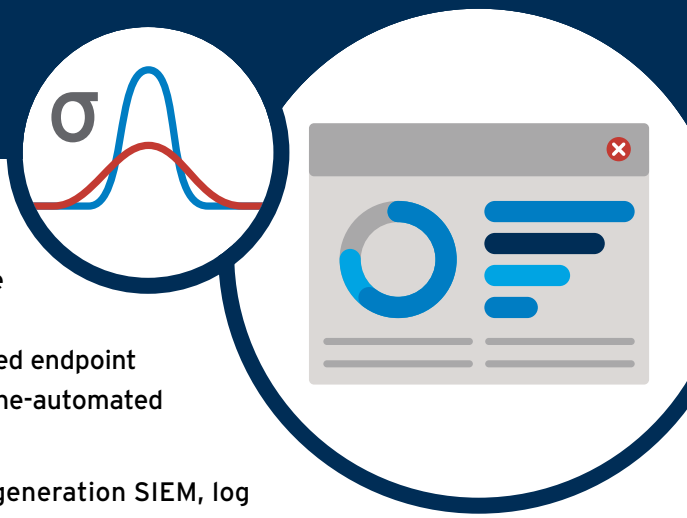
LOGRHYTHM'S SECURITY INTELLIGENCE PLATFORM

LogRhythm



Protecting against today's rapidly evolving threat landscape requires broad and deep visibility across the entire IT environment. Threats arrive from many angles and evidence of their existence can be found within existing log and machine data. Further visibility is gained through targeted endpoint and network forensic monitoring. When this is applied to multiple, machine-automated analysis techniques, threats and risks are exposed like never before.

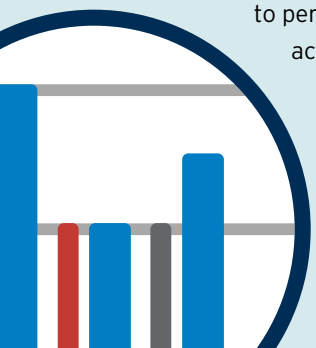
LogRhythm delivers solutions for threat lifecycle management, next-generation SIEM, log management, endpoint/network monitoring and forensics, and security analytics in a unified Security Intelligence Platform. The LogRhythm platform provides profound visibility into threats and risks to which organizations are otherwise blind. Designed to help prevent breaches before they happen, LogRhythm accurately detects an extensive range of early indicators of compromise, enabling rapid response and mitigation. The deep visibility and understanding delivered by LogRhythm's Security Intelligence Platform empowers enterprises to secure their networks and comply with regulatory requirements.

A Higher Standard In SIEM & Security Intelligence

LogRhythm delivers a unified set of capabilities for detecting, prioritizing, and neutralizing cyber threats and associated risks. LogRhythm's Security Intelligence Platform 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, Pattern Recognition, and Machine Learning
  - Multi-dimensional User / Network / Endpoint Behavior Anomaly Detection
- Rapid contextual and unstructured search
- Data set analysis via visual analytics, pivot, and drill down
- Workflow-enabled automatic response via Smart**Response**™
- Integrated Case and Security Incident Management

True visibility can be attained by analyzing all available log and machine data and combining it with deep forensic visibility at the endpoint and network levels. This insight is leveraged by AI Engine, our patented Machine Analytics technology, to perform continuous, real-time analysis of all activity observed within the environment. AI Engine empowers organizations to identify previously undetected threats and risks. The integrated architecture ensures that when threats are detected, customers can quickly access a unified view of activity, enabling deep visibility and rapid response. LogRhythm delivers the actionable intelligence and incident response capabilities necessary to address today's most sophisticated cyber threats.



Rapid Time-to-Value

Whether you are protecting a small network or running a global security operations center (SOC), time-to-value and total cost of ownership matter. LogRhythm's integrated architecture and unified analyst workflows help customers efficiently address their most pressing security issues.

LogRhythm Labs™ delivers critical out-of-the box functionality that expedites threat detection and response. Automatically delivered and continuously updated with new threat and compliance research, LogRhythm's extensive embedded expertise arms customers against emerging threats and helps keep them current with compliance and audit requirements. LogRhythm Labs delivers:

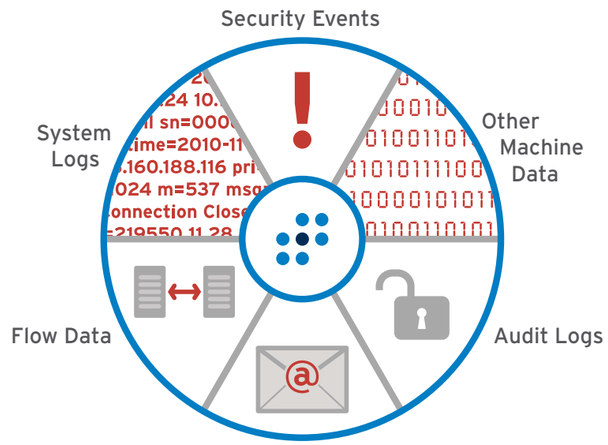
- Log parsing and normalization rules for over 700 unique operating systems, applications, databases, devices, etc.
- Compliance Automation Modules for 14+ regulatory frameworks (PCI, SOX, HIPAA, FISMA, GLBA, ISO 27001, DODI 8500.1, NERC-CIP, and more)
- Threat Management Modules
  - User / Network / Endpoint Threat Detection
  - Advanced Persistent Threat (APT)
  - Honeypot Analytics
  - Retail Cyber Crime
  - And many others...

LOGRHYTHM'S SECURITY INTELLIGENCE PLATFORM

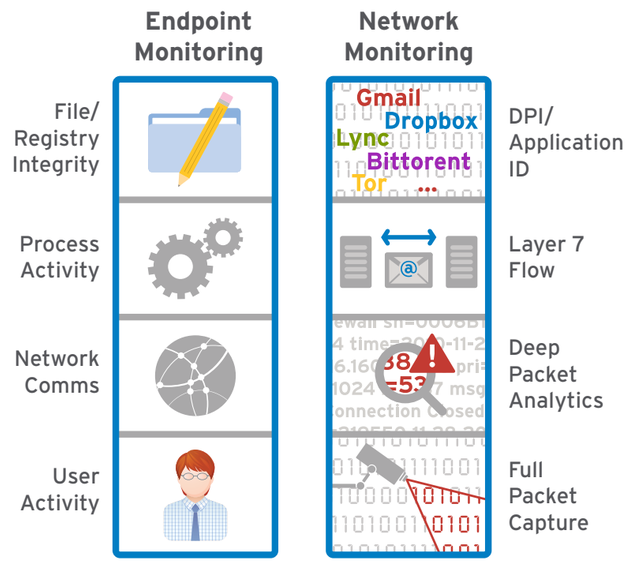
LogRhythm

INPUT

REAL-TIME FORENSIC DATA COLLECTION



REAL-TIME FORENSIC DATA GENERATION



ANALYTICS

PROCESSING

Time Normalization

Uniform Data Classification

Metadata Extraction & Tagging

Threat & Risk Contextualization

MACHINE ANALYTICS

Machine Learning

Behavioral Profiling

Statistical Analysis

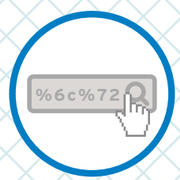
Whitelisting

Blacklisting

Advanced Correlation

FORENSIC ANALYTICS

Contextual Search



Unstructured Search

Visualization

Pivot / Drill Down

MACHINE DATA INTELLIGENCE (MDI) FABRIC

LogRhythm Labs Research & Intelligence

OUTPUT

ACTIONABLE INTELLIGENCE

Risk Prioritized Alarms

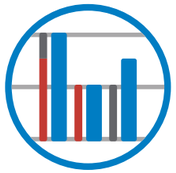
Real Time Dashboards

Reports

INCIDENT RESPONSE

Case Collaboration

Evidence Locker



Incident Tracking & Metrics

Automated Response

Flexible Deployment Options

High Performance Appliances

	ALL-IN-ONE (XM) (INCLUDES PM, DPX, AIE)		DEDICATED PLATFORM MANAGER (PM) (INCLUDES AI ENGINE LICENSE)		DEDICATED DATA PROCESSOR (DP)		DEDICATED DATA INDEXER (DX)			DEDICATED AI ENGINE (AIE)		DATA COLLECTOR (DC)	NETWORK MONITOR (NM)		WEB APPLIANCE
Appliance Lines	4301	6400	5400	7400	5300	7400	3300	5300	7400	5400	7400	3300	3300	5400	3300
Max Archiving Rates	10,000 MPS	25,000 MPS	N/A	N/A	10,000 MPS	50,000 MPS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Max Processing Rates	1,000 MPS	5,000 MPS	N/A	N/A	5,000 MPS	15,000 MPS	N/A	N/A	N/A	30,000 MPS	75,000 MPS	N/A	1 Gbps	2.5 Gbps	N/A

> **THE SANS COMMUNITY** has voted LogRhythm the Best SIEM of 2014.
>
> SANS INSTITUTE

> LogRhythm earns **HIGH MARKS FROM READERS** across the board.
>
> INFOWORLD

Software & Virtualization

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

vmware® Windows Server 2012 CITRIX® XenServer

LogRhythm Services

LogRhythm is the industry's largest focused provider of SIEM and Security Intelligence. Its world class support and professional services teams are dedicated to maximizing customer success by providing responsive and practical solutions.

LogRhythm Labs

LogRhythm Labs

LogRhythm Labs is a security and compliance research team focused on empowering customers by delivering embedded expertise and pre-configured tools for advanced threat management and compliance automation. The team includes recognized experts on intrusion detection, advanced malware, incident response, IT compliance, and many other essential subjects. The researchers at LogRhythm Labs hold several industry certifications (e.g., CISSP, CISA, CEH, etc.) and use ongoing research and education to stay current with the latest developments in threats, methods, compliance, and security best practices.

LogRhythm in Action

Detecting Custom Malware with Endpoint Behavior Anomaly Detection

Challenge: Custom malware tied to zero-day attacks is created to evade traditional security solutions that are built to detect specific signatures and known malicious behavior.

1. LogRhythm baselines "normal" endpoint behavior and creates a whitelist of acceptable process activity.
2. Endpoint Activity Monitoring independently detects a new process starting.
3. LogRhythm automatically recognizes that the new process is non-whitelisted.
4. LogRhythm's machine analytics corroborates the event against related activity such as abnormal network traffic, accurately identifying the activity as high risk.
5. An alarm is sent to a Security Administrator, who easily accesses forensic details to investigate.

Exposing Compromised Credentials with User Behavior Anomaly Detection

Challenge: With an increasingly mobile workforce and the accelerating adoption of BYOD, enterprises find it difficult to distinguish between "normal" behavior and activity indicating that a user's credentials have been compromised.

1. LogRhythm automatically establishes a profile for specific users, including whitelists of acceptable activity and behavioral baselines of observed user activities.
2. AI Engine detects when a user engages in abnormal activity, like logging in from a suspicious location or deviating from a behavioral norm, such as accessing significantly more or different data and uploading that data to a non-whitelisted cloud sharing application.
3. Smart**Response**™ either automatically disables the account or queues up the response for validation pending a more detailed forensic investigation into the user's activity.

Identifying Data Exfiltration with Network Behavior Anomaly Detection

Challenge: The constant flow of data into and out of an enterprise makes it difficult to detect when sensitive data leaves the corporate network.

1. Network Monitor provides critical visibility at network ingress/egress points, with SmartFlow™ data providing deep packet visibility into each network session observed and the applications in use.
2. LogRhythm's machine analytics establish behavioral baselines across observed network activities, leveraging the extensive packet metadata delivered via SmartFlow™.
3. Network-based anomalies are identified and corroborated against other log and machine data to provide accurate visibility into high risk activity.
4. SmartCapture™ automatically captures all packets associated with suspicious sessions for full packet forensics.