and reporting

Simply collecting data is one thing — making it actionable is another consideration. An element of any log management or analysis program involves making crucial system performance information and other related metrics easy to access, understand and act on. Intuitive and customizable dashboards ensure that everyone operates with the same data and well-aligned priorities.

What are the benefits of log management and analytics?

→ Identify opportunities to streamline business operations and optimize system performance for greater efficiency, including potential IT automation.

→ Implement a framework for improved root cause analysis, effective troubleshooting and speedier incident response and resolution.

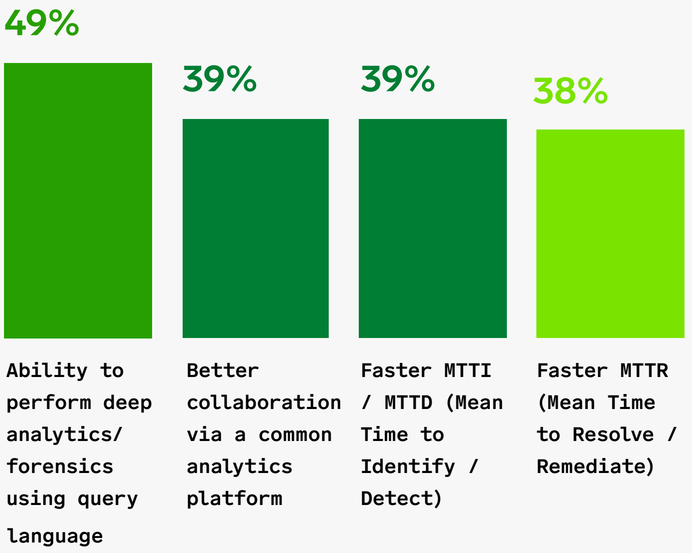
→ Improve resource allocation and provisioning to prioritize key items and use bandwidth appropriately.

→ Enhance cybersecurity measures through proactive and ongoing monitoring.

→ Ensure compliance with industry-specific regulatory bodies, such as HIPAA and GDPR.

→ Increase opportunities for timely, meaningful collaboration (between cloud architects and operators, for example).

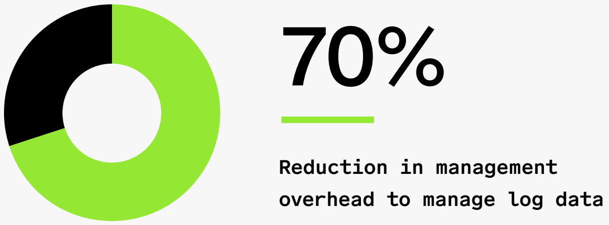
→ Strengthen the effectiveness of sales and marketing campaigns by evaluating metrics like website traffic, conversion errors and more.



■

Top operational benefits from using Sumo Logic

N=112



■

Top cost benefit from using Sumo Logic

N=93

Source: UserEvidence survey of Sumo Logic users. Statistic verified 02/2/2023.

What role does analytics play in the log management process?

A log management process generally consists of four stages, each of which benefits log analytics:

1 The first stage is log collection, which involves collecting logs from operating systems, applications, cloud infrastructure, network devices, etc. Collection and aggregation of logs provide a foundation for ongoing monitoring and timely log analysis. The best log aggregation tools offer reliable and consistent procedures to streamline the log analysis process.

2 Centralizing and indexing logs into a single repository or location accessible across the IT infrastructure provides a necessary foundation for log analytics. In complex environments with many types of data-generating systems and processes, adhering to centralized logging best practices ensures a reliable, shared source of truth.

3 Searching and analyzing data would be cumbersome if it depended on manual processes. It would take so long to compile this data, ensure it is error-free and complete that it becomes difficult to act on it promptly. Solutions like Sumo Logic provide the log analytics you need to meaningfully and efficiently interpret log data and uncover actionable insights.

4 Monitoring system performance and data to efficiently uncover anomalies or other issues. With Sumo Logic's analytics platform, you can enhance continuous monitoring with custom alerts to notify you when certain events occur or conditions are met.

Log analysis best practices

Adhering to the following best practices should provide an effective and repeatable framework for log analysis, interpretation and action. You can't effectively analyze data that hasn't been properly collected and standardized.

Develop your strategy

The last thing you want is to waste time or work through inefficient processes. Strategize before jumping in. Start with what's most important. You might start by asking questions like:

→ Is our infrastructure working optimally, and where might there be opportunities to streamline or improve processes?

→ What factors are causing reporting or application issues? Consider indicators such as latency and error rate.

→ Do our authentication procedures make sense, and are they providing the appropriate degree of security?

→ What content, products or services do our users rely on the most, and are they meeting their expectations?

→ Are we tracking password changes, unauthorized logins, network port scans, and newly created user accounts across our on-prem and cloud systems?

Get your data in order

This means structuring the data for accessibility and analysis and centralizing it in a repository. This enables more efficient analysis and interpretation and the capability for cross-analysis.

Identify data correlations

When you can access and analyze data throughout your organization (the opposite of siloed data), it becomes easier to detect and understand meaningful correlations in that data. This is essential for efficient root cause analysis and related improvements to log management frameworks and analysis capabilities.

Keep an eye on your real-time data

Ongoing monitoring and proactive analysis are hallmarks of well-developed log management and analytics. With these processes in place, organizations can streamline root cause analysis and remedy issues faster.

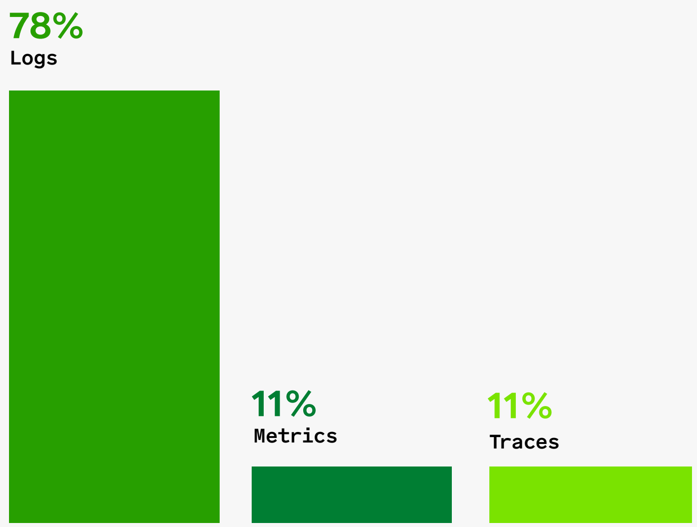
Set up alerts

Establish thresholds for application performance and security activities, then set alerts that automatically trigger when something happens to cause the indicator to go above or below that threshold. Then you can troubleshoot by digging into the data analytics.

The right log analytics solution

Leveraging a SaaS analytics platform like Sumo Logic empowers organizations to make smarter — and speedier — decisions. It equips DevOps and security teams with timely recommendations based on real-time analytics and insights, all within a single platform.

This is especially important as data complexity and volume increase over time. Proactive and ongoing monitoring is extremely difficult for companies that have fallen behind on their digital transformation. Modern solutions identify, understand and address intelligence gaps, including those related to siloed application architecture or teams.



The data that is most helpful to Sumo Logic users when they need to troubleshoot a performance problem.

N=139

Source: UserEvidence survey of Sumo Logic users. Statistic verified 02/2/2023.

> “Since moving over to Sumo Logic it has been extremely easy for our enterprise to detect even the smallest glitches in the operations and action them accurately within no time.”

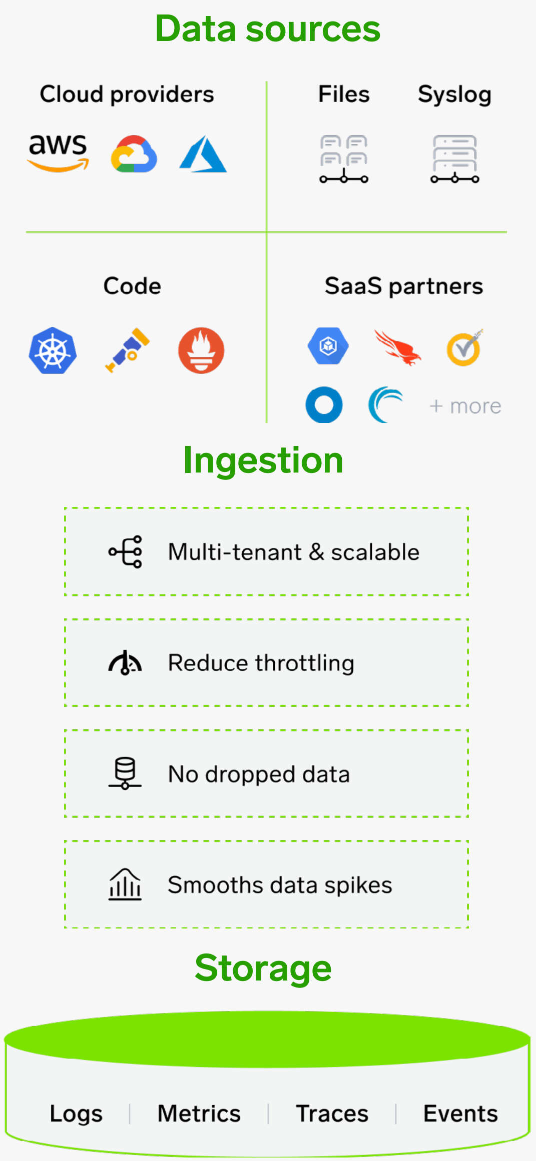
Manager, Large enterprise bank

MODERN SOLUTIONS SHOULD ADDRESS:

Complex application architecture and multi-cloud adoption

When workloads are broken into smaller components and delegated throughout an organization, it creates a more complex data environment. This reduces the usefulness and actionability of the data by making it less comprehensive and less accessible to teams. Sumo Logic brings these systems and the data they generate into an intuitive repository — increasing the speed to implement quality improvements and tell a complete story.

Further, siloed architecture and infrastructure make achieving a complete and scalable data system challenging. Sumo Logic's multi-cloud solution aggregates data from across the entire organization and cloud environments into a single interface, increasing accessibility and enabling ongoing, real-time monitoring.



Sumo Logic data ingestion and storage

MODERN SOLUTIONS SHOULD ADDRESS:

Security threats

The less-cohesive an organization's log management and analytics systems, the more difficult it is to proactively guard against the latest security threats. Sumo Logic's platform helps speed up key processes like threat detection and response, making it quicker and easier to detect threats, evaluate their risk and address them accordingly.

Opportunities for collaboration

"Knowledge is power" is a cliche for a good reason — it's generally true. In the context of log analysis, this means establishing a single source of truth that keeps everyone informed and on the same page. As much as possible, organizations should work to move away from a heavily-siloed approach. Sumo Logic provides a single place for technical and business teams to benefit from compelling, real-time insights.

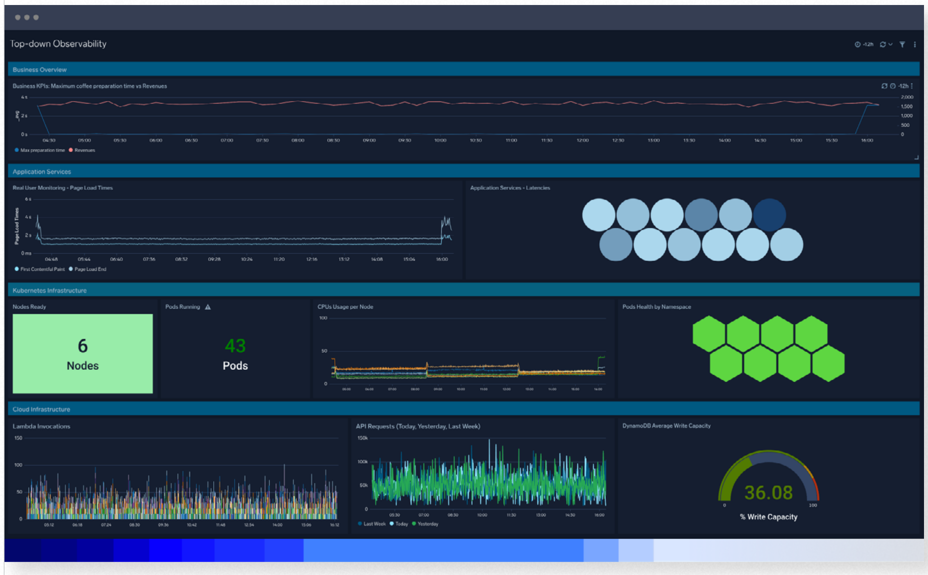
Custom integrations

Sumo Logic empowers organizations to streamline workflows with native integrations for popular applications like Amazon Web Services, Google Cloud Platform, Microsoft Azure and more. Built for scale and flexibility, Sumo Logic enables you to implement your own custom queries as needed.

Start doing more with your logs

Sumo Logic's real-time SaaS analytics gives DevOps and SecOps teams the ability to aggregate and centralize event logs from various applications and infrastructure components. This empowers businesses with the tools and insights they need to:

- → Collect and centralize
- → Monitor and visualize
- → Search & investigate
- → Alert & notify



With the right partner, you can tame the mind-bending growth of data. Use Sumo Logic Log Analytics to turn data black holes into your biggest growth opportunity. Learn more.

Sumo Logic.
The infinite power of log analytics.

About Sumo Logic

Sumo Logic, Inc. (NASDAQ: SUMO) empowers the people who power modern, digital business. Through its SaaS analytics platform, Sumo Logic enables customers to deliver reliable and secure cloud-native applications. The Sumo Logic Continuous Intelligence Platform™ helps practitioners and developers ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures. Customers around the world rely on Sumo Logic to get powerful real-time analytics and insights across observability and security solutions for their cloud-native applications. For more information, visit: SUMOLOGIC.COM

sumo logic