

LogRhythm high-performance appliances combine LogRhythm software with the appropriate hardware elements 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 enables deployments to scale both horizontally and vertically.

Benefits include:

- Building block architecture and geographic flexibility
- Expandable storage options with any sized model
- Centralized management
- Flexible high availability and disaster recovery options

LogRhythm XM

All-in-One (XM): LogRhythm XM appliances perform the work of a PM, DP, DX, and AIE, all on a single appliance. Many deployments begin with an XM appliance and are expanded over time to include additional components to increase fault tolerance, capacity and performance.

LogRhythm Enterprise

Platform Manager (PM): LogRhythm PM appliances perform centralized event management and administration for a LogRhythm deployment, including alarming, case management and APIs, workflow automation and more. Each LogRhythm deployment has a single Platform Manager.

Data Processor (DP): LogRhythm DP appliances receive machine and forensic data from Data Collectors and System Monitor agents and then perform distributed processing. DPs use our Machine Data Intelligence Fabric to transform data into a structured and contextualized form. Processors archive data and distribute both original and structured copies to platform components that perform indexing, machine-based security analytics, and alarming.

Data Indexer (DX): LogRhythm DX appliances perform distributed and highly scalable indexing of machine and forensic data. Multiple DXs can be clustered to improve performance and availability. Indexers store original raw data as well as structured data to enable structured and unstructured search-based analytics.

AI Engine (AIE): LogRhythm AIE appliances deliver highly scalable, patented machine analytics for advanced correlation and behavioral analysis, including automated behavioral, histogram, statistical and whitelist profiling. AI Engine scales horizontally to perform distributed analysis of massive workloads.

Add-on Appliances

Data Collector (DC): LogRhythm's optional DC appliances collect log, flow, and machine data. They encrypt, compress and transport data from remote locations to LogRhythm DPs, either in real time or on a schedule.

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

Disaster Recovery and High Availability Options

LogRhythm's flexible Disaster Recovery and High Availability solutions can be tailored to meet the specific requirements of your organization. LogRhythm appliances are built with onboard redundancy for maximum fault-tolerance, and our active/active architectures maximize the return on your investment.

Threat Lifecycle Management Platform

LogRhythm provides deep visibility into your environment, empowering you to secure your networks and comply with regulatory requirements.

LogRhythm delivers the following functionality on a unified platform:

- SIEM and log management on an Elasticsearch backend
- Network forensics with application ID and full packet capture
- Endpoint forensics and file integrity monitoring (FIM)
- Machine-automated security analytics
 - User and entity / network traffic / endpoint behavior analysis
 - Statistical analysis, advanced correlation, and other techniques
- Unstructured and structured search
- Intuitive dashboards and visualizations
- Integrated case management
- SmartResponse™ automation platform

“ It has been extremely easy for us to not only implement LogRhythm, but also extend LogRhythm to be a solution for a number of other monitoring challenges. ”

IT Professional, Large Retail Firm

Appliance Specifications

	Appliance Lines	Max Archiving Rates	Max Processing Rates	Chassis	CPU Physical/ Physical + Virtual (HT)	Memory (Expandable)	Internal Storage (Usable/Raw)	Expandable To (Usable/Raw)	Compression	Power	Ethernet	Height (in / cm)	Width (in / cm)	Length (in / cm)	Weight (lb / kg)
ALL-IN-ONE (XM) (Includes PM, DP, DX, AIE)	4401	10,000 MPS	1,000 MPS	1U	6 Core / 12 Core	64 GB	2.44 TB / 3.80 TB	26.33 TB / 29.86 TB	20:01	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	1.68 / 4.28	18.98 / 48.24	27.57 / 70.05	40.96 / 18.6
	6401	25,000 MPS	5,000 MPS	2U	12 Core / 24 Core	128 GB	13.30 TB / 15.74 TB	37.19 TB / 41.80 TB	20:01	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	3.44 / 8.73	18.99 / 48.24	28.46 / 72.30	69.23 / 31.4
	8400	40,000 MPS	10,000 MPS	2U	28 Core / 56 Core	256GB	24.43 TB / 27.15 TB	48.32 TB / 53.21 TB	20:01	100-240 VAC	Intel x540 DP (2 x 10Gb) 10GBASE-T, Intel I350 DP (2 x 1Gb)	3.44 / 8.73	18.98 / 48.24	29.75 / 75.58	67.02 / 30.4
DEDICATED PLATFORM MANAGER (PM) (Includes AIE license)	5400	N/A	N/A	1U	12 Core / 24 Core	128 GB	2.44 TB / 4.89 TB	15.48 TB / 30.95 TB	20:01	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	1.68 / 4.28	18.99 / 48.24	29.72 / 75.51	43.56 / 19.8
	7400	N/A	N/A	2U	16 Core / 32 Core	128 (256) GB	7.33 TB / 13.57 TB	26.89 TB / 52.66 TB	20:01	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	3.44 / 8.73	18.98 / 48.24	29.75 / 75.58	67.02 / 30.4
DEDICATED DATA PROCESSOR (DP)	5400	10,000 MPS	5,000 MPS	1U	6 Core / 12 Core	32 GB	556 GB / 1.08 TB	24.43 TB / 27.14 TB	20:01	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	1.68 / 4.28	18.98 / 48.24	27.57 / 70.05	40.96 / 18.6
	7400	50,000 MPS	25,000 MPS	1U	16 Core / 32 Core	64 GB	1.08 TB / 2.17 TB	24.97 TB / 28.23 TB	20:01	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	1.68 / 4.28	18.99 / 48.24	29.72 / 75.51	43.56 / 19.8
DEDICATED DATA INDEXER (DX)	5401	N/A	N/A	1U	6 Core / 12 Core	64 GB	6.79 TB / 10.32 TB	54.57 TB / 62.45 TB	N/A	100-240 VAC	Broadcom 5720 QP (2 x 1Gb)	1.68 / 4.28	18.98 / 48.24	27.57 / 70.05	40.96 / 18.6
	7401	N/A	N/A	2U	12 Core / 24 Core	128 (256) GB	24.16 TB / 26.61 TB	95.83 TB / 104.80 TB	N/A	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	3.44 / 8.73	18.98 / 48.24	26.92 / 68.40	67.02 / 30.4
	7500	N/A	N/A	2U	28 Core / 56 Core	256 (512) GB	36.38 TB / 40.18 TB	N/A	N/A	100-240 VAC	T Intel I350 DP (2x1Gb)	3.42 / 8.68	18.98 / 48.24	29.58 / 75.13	61.95 / 28.1
DEDICATED AI ENGINE (AIE)	5400	N/A	30,000 MPS	1U	16 Core / 32 Core	128 (256) GB	1.08 TB / 2.17 TB	N/A	N/A	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	1.68 / 4.28	18.98 / 48.24	27.57 / 70.05	40.96 / 18.6
	7400	N/A	75,000 MPS	1U	28 Core / 56 Core	256 (512) GB	1.08 TB / 2.17 TB	N/A	N/A	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	1.68 / 4.28	18.98 / 48.24	27.57 / 70.05	40.96 / 18.6
DATA COLLECTOR (DC)	3400	N/A	N/A	1U	4 Core	16 GB	278 GB / 556 GB	N/A	N/A	100-240 VAC	Broadcom 5720 DP (2 x 1Gb)	1.68 / 4.28	18.99 / 48.24	26.65 / 67.69	30.42 / 13.8
NETWORK MONITOR (NM)	3400	N/A	1 Gbps	1U	10 Core / 20 Core	64 GB	1.9 TB / 3.8 TB	25.9 TB / 28.9 TB	N/A	100-240 VAC	Intel I350 QP (4 x 1Gb)	1.68 / 4.28	18.98 / 48.24	27.57 / 70.05	40.96 / 18.6
	5400	N/A	5 Gbps	2U	24 Core / 48 Core	128 GB	12.5 TB / 13.9 TB	60 TB / 66 TB	N/A	100-240 VAC	Broadcom 5720 QP (4 x 1Gb) Intel X540 DP (2 x 10Gb) 10GBASE-T	3.44 / 8.73	18.98 / 48.24	29.75 / 75.58	67.02 / 30.4
WEB APPLIANCE	3400	N/A	N/A	1U	8 Core / 16 Core	32 GB	556 GB / 1.08 TB	N/A	N/A	100-240 VAC	Broadcom 5720 QP (4 x 1Gb)	1.68 / 4.28	18.99 / 48.24	27.57 / 70.05	40.96 / 18.6

Storage Arrays

Direct Attached Storage	Hard Drives	Wattage	Power	Heat Dissipation	Chassis	Heigh (in / cm)	Width (in / cm)	Length (in / cm)	Weight (lb / kg)
LR-SA3450	24 x 300 GB 10K RPM. SASI 12Gbps, 2.5 in. Hot Plug Hard Drives	600 W	100-240V	188 W	2U	3.39 / 8.7	18.8 / 48.2	29.1 / 54.1	53.35 / 24.2
LR-SA3490	24 x 1.2 TB 10K RPM, SAS 12GBPS, 2.5 in. Hot Plug Hard Drives	600 W	100-240V	188 W	2U	3.39 / 8.7	18.8 / 48.2	29.1 / 54.1	53.35 / 24.2
LR-SA5410	24 x 1.8 TB 10K RPM SAS 12Gbps, 2.5 in. Hot Plug Hard Drives	600 W	100-240V	188 W	2U	3.39 / 8.7	18.8 / 48.2	29.1 / 54.1	53.35 / 24.2
LR-SA7470	24 x 600 GB 15K RPM, SAS 12Gbps, 2.5 in. Hot Plug Hard Drives	600 W	100-240V	188 W	2U	3.39 / 8.7	18.8 / 48.2	29.1 / 54.1	53.35 / 24.2