CASE STUDY GUIDEBOOK

Selecting TIBCO LogLogic® for Centralized Machine Data Management

BLUE HILL RESEARCH

Built from **Blue Hill Research**

BLUE HILL
RESEARCH

WHAT YOU **NEED TO KNOW**

The machine data generated by the various components of an IT environment offer a treasure trove of data regarding system operations and interactions, providing insight into current needs, pending issues, or historical trends. As such, the ability to read and identify patterns and anomalies in machine data can be used to detect security threats, manage IT compliance, avoid events that result in downtime, or improve system performance and IT resource deployment. For many organizations, the complexity and heterogeneity of their environments results in ongoing production of large volumes of unstructured data that is difficult to decipher and challenging to relate to operational processes.

Blue Hill Research profiled six organizations' investigation and evaluation of centralized machine data management solutions, and ultimate selection of ***TIBCO LogLogic***. The underlying investment drivers largely related to the need for insight supporting a variety of initiatives related to enterprise IT security, operational performance, and compliance.

Whatever the underlying motivation, all profiled organizations revealed a need for improved insight into the behavior of IT systems and devices in order to identify and prevent events that impacted system performance.

As a group, participants identified complex and disconnected data generation across enterprise systems as a common obstacle preventing needed insight.

MACHINE DATA MANAGEMENT CHALLENGES
DRIVING INVESTMENTS

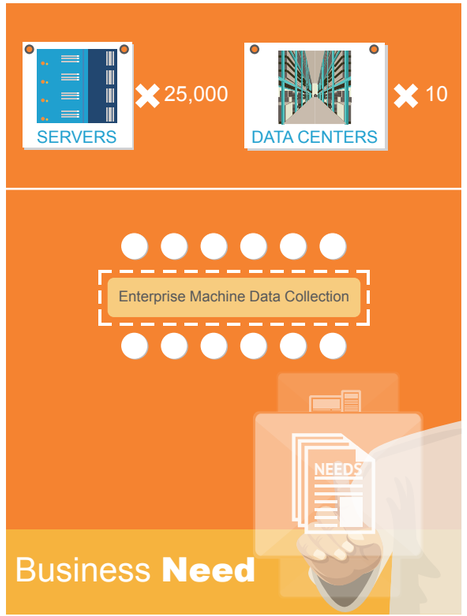
Volume of Machine Data

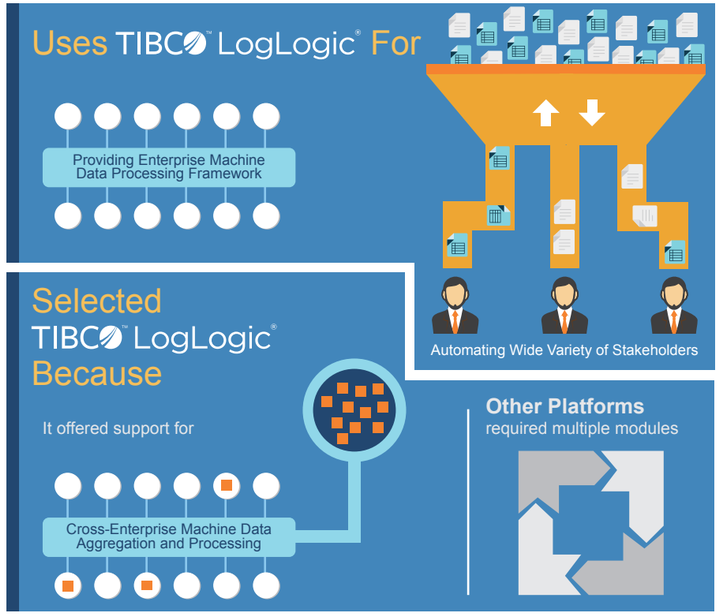
Contributing Factors

- Active IT environment
- Large number of operations
- Large number of data centers and systems

Multiple Disconnected Systems Generating Data

- Multiple systems generating machine data
- Lack of connection between systems and data centers
- Multiple redundant machine data collection silos





TELECOMMUNICATIONS PROVIDER

Over **$100** billion in revenue

Over **150,000** employees

Operations spread across the **globe**

Business **Need**

- Maintain IT compliance across complex and widely distributed systems
- High volumes of machine data across 25,000 servers and 10 data centers
- Single point of enterprise machine data collection needed

Uses TIBCO LogLogic For

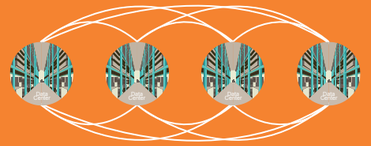
- Providing a single enterprise machine data processing framework
- Automating reporting across wide variety of stakeholders

Selected TIBCO LogLogic Because

- It offered support for cross-enterprise machine data aggregation and processing
- Other platforms were too difficult to use and required multiple modules to get the capabilities needed

Business **Need**

Challenge



Uses TIBCO LogLogic® For

Selecte TIBCO LogLogic® For

SOFTWARE PROVIDER

Focuses on **financial** sector

100 employees

4 offices

Business **Need**

- Products process high volumes of personally identifiable information
- Security is a market requirement and differentiator

Challenge

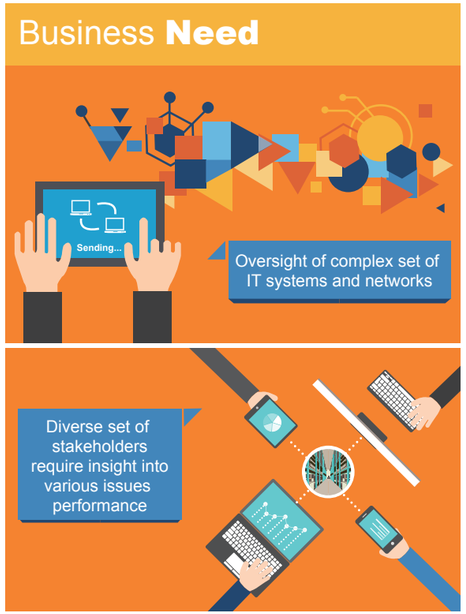
- Products run in highly robust environments across multiple data centers

Uses TIBCO LogLogic® For

- Monitoring operations logs
- Troubleshooting system issues

Selected TIBCO LogLogic® For

- Quality
- Cost Structure
- Ease of Use



REGIONAL BANK

Over **$90** billion in assets managed

Over **14,000** employees

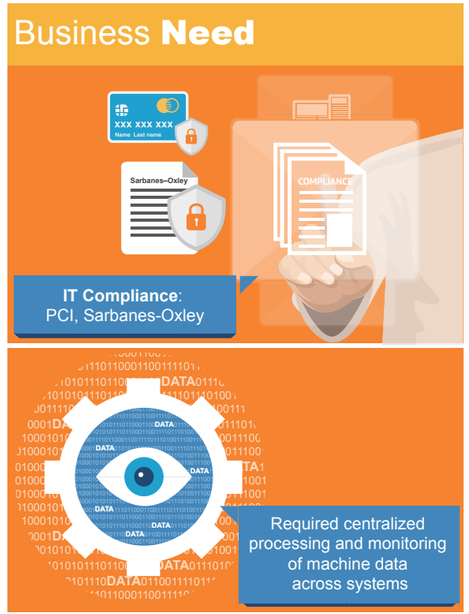
1,052 branches

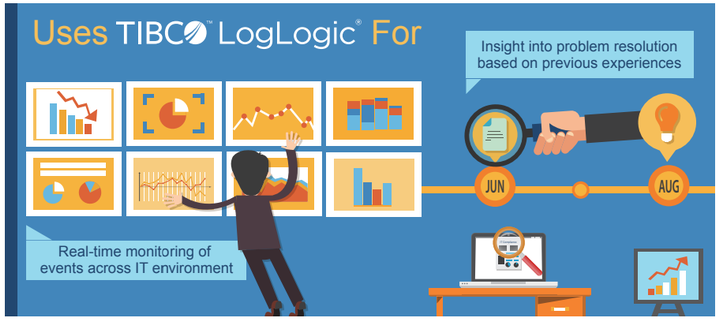
Business **Need**

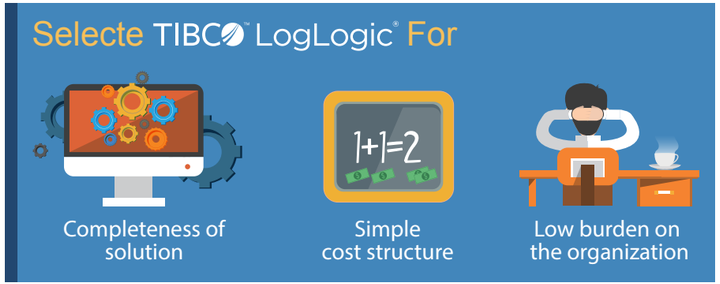
- Oversight of complex set of IT systems and networks
- Diverse set of stakeholders require insight into various issues performance

Uses TIBCO LogLogic For

- Monitoring IT operations and intelligence gathering
- Instant feedback on the environment and daily planned activities
- Strategic insight into historic trends and data to optimize performance







INSURANCE PROVIDER A

$3.1 billion in revenue

Over $17 billion in assets

Over 4,500 employees

3 offices

Business **Need**

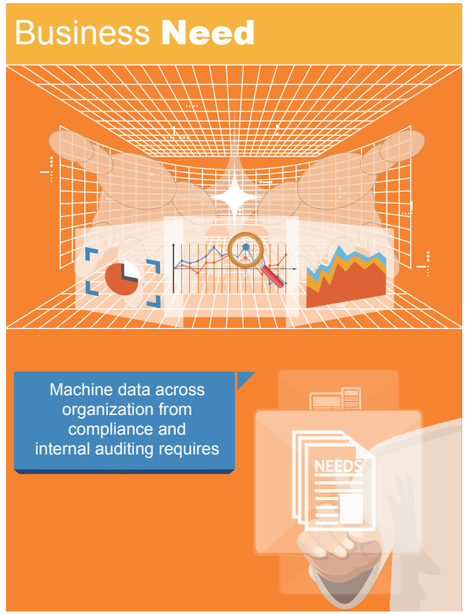
- IT Compliance: PCI, Sarbanes-Oxley
- Required centralized processing and monitoring of machine data across systems

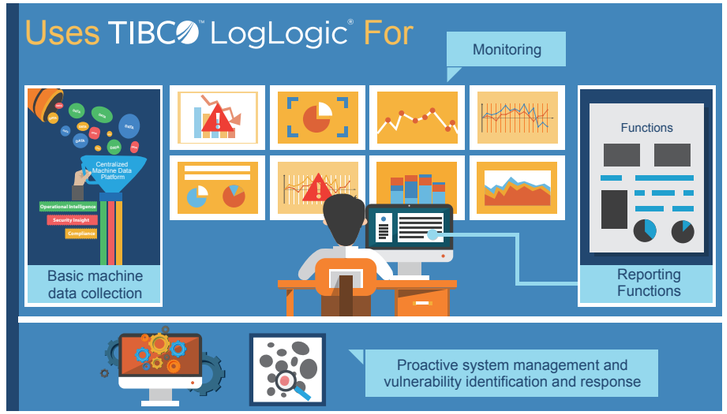
Uses TIBCO LogLogic For

- Real-time monitoring of events across IT environment
- Insight into problem resolution based on previous experiences
- Supporting compliance audits and due diligence requests

Selected TIBCO LogLogic For

- Completeness of solution
- Simple cost structure and deployment
- Low burden on the enterprise IT





INSURANCE PROVIDER B

Over **1** million policy-holders

Over **5,000** employees

10 offices

Business **Need**

- Compliance and internal auditing requires machine data across organization

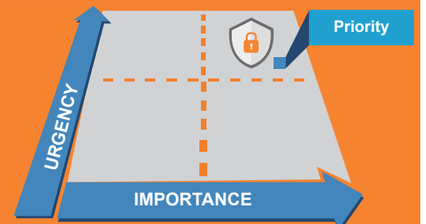
Uses TIBCO LogLogic® For

- Basic machine data collection, monitoring, and reporting functions
- Proactive system management and vulnerability identification and response

Selected TIBCO LogLogic® Because

- It was the best in class for machine data collection appliances

Investment **Driver**



CISO focused on transforming **security** into a strategic **priority**

Challenge

Solution **Evaluation** and **Selection**

A Central Machine Data Management Platform


Machine Data Aggregation


Data Processing & Analysis


Reporting and Alerting


Actual Access to Logs and Data

Evaluated

Selection Criteria


Functionality

Ease of Use

Cost

STATE HUMAN SERVICES AGENCY


Over **570** employees


2 IT support staff in CISO's office


Over **58** offices


Complex set of systems and data centers

Investment **Driver**

- CISO focused on transforming security into a strategic priority for the organization

Challenge

- Logs "were everywhere" and needed to be consolidated. Because of this, security investigations became nearly impossible to conduct. It took days to track down needed information.

Solution **Evaluation** and **Selection**

- Needed a central machine data management platform providing
  - Machine data aggregation
  - Data processing and analysis
  - Reporting and alerting
  - Actual access to logs and data
- Evaluated
  - LogLogic, splunk, ArcSight, Q1
- Selection Criteria
  - Functionality, Ease of use, Cost

EVALUATION OF LOGLOGIC AND COMPETITIVE OPTIONS

	TIBCO LOGLOGIC	OTHER SOLUTIONS EVALUATED
FUNCTIONALITY	• All requirements met • Best functionality available • Strongest mix of machine data management capabilities available • Lacked advanced capabilities of full SIEM suite that might be relevant to future investments	• Most requirements met • Machine data and log management capabilities generally described as 'adequate' • Often included additional capabilities that were not focus of investment but had value in SIEM or other future investments • Too many modules required to get needed functionality
EASE OF USE	• "Extremely easy" to use • Intuitive • "Much better than competitors" • "Nice clean solution"	• Complex and challenging to use • "Frustrating"
EASE OF INTEGRATION WITH INFRASTRUCTURE	• Fit architecture with no problems • Easy to implement • Hardware-based option found to be stable with minimal burdens	• Some customization required • Complexity of deployment models created redundant work
COST & PRICING	• Reasonably priced • Pricing model simple • Flat fees with no surprises	• Tended to be more expensive • Complexity of pricing models based on use and searches made it difficult to understand cost of solution • Represented financial risk, value for organization could not be determined until investment was made

Blue Hill Research | bluehillresearch.com | @BlueHillBoston
24 School Street, Mezzanine, Boston, MA 02108