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 Blind Spots:** 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