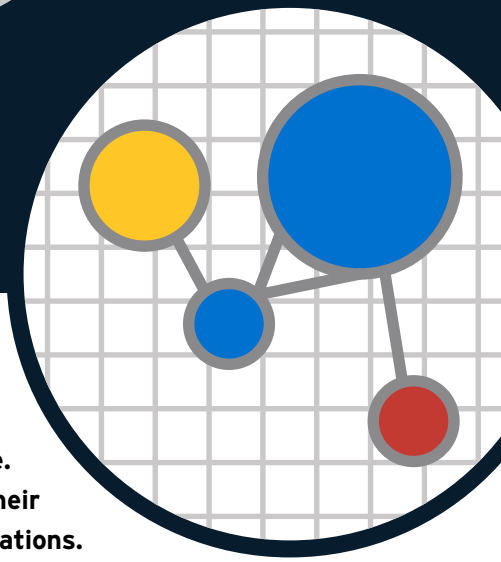
LogRhythm™

THE PLATFORM FOR BIG DATA SECURITY ANALYTICS



The indicators of today's advanced threats and breaches lie in the billions of logs, flows and other machine data generated every day across an enterprise. LogRhythm's award-winning Big Data Security Analytics Platform enables customers to detect and respond to those threats faster and with greater accuracy than ever before. LogRhythm's SIEM 2.0 solution empowers customers around the globe to secure their networks, comply with regulations and gain operational intelligence for their IT organizations.

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
- Smart**Response**™

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

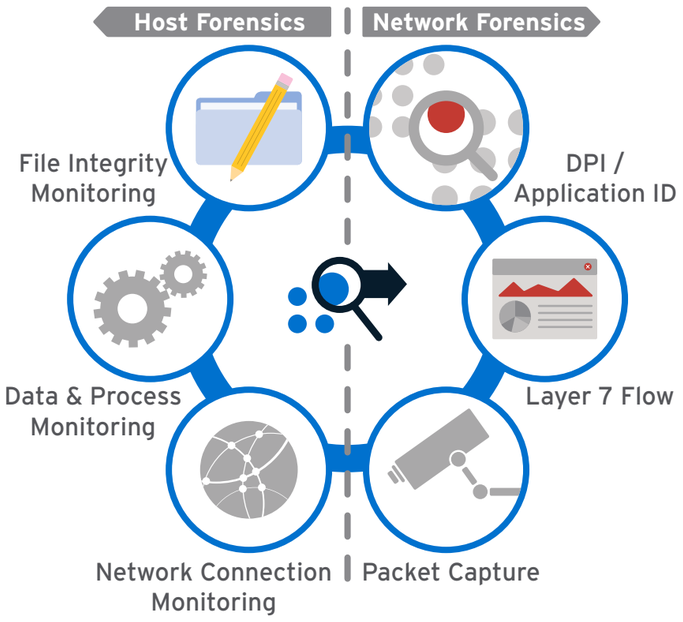
LogRhythm solutions are available in flexible appliance and software deployment options to meet the unique operating requirements of any enterprise.

THE PLATFORM FOR BIG DATA SECURITY ANALYTICS

Input

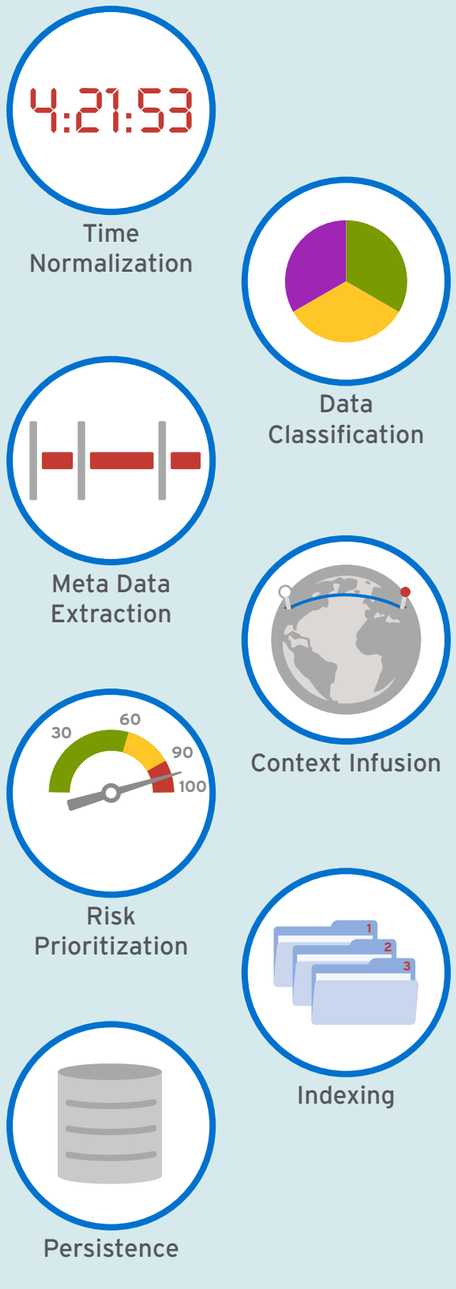
FORENSIC DATA COLLECTION

FORENSIC DATA GENERATION

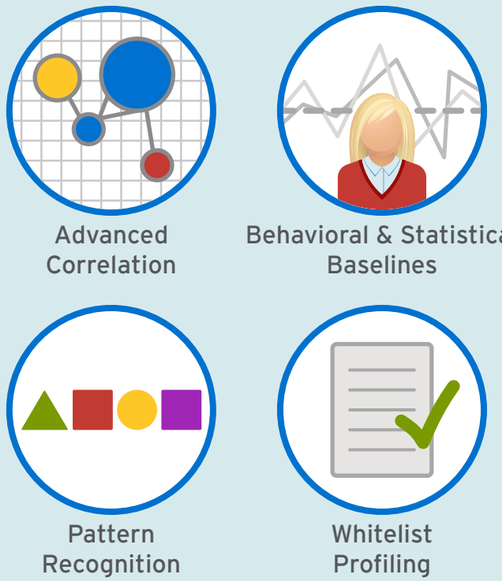


LogRhythm Analytics™

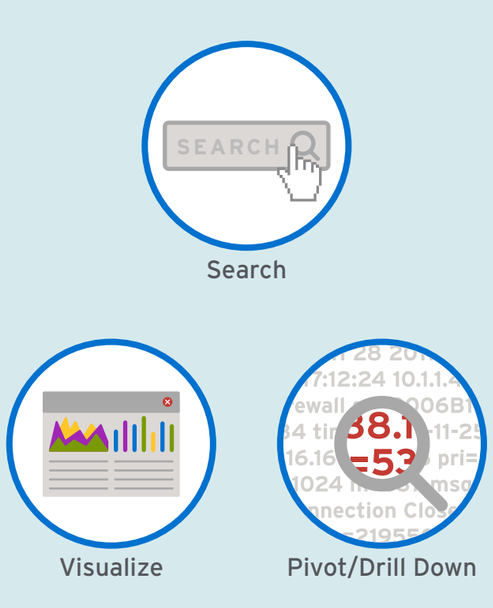
PROCESSING



REAL-TIME ANALYSIS



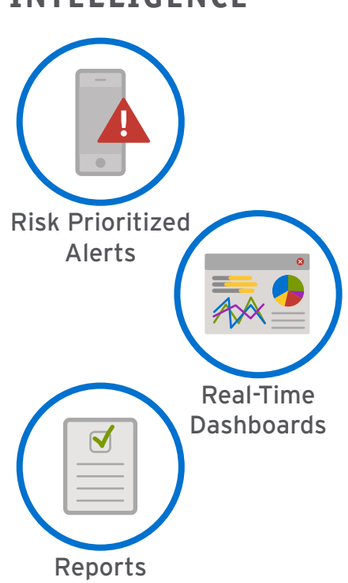
FORENSIC ANALYSIS



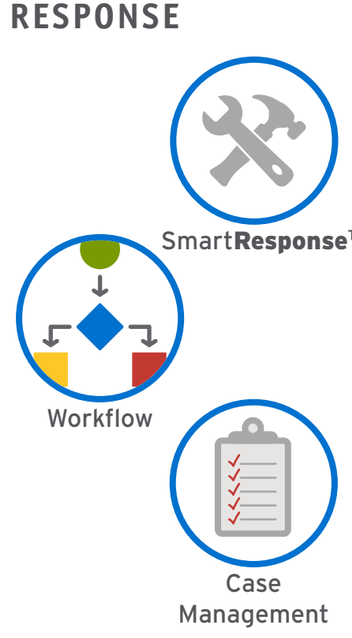
ADAPTIVE CYBER DEFENSE

Output

ACTIONABLE INTELLIGENCE



INCIDENT RESPONSE



Flexible Deployment Options
High Performance Appliances

	ALL-IN-ONE (XM) (Includes EM, LM, AIE)		DEDICATED EVENT MANAGER (XM) (Includes AI Engine license)		DEDICATED LOG MANAGER (LM)			DEDICATED AI ENGINE (AIE)	
Appliance Lines	**4300**	**6300**	**5300***	**7300***	**3300**	**5300**	**7300**	**5300**	**7300**
Performance Rates Messages Per Second (MPS)	MPS		MPS		MPS			MPS	
Max Archiving Rates ***	10,000	25,000	N/A	N/A	10,000	25,000	50,000	N/A	N/A
Max Processing Rates ***	1,000	5,000	N/A	N/A	2,000	5,000	15,000	5,000	30,000
APPLIANCE SPECIFICATIONS									
Chassis	1U	2U	2U	2U	1U	2U	2U	1U	1U
CPU	6 Core	12 Core	12 Core	16 Core	6 Core	12 Core	16 Core	6 Core	16 Core
Memory **(Expandable)**	32 (64) GB	64 (128) GB	64 (128) GB	128 (256) GB	32 (64) GB	64 (128) GB	128 (256) GB	64 (128) GB	128 (256) GB
Internal Storage **(Usable/Raw)**	1 TB / 2 TB	1.5 TB / 3 TB	1.5 TB / 3 TB	3 TB / 6 TB	1 TB / 2 TB	1.5 TB / 3 TB	3 TB / 6 TB	1 TB / 2 TB	2.5 TB / 5 TB
Expandable To **(Usable/Raw)**	5 TB / 10 TB	5.5 TB / 11 TB	9.5 TB / 19 TB	15 TB / 30 TB	5 TB / 10 TB	9.5 TB / 19 TB	15 TB / 30 TB	N/A	N/A

*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 Hyper-V · 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:

LogRhythm LABS

- Comprehensive Device Support
- Expert Event and Threat Level Identification
- Intelligent Alarms, Investigations and Reports
- Smart**Response**™ 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