NETWORK MONITOR

LogRhythm
The Security Intelligence Company

Erkennen Sie die Bedrohungen in Ihrem Netzwerk

Unternehmen brauchen Sichtbarkeit für ihre Netzwerke, um Bedrohungen zu finden, forensische Untersuchungen durchzuführen, Audits zu bestehen und betriebliche Probleme zu ermitteln. Angriffe auf Unternehmen können sowohl von außen als auch von innen erfolgen und gravierende Schäden anrichten. Da Cyberangriffe oft erst bemerkt werden, wenn die Angreifer bereits im Netz sind, spielt die Netzwerküberwachung eine entscheidende Rolle bei der Erkennung und Bekämpfung von Angriffen sowie der Wiederherstellung nach einem Angriff.

LogRhythm Network Monitor bietet Transparenz für das gesamte Unternehmensnetz und zeigt wesentlich mehr Details als herkömmliche Netzwerk- und Sicherheitslösungen, wie beispielsweise Tools zur Datenflussanalyse und Next-Generation Firewalls. Dank der tieferen Einblicke, die Network Monitor vermittelt, können Unternehmen hochentwickelte Bedrohungen erkennen und abwehren, wie etwa staatliche Spionage, Zero-Day-Malware und Datenexfiltration. Die Out-of-Band-Bereitstellung gewährleistet, dass die Kapazität und Leistung der Netzwerkgeräte nicht beeinträchtigt werden.

Hochentwickelte Bedrohungen erkennen

Nutzen Sie marktführende Funktionen zur Anwendungserkennung, umfassende, anpassbare Analysen für Daten auf der Netzwerk- und Anwendungsebene sowie mehrdimensionale Verhaltensanalysen, um hochentwickelte Bedrohungen in Echtzeit zu entdecken.

- Finden Sie komplexe Bedrohungen, einschließlich hochentwickelter Malware
- Erkennen Sie Datendiebstahl, Botnetz-Kommunikation via Beacons, unzulässige Netzwerknutzung und andere Bedrohungen
- Nutzen Sie die Erkenntnisse von SIEM-Tools zu Aktivitäten in der IT-Umgebung, um die Gefährlichkeit von Ereignissen zu bestätigen, die auf der Netzwerk- oder Anwendungsebene ermittelt wurden

Schnelle Reaktion auf Ereignisse

Beenden Sie das Rätselraten bei der Reaktion auf Sicherheitsereignisse. Speichern Sie sitzungsbasierte Packet Captures (selektiv oder komplett) und analysieren Sie sie mit out-of-the-box bereitgestellten Funktionen zur Anwendungsidentifikation und anwendungsspezifischen Metadatenerkennung. Befähigen Sie Ihr Incident Response Team, effektiv und effizient zu arbeiten: mittels unstrukturierter Suche, späterer Wiedergabe von Sitzungen und Rekonstruktion von Dateien.

- Bestimmen Sie das Ausmaß von Sicherheitsvorfällen und stellen Sie genau fest, welche Daten und Systeme kompromittiert wurden
- Generieren Sie unwiderlegbare, netzwerkbasierte Nachweise zur Bedrohungsanalyse, Durchsetzung von Richtlinien und Einleitung rechtlicher Schritte
- Rekonstruieren Sie Dateien, die über Netzwerke hinweg übertragen wurden, um vermutete Datenexfiltration, Malware-Infiltration und unautorisierte Datenzugriffe zu untersuchen

Unterstützung für Audits & den IT-Betrieb

Network Monitor erfasst und analysiert Daten, die Ihnen helfen, betriebliche Probleme zu lösen und Audit- und Compliance-Anforderungen zu erfüllen:

- Erkennt Bandbreitenprobleme und andere Leistungsengpässe
- Erkennt die Geräte in Ihrem Ökosystem, einschließlich Cloud und IoT
- Ermittelt Compliance-Hindernisse wie ungeschützte personenbezogene Daten, in Klartext gespeicherte Passwörter und veraltete Protokolle
- Warnt bei Verletzung und Umgehung von Richtlinien

Ganzheitliche Security Intelligence

Network Monitor ist wahlweise als eigenständige Netzwerkforensik-Lösung erhältlich oder als Komponente der LogRhythm Security-Intelligence-Plattform.

Die integrierte Lösung bietet:

- Sicherheitsanalysen für eine breitere Datenbasis zur Erstellung fundierter Beweisketten, einschließlich:
  - aller in der IT-Umgebung erzeugten Log- und Audit-Daten
  - Aktivitäten auf Endpunkten, die von den Endpunktsensoren erfasst werden
  - Layer-7-Anwendungsfluss- und Paketdaten, die LogRhythm Network Monitor erfasst
- Verhaltensanalysen zu den Network Monitor-Daten, um kritische Anomalien zu entdecken, die auf Spear Phishing, laterale Bewegungen und verdächtige Dateitransfers hindeuten
- Zentralisierte Suche und Visualisierung, um Untersuchungen zu beschleunigen, einschließlich direkten Zugriffs auf die sitzungsbasierten Packet Captures
- Funktionalitäten zur durchgängigen Steuerung und Automatisierung von Ereignisreaktionen

> *“Mit Network Monitor konnten wir unsere Abwehr, die Bedrohungserkennung und die Vorfallsreaktion in mehreren sicheren Datenumgebungen erheblich verbessern.”*
>
> **Erin Osminer**
> Network Engineer, StoneRiver

Leistungsstarke Funktionen

Zuverlässige Identifikation von Anwendungen: Identifizieren Sie automatisch mehr als 2.700 Anwendungen, um mit fortschrittlichen Klassifizierungsmethoden und umfassender Paketinspektion (DPI) die Netzwerkforensik zu unterstützen.

SmartFlow Sitzungsklassifizierung: Zeichnen Sie mit SmartFlow™ Layer 7-Anwendungsdetails und Paketdaten für alle Netzwerksitzungen auf. Gewinnen Sie Einsicht in die Sitzungen, ohne Paketschichtanalysen oder großen Speicherbedarf.

Umfassende Paketanalysen (DPA): Führen Sie mithilfe von Out-of-the-Box-Regeln und anpassbaren Skripten laufend Korrelationen gegen alle Paket-Payloads und SmartFlow™-Metadaten durch.

Automatisieren Sie die Bedrohungserkennung, die bislang nur mit manuellen Paketanalysen möglich war.

Vollständige Paketerfassung: Sehen Sie alles, was sich in Ihrem Netz bewegt: Die vollständige Erfassung der Pakete auf den Schichten 2 bis 7 gewährleistet bestmögliche Transparenz. Alle Captures werden im branchenüblichen PCAP-Format gespeichert, sodass Ihr Team bereits vorhandene Tools und Kenntnisse aus Schulungen weiter nutzen kann.

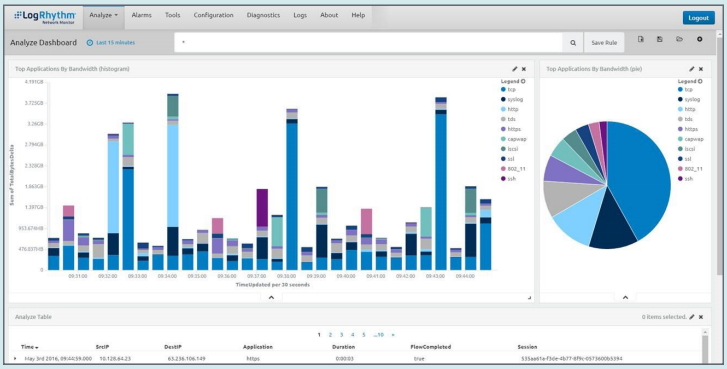
SmartCapture™: Mit SmartCapture™ können Sie automatisch Sitzungen auf Basis von Anwendungen oder Paketinhalten erfassen. So reduzieren Sie Ihren Speicherbedarf drastisch und haben trotzdem alle benötigten Informationen zur Hand.

Unstrukturierte Suche: Führen Sie Ad-hoc-Analysen durch. Erhalten Sie schnellen Einblick in kritische Fluss- und Paketdaten. Mit unserem Elasticsearch-Backend steht Ihnen eine leistungsstarke, Google-ähnliche Suchmaschine zur Verfügung, die Ihre Untersuchungen beschleunigt.

Rekonstruktion von Dateien: Rekonstruieren Sie Dateianhänge von E-Mails, um Malware-Analysen und die Überwachung auf Datenverluste zu unterstützen.

Alarme & Dashboards: Führen Sie kontinuierliche, automatisierte Analysen zu gespeicherten Suchen durch, um sofort festzustellen, ob spezifische Bedingungen zutreffen. Machen Sie diese Vorgänge dann auf anpassbaren Analyse-Dashboards sichtbar.

API-Integration: Gewähren Sie Drittanbieter-Tools mit einer REST-ful API Zugriff auf sitzungsbasierte Packet Captures und rekonstruierte Dateien.



Steigen Sie mit Network Monitor Freemium ein

Network Monitor Freemium bietet Ihnen die gleichen Funktionalitäten wie eine Volllizenz für Network Monitor, allerdings mit Einschränkungen hinsichtlich Verarbeitung, Paketspeicherung und Datenweiterleitung. Alle anderen Leistungsmerkmale und Funktionalitäten sind aktiviert und nutzbar, einschließlich der unstrukturierten Suche, umfassenden Paketanalyse, Paketerfassung und mehr. Network Monitor Freemium ist keine Probeversion und läuft nicht ab. Holen Sie sich Network Monitor Freemium jetzt auf **www.logrhythm.com/freemium**.

Flexible Bereitstellungsoptionen

Network Monitor wird über eine einfache, intuitive Benutzerschnittstelle installiert und mit Updates versorgt. Passive Sensoren werden via TAP, SPAN oder durch Integration mit einem Network Packet Broker eines Drittanbieters implementiert. Network Monitor beginnt unverzüglich mit der Analyse des Netzwerkverkehrs und der Erkennung von Anwendungen. Optional können SmartFlow™-Daten von Layer 7 zur weiteren Analyse an ein SIEM übermittelt werden.

Hardware Appliances:

ANWENDUNGEN	DATENDURCHSATZ	CPU	ARBEITS-SPEICHER	SPEICHER	CHASSIS	STROM	ETHERNET	ABMESSUNGEN	GEWICHT
LR-NM3400	1 Gbps	12 Kerne	64 GB	1,9 TB - 25,9 TB	1U	100-240 V	2 X 1 GB	H 4,28 cm X B 48,24 cm X T 70,05 cm	18,6 kg
LR-NM5400	5 Gbps / 10 Gbps Spitze	24 Kerne	128 GB	12,5 TB - 60 TB	2U	100-240 V	2 X 10 GB	H 8,73 cm X B 44,4 cm X T 68,4 cm	30,4 kg

Software Appliances für dezentrale Standorte: Network Monitor ist auch als Appliance auf Software-Basis verfügbar. Diese kosteneffiziente und flexible Lösung ist ideal zur Überwachung von Außenstellen mit niedrigen Bandbreiten.

Virtuelle Sensoren für virtuelle Umgebungen: Verbessern Sie Ihre Übersicht über virtuelle Umgebungen und Cloud-Infrastrukturen, indem Sie Network Monitor als virtuellen Sensor für virtuelle Switches einsetzen.