LogRhythm is a leading provider of unified security intelligence and analytics solutions, empowering organisations to expedite the detection, prioritisation and neutralisation of cyber-threats originating from inside and outside the network. The LogRhythm Security Intelligence Platform is designed to significantly reduce the mean-time-to-detect (MTTD) and respond (MTTR) to threats, enabling organisations to neutralise them before they cause a damaging cyber-incident or data breach. The deep visibility and understanding delivered by LogRhythm empowers enterprises to secure their networks and comply with regulatory requirements. LogRhythm delivers:

- Next-generation SIEM and Log Management
- Independent Endpoint Forensics and File Integrity Monitoring
- Network Forensics with Application ID and Full Packet Capture
- State-of-the-art Machine Analytics
  - Advanced Correlation and Pattern Recognition
  - User / Network / Endpoint Behaviour Anomaly Detection
- Structured and Unstructured Search
- Large data set analysis via visual analytics, pivot, and drill down
- Workflow enabled automatic response via LogRhythm's SmartResponse™
- Integrated Case Management

LogRhythm appliances
LogRhythm high performance appliances are built to deliver maximum flexibility, with options ranging from convenient all-in-one platforms to high performance, dedicated appliances for massive scalability in extremely large environments. LogRhythm’s distributed, incrementally scalable architecture ensures that deployments can scale horizontally and vertically by simply adding appliances. Benefits include:

- Building block architecture and geographic flexibility
- Expandable storage options with any sized model
- Centralised management
- Flexible high availability options with automatic failover
- Dedicated high performance collectors

Appliance options

**Platform Manager (PM)** - LogRhythm PM appliances provide alarming, notifications, case and security incident management, workflow automation, and centralised administration for a LogRhythm deployment. Each LogRhythm deployment has a single Platform Manager.

**Data Processor (DP)** - LogRhythm DP appliances provide high performance, distributed, and highly available processing of machine and forensic data. They receive machine and forensic data from Collectors and Forensic Sensors, leveraging LogRhythm’s Machine Data Intelligence taxonomy to transform data into a structured and contextualised form. Processors archive data and distribute both the original copy and the structured copy to other LogRhythm components in support of indexing, machine-based analytics, and alarming.

**Data Indexer (DX)** - LogRhythm DX appliances provide high performance, distributed, and highly scalable indexing of machine and forensic data. Indexers can be clustered to enable high availability and improved performance. Indexers store original raw data as well as structured data to enable structured and unstructured search-based analytics.

**All-in-one (XM)** - LogRhythm XM appliances provide the functionality of the PM, DP and DX appliances on a combined platform, as well as a fully portable AI Engine license. Many deployments begin with an XM configuration and are later combined with additional components to enable fault tolerance and increase capacity and performance of a LogRhythm deployment.

**AI Engine (AIE)** - LogRhythm AIE appliances deliver highly-scalable, patented machine analytics for advanced correlation and behavioural analysis, including automated behavioural, histogram, statistical and whitelist profiling. Multiple AI Engine nodes can be deployed in support of distributed analysis and workload scaling.

**Network Monitor (NM)** - LogRhythm NM appliances offer full visibility into network traffic, identifying applications via deep packet inspection, providing real-time unstructured search access to all metadata and packet captures. Network Monitor can also forward Layer 7 SmartFlow™ to the SIEM or other solutions for additional analysis.

**Data Collector (DC)** - LogRhythm’s optional DC appliances collect log, flow, and machine data for secure transport from remote locations to LogRhythm DCs and can encrypt and compress data prior to transport.

**High Availability and Disaster Recovery**
LogRhythm appliances are built with onboard redundancy for maximum fault-tolerance. LogRhythm’s flexible High Availability and Disaster Recovery solutions can be tailored to meet the specific requirements of any organisation. LogRhythm’s optional, integrated agents are configurable to failover to secondary and tertiary Data Processors, allowing for uninterrupted collection of data in the event a Data Processor is unavailable.
PRODUCT OVERVIEW - LOGRHYTHM HIGH PERFORMANCE APPLIANCES

LogRhythm appliance specifications
LogRhythm’s quick and easy installation, combined with flexible expansion capabilities provide a rapid time-to-value. Most commonly delivered via high-performance appliances with a building-block approach to architecture maximizes deployment flexibility and scalability. Whether you are expanding to meet growing enterprise-wide needs, or you have short-term compliance requirements and intend to expand the scope of your deployment later, LogRhythm can quickly and simply scale by adding additional appliances.

LogRhythm Storage Arrays
Optional LogRhythm Storage Arrays are optimised to provide maximum performance and enterprise-level expansion.