PRODUCT OVERVIEW

Network Monitor

LogRhythm™

True enterprise security intelligence requires real-time awareness and an understanding of all data traversing the network. The LogRhythm Network Monitor provides both application level awareness and rich network session details, delivering enterprise-wide network visibility. By deriving a rich set of fully searchable metadata, Network Monitor provides rapid access to highly valuable forensic evidence, resulting in rapid and in-depth understanding of network activity. In addition, Network Monitor's ability to perform full packet capture provides access to each session's raw packet details for additional forensic evidence.

The LogRhythm Network Monitor provides visibility critical to detecting and responding to today's advanced threats. It enables organizations to:

- Baseline network behavior to immediately pinpoint abnormal activity
- Detect unauthorized or suspicious application activity
- Expedite network forensic investigations
- Perform full session packet capture for advanced forensics
- Prevent sensitive data loss
- Monitor application bandwidth consumption

True application identification – identifies more than 1,700 applications for in-depth analysis by performing deep packet inspection and applying multiple classification methods to determine the true identity of the application. True application ID provides the visibility necessary to detect critical activities such as suspicious data transfers, network usage policy violations and advanced attacks.

SmartFlow™ – delivers a rich set of packet metadata derived from each network session, appropriate to the type of application used. The high degree of detail available in SmartFlow™, cataloguing every session on the network, provides deep understanding of an application's network activity in a quickly accessible format.

Unstructured Search, Powerful Analysis – provides rapid access to SmartFlow™ details via a powerful, "Google-like" search engine that streamlines and simplifies network forensic investigations. Results are presented in highly informative visualizations and custom layouts, enabling blazingly fast analysis of network packet data.

Full session packet capture – captures full layer 2 through 7 packet header and payloads from each session for a complete record of network activity. All information is organized by session, providing full context of application communications and content transferred across the network.

SmartCapture™ – provides full packet capture without the extensive storage requirements of traditional solutions by retaining only sessions of interest.

Security Analytics Integration – delivers a rich, real-time feed of SmartFlow™ data to LogRhythm's, third-party, and proprietary security analytics solutions.

LogRhythm Security Analytics

The LogRhythm Network Monitor can be deployed stand-alone or as a fully integrated component of LogRhythm's award winning SIEM, delivering unparalleled security analytics across the entire network's activities. The integrated platform includes:

- Real-time security analytics across all forensic data recognizing highly concerning events across:
  - Network-wide log and audit data
  - Independently collected host activity via LogRhythm System Monitor
  - Independently collected network activity via LogRhythm Network Monitor
- Comprehensive, out-of-the-box capabilities for Network Behavior Anomaly Detection (NBAD)
- Powerful search and visualization, including drill down, pivoting, and correlation, to expedite investigations
- Triggering of full session packet capture by Network Monitor's SmartCapture™ in response to high priority activities recognized by the SIEM.

> "The out-of-the-box NBAD capabilities allow us to detect and investigate suspicious traffic to identify a range of issues, from the presence of malware to excessive bandwidth consumption by videoconferencing."
>
> *Vaughn Adams* Senior Manager of IT, InterDigital.

Network Monitor in Action

The LogRhythm Network Monitor fulfills real-world use cases to solve critical security concerns and shed light on network abnormalities and inappropriate user activity. Whether concerned with custom malware, nation state espionage, or routine network misuse, LogRhythm delivers the deep insight necessary to detect a variety of threats while enabling much more efficient and informed responses.

Data Theft

Quickly recognizing relevant events surrounding a breach can help reduce exposure and decrease the cost of remediation.

1. Network Monitor's dashboard illuminates long running SSH sessions.
2. Details from Network Monitor's SmartFlow™ expose that SSH is used to tunnel to the host, providing remote access to the system.
3. Additional steps can now be taken to protect targeted hosts and to deny network access to the attacking system.

BotNet Detection

Today's botnet callbacks use standard ports and possibly legitimate applications to disguise their traffic in order to avoid detection.

1. Network Monitor observes non-HTTP traffic on port 80 and either identifies the true application or exposes malformed HTTP packet headers.
2. Full packet capture of the session discloses additional content not identified via traditional security tools, allowing further analysis and verification of identified threats.

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

Inappropriate Network Use

Without additional intelligence beyond what traditional flow data provides, it is difficult to distinguish legitimate activity from suspicious behavior.

1. Traditional flow analysis identifies excessive bandwidth usage from a website over HTTP, however no additional information is provided.
2. Network Monitor derives extensive metadata from the network session that identifies details such as the presence of a large file download, the source or destination URL, and the names of files transferred.
3. Rapid access to SmartFlow™ details through Network Monitor's intuitive search, quickly identifies inappropriate activity, such as the transfer of copyrighted materials or the use of a non-sanctioned cloud sharing application.

Deployment

Network Monitor employs a simple and intuitive web-based UI to manage both installation and updates. It is deployed out of-band on TAP, SPAN, or via integration with 3rd party network packet broker solutions. Network Monitor begins analyzing traffic and recognizing applications immediately, providing real-time "Google-like" search across all packet captures and metadata, as well as optionally forwarding Layer 7 SmartFlow™ to the SIEM or other solutions for additional analysis.

APPLIANCE LINE	MAX PROCESSING	CPU	MEMORY	STORAGE	CHASIS	POWER	ETHERNET	DIMENSIONS	WEIGHT
LR-NM3330	500 Mbps	2.1 GHz	64GB	2TB	1U	100-240V	4 X 1GB	H4.28CM X W48.24CM X D67.73CM	19.3kg
LR-NM3359	1 Gbps	2.1 GHz	64GB	2TB	1U	100-240V	4 X 1GB	H4.28CM X W48.24CM X D67.73CM	19.3kg

Additional Direct Attached Storage options are available, delivering expanded capacity for storing SmartFlow™ data and raw packet captures. Network Monitor also supports moving packet captures to SAN or alternative storage for long term retention.