ATTACKFENCE
Autonomous Cyber Defense Platform

Network Detection and Response (NDR) Datasheet

Unlocking a New Era of Network Security

In an ever-evolving digital landscape, securing your network against a myriad of threats requires cutting-edge solutions and unwavering vigilance. That's where AttackFence® steps in, redefining network security with our advanced Network Detection and Response(NDR) solution.

At the heart of our NDR is the capability to capture network traffic at speeds of up to 40Gb/s, providing unparalleled visibility into your network's activities. Leveraging state-of-the-art Machine Learning(ML), our real-time threat detection system identifies even the most elusive threats, from zero-day exploits to advanced persistent threats.

Use Cases

Advanced Threat Detection

Identify & stop sophisticated threats such as zero-day attacks, APTs, and ransomware in real time.

Incident Response Acceleration

Streamline incident response with automated alerts, added threat context, & actionable insights.

Cloud Security Monitoring

Extend threat detection and response capabilities to cloud environments for comprehensive cloud security.

Insider Threat Detection

Monitor & detect anomalous behaviour & data exfiltration by insider threats, including employees & contractors.

Compliance Monitoring

Ensure compliance with industry regulations & internal security policies by monitoring for policy violations.

Network Traffic Analysis

AttackFence NDR employs advanced network traffic analysis to detect and respond to threats utilizing entropy based anomaly detection.

Identify Policy Violations

Supports network security initiatives by continuously validating & verifying unsanctioned apps, security posture gaps, inadvertent exposures and securing network access.

Key Features

1. High-Speed Network Sensors:
Capture network traffic at speeds of up to 40Gb/s for comprehensive visibility.

2. Real-Time Threat Detection:
Utilizes Advanced Machine Learning (ML) capabilities for immediate threat detection.

3. Threat Correlation with Threat Intelligence:
Real-time correlation of threats with Threat Intelligence feeds and adherence to the MITRE ATT&CK™ Framework.

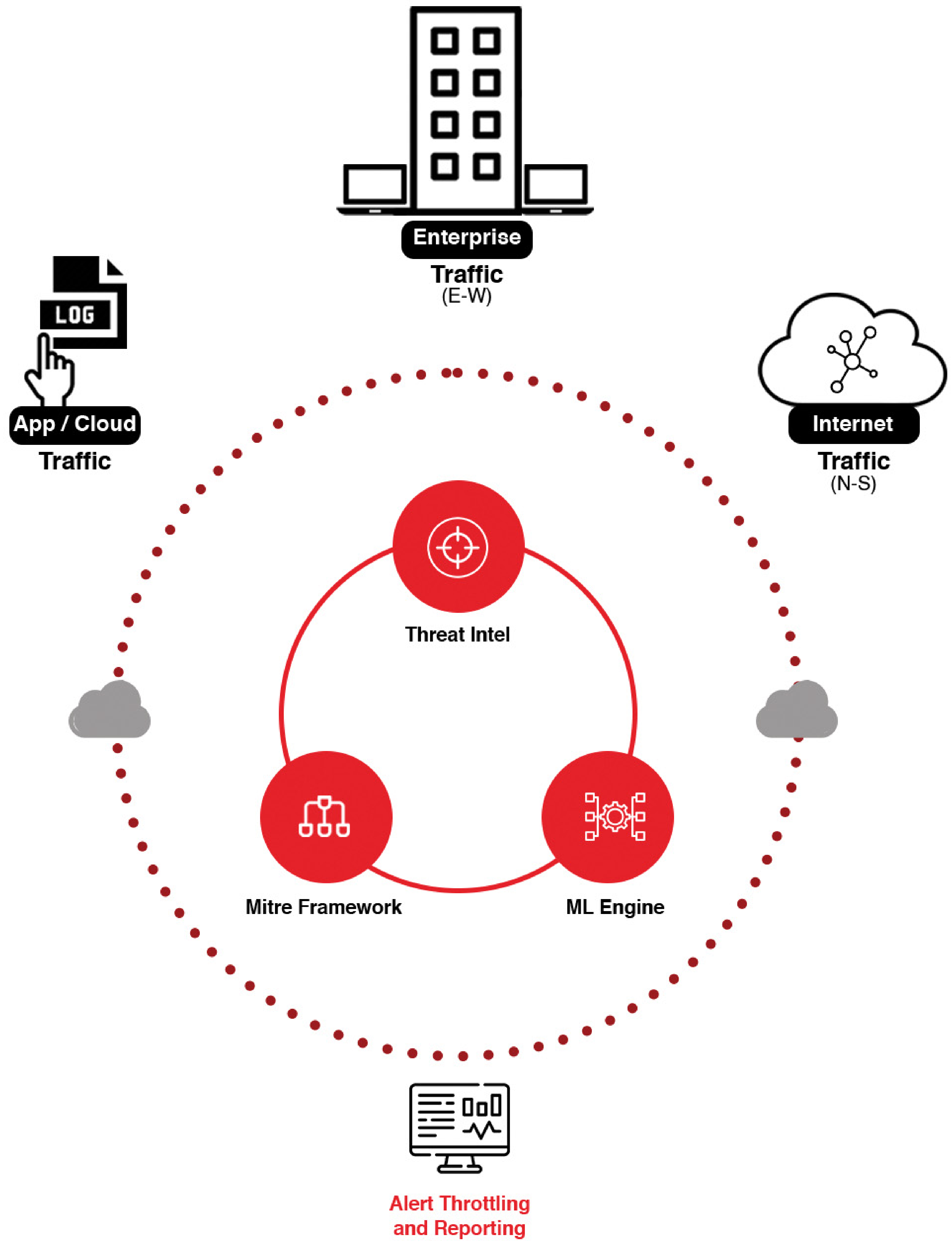
4. Current State Awareness:
Provides a real-time view of the network's security posture and threat landscape.

5. Centralized Monitoring:
Centralized dashboard and reporting for streamlined monitoring and analysis

6. Alert Throttling:
The intelligent alerting mechanism prevents alert fatigue and deluge by prioritising critical threats.

7. Incident Response:
Robust incident response capabilities to mitigate and remediate threats promptly.

8. Managed NDR Services:
Offered through trusted partners for expert management and support.



Our Offerings

Solution Components	Capacity
Sensor for Network Flow	40Gb/second or 200,000 Flows/second

Scalability & Availability	Method
Redundant Deployment	Supported. Active-Standby for Network Sensor
Throughput scalability	Supported. Using an external Network Packet Broker to cascade multiple sensors.

Support and Services

24x7 Support
E-mail and Telephonic

Engineering Services
Incident Response and Customization

Professional Services
Solution sizing, system architecture, implementation & commissioning

Managed Services
Managed Detection & Response

Reach us:
connect@attackfence.com | +91 9818855853

ATTACKFENCE
Autonomous Cyber Defense Platform

AttackFence Techlabs Pvt. Ltd.
426,428, Tower A,
Spaze I-tech Park, Sector 49,
Sohna Road, Gurugram-122018

www.attackfence.com

About AttackFence

We are a cybersecurity product company offering XDR [Extended Detection and Response] solution. Superior effectiveness of our solution emanates from our leveraging knowledge of attacker behavior during different phases of an attack. The solution provides comprehensive visibility across network, endpoint, cloud workloads, containers and SaaS for improved profiling and compliance. Multi-pronged analytics approach based on MITRE ATT&CK™ framework and Machine Learning algorithm mesh enables the solution to detect even stealthiest of malware. Deployment can be on-premises, 100% in the cloud or hybrid. Our XDR's Detection based on attacker's behavior and swifter response via integrations with existing security and infrastructure components would make you more effective against cyber-threats while keeping TCO low.