LogRhythm NDR

Real-time threat detections across endpoints, data centers, and the cloud

Combining machine learning, scenario analytics, and threat intelligence for improved detection with fewer alerts

Advanced persistent threats (APTs) are leveraging more unique and sophisticated techniques to compromise organizations across the globe. Detecting these new attacks requires in-depth holistic visibility into your networks, to detect, mitigate, and reduce your response times. As these threats increase and your enterprise network and services grow in reach and sophistication, intelligent and scalable network detection and response (NDR) is key to protect corporate information.

LogRhythm NDR s a network detection and response solution powered by machine learning (ML) with a built-in MITRE ATT&CK™ Engine that eliminates blind spots and monitors your organization’ s network in real time. This SaaS-based NDR solution works with existing endpoint detection and response (EDR) solutions to add network visibility and provide threat detection holistically across endpoints, data centers, and the cloud.

Use LogRhythm NDR to secure:

- North-South traffic to and from your data center
- East-West traffic flowing within your organization
- Cloud traffic flowing to and from the public cloud

LogRhythm NDR addresses these use cases using hybrid analytics and a powerful combination of ML, rules-based detection, threat intelligence, and user and host contextualization that protects against both known and unknown threats.

More detection with fewer alerts

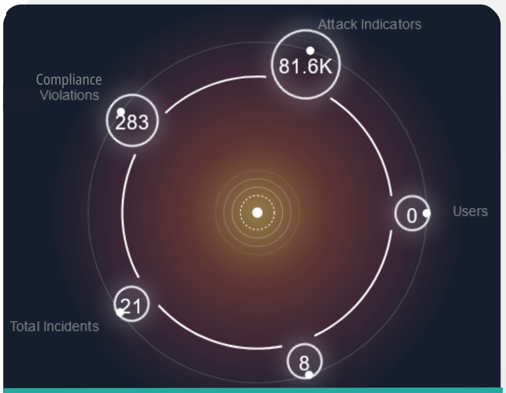
While other NDR solutions rely solely on ML applied to single streams of data to detect network security issues, LogRhythm NDR uses advanced learning models to analyze network, user, and host activity, providing a true representation of all activity within your organization’ s domain. This blended approach detects more attack indicators while also helping to reduce false positives.

Network, host, and user visibility

LogRhythm NDR provides a complete and accurate model of end-to-end enterprise activity at the network, host, and user level. Each level maps back to the MITRE ATT&CK framework, giving you an easy-to-understand security narrative that includes a timeline of activity and descriptions of the attack and techniques used. It also provides possible mitigations, helping you quickly respond to threats like lateral movement, exfiltration, malware compromise, and ransomware.

Benefits

- Eliminate: Remove blind spots with machine learning and rules-based network threat detection and response
- Minimize: Decrease mean time to respond (MTTR) with a built-in MITRE ATT&CK Engine
- Reduce: Lower operating costs and data movement with easy-to-scale TensorMist-AI™ architecture
- Protect: Safeguard data center and cloud with real-time detection
- Integrate: Connect with market-leading firewalls and EDR solutions for holistic threat detection and response



Real-time dashboard shows detected attack indicators, compliance violations, hosts, users, and incidents.

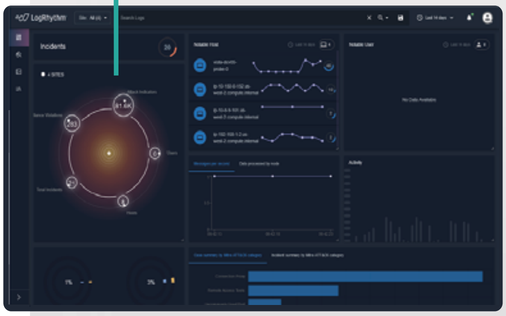


Figure 1: Accurate threat detection with user and host visibility

Scalable architecture

LogRhythm NDR is powered by a mesh of distributed collector/analytics (C/A) nodes that deliver a global analytics view without moving data to a central location. Our patented TensorMist-AI™ technology enables the construction of a big data mesh with the ability to collect and enrich security data on location, generating exceptionally accurate behavioral and threat models without having to move any of the data LogRhythm SaaS delivery, combined with this mesh-network analytics processing, makes it easy to scale, protect privacy, and avoid hidden operational expenditures for data movement.

LogRhythm C/A nodes are typically installed at each site and positioned close to network taps that can present the majority of the communication traffic traversing and ingressing/egressing the environment. Customers can felxibly:

- Deploy rack-mounted C/A appliances in offices, data centers, co-location facilities, and IoT environments
- Use agentless and serverless options for cloud properties
- Bring your own server

EDR and firewall integrations

EDR integrations support CrowdStrike, VMware Carbon Black, SentinelOne, Cybereason, and Cisco Secure Endpoint deployments. LogRhythm NDR also integrates with market-leading firewalls, such as Palo Alto Networks, for log coolection. Analsts can configure the third-party solutions in ruinutes from the Log Rhythm NDR console to activate data ingestion.

Deployment options

LogRhythm NDR can run standalone where all threat detection, defense, and hunting functions are managed and visualized through its user interface. Alternatively, the solution works in combination with the LogRhythm SIEM Platform using bi-directional integration to forward detections to the LogRhythm platform and relevant data sources to LogRhythm NDR.

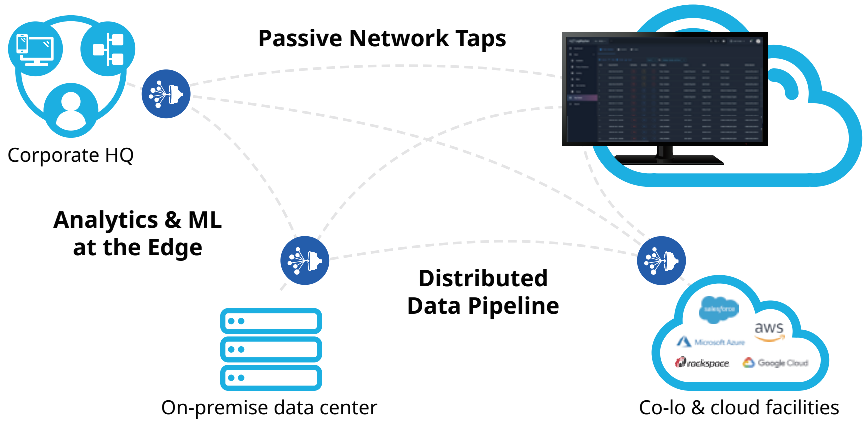


Figure 2: TensorMist-AI: Simple to start, flexible to deploy, and easy to scale

Features

MITRE ATT&CK Engine provides analysts with an easy-to-understand security narrative

- AI-assisted MITRE ATT&CK hunting with real-time and historical visualization tools
- Automatic mapping of threats to MITRE threats and techniques
- Threat hunting includes structured and unstructured search, "side-by-side" hunting, and filtering by MITRE ATT&CK threat type
- Incident Detail compiles all related attack indicators and displays them in a timeline

Rules-based detection delivers out-of-the-box-protection and security compliance

- Over 20,000 out-of-the-box detection rules with weekly updates and ML-based tuning
- Rule customization for specific industry security and compliance needs

High fidelity reporting minimizes noise and alert fatigue

- Supervised and unsupervised ML-driven detection models for network, host, user, and process activity
- Real-time behavior modeling for lateral movement, exfiltration, malware compromise, and ransomware detection

Integrated threat intelligence feeds provide highly contextualized incidents

- Integration with commercial threat intelligence feeds enables LogRhythm NDR to report accurate and highly contextualized incidents for faster detection and response

EDR and firewall integrations expand threat detections

- Existing EDR and firewall solutions add network visibility and provide threat detection holistically across endpoints, data centers, and the cloud