See Threats Traversing Your Network

Organizations need visibility into their networks to detect threats, perform forensic investigations, support audits, and identify operational issues. Attacks originate from both within and outside organizations and can cause significant damage. Because cyber-attacks are often first observed within the network itself, network monitoring plays an essential role in helping detect, stop, and recover from attacks.

LogRhythm Network Monitor provides enterprise-wide network visibility in more detail than traditional network and security solutions like flow analysis tools and next-generation firewalls. The deep insight delivered by Network Monitor helps organizations detect and respond to advanced threats, including nation-state espionage, zero-day malware, and data exfiltration. Out-of-band deployment removes any impact on network device capacity and performance.

Advanced Threat Detection

Detect advanced threats in real-time via market-leading application recognition, customizable Deep Packet Analytics across network and application level data, and multidimensional behavioral analytics.

- Detect sophisticated threats, including advanced malware
- Recognize data theft, botnet beaconing, inappropriate network usage, and other threats
- Corroborate high-risk events observed at the network or application level with environmental activity collected by the SIEM

Rapid Incident Response

Take the guesswork out of incident response. Store session-based packet captures (either selectively or in full) and analyze them using out-of-the-box application identification and application-specific metadata recognition. Enable your incident response team to work effectively and efficiently with unstructured search, session playback, and file reconstruction.

- Determine incident scope and understand exactly which data and systems have been compromised
- Generate irrefutable network-based evidence for threat analysis, policy enforcement, and legal action
- Reconstruct files transferred across networks to investigate suspected data exfiltration, malware infiltration, and unauthorized data access

Auditing & Operations Support

Network Monitor captures and analyzes data that helps resolve operational issues and meet audit and compliance requirements:

- Detect bandwidth issues and other performance bottlenecks
- Discover the devices on your ecosystem, including cloud and IoT
- Identify compliance issues like exposed PII, plain text passwords, and outdated protocols
- Alert on policy violation and evasion

Unified Security Intelligence

Network Monitor is available as an independent network forensics solution or as a component of LogRhythm's Security Intelligence Platform. The integrated solution delivers:

- Security analytics across a broader data set for corroborated evidence chaining, including:
  - All IT environment-generated log and audit data
  - Endpoint activity captured by endpoint sensors
  - Layer 7 application flow and packet data captured by LogRhythm Network Monitor
- Behavior Analytics on Network Monitor's data to detect critical anomalies indicative of spear phishing, lateral movement, and suspicious file transfers
- Centralized search and visualization to expedite investigations, including direct access to stored session-based packet capture
- End-to-end incident response orchestration and automation functionality

> *“With Network Monitor, we've materially improved our defense, detection and response capabilities for multiple secure data environments.”*
>
> **Erin Osminer**
> Network Engineer, StoneRiver

Powerful Capabilities

True Application Identification: Automatically identify over 2,700 applications to expedite network forensics using advanced classification methods and deep packet inspection (DPI).

SmartFlow Session Classification: Record Layer 7 application details and packet data for all network sessions using SmartFlow™. Get clear session visibility without requiring packet layer analysis or significant storage requirements.

Deep Packet Analytics (DPA): Continuously correlate against full packet payload and SmartFlow™ metadata using out-of-the-box rules and customizable scripts. Automate threat detection that was previously only possible via manual packet analysis.

Full Packet Capture: See every bit crossing your network with full Layer 2 through Layer 7 packet capture for the deepest insight possible. All captures are stored in industry-standard PCAP format so your team can use existing tools and training.

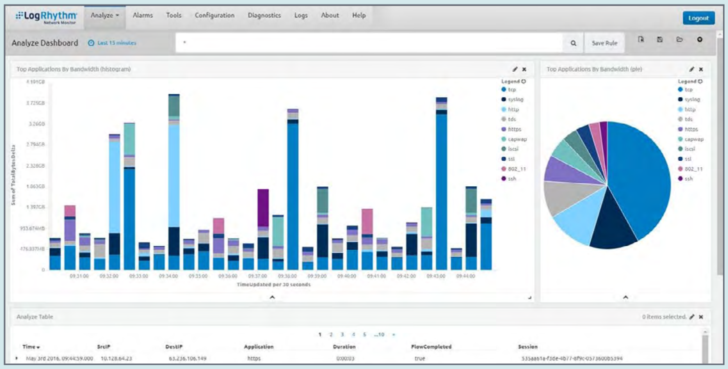
SmartCapture™: SmartCapture™ allows you to automatically capture sessions based on application or packet content to drastically reduce your storage requirements while preserving the information you need.

Unstructured Search: Perform ad hoc analysis. Drill down to critical flow and packet data quickly. With our Elasticsearch backend, you have a powerful "Google-like" search engine to streamline your investigation.

File Reconstruction: Reconstruct email file attachments to support malware analysis and data loss monitoring.

Alerts & Dashboards: Perform continuous, automated analysis on saved searches to immediately detect when specific conditions are met, and then surface these instances through customizable analyst dashboards.

API Integration: Use a REST-ful API to provide third-party tools access to session-based packet captures and reconstructed files.



Time	SrcIP	DestIP	Application	Duration	FlowCompleted	Session
May 3rd 2016, 09:44:59.000	10.128.64.23	63.236.106.149	https	0:00:03	true	535aab1a-f3de-4b77-8f9c-0573600b5394

Get Started with Network Monitor Freemium

Network Monitor Freemium provides the same functionality as a full Network Monitor license, but with limits on processing, packet storage, and data forwarding. All other features and functionality are enabled and usable, including unstructured search, deep packet analytics, packet capture, and more. Network Monitor Freemium is not a trial and doesn't expire, so get started by visiting **www.logrhythm.com/freemium**.

Flexible Deployment Options

Network Monitor uses a simple and intuitive UI for both installation and updates. Passive sensors deploy via TAP, SPAN, or via integration with a third-party network packet broker. Network Monitor begins analyzing traffic and recognizing applications immediately. Optionally, Layer 7 SmartFlow™ can be forwarded to a SIEM for further analysis.

Hardware Appliances:

APPLIANCES	SUSTAINED THROUGHPUT	CPU	MEMORY	STORAGE	CHASSIS	POWER	ETHERNET	DIMENSIONS	WEIGHT
LR-NM3400	1 Gbps	12 Core	64GB	1.9TB - 25.9TB	1U	100-240V	2 X 1GB	H4.28cm X W48.24cm X D70.05cm	18.6kg
LR-NM5400	5 Gbps / 10 Gbps Peak	24 Core	128GB	12.5TB - 60TB	2U	100-240V	2 X 10GB	H8.73cm X W44.4cm X D68.4cm	30.4kg

Software Appliances for Remote Sites: Network Monitor is also available as a software-based appliance. This cost-effective and flexible solution is an ideal choice for monitoring low-bandwidth remote sites.

Virtual Sensors for Virtual Environments: Improve your visibility into virtual environments and cloud infrastructure by using Network Monitor as a virtual sensor for virtual switches.