LogRhythm™

Data Sheet

MistNet NDR by LogRhythm

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.

MistNet NDR by LogRhythm is 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.

Use it 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

MistNet NDR addresses these use cases with a powerful combination of ML, rules-based detection, threat intelligence,and user and host contextualization that protects against both known and unknown threats. MistNet NDR comes with an architecture that makes it simple to deploy, scale, and use.

More Detection with Fewer Alerts

While other NDR solutions rely solely on machine learning applied to single streams of data to detect network security issues, MistNet NDR uses advanced learning models to analyze network, user, and host activity, providing a true representation of all activity within the organization' s domain. This blended approach effectively detects more attack indicators while also reducing false positives by over 90 percent.

Network, Host, and User Visibility

MistNet 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 blind spots with machine learning and rules-based network threat detection and response.
- Minimize MTTR with a built-in MITRE ATT&CK Engine Reduce operating costs with easy-to-scale TensorMist-AI architecture.
- Protect data center and cloud with real-time detection.

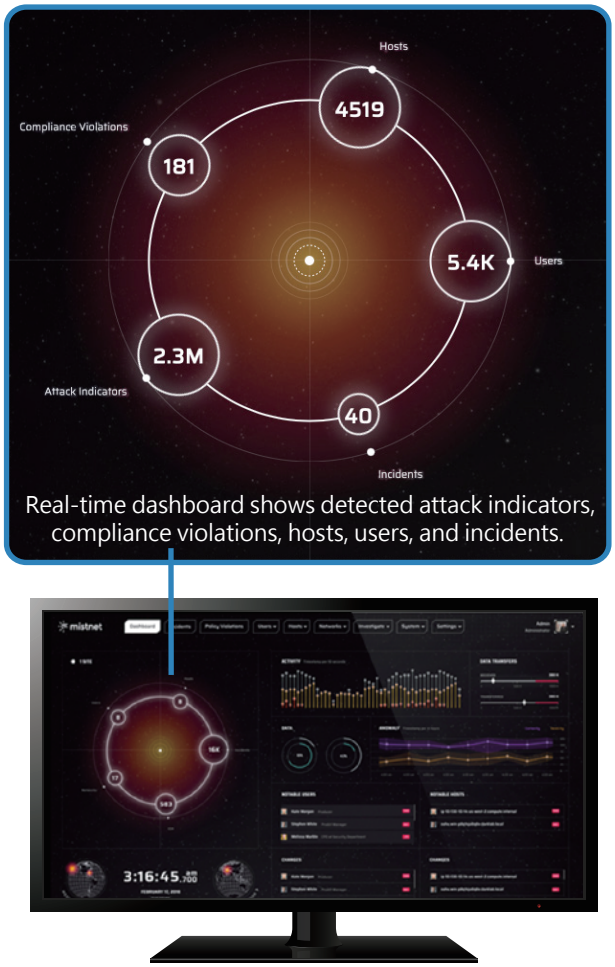

Figure 1: Accurate threat detection with user and host visibility

No Data Movement

MistNet 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. Patent-pending 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' s SaaS delivery, combined with this mesh-network analytics processing, makes it easy to scale, protect privacy, and avoid hidden operational expenditures for data movement.

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 operational environment and 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 with weekly updates and ML-based tuning.
- Rule customization for specific industry security and compliance needs.

ML-Based Detection Reduces False Positives by More than 90 Percent

- 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.

TensorMist-AI Eliminates Data Movement and Reduces Bandwidth Costs, Privacy Risk, and Compliance Issues

- Patent-pending TensorMist-AI™ technology for distributed data collection and analytics with local data enrichment and zero data movement.

Deployment Options

MistNet 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 NextGen SIEM Platformusing bi-directional integration to forward detectionsto the LogRhythm platform and relevant data sources to MistNet NDR.

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

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

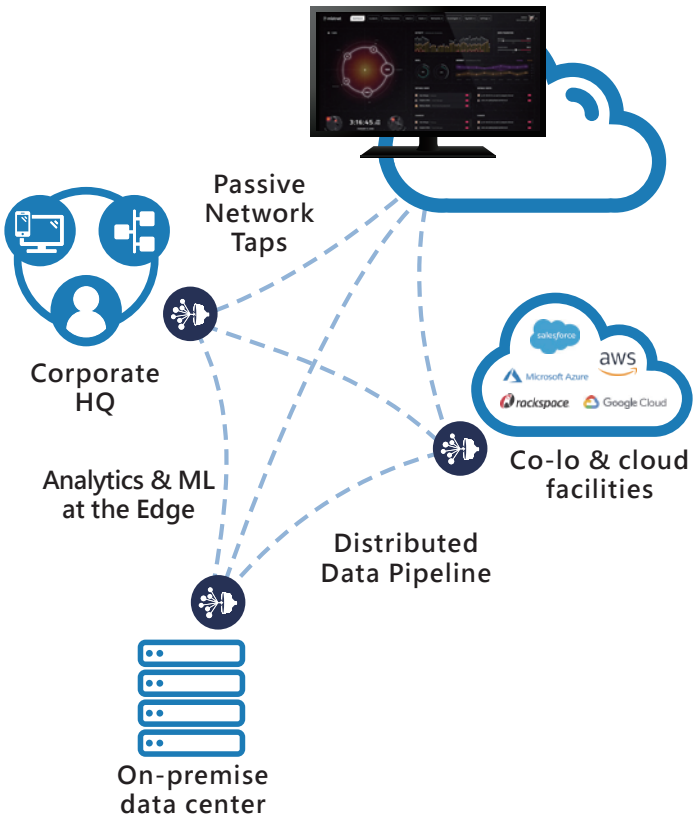

Figure 2:
TensorMist-AI: Simple to start, flexible to deploy, and easy to scale.

LogRhythm™ 漢領國際有限公司 JAS Lead

106414台北市大安區敦化南路二段77號8樓之2
電話：+886-2-2709-6983
傳真：+886-2-2707-6983
www.jas-solution.com sales@jas-solution.com