A Higher Standard In SIEM & Security Analytics

LogRhythm delivers unparalleled cyber threat defense, detection & response. At its core is the ability to collect log, flow and machine data from any source and apply advanced analytics to detect and respond to even the most sophisticated cyber threats and breaches. Our SIEM 2.0 solution includes:

- Multi-Dimensional Behavioral Analytics
  - Advanced Correlation & Pattern Recognition
  - Automated Behavioral Whitelisting
  - Statistical Baselining
- Real-Time Alarming
- Flexible and Powerful Reporting
- Advanced Forensic Analysis
- Dynamic Visualization Tools
- SmartResponse™

LogRhythm is operated and managed through an easy-to-use and individually customizable console. It correlates native log, flow and machine data with independently-generated host and network forensics and network forensics, performing both real time and forensic analysis across all data. LogRhythm analytics delivers the actionable intelligence and incident response required to address today’s most sophisticated cyber threats.

Rapid Time-to-Value

Few organizations have the budget or manpower for an expensive and protracted implementation of a SIEM or Security Analytics solution. LogRhythm is quick to install, easy-to-use and manage, and scales quickly to meet any future requirements.

Architected from the ground up to provide Rapid Time-to-Value while reducing the Total Cost of Ownership (TCO), LogRhythm delivers:

- Fast & Easy Deployment
- Intuitive, Customizable Dashboard
- Out-of-the-box Compliance Automation Suites
- Over 300 Out-of-the-box Advanced Analytic Rule Sets
- Ready-to-use Reports, Alerts and Investigations
- Embedded LogRhythm Labs™ Expertise

LogRhythm solutions are available in flexible appliance and software deployment options to meet the unique operating requirements of any enterprise.
THE PLATFORM FOR BIG DATA SECURITY ANALYTICS

Input
FORENSIC DATA COLLECTION
- Packet Capture
- Network Connection Monitoring
- DPI / Application ID
- Host Forensics
- Network Forensics
- File Integrity Monitoring
- Data & Process Monitoring
- Layer 7 Flow
- Network Connection Monitoring
- Packet Capture Monitoring

FORENSIC DATA GENERATION
- Log Data
- Application Data
- Flow Data
- Vulnerability Data
- Event Data
- Other Machine Data

Output
ACTONABLE INTELLIGENCE
- Risk Prioritized Alerts
- Real-Time Dashboards
- Reports

REAL-TIME ANALYSIS
- Advanced Correlation
- Behavioral & Statistical Baselines
- Meta Data Classification
- Pattern Recognition
- Whitelist Profiling
- Search
- Context Infusion
- Persistence

FORENSIC ANALYSIS
- Risk Prioritization
- Context Infusion
- Indexing
- Visualization
- Pivot/Drill Down

ADAPTIVE CYBER DEFENSE
- THE PLATFORM FOR BIG DATA SECURITY ANALYTICS
- LogRhythm Analytics™
- 4:21:53
- Time Normalization
- Data Classification
- Behavioral & Statistical Baselines
- Real-Time Analysis
- Advanced Correlation
- Behavioral & Statistical Baselines
- Risk Prioritization
- Context Infusion
- Persistence
- Visualization
- Pivot/Drill Down

Search

Indexing

Persistence

Behavioral & Statistical Baselines

LogRhythm Analytics™

4:21:53

Time Normalization

Data Classification

Pattern Recognition

Whitelist Profiling

Search

Context Infusion

Persistence

Behavioral & Statistical Baselines

Real-Time Analysis

Advanced Correlation

Behavioural & Statistical Baselines

Risk Prioritization

Context Infusion

Persistence

Visualization

Pivot/Drill Down

LogRhythm Analytics™

4:21:53

Time Normalization

Data Classification

Pattern Recognition

Whitelist Profiling

Search

Context Infusion

Persistence

Behavioral & Statistical Baselines

Real-Time Analysis

Advanced Correlation

Behavioural & Statistical Baselines

Risk Prioritization

Context Infusion

Persistence

Visualization

Pivot/Drill Down

LogRhythm Analytics™

4:21:53

Time Normalization

Data Classification

Pattern Recognition

Whitelist Profiling

Search

Context Infusion

Persistence

Behavioral & Statistical Baselines

Real-Time Analysis

Advanced Correlation

Behavioural & Statistical Baselines

Risk Prioritization

Context Infusion

Persistence

Visualization

Pivot/Drill Down
### Flexible Deployment Options

#### High Performance Appliances

<table>
<thead>
<tr>
<th>Appliance Lines</th>
<th>ALL-IN-ONE <em>(XM)</em> (Includes EM, LM, AIE)</th>
<th>DEDICATED EVENT MANAGER <em>(XM)</em> (Includes AI Engine license)</th>
<th>DEDICATED LOG MANAGER <em>(LM)</em></th>
<th>DEDICATED AI ENGINE <em>(AIE)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Lines</td>
<td>4300</td>
<td>6300</td>
<td>5300*</td>
<td>7300*</td>
</tr>
<tr>
<td>Performance Rates</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Per Second (MPS)</td>
<td>MPS</td>
<td>MPS</td>
<td>MPS</td>
<td>MPS</td>
</tr>
<tr>
<td>Max Archiving Rates ***</td>
<td>10,000</td>
<td>25,000</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Max Processing Rates ***</td>
<td>1,000</td>
<td>5,000</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**APPLIANCE SPECIFICATIONS**

<table>
<thead>
<tr>
<th>Chassis</th>
<th>1U</th>
<th>2U</th>
<th>2U</th>
<th>2U</th>
<th>1U</th>
<th>2U</th>
<th>2U</th>
<th>1U</th>
<th>1U</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>6 Core</td>
<td>12 Core</td>
<td>12 Core</td>
<td>16 Core</td>
<td>6 Core</td>
<td>12 Core</td>
<td>16 Core</td>
<td>6 Core</td>
<td>16 Core</td>
</tr>
<tr>
<td>Memory (Expandable)</td>
<td>32 (64) GB</td>
<td>64 (128) GB</td>
<td>64 (128) GB</td>
<td>128 (256) GB</td>
<td>32 (64) GB</td>
<td>64 (128) GB</td>
<td>128 (256) GB</td>
<td>64 (128) GB</td>
<td>128 (256) GB</td>
</tr>
<tr>
<td>Internal Storage (Usable/Raw)</td>
<td>1 TB / 2 TB</td>
<td>1.5 TB / 3 TB</td>
<td>1.5 TB / 3 TB</td>
<td>3 TB / 6 TB</td>
<td>1 TB / 2 TB</td>
<td>1.5 TB / 3 TB</td>
<td>3 TB / 6 TB</td>
<td>1 TB / 2 TB</td>
<td>2.5 TB / 5 TB</td>
</tr>
<tr>
<td>Expandable To (Usable/Raw)</td>
<td>5 TB / 10 TB</td>
<td>5.5 TB / 11 TB</td>
<td>9.5 TB / 19 TB</td>
<td>15 TB / 30 TB</td>
<td>5 TB / 10 TB</td>
<td>9.5 TB / 19 TB</td>
<td>15 TB / 30 TB</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*Includes Embedded AIE License of 5,000 MPS. **Includes Embedded AIE License of 10,000 MPS. ***Individual rates vary based on customer environment/requirements.

---

**LogRhythm has set the standard for SIEM 2.0.**

**ASCENT MEDIA**

**One terrific product and an equally terrific value. We make it our BEST BUY.**

**SC MAGAZINE**

**LogRhythm is long on FEATURES & FLEXIBILITY.**

**INFOWORLD**

---

**Software | Virtualization**

LogRhythm Solution Software can be easily deployed on customer provided hardware and several major virtualization platforms:

- VMware
- Windows Server 2008
- Citrix XenServer

**Professional Services**

**Expertise, Availability & Assurance**

Our professional services team applies industry and regulatory expertise to ensure customer success through:

- Deployment
- Health Checks
- Tune-ups
- Upgrades
- Compliance Support
- Search, Report & Alert Optimization
- Custom Device Support
- Classroom-based, Web-based & On-site Training Programs

---

**LogRhythm Labs**

LogRhythm Labs automates the process of turning raw data into actionable intelligence with relevant context, delivering enterprise correlation and meaningful visibility into the entire network. Customers benefit from continuous research and development and receive:

- Comprehensive Device Support
- Expert Event and Threat Level Identification
- Intelligent Alarms, Investigations and Reports
- SmartResponse™ Scripts for Common Use Cases
- Out-of-the-box, Compliance Automation Suites (PCI, SOX, HIPAA, FISMA, GPG 13, GLBA, NERC CIP, etc.)

**Support Services**

**Dedicated to Customer Satisfaction**

- 11/5 Mon-Fri or 24/7 Support Options
- 24/7 Access to Support Portal
- Knowledgebase Updates
- Web-based Tutorials
- Custom Support Programs