IT Big Data Solution

A SCALABLE LOG INTELLIGENCE PLATFORM FOR SECURITY, COMPLIANCE, AND IT OPERATIONS

More than 1,300 customers across a variety of industries trust TIBCO LogLogic® solutions for compliance, security, and IT operations management. Our suite of log management products can help your organization overcome business and IT challenges:

- Big Data
- Regulatory Compliance
- Incident Management
- Risk Management
- Network Utilization and Troubleshooting
- Cloud
- Advanced Persistent Threats (APTs)
- Forensics
- Operations Management
- Service Level Agreements

The Problems We Solve

The problems we address are easy to define but harder to solve, namely the lack of control, visibility, and security in today’s IT environments. Valuable log and IT data is continuously generated from hundreds of sources such as network devices, security devices, servers, applications, databases, end-point devices, and more. This “big data” has become a big headache for IT and security professionals. But, if you could harness the power of this data, it can turn into a big advantage.
Driven By Insight
Regardless of whether you are required under a legal mandate to maintain compliance, need to improve your security stance, or simply want a more efficient IT infrastructure, the prerequisite is the same – you need deep insight to answer critical business questions such as:

• How well are you able to manage big data?
• How are you tracking log and IT data for your cloud infrastructure?
• How well is your organization adhering to regulatory compliance mandates or corporate policies?
• How quickly can you conduct forensics for a specific incident or event, such as a security breach?
• How effectively can you troubleshoot your network when a resource goes down?
• How are your IT networks and applications impacting your business?

Comprehensive Big Data Management
TIBCO LogLogic has one of the only scalable log and security intelligence platforms in the industry for enterprise and cloud infrastructures. More than 1,400 major global enterprises, including many of the Fortune 500, have turned to us to sustain their compliance, security, and information asset protection initiatives.

The award-winning LogLogic family of products works to deliver a comprehensive and scalable log and security intelligence platform that provides deep insight into IT infrastructure and provides actionable intelligence – for greater compliance, better security, and improved operational performance.

Solving Compliance Issues
With the increase in regulation across all industries, compliance has become one of the great challenges facing businesses today. LogLogic’s family of products helps you monitor enterprise activity, identify and respond to threats, and manage and review network policies according to industry and government rules. TIBCO LogLogic® Compliance Manager can not only help with your compliance reports, but also provide a complete compliance workflow for audit and review.

• PCI DSS
• Sarbanes-Oxley
• COBIT
• HIPAA
• ISO
• NERC
• FISMA
• ITIL-ITSM
Key Benefits

- **Minutes to install, seconds to troubleshoot.** Easy to install, deploy, and review key data.

- **Compliance without the complexity.** Automation of key compliance activities such as log data collection, retention, review, and analysis.

- **Quick and useful insights.** Customizable dashboards and management reports.

- **Fastest response times in search.** Google-like search without the massive index size of competing products.

- **Shorter time to resolution.** Finding and fixing issues dramatically faster, from days to minutes.

- **Better storage and retention.** Less storage required for IT data and better utilization of network attached storage (NAS) and storage area network (SAN) resources.

- **Easy integration with your existing investments.** Patented IT data forwarding to third-party technologies.

- **Out-of-the-box real-time protection.** Automatic mapping of your IT assets against known patterns of behaviors.
Collect, Centralize, Consume

LogLogic eliminates point-to-point connections between data sources and consuming applications, replacing them with a centralized virtual pool of data for greater efficiency and reuse.

Collect

Universal collection is the ability to collect IT data from network devices, security devices, servers, applications, point-of-sale systems, and any other sources whether physical, virtual, on-site, or in the cloud. The key requirement is the ability to collect 100% of all log and IT data, 100% of the time. Because data is everywhere, LogLogic provides a wide array of tools to accomplish thorough collection – agent or agent-less collection methods. Our solution out-of-the-box comes with the most comprehensive support for devices and applications. In addition, customers can easily configure the solution to import data from any device.

Centralize and Contextualize

One key value of log and IT data management is data reuse and efficiency. These capabilities are accomplished by eliminating the point-to-point connections between sources and applications and replacing them with a centralized virtual pool of data to be used again and again across applications. With LogLogic’s massively scalable log and security intelligence platform, companies can effectively store and archive data to see every aspect of their IT operations and garner unprecedented insight into the workings of their IT infrastructure.

Centralizing all IT data in one place eliminates duplicate application storage silos, which in turn reduces network bandwidth usage, especially over the WAN. A consolidated, historical view of your organization’s data reduces the time it takes for searching or conducting root-cause analysis during a security breach or IT operations incident. Further, unlike data in operational systems that changes over time, IT data stored in our platform cannot be changed. It is immutable by design, with unchanging integrity and the ability to prove that something did or did not occur.

Consume

IT data is extremely useful, whether it’s employed to discover an incident or understand historical patterns. LogLogic helps you better use and manage your IT data. We offer a number of solutions and visualization tools that help you find the insight you need – whether for fast, real-time searches; root-cause analysis; forensics on particular incidents; internal and external pattern correlation for potential threats; or easy review of adherence to compliance mandates. In addition, our log management systems can connect and forward designated IT data to third-party solutions for analysis and reporting, helping you fully leverage your existing investments in compliance, security event management, IT operations management, SLA monitoring, custom applications, and more.