LogRhythm

Data Sheet

LogRhythm NetMon

Reveal Threats with Network Data

Security teams need visibility into their organization's networks to detect threats, perform forensic investigations, support audits, and identify operational issues. Because cyberattacks are often first observed within the network itself, network monitoring plays an essential role in helping detect, neutralize, and recover from attacks.

LogRhythm NetMon delivers more detailed network visibility than nextgeneration firewalls, IDS/IPS systems, and other common network equipment. The rich data and deep insights delivered by NetMon help organizations detect and respond to advanced threats, including nation-state espionage, zero-day malware, and data exfiltration. Out-of-band deployment prevents any impact on network device capacity and performance.

Detect Advanced Threats

Detect advanced threats with market-leading application recognition, script-based analytics across network and application data, and rich data for centralized scenario-based analytics. With NetMon, you can:

- Recognize data theft, advanced malware, botnet beaconing, inappropriate network usage, and other threats.
- Corroborate high-risk events observed at the network and application level with environmental activity collected by the SIEM.
- Create powerful custom analysis rules to alert on advanced threats.
- Act on hundreds of attributes, including individual application, application family, SSL information, IP address, and more.

Unified Security Intelligence

LogRhythm NetMon is available as a standalone network forensics solution or as a component of the LogRhythm SIEM platform. The integrated solution delivers:

- Security analytics across a centralized data set for corroborated evidence chaining, including:
  - All machine data generated by the environment
  - Host activity captured by endpoint sensors
  - Layer 7 application flow and packet data captured by LogRhythm NetMon
- Analysis of sensor data to detect critical anomalies indicative of spear phishing, lateral movement, and suspicious file transfers
- Centralized search and visualization to expedite investigations, and contextual access to session-based PCAPs
- Embedded security orchestration, automation, and response (SOAR) function

Empower Incident Responders

NetMon provides the option to capture and store session-based PCAPs selectively or in full. The product provides out-of-the-box application identification and application-specific metadata. NetMon further enables your incident response team with unstructured search, session playback, and file reconstruction.

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

Support Auditing and Operations

NetMon captures and analyzes data to help resolve operational issues and meet audit and compliance requirements:

- Alert on policy violations and workarounds.
- Detect bandwidth bottlenecks and other performance issues.
- Identify compliance issues like exposed PII, plain text passwords, and outdated protocols.

Flexible Deployment Options

NetMon sensors deploy via TAP, SPAN, or integration with a third-party network packet broker. NetMon begins analyzing traffic and recognizing applications immediately upon installation. SmartFlow can be forwarded to an analytics platform for further analysis.

- Physical appliances provide significant scalability in a purposebuilt form factor.
- Software-based NetMon provides a cost-effective choice for monitoring low-bandwidth sites, such as remote locations.
- Virtual sensors illuminate activity on cloud infrastructure and virtual environments.

Powerful Capabilities

True Application Identification: Expedite network forensics by automatically identifying and categorizing traffic from over 3,300 applications using deep packet inspection (DPI) and advanced classification methods.

Metadata Generation: Leverage NetMon-generated SmartFlow™ metadata revealing Layer 2–7 details to enable automated analysis, provide rich data for effective investigation, and support automated response — all without packet analysis or significant storage requirements.

Deep Packet Analytics (DPA): Automate threat detection by continuously correlating against full packet payload and SmartFlow™ metadata with out-of-the-box, customizable scripts.

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

Full Packet Capture: Empower your incident responders by capturing every bit crossing your network in industry standard PCAP format.

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

Packet Replay: Replay previously captured packets through NetMon for deeper analysis. Replay traffic manually or automatically through the NetMon REST API.

Alerts and Dashboards: Perform continuous analysis via saved searches to immediately detect when specific conditions are met, then surface alerts on customizable monitoring dashboards.

SIEM Integration: Empower analysis and administrators by integrating with third-party analysis and orchestration tools via REST APIs providing direct access to session-based PCAPs and reconstructed files.