ATTACKFENCE
Autonomous Cyber Defense Platform

Network Behaviour Analysis & Detection (NBAD)

Unlocking a New Era of Network Security

In today's ever-evolving digital landscape, securing your network demands cutting-edge solutions. AttackFence® introduces an advanced NDR solution, embodying Network Behavior Analysis and Detection (NBAD) capabilities to redefine network security. With a focus on comprehensive visibility, real-time threat detection, and robust incident response, AttackFence® stands as a stalwart guardian of your digital assets.

Use Cases

Advanced Threat Detection

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

Incident Response Acceleration

- Streamline incident response with automated alerts, enhanced threat context, and actionable insights.

Cloud Security Monitoring

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

Insider Threat Detection

- Monitor and detect anomalous behavior and data exfiltration by insider threats, including employees and contractors.

Compliance Monitoring

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

Network Traffic Analysis

- Utilize advanced network traffic analysis for the detection and response to threats using entropy-based anomaly detection.

Identify Policy Violations

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

Customizable Reports and Audit Logs

- Generate customizable reports viewable within the Sensor/Probe GUI.
- Ensure audit logs and reports are available for offline analysis.

System Alerts and Severity Classification

- Generate system alerts of different severity levels (Critical, Major, Minor, Notice).
- Reporting on RTT, SRT, delay, jitter, retransmission, and out-of-order packets included in flow statistics.

Use Cases

HTTP Traffic Monitoring and Analysis

- Monitor and analyze HTTP traffic, including URL, method type, status codes, and hostname.
- Report hostname as SNI for HTTPS traffic.

Access Management and User Roles

- Provide Role-based user and access management.
- Data separation with access limitation for individual roles/users.
- Only superuser of GUI/CLI configures system-level parameters, while normal users view system parameters and current statistics.

Custom Profiles and User-Defined Filters

- Users can define custom profiles for persistent views of the data.
- Create profiles for data storage according to defined filters, e.g., HTTP, FTP, SMTP, SSH traffic.

Encryption and Tunneling Protocol Support

- Analyze encrypted communication without decryption technology.
- Process tunnelled protocols/applications such as GTP, GRE, IPSEC, MPLS.
- Support a base level of threat information and detect security incidents in different network segments.

Threat Identification and Anomaly Detection

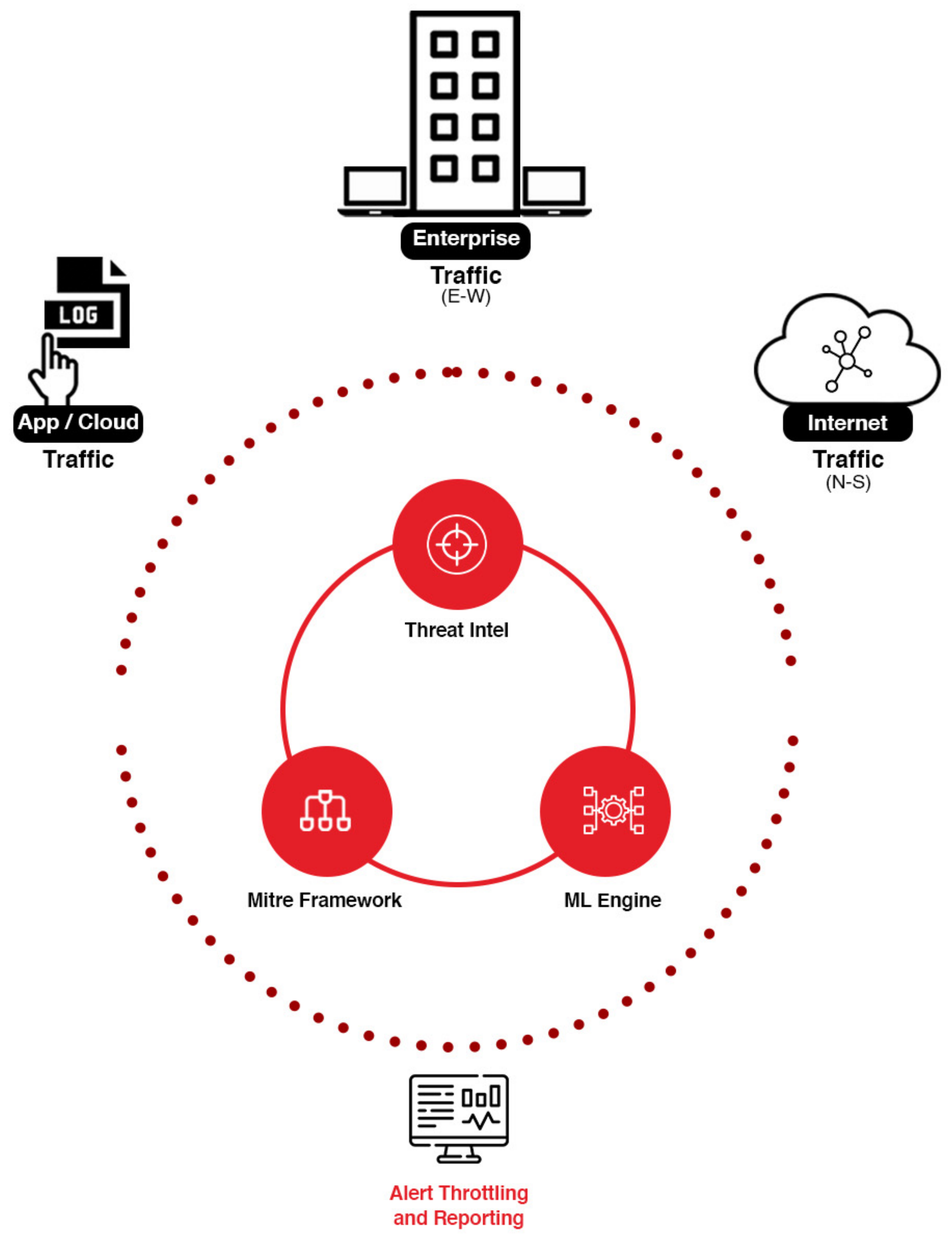
- Enrich flow records with additional information for threat identification.
- Flow records enriched with entity information, IP reputation, and geolocation.
- Utilize non-statistical machine learning methods to build and continuously update the model of network behavior.

Integration and Alerting

- Integrate with SIEM solutions and provide RESTful API and syslog forwarding for alerting.
- Provide a RESTful API for implementing response actions.

Visualization and Reporting

- Web-browser based end-user interface for configuration, monitoring, management, and analysis.
- Dashboard with custom dashboards and visualizations supporting identification and investigation of events.
- Central overview screen showing real-time alerts and live traffic.
- Visualization types include charts, graphs, tables, and counts.
- Ability to query data of variable time ranges and generate custom reports.
- Support for sharing/limiting dashboards and visualizations to specific user groups.
- Queries targeted at specific indexes to refine results and reduce response time.



Our Offerings

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

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

Key Features

High-Speed Network Sensors

-Capture network traffic at speeds up to 40Gb/s for comprehensive visibility.

- Sensors with up to 4x 1 GbE monitoring ports per device or 2x 1/10 Gb SFP monitoring ports per device.

- Full packet capture and export.

Real-Time Threat Detection

- Advanced Machine Learning (ML) for immediate threat detection.

- System-generated alarms with severity classification for various packet metrics.

Threat Correlation with Threat Intelligence

- Correlate threats in real-time with Threat Intelligence feeds.

- Adherence to the MITRE ATT&CK™ Framework for threat intelligence.

Network Traffic Analysis

- Employ advanced network traffic analysis for detecting and responding to threats using entropy-based anomaly detection.

- Layer 7 support, including SSL, DNS, HTTP, SIP, and TCP session timing information.

- Support for IPFIX protocol IETF RFC7011 and the latest version of Netflow-V9, NetFlow v5, IPFIX, jFlow, cflowd, Net Stream, slow, NetFlow Lite, etc.

- Configurable sampling rates for manual configuration or 1:1 processing of flows.

- Combine/stitch flow records from different network devices associated with a single conversation.

Centralized Monitoring

- Centralized dashboard and reporting for streamlined monitoring and analysis.

- Customizable dashboards and visualizations for event identification and investigation.

Incident Response

- Robust incident response capabilities to mitigate and remediate threats promptly.

- Replication of flow records to multiple collectors.

Managed NDR Services

- Offered through trusted partners for expert management and support.

- 24x7 support via E-mail and Telephonic.

Solution Components and Capacity

- Sensor for Network Flow and Data Lake.

- Handle network traffic at speeds of up to 40Gb/s or 200,000 Flows/second.

Support and Services

24x7 Support	Professional Services
E-mail and Telephonic	Solution sizing, system architecture, implementation & commissioning
Engineering Services Incident Response and Customization	**Managed Services** Managed Detection & Response

ATTACKFENCE
Autonomous Cyber Defense Platform

Specifications

Flow Record Formats

IPFIX protocol support (IETF RFC7011). Support for various NetFlow versions including NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, Net Stream, slow, NetFlow Lite. Layer 7 monitoring for SSL, DNS, HTTP, SIP, TCP session timing, Samba/CIFS, DHCP, SMTP, POP3, IMAP, and MS SQL (TDS). Configurable sampling rates for flow/packet-level processing. Combining/stitching flow records from different network devices.

Network Sensor Specifications

High-speed network sensors capable of capturing traffic at speeds of up to 40Gb/s. Appliance-based probe with up to 4x 1 GbE monitoring ports or 2x 1/10 Gb SFP monitoring ports per device. Un-sampled flow-based monitoring for detailed and accurate communication session information. De duplication of packets and thorough analysis.

Advanced Network Traffic Analysis

Comprehensive support for IPv4 and IPv6 traffic, including TCP, UDP, UDP over IPv6, ICMP, and ICMPv6. Analysis up to the application layer. Capable of analyzing encrypted communication without decryption technology. Support for tunnelled protocols/applications such as GTP, GRE, IPSEC, MPLS. Passive sensors/probes for non-intrusive monitoring.

Purpose-Built Hardware

Purpose-built HW Probe appliances with 4 x 1GbE interface for each branch location, supporting up to 1 GBPS traffic. Purpose-built HW Probe appliances for DC and DR supporting a minimum of 4* 10 Gbps. Purpose-built HW Collector at each site of DC & DR with minimum 2 x 10Gig traffic interfaces.

Records Replication & Load Balancing

Replication of IPFIX/Netflow-v9/JSON records to multiple collectors (at least 3 remote collectors). Load balancing of IPFIX/Netflow-v9/JSON records to multiple sub-collectors (at least 5 sub-collectors).

SNMP Integration & Management Ports

Support for SNMP integration, providing a management port for out-of-band management with minimum 2 x 1GbE for system access and management. SNMP interface for remote monitoring of the probe (2 x 1GbE Ethernet for system access and management).

Audit Logs, Alarms & Traffic Analysis

Availability of audit logs and reports for offline analysis. System-generated alarms of different severity levels. Monitoring and analysis of HTTP traffic, including URL, method type, status codes, hostname.

Data Purging & Retention

Automatic purging of local collector data files based on allocated storage size and time in FIFO logic. Automatic purging of logs with configuration (e.g., 70% of allocated size). Data retention to store records for up to and beyond 30 days with scalability for several months.

Support and Services

24x7 support through E-mail and Telephonic. Engineering services for incident response and customization. Professional services for solution sizing, system architecture, implementation & commissioning. Managed services for Managed Detection & Response. Subscription-based warranty.

Threat Detection & Analysis

Detection and analysis of threats, including advanced threat detection (zero-day attacks, APTS, ransomware). Enrichment of flow records with additional information for threat identification. Integration with threat intelligence feeds, support for machine learning methods, and alerts with associated severity scores.

User Interface & Visualization

Web-browser based end-user interface for configuration, monitoring, management, and analysis. Customizable dashboards and visualizations supporting identification and investigation of events. Central overview screen showing real-time alerts and live traffic. Visualization types include charts, graphs, tables, and counts. Query functionalities, automatic report generation, and support for sharing/limiting dashboards and visualizations to specific user groups.

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

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.

ATTACKFENCE
Autonomous Cyber Defense Platform

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

www.attackfence.com