Machine Big Data – Filtering and Forwarding
Table of Contents

3 | State of Affairs
3 | The Problems
4 | The Solution
4 | How it Works
5 | Solution Benefits
State of Affairs
Every successful enterprise requires a myriad of information technologies to function. Whether these are applications, networks, or security devices, every platform is generating a continuous stream of log data. This log data contains vital information about your business, but most of it will go unnoticed. The sheer amount of data makes it difficult to use. This problem, Machine Big Data, can lead to unnecessary spending, complexity, and risk.

As with every form of vital information, Machine Big Data needs to be collected, stored, and distributed to the systems and people who need it. When this data is properly distributed, it can be used to reduce costs, improve efficiency, and foster growth in the enterprise. A better understanding of the technologies at the core of your organization helps you to make better choices when it comes to making improvements, changing things that aren’t working, or preparing yourself for what’s next.

The Problems
The initial challenge around Machine Big Data is simply discovering and dealing with the volumes generated by all machines and devices in the enterprise; is the device itself or the data generated by it critical to the business? If not, can it (or should it) be disposed of in a timely manner? Once the “business critical” data sources have been identified, the next challenge arises when filtering and distributing the data. which must reach the right destination at the right time and in a format that will be understandable to the target machine, application or stakeholder. Furthermore, most stakeholders and systems are only interested in a portion of the data, not all of it.

Redundant data causes network congestion and the need for storage expansion, which creates complexity that is costly and difficult to manage. The situation also creates a security issue if sensitive Machine Big Data is sent to the wrong destination or intercepted in transit.
The Solution

Just as normal Internet traffic needs to be routed, filtered, and secured, the same is true for Machine Big Data. Similar to a proxy server, load balancer, or any other network device that can act transparently, a Machine Big Data solution needs the ability to not only collect this data, but filter and forward it transparently and securely to its destination while maintaining data integrity.

The TIBCO Loglogic® solution is unique in its filtering and forwarding functionality.

How it Works

TIBCO Loglogic software can securely collect Machine Big Data via a variety of methods as required by the log source. For example, this data may be transmitted through a Secure Shell (SSH) connection or retrieved via a Secure Copy (SCP) file transfer. Once the Machine Big Data is collected, the TIBCO Loglogic software performs a Secure Hash Algorithm (SHA-256) of the data to prove integrity. Additionally, granular data retention policies allow for custom retention periods for each log source or log source group so that only the data your enterprise needs is retained. This data can be retained on the TIBCO Loglogic software for up to 10 years, as well as searched, reported, and alerted on.

Most enterprises will also need this data transparently filtered and forwarded in real time to a variety of destinations. Some examples include security event management (SEM) systems; security operations centers (SOC); managed security service providers (MSSPs); governance, risk, and compliance (GRC) applications; data analytics software; network monitoring solutions; and software development tools. The TIBCO Loglogic Filtering and Forwarding functionality allows for the creation of rules to securely and transparently route the Machine Big Data to any destination in real time. Additionally, each destination will only receive the data it needs, helping to avoid overloading the destination or over-extending its licensing. The end result is a streamlined architecture that reduces enterprise costs in a variety of ways including management overhead, network congestion, storage requirements, data security, and licensing needs.
Solution Benefits

The Filtering and Forwarding functionality of the TIBCO LogLogic solution benefits both IT operations and line of business stakeholders in several ways. For line of business stakeholders, the data is automatically, securely, and centrally collected for ease of access via a preferred “system of record,” meaning the users do not need to log into, search, or manually collect data from multiple sources, saving time and resources. From there, the data can be filtered and securely forwarded to enable other business critical applications and systems. IT operations get the benefit of a secure, user-friendly management console which completely automates the process of forwarding data to the appropriate systems and subsequently managing or auditing these systems centrally. Lastly, both IT operations and line of business stakeholders experience an increase in data quality and reduced risk of human error by allowing the TIBCO Loglogic solution to automate these processes.

“LogLogic really surpassed our expectations in every way, from the product’s capabilities and effectiveness, as well as the company’s commitment to customer service at every level.”

— Dan Barone
System Administrator
Plantronics

“LogLogic was the only product we evaluated that fit both my technical and budget criteria out-of-the-box. LogLogic installation is so simple – within a few days my IT team had it deployed properly, saving NARA time and money.”

— Elvis Morelan
Enterprise Level Security Architect
National Archives and Records Administration