Data Analytics Platform

Derive Network Security Intelligence with Log Management Solutions

Business Challenges

Failure to analyse vast amount of machine data for untapped business value

With billions of connected devices, cloud technologies, distributed computing etc. it has almost become mandatory for every organization – big or small to proactively monitor, track and analyse IT Infrastructure for any suspicious activity. Moreover, Ensuring availability, reliability, and security of business services has always been very challenging for the network professionals, who have to manage an increasingly complex IT infrastructure.

Motadata Solution

Get real-time actionable insights from machine data to secure network with log management

Analyse machine data to identify trends and unleash meaningful insights with log management capabilities. Derive undiscovered insights from the vast untouched data with Elastic search precision from our log management & big data analytics platform. Motadata lets users search, monitor, alert and generate reports for all log data in real time. It proactively fights threats with event correlation analytics. The platform processes all kind of log data generated from multiple heterogeneous sources.

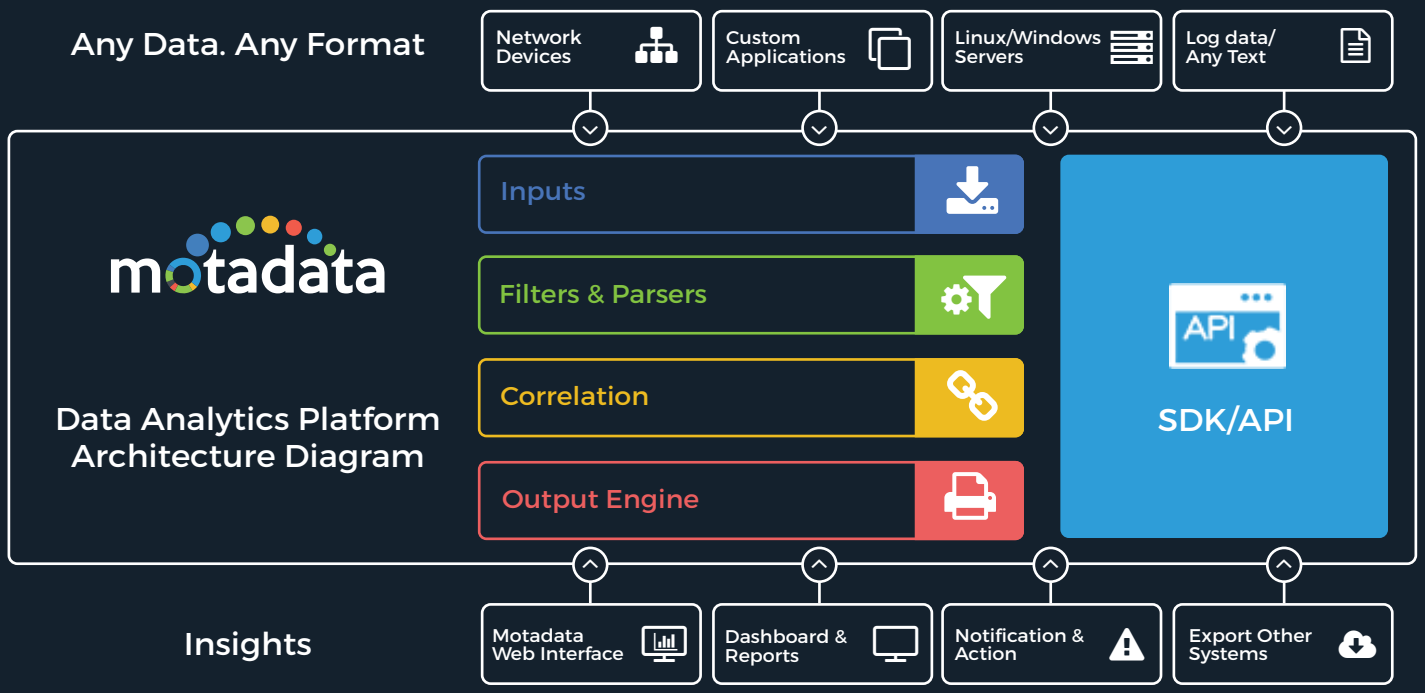
Motadata's Log Management Solution (Data Analytics Platform) collects, consolidates, indexes, stores any log and machine generated data, whether structured or unstructured. The data is then used to search, correlate, analyse and report any operational or security related issues in the network quickly. Motadata DAP acts as a central data repo by collecting data across sources from multiple locations to index and search them for review and retention requirements. The built-in correlation algorithms also provide proactive analytics to detect critical events. The platform enables organization to meet compliance standards such as PCI DSS, FISMA, HIPPA.

Features

- End-to-end traffic monitoring from single console
- Unlimited Logs Export
- Normalize bulk log data without any data compression & retain them for longer period
- Analyse machine data to identify trends and unleash undiscovered insights
- Detect and identify operational and configuration issues immediately
- Perform security forensic analytics & get notified on audit violations
- Satisfy compliance requirements with proactive log management
- Gain deep level insights into bandwidth usage & traffic patterns
- Identify user, application or network element consuming maximum bandwidth
- Network traffic visibility in real-time to keep network under control
- Real-time & historical bandwidth usage

Benefits

- Lower the risk and improve security posture to reduce operational complexity
- Substantial reduction in network implementation, operation and management costs
- Real time business operations using log data
- Prevention of security intrusion and unauthorized access with proactive alerts
- Better protect infrastructure against both internal and external threats
- Snap out of Security Breaches & secure the network confidently
- Boost your network traffic analysis capability



Log Management

Get the most out of your machine and log data with the help of Motadata's log management. It is all about collecting, parsing and storing logs that helps IT teams to understand & derive intelligence. Motadata helps you, use your log and machine data for meeting compliances & IT security. The platform ensures real-time high availability along with efficient log data management with the use of fast & flexible search & indexing interface.

Monitored Elements

- Network Logs
- Custom Logs
- OOB Collectors Parsers (Windows, Linux, VMWare)
- Application Logs
- Syslog
- Server Logs

Key Highlights

- It supports logs from PostgreSQL, JDBC databases – Oracle, MS SQL, MySQL, IBM Informix, IBM DB2, Sybase, etc.
- Collect, index, correlate, search and analyse log data regardless of the format at sing location
- Analyse the aggregated logs of different formats from a single platform
- Access user friendly GUI and real-time visibility of dashboards in various formats
- Monitor and manage your AWS infrastructure logs
- It can retain logs for 180 days.
- It comes with RDBMS for data storage.

- Upload and index log data from a local PC/device to Motadata quickly
- No addition charge for native log collectors
- Keep track on who accessed or modified the files that are important
- Leverage pre-defined rules to find pattern in collected logs
- It is capable of accepting system logs via SNMP, IPMI, JMX, agent, etc.
- Forward logs with or without agents
- It can generate email responses to an administrator for incoming events.
- It can export collected data into any databases (SQL, NoSQL) via ODBC connectors.
- It can export collected syslog messages to any file types like CSV, XML, JSON, etc.
- It can determine log source type and handle them for reporting.
- It can selectively store syslog messages with severity levels for a defined period.
- It supports automated deployment & update, discovery, problem identification, baselining, etc.
- It supports integration with a service desk solution.
- It is capable to monitor min 500 IT Infrastructure nodes & 500 Applications (microservices based)
- Supports HA and auto discovery of network topology.
- It can handle an environment of mixed operating systems/OEMs.
- It can identify problems and issues based on triggers.
- It has management and filtering features to identify relevant logs and can correlate multiple events for RCA.
- It can display in human readable logs formats from devices like servers, firewalls, WAF, switches, routers, IPS, VMs, blades, etc.
- It identifies application failure and root cause analysis through correlation.
- Our solution supports IPv4/IPv6 pro and syslog over UDP and TCP.

motadata

sales@motadata.com
+91.79.2680.0900
www.motadata.com

Mindarray Systems Pvt. Ltd. a global IT product company, offers state of the art affordable yet powerful product suite - Motadata consisting of Network Management & Monitoring, Log Management, IT Service Management and Unified NMS Platforms. The platform empowers both IT administrators and CXOs to analyze, track & resolve IT operational issues by effectively monitoring various systems and devices from multiple vendors through a unified and centralized dashboard.

FEB2108