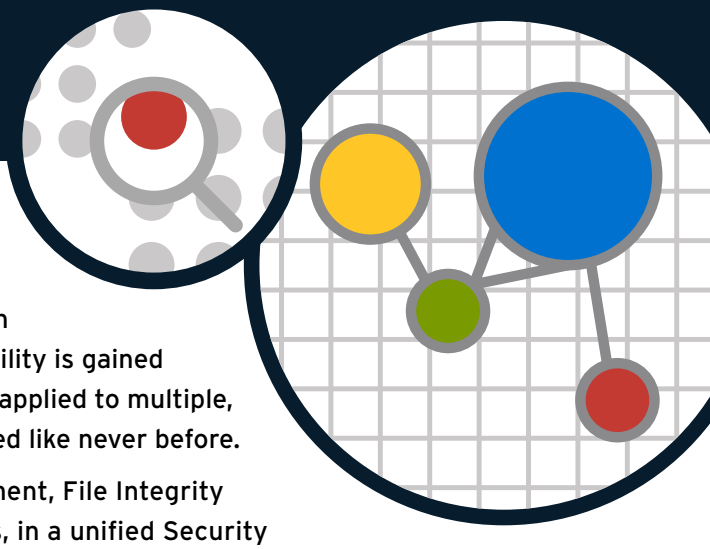
LOGRHYTHM'S SECURITY INTELLIGENCE PLATFORM

LogRhythm™



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

LogRhythm uniquely combines enterprise-class SIEM, Log Management, File Integrity Monitoring and Machine Analytics, with Host and Network Forensics, in a unified Security Intelligence Platform. The LogRhythm solution 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 new generation of capabilities when it comes to detecting, defending against, and responding to cyber threats and associated risks. LogRhythm's Security Intelligence Platform delivers:

- Next Generation SIEM and Log Management
- Independent Host 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
  - Multi-dimensional User / Host / Network Behavior Anomaly Detection
- Rapid, Intelligent Search
- Large data set analysis via visual analytics, pivot, and drill down
- Workflow enabled automatic response via LogRhythm's Smart**Response**™
- Integrated Case Management

Analyzing all available log and machine data and combining it with deep forensic visibility at both the host and network level delivers true visibility. This insight is leveraged by AI Engine, our patented Machine Analytics technology, to deliver automated, continuous 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 global view of activity, enabling exceptional security intelligence and rapid response. LogRhythm delivers the actionable intelligence and incident response capabilities required to address today's most sophisticated cyber threats.

Rapid Time-to-Value

Whether you are protecting a small business network or running a global security operations center (SOC), time-to-value and total cost of ownership matter. LogRhythm's integrated architecture, combined with our focus on ease-of-use, helps customers quickly leverage powerful capabilities while keeping long-term costs in check. We take pride in overcoming challenging problems by creating simple, usable solutions.

LogRhythm Labs™ delivers critical out-of-the box capabilities that align customer deployments to meet their business objectives. Automatically delivered and continuously updated with the latest in threat and compliance research, LogRhythm's extensive embedded expertise enables customers to quickly arm themselves against emerging threats, while staying current with compliance and audit requirements. The Knowledge Base includes:

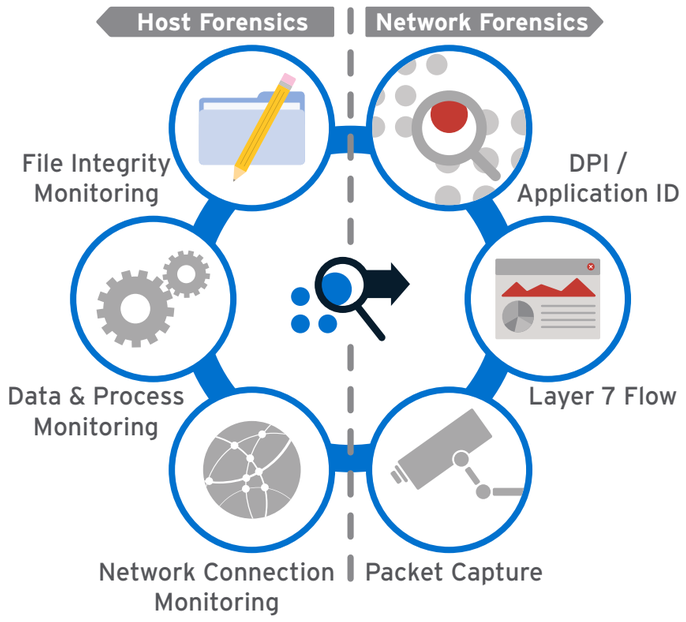
- Log parsing and normalization rules for over 600 unique operating systems, applications, databases, devices, etc.
- Compliance Automation Suites for a broad range of regulations (PCI, SOX, HIPAA, FISMA, GLBA, ISO27001, DODI 8500.1, NERC-CIP, etc.)
- Security Intelligence Modules
  - Privileged User Monitoring
  - Advanced Persistent Threat (APT)
  - Web Application Defense
  - User / Host / Network Behavior Anomaly Detection
  - And many others...

LOGRHYTHM'S SECURITY INTELLIGENCE PLATFORM

Input

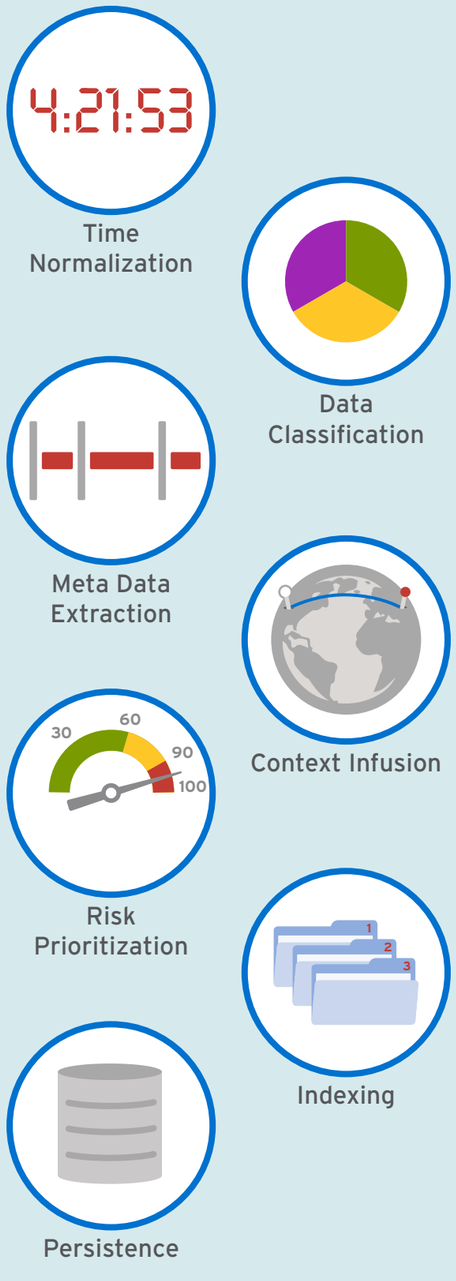
FORENSIC DATA COLLECTION

FORENSIC DATA GENERATION

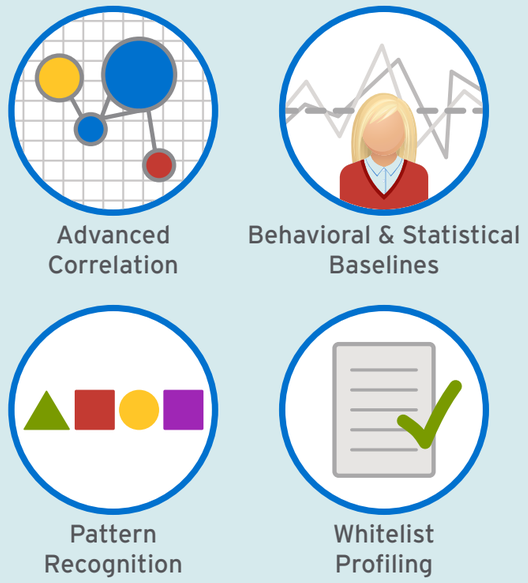


Analytics

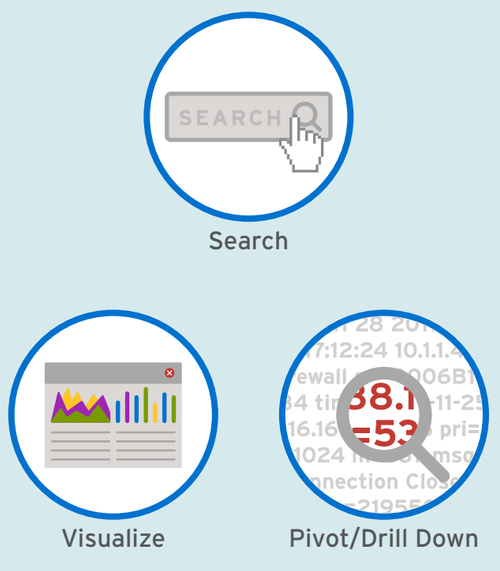
REAL-TIME PROCESSING



MACHINE ANALYTICS



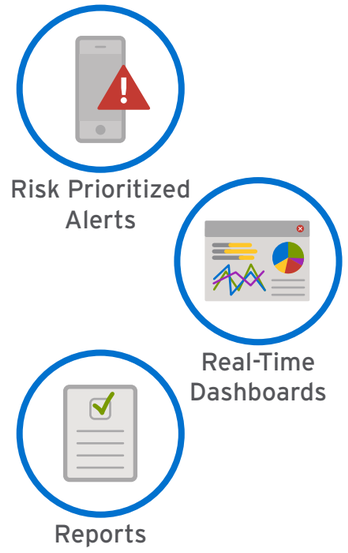
FORENSIC ANALYTICS



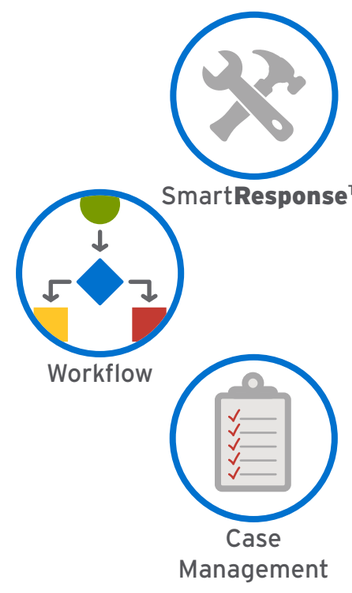
ADAPTIVE CYBER DEFENSE

Output

ACTIONABLE INTELLIGENCE



INCIDENT RESPONSE



Flexible Deployment Options

High Performance Appliances

	ALL-IN-ONE (XM) (Includes EM, LM, AIE)		DEDICATED EVENT MANAGER (EM) (Includes AI Engine license)			DEDICATED LOG MANAGER (LM)			DEDICATED AI ENGINE (AIE)			SITE LOG FORWARDER (SLF)	NETWORK MONITOR (NM)
Appliance Lines	4300	6300	3300 [3]	5300 [4]	6300 [5]	3300	5300	7300	5300	7300	9300	3310	3300
Max Archiving Rates	10,000 MPS	25,000 MPS	N/A	N/A	N/A	10,000 MPS	25,000 MPS	50,000 MPS	N/A	N/A	N/A	N/A	N/A
Max Processing Rates	1,000 MPS	5,000 MPS	N/A	N/A	N/A	2,000 MPS	5,000 MPS	15,000 MPS	5,000 MPS	30,000 MPS	75,000 MPS	N/A	1 Gbps

[1] MPS = Messages Per Second. [2] Individual rates vary based on customer environment/requirements. [3] Includes Embedded AIE License of 2,000 MPS. [4] Includes Embedded AIE License of 10,000 MPS. [5] Includes Embedded AIE License of 20,000 MPS

> "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 most major virtualization platforms including:

vmware · Windows Server 2008 Hyper-V · CITRIX XenServer

LogRhythm Services

LogRhythm delivers world class support and professional services with an unparalleled focus on delivering practical solutions and value. From the world's largest organization to small and medium enterprises, LogRhythm maintains a relentless dedication to maximizing customer success and satisfaction.

LogRhythm Labs

LogRhythm Labs empowers customers by acting as a virtual security threat and compliance research team, delivering out-of-the box intelligence and embedded expertise for advanced threat management and compliance automation and assurance. The team is comprised of dedicated information security specialists, with subject matter experts on a variety of topics, including intrusion detection, advanced malware, incident response, IT audit and compliance. Researchers in LogRhythm Labs hold a wide range of industry certifications (e.g., CISSP, CISA, CEH, etc.) and use extensive continuing education and ongoing research to stay current with the latest developments in threats, methods, compliance, and best practices.

LogRhythm in Action

Detecting Custom Malware with Host Behavior Anomaly Detection

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

1. LogRhythm baselines "normal" host behavior and creates a whitelist of acceptable process activity.
2. Host 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 organizational challenges such as an increasingly mobile workforce and 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, such as logging in from a suspicious location, or deviating from a behavioral norm, such as accessing significantly different data or volume of data and uploading that data to a non-whitelisted cloud sharing application.
3. SmartResponse™ 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 generated SmartFlow™ data providing deep packet visibility into each network session observed and the applications in use.
2. LogRhythm's machine analytics establishes various behavioral baselines across observed network activities, leveraging the extensive packet meta-data 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.