

LogRhythm NDR

360-Degree Visibility that Protects Your Network



Digital transformation has upended the cybersecurity landscape. With the market shifting due to the Internet of Things (IoT), Artificial Intelligence (AI), a hybrid workforce, remote working, and cloud adoption, the demands placed on security and network teams is greater than ever. Gaps in visibility across the landscape are expanding and the amount of network traffic that must be analyzed to prevent attacks is growing exponentially every day. Relying only on perimeter tools is no longer the only option to protect your business when attackers are continually learning and adapting.

[LogRhythm NDR](#) enables overwhelmed security teams to detect network cyberattacks efficiently and effectively with advanced analytics. NDR collects user, host, and network data and utilizes both machine learning and deterministic detection techniques to gain seamless visibility, reducing the dwell time of threats that live outside the perimeter. With LogRhythm NDR, network teams can easily hunt and investigate surfaced incidents to help reduce the cost associated with attacks that usually go unnoticed.

Benefits

- **Eliminate Gaps in Visibility:** Not every device can have an agent installed, and not every device can send a log. LogRhythm NDR provides a comprehensive view into all enterprise devices, entities, and network traffic while analyzing all traffic flows across the environment, including activity that moves laterally.
- **Detect the Undetectable:** It's the invisible threat that can harm your business. LogRhythm NDR identifies traffic anomalies that signal malicious activity such as command and control, lateral movement, data exfiltration, and malware activities. LogRhythm NDR can detect sophisticated evasion methods or "known unknown" cyber threats and brand new zero-day threats or "unknown unknowns."
- **Reduce Dwell Time:** Reduce the pool of threats that need investigation. Our advanced analytics provides higher-fidelity alarms across the entire network to surface the most pertinent threats and reduce attacker dwell time by exposing their activity without them knowing.
- **Lower Costs:** Our flexible, centralized patented mesh technology ensures on-site analysis of network traffic as the data is not shipped to the cloud to perform the analytics; keeping costs predictable and affordable.

See What Dwells in the Dark



Threat Detection
and Investigation



Advanced Analytics



Network Monitoring



Mesh Architecture

Key Features

Advanced Analytics

While other NDR solutions rely solely on machine learning applied to single streams of data to detect threats, LogRhythm uses analytics that combine machine learning and deterministic detection techniques to analyze network, user, and host activity. This holistic approach provides a true representation of all activity within the enterprise domain, making it possible to detect in real time lateral movement, exfiltration, malware compromise, ransomware, and unknown threats.

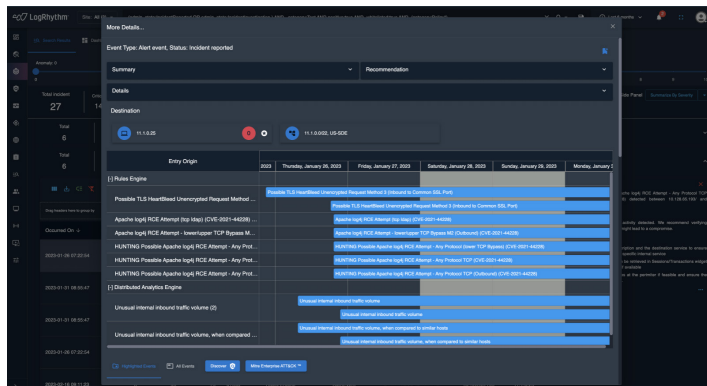


Figure 1: Gain insight into potential threats through advanced analytics

Mesh Architecture

LogRhythm NDR's mesh architecture technology eliminates data movement between locations to minimize transport charges and to optimize scalability. By utilizing distributed computing to scale data collection and analytics, NDR co-locates analytic processing alongside our collection engines constructing a distributed mesh for data processing. By easily collecting and enriching data on location, operating costs are reduced, and privacy risk and compliance issues are eliminated.

Built-in MITRE ATT&CK Framework

Built-in [MITRE ATT&CK™](#) engine combined with real-time and historical visualization tools help analysts hunt for threats. Gain a complete security narrative with automatic mapping of threats to MITRE ATT&CK tactics, techniques, and threat group signatures that gives detailed descriptions, recommended remediation tips, and reporting tools.

About LogRhythm

LogRhythm helps busy and lean network teams save the day— day after day. With a potent combination of its comprehensive security operations platform, technology partnerships, and advisory services, LogRhythm empowers network teams to navigate a changing threat landscape with confidence. Together, we are ready to defend.

Interested in seeing LogRhythm NDR in action? Request a demo today!

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 2 8019 7185

© LogRhythm Inc. | DS221023-06

Network, Host, and User Visibility

Real-time network monitoring gathers data from within your environment across users, networks, and hosts to provide relevant, contextual information that streamlines your investigations. NDR is agentless and ingests data and logs to monitor OS and workload behaviors across environments which provide flexible and scalable monitoring of applications workloads regardless of their location.

Threat Hunting and Investigation

Easily discover anomalous activity across various attributes, protocols, and geographies with high-level summaries and side-by-side threat hunting that give context into threat activities. Gain greater clarity and faster analysis and decision making through incident timelines that combine detections and engines. Network forensics provides anomaly detection and investigative capabilities for better incident response (PCAPS, Netflow). And over 20,000 out-of-the box detection rules provide immediate protection against known security threats and rules customization helps meet specific industry security and compliance needs.

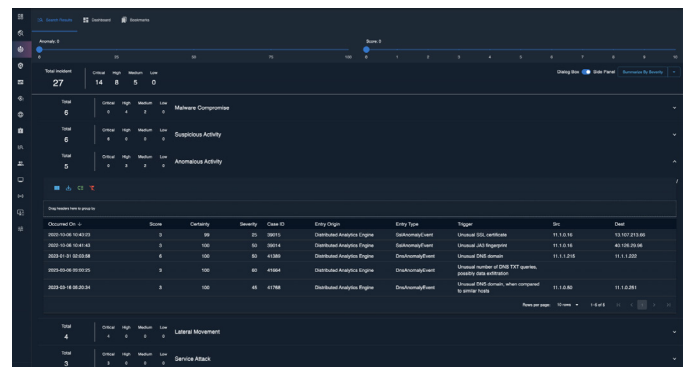


Figure 2: Easily drill down into incidents to obtain detailed threat information

SIEM, EDR, and Firewall Integrations

Plug & play integration with SIEM, EDR and other security solutions simplifies deployment, delivers broader threat detection, and provides comprehensive visibility across your environment.

Professional and Consulting Services

Gain a faster time to value with guidance from our experts.

www.logrhythm.com