LOGRHYTHM'S SECURITY INTELLIGENCE PLATFORM

Protecting against today's rapidly evolving threat landscape requires broad and deep visibility across your IT environment. Threats arrive from many vectors and evidence of their existence can be found in existing log and machine data. Further visibility can be generated through endpoint and network monitoring and forensics. When this rich data is examined using security analytics, threats and risks are exposed like never before.

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

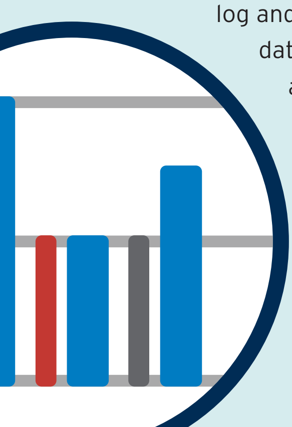
Detect & kill threats on a unified platform

LogRhythm empowers organisations to detect, respond to and neutralise emergent cyber threats, preventing damaging data breaches and cyber incidents.

LogRhythm's Security Intelligence Platform integrates:

- Next-generation SIEM and log management
- Endpoint forensics, with registry and file integrity monitoring
- Network forensics, with application ID and full packet capture
- Behavioural analytics for holistic threat detection (users, networks and endpoints)
- Rapid unstructured and contextual search
- End-to-end incident response orchestration workflows to support team collaboration
- Smart**Response**™ automation framework

LogRhythm addresses today's most sophisticated cyber threats. The platform attains full visibility by aggregating log and machine data with network and endpoint data. LogRhythm's patented machine analytics technology continually performs real-time analysis on this environmental activity, helping identify previously unknown threats. When a threat is detected, analysts can quickly qualify and investigate it by pivoting and drilling down into rich forensic data. The platform's collaborative incident response orchestration and patented Smart**Response**™ automation framework help security teams efficiently perform threat lifecycle management.



Accelerate time-to-value

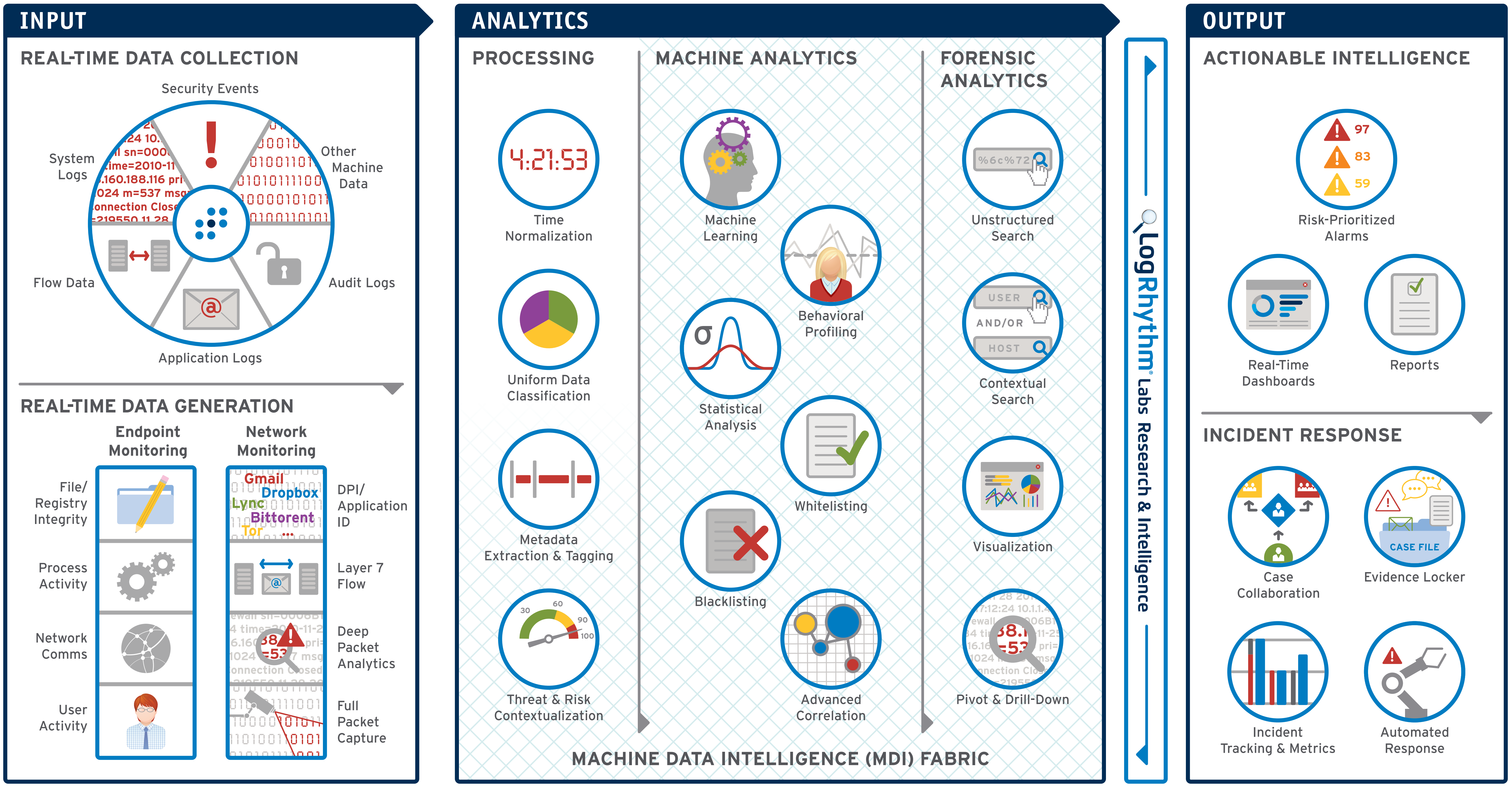
LogRhythm's integrated architecture, out-of-the-box security analytics, and end-to-end analyst workflows help customers efficiently address their most pressing security issues.

LogRhythm Labs™ delivers critical out-of-the box functionality that expedites threat detection and response. Automatically delivered and continuously updated, this embedded expertise arms customers against emerging threats and evolving compliance requirements. LogRhythm Labs delivers:

- Log parsing and normalisation rules for over 750 unique operating systems, applications, databases and devices
- Compliance Automation Modules for 15+ frameworks (PCI, SOX, HIPAA, FISMA, GLBA, ISO 27001, NERC CIP, and more)
- Threat Management Modules:
  - User / Network / Endpoint Threat Detection
  - Honeypot and Threat Intelligence Integration
  - Retail Cyber Crime and Financial Fraud Detection
  - And many others...

LOGRHYTHM'S SECURITY INTELLIGENCE PLATFORM

LogRhythm



INPUT

REAL-TIME DATA COLLECTION

- Security Events
- System Logs
- Other Machine Data
- Flow Data
- Audit Logs
- Application Logs

REAL-TIME DATA GENERATION

Endpoint Monitoring

- File/ Registry Integrity
- Process Activity
- Network Comms
- User Activity

Network Monitoring

- DPI/ Application ID
- Layer 7 Flow
- Deep Packet Analytics
- Full Packet Capture

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

- Unstructured Search
- Contextual 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 2015.”
>
> SANS INSTITUTE

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

Software & virtualisation

LogRhythm can be deployed easily on customer-provided hardware and most major virtualisation 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 maximising customer success by providing responsive and practical solutions.

LogRhythm Labs

LogRhythm® Labs

LogRhythm Labs is a research team focused on security and compliance. They provide customers pre-configured analytics and content for threat management and compliance automation. LogRhythm Labs includes recognised experts in intrusion detection, advanced malware, incident response, compliance, and other critical subjects. Its researchers hold many industry certifications (e.g., CISSP, CISA, CEH) and perform ongoing research and education to explore the latest developments in security, compliance, and associated best practices.

LogRhythm in action

Expose compromised credentials with User Behaviour Analytics

Challenge: With an increasingly mobile workforce and the accelerating adoption of BYOD, firms struggle to distinguish between “normal” behaviour and activity indicating a potential account compromise.

1. LogRhythm establishes behaviour profiles, including behavioural baselines and whitelists of acceptable activity.
2. AI Engine detects when a user engages in abnormal activity (like logging in from a suspicious location), or deviating from a behavioural norm (like accessing significantly more or different data).
3. LogRhythm corroborates behavioural shifts with other high-risk activity, like uploading data to a non-whitelisted cloud sharing application.
4. Smart**Response**™ empowers an analyst to disable the account pending a detailed forensic investigation into the user's activity.

Identify data exfiltration with Network Behaviour Analytics

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 deep packet inspection and SmartFlow™ metadata, including the application in use and more.
2. LogRhythm's machine analytics establish behavioural baselines across observed network activities, leveraging Layer 7 SmartFlow™ metadata.
3. Network-based anomalies are identified and corroborated against other data to surface high-risk activity.
4. SmartCapture™ automatically stores all packets associated with suspicious sessions to support forensic investigations.

Detect custom malware with Endpoint Behaviour Analytics

Challenge: Custom malware tied to zero-day attacks evades traditional, signature-based detection solutions.

1. LogRhythm baselines “normal” endpoint behaviour and creates a whitelist of acceptable process activity.
2. Endpoint Activity Monitoring detects a new process starting.
3. LogRhythm automatically recognises that the new process is non-whitelisted.
4. LogRhythm's machine analytics corroborates the event with 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.