TIBCO LogLogic—The Essential Logging as a Service Solution

STATE OF AFFAIRS

Every successful enterprise requires a myriad of information technologies. Whether these are applications, networks, or security devices, they are all generating a continuous stream of log data containing vital information about business operations. The sheer amount of log data creates a big data problem, specifically a Machine Big Data problem. Operational, security, and compliance mandates require that organizations collect log data generated by critical sources. As with every form of vital information, Machine Big Data needs to be managed and distributed to the systems and people who need it—for security, operational intelligence, compliance, service level assurance, and other purposes. Solving the Machine Big Data storage and access problem is a balancing act involving cost, complexity, and risk.

THE CHALLENGES

The first Machine Big Data challenge is how to identify logging requirements and the best solution for these requirements:

- Security teams need to respond quickly to alerts and breaches.
- Operational teams want efficiency improvements that reduce time-to-recover from failures.

Questions include:

- Do I opt for a hardware, software or a cloud-based solution?
- Which implementations are most scalable and require the least bandwidth to deploy and manage?
- How do I understand and address the cost of ownership of the solution, including licensing the application, installing and administering the solution, and the associated storage costs?

Storage is a costly consideration. Many companies require long term storage of Machine Big Data for future searching and must be able to present the log data in its original format for forensics and compliance requirements. As infrastructures grow in size and complexity, the sheer amount of data can grow exponentially, exacerbating the costly problem of how and where to store log data.

- How quickly can the solution be deployed?
- When my team is already tasked with operational responsibilities, where do I find the resources to install and configure a comprehensive solution, one capable of searching historically across a variety of different log sources?
- Are managed service providers a viable option?
- Once the solution has been selected and implemented, how do the consumers access it and make meaningful use of the intelligence it is capable of providing?

"LOGLOGIC OFFERS IMPRESSIVE REAL-WORLD PERFORMANCE, AT ONE CUSTOMER SITE SCALING TO OVER 80 BILLION EVENTS PER DAY."

These matters are complex and often perplexing for IT decision makers. Miscalculations, changes in the environment and business initiatives, and sheer human error can hamper your efficiency, exhaust human and financial resources, and fail to deliver the required information to consumers.

- How do decision makers know when they have made the best decision for their organization's requirements?

THE SOLUTION

TIBCO LogLogic® allows organizations to address all of these concerns efficiently and quickly with a solution known as Logging as a Service. Applying the same concepts to Machine Big Data as normal Internet traffic, LogLogic enables organizations to filter, route, and secure log data. The solution is capable of not only ingesting large volumes of data, but also filtering and forwarding it securely to its destination while maintaining data integrity. Acting as a central repository for Machine Big Data, LogLogic can also search intelligently across historical and previously siloed data. This easy access to critical information for your security, operational, and compliance teams provides new insights faster. With enterprise-strength scalability—handling 80 billion events per day for one customer—the control, insight, and data assurances provided are some of the reasons many large companies chose TIBCO LogLogic as an enterprise Logging as a Service (LaaS) platform.

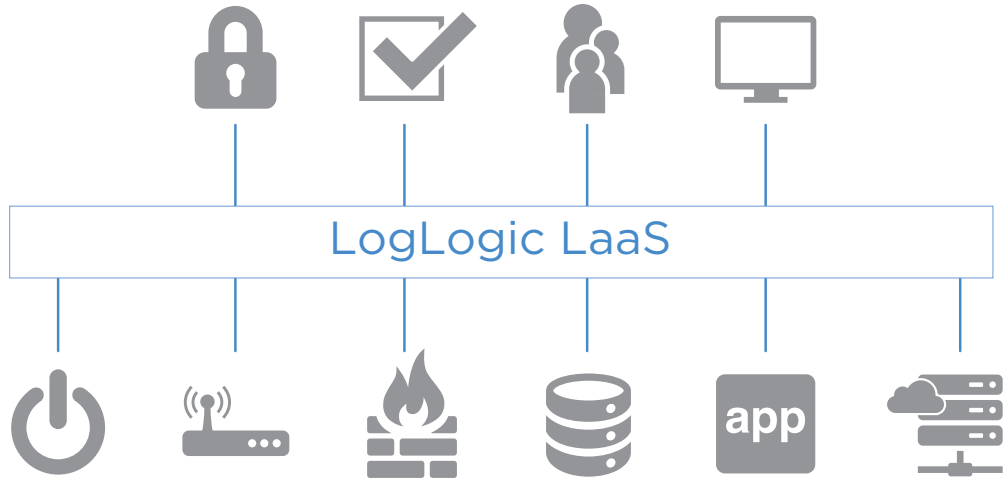
HARDWARE VERSUS SOFTWARE

The LogLogic solution can be deployed as a traditional hardware solution or as a virtual appliance. Both implementations offer the same capabilities and functionality and can be mixed and matched within your environment. Interoperability between both platforms reduces global deployment times without compromising your requirements. TIBCO LogLogic hardware is highly specialized to support the needs of large scale enterprises, with optimizations for both storage and analysis. The appliances have a small mountable form factor to conserve rack space. TIBCO Logging as a Service allows intermingling of all hardware and software lines allowing you to create a Machine Big Data infrastructure capable of routing data securely to the necessary consumers—whether SIEMs, managed security services providers, custom internal applications, or our own search and reporting solutions.

FIGURE 1
Accidental Architecture:
Complex, Costly, Risky

In the accidental architecture, log and event data accumulates from multiple sources that are connected to multiple applications. Cost increases because you have to manage the log data in each application. Complexity increases as you add sources, creating new connections that can add up to thousands of endpoints. Risk increases because you may not know which applications have which data.

FIGURE 2
Logging as a Service:
Control, Insight, Assurance



Logging as a Service (Laas) provides a single source of truth for all log and event data. All applications and sources plug directly into the LaaS platform where you control what information is delivered to each end point. You can reduce storage costs, and configuring applications does not require changes to each endpoint. You can search across all logs and filter to make sure that log data goes where it's supposed to, which enhances security.

The TIBCO LogLogic virtual appliance lets you deploy a modularized infrastructure optimized for your use case. New virtual appliances can be spun up seamlessly and instantly to address capacity needs and operational requirements with complete interoperability. Distributed search options allow for faster results because of optimized load sharing. Virtual appliances are easily expanded, which eliminates the need to replace hardware, ensuring maximum uptime and reducing operating expenses.

"LOGLOGIC PROVIDES A ONE-TIME LICENSING COST, WHICH ELIMINATES BUDGETING GUESS WORK."

TIBCO LogLogic also provides a set of feature-rich applications that provide great ROI by utilizing log data. Besides its distributed search options, Google-like in their performance, the LogLogic system has an auditor-friendly workflow and was rated the number one compliance solution by Gartner in 2013. Our analytics engine provides visual insight into your data, with the ability to view many variables from a single overlay. Imagine being able to track your traffic by most active talkers, overlay a geographic intelligence map to understand where this activity originates, and link that to acceptable policies within your organization, all from a single view.

LICENSING COSTS

The TIBCO LogLogic solution provides a one-time licensing cost, which eliminates budgeting guess work. There are no hidden costs or additional fees, reducing the total cost of ownership, while ensuring reliable delivery. Many other log data management solutions have consumption pricing models. Some providers that license their application based on how much machine data is ingested and indexed per day will shut-off system access if license levels are exceeded, introducing a large operational risk. Besides this operational risk, another challenge with volume-based licensing is that you may never be able to establish a fixed cost. Many times unforeseen events such as a Denial of Service (DOS) attack can cause licensing costs to increase rapidly. By providing fixed licensing costs, TIBCO LogLogic helps you predict and control your total cost of ownership without compromising operational efficiencies, providing a more scalable, comprehensive solution.

Cloud solutions are emerging now as well, but decision-makers must be careful to be aware of how cloud storage relates to compliance and governance requirements. For example, with PCI 3.0, on-site storage is mandatory. A popular deployment model for Logging as a Service is to leverage a private cloud to deliver a service across the enterprise. This way information can be shared seamlessly and securely with all data consumers. LogLogic Logging as a Service delivers this functionality, reducing licensing cost, storage requirements, and providing a fixed, predictable model ensuring accurate budgeting.

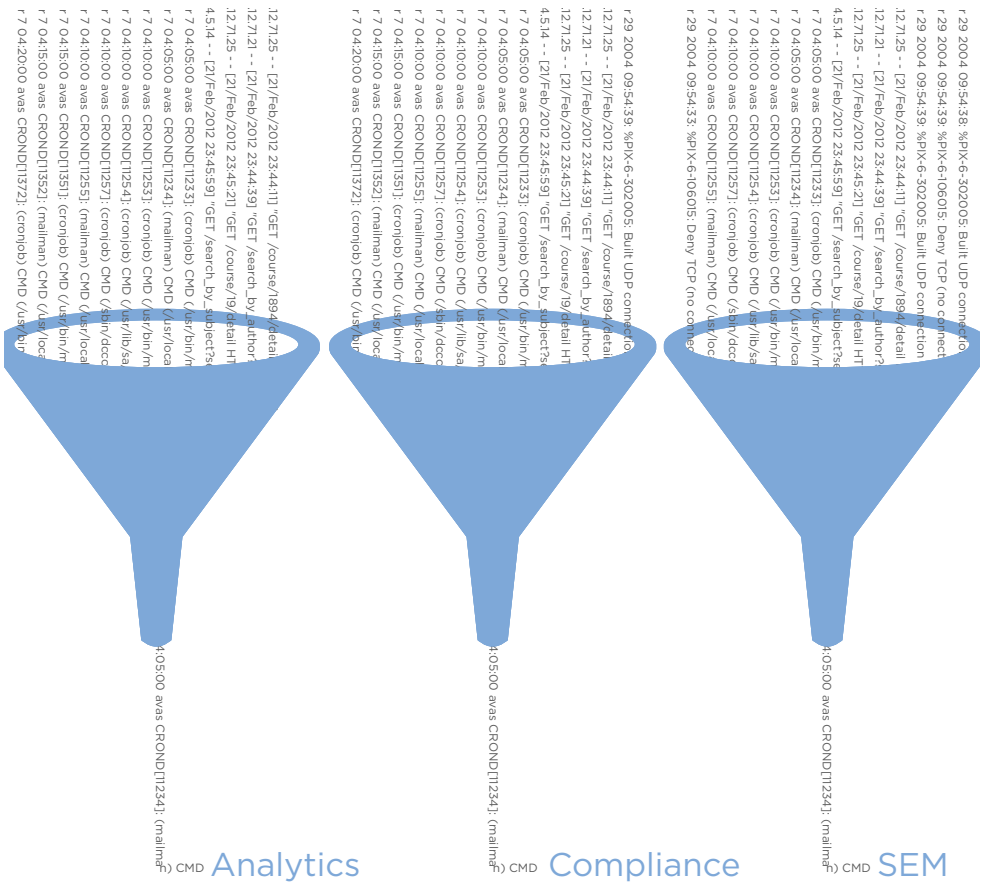
SPEED TO DEPLOY

TIBCO LogLogic's solutions are quick to deploy, and they are built on the strength of our data collection capabilities that auto identify over 200 common log sources. The ability to ingest log data quickly and make intelligent sense of this Machine Big Data helps you gain rapid insight and determine the causes of issues faster than competing solutions. LogLogic automatic log parsing eliminates the need for complex collectors and rules to manipulate and interpret data. Data can be forwarded with the necessary intelligence to operational, security, and compliance applications with little or no administrative overhead. The interoperability between the hardware and virtual appliances allows administrators to deploy virtual solutions as business requirements mandate, eliminating the time to order, ship, and "rack and stack" hardware solutions. Most organizations are able to deploy within a few hours and begin to see immediate return on their investment with minimal involvement from their operational teams.

FILTER FORWARDING

Filter Forwarding lets you use a centralized data collection strategy to optimize log data that is shared among different users including security event managers (SEMs); security operations centers (SOCs); managed security service providers (MSSPs); governance, risk, and compliance (GRC) applications; data analytics software; network monitoring solutions; and software development tools. TIBCO LogLogic filtering and forwarding functionality allows for the creation of rules to securely and transparently route Machine Big Data to any destination in real time. This technology is essential to any Logging-as-a-Service solution. Filter forwarding ensures access to the necessary data across the enterprise, providing administrators, security experts, compliance officers, and service providers with a powerful set of tools capable of searching and alerting across multiple system types. Alerts and Machine Big Data can be filtered by use case, business requirements, system type, location, and other factors, and then forwarded to the experts responsible, providing comprehensive visibility across platforms, adherence to compliance requirements, reduced diagnostic and mean time to repair, and overall efficiency improvement. An additional benefit of the filter and forward process is that it reduces the amount of data received by machine data consumers, which in turn results in improved performance of those solutions.

"FILTERING AND FORWARDING ALLOWS FOR THE CREATION OF RULES TO SECURELY AND TRANSPARENTLY ROUTE MACHINE BIG DATA TO ANY DESTINATION."



GRANULAR RETENTION

Machine Big Data collection requires sufficient storage to accommodate the large number of log sources. Storage schemes must maintain data online for users to access for quick searches (often to address critical security and operational needs) as well as provide archive capabilities for long term retention. Some compliance and operational requirements call for data retention for up to 10 years in raw format and searchability for audit and forensic purposes. Failure to retain or produce this data may be punishable with financial penalties, legal repercussions, and resulting loss of business. The primary challenge is how to archive and ensure access to this data and accommodate growing storage requirements with finite storage resources and budgets.

"GRANULAR RETENTION POLICIES ADDRESS THE SEEMINGLY CONTRADICTORY NEED FOR IMMEDIATE ACCESS TO DATA AND THE EVER-PRESENT PRESSURE TO KEEP STORAGE COSTS LOW."

TIBCO LogLogic has granular retention policies specifically constructed to address the seemingly contradictory needs for immediate access to data and the ever-present pressure to keep storage costs low. When built-in granular retention rules aren't sufficient, administrators can create custom retention rules to address business-specific needs. This flexibility lets you leverage storage, keep essential data only for the mandated time periods, and assign less critical log sources shorter retention periods. Additionally, granular data retention policies allow for custom retention periods for different sets of log data so that only the data you need is retained. This data can be managed using TIBCO LogLogic software for up to 10 years, as well as searched, reported, and alerted on.

SOLUTION BENEFITS

The TIBCO LogLogic LaaS platform is a highly scalable solution that offers an effortless lifecycle and true plug and play convenience. LogLogic licensing is not volume based so costs are predictable. Separate retention policies for high-speed indexed data and raw machine data result in improved use of storage resources while preserving the ability to search all machine data even outside of the indexed data retention period. Additionally, while LogLogic can parse and normalize machine data, it always stores 100 percent of the raw machine data, thereby functioning as the Machine Big Data system of record. LogLogic also supports many enterprise needs such as high availability (HA) and ensures that machine data is never lost. Growth and expansion capabilities are addressed quickly through the interoperability of hardware and virtual appliances, providing quick deployment of new capacity.

The TIBCO LogLogic Logging-as-a-Service solution has a fixed cost that in most cases provides savings and ROI in less than 2 years. Look to TIBCO LogLogic for a true LaaS platform to manage all Machine Big Data, ensure its real-time delivery to consumers, and continue advancing your operational capabilities.

TIBCO™

Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304
+1 650-846-1000 TEL
+1 800-420-8450
+1 650-846-1005 FAX
www.tibco.com

04/01/14