CounterFlow ai

ThreatEye® Network Visibility

Cloud-Native Analytics for Network & Security Operation Centers

Product Overview

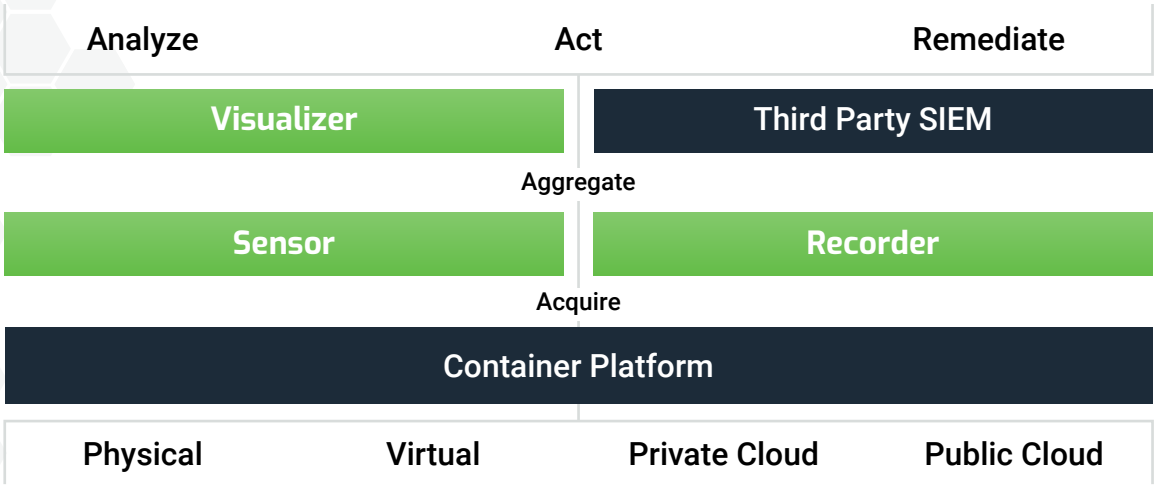
Network visibility is a growing concern for today's network security and operations personnel. From a network security perspective, visibility into threats is disappearing as over 70% of traffic is now encrypted. In addition, understanding where traffic is with today's hybrid network environments requires visibility into cloud workloads, remote sites, roaming end users, and IoT device activity. Dependent on payload inspection and deployed in a central network stack, older network sensors employing Deep Packet Inspection (DPI) technologies are no longer effective.

CounterFlow's ThreatEye platform brings together next generation traffic visualization, machine learning, and full packet capture to provide complete visibility, actionable insights, and forensics capabilities. Unlike many network traffic analysis (NTA) solutions built on legacy DPI or proprietary black-box architectures, for:

- Anomaly Detection
- Encrypted Traffic Analysis
- Network Performance Monitoring
- Incident Response
- Threat Hunting
- Visibility & Device Discovery
- Policy Compliance & Audit

Hybrid Cloud Platform

Unlike older legacy tools, the ThreatEye platform includes network visibility, analysis, and forensics products deployed as containerized applications. The core of this offering is made up of ThreatEye Sensor, ThreatEye Recorder, and ThreatEye Visualizer. Each can be deployed as a standalone product and integrates easily with third-party applications like SIEMs and Orchestration tools.



Because ThreatEye products are containerized, they offer flexible deployment options that include cloud, virtual, and on-premise hardware. Regardless of the deployment option, ThreatEye Sensor and Recorder can scale to ingest network data directly from physical or virtual network taps at wire-speeds up to 100Gbps.

ThreatEye Sensor

ThreatEye Sensor is a real-time network traffic flow sensor that combines a robust set of feature extractions with the data-driven insights of Machine Learning, at speeds of 100 Gbps and beyond:

Machine Learning

ThreatEye Sensor enables streaming machine learning (ML) to be deployed at any network vantage point. A flexible, open architecture allows integrated or distributed ML processing for network traffic analysis with user-customizable ML models.

Comprehensive Data

Built on Argus data collection—a proven open-source project—ThreatEye Sensor extracts features and performance enhancements that support machine learning for next-gen traffic analyzers like encrypted traffic analysis. Sensor also provides over 100 network data fields that include flow monitoring, extended flow attributes, latency/RTT, packet dynamics, computed statistics, management records, per flow metrics, tcp metrics, behavioral metrics, L7 applications classification, and intra-flow statistics. An open architecture supports the output of both raw flow data and analyzed results directly to a file, to ThreatEye Visualizer, or to third-party tools. A RESTful API enables easy integration with other network security devices easing integration into existing security and automation workflows.

Intelligent

ThreatEye Sensor's streaming ML analyzers run in parallel and allow for multiple traffic insights and anomaly detections in tandem, some of which include:

- User behavior profiling
- Traffic anomaly detection
- DNS, HTTPS, SSL, SSH, HTTP
- DGA detection
- Policy violations
- External DNS, encrypted DNS
- Weak or unencrypted traffic
- TLS Enforcement
- GEO & Time Fencing
- Layer 7 Mismatch
- Encrypted Traffic Analysis
- Application Identification
- OS and Host Fingerprinting
- TLS protocol tracking, fingerprinting

Additionally, ThreatEye Sensor includes threat feeds from CrowdStrike. These feeds are first curated by numerous ThreatEye ML analyzers to mitigate false positives.

ThreatEye Recorder

ThreatEye Recorder is a high-performance network traffic recorder that guarantees line-rate, full packet capture with lossless write-to-disk performance. Designed as a multi-threaded application, ThreatEye Recorder scales to retain petabytes of data and supports a range of on-premise and cloud storage options with advanced indexing and search features. ThreatEye Recorder integrates advanced packet acquisition technologies like Linux eXpress Data Path (XDP) and Napatech SmartNIC to scale in either physical or virtual deployments.

In addition, it ships with an optional packet analysis viewer allowing full reconstruction of data payloads and threat analysis tools.

ThreatEye Recorder Continued

Intelligent Recording

Deploying bulk packet capture on bare metal within an enterprise has become more costly and impractical year after year as a company's network increases in bandwidth, footprint, and complexity. While ThreatEye's Recorder can provide full lossless packet capture up to 100Gbps, ThreatEye Recorder coupled with ThreatEye Sensor software can classify and select how much data per flow to record and where to store it on a per flow basis. This could range from the initial connection setup to full packet capture, stored on local or cloud storage. Discarding traffic such as encrypted data payloads, streaming video, and data backups can save valuable storage space while enabling security analysts to access data faster with better insights.

ThreatEye Visualizer

Explore and visualize network forensics data with ThreatEye Visualizer, a powerful, interactive application which allows indexing, search, and analysis of all flow data. Whether an analyst is investigating from a security or performance perspective, ThreatEye Visualizer distills data and presents it within the appropriate context.

Designed to ingest augmented flow records, and alerts, ThreatEye Visualizer is capable of storing petabytes of enriched flow data. These resources enable analysts to query and interactively explore forensically relevant data for insights, including threat hunting and incident response operations. ThreatEye Visualizer supports traditional and advanced visualization including Time Series, Geospatial, and Graph Analysis. These visualizations provide explanations of the data and features behind ThreatEye 's machine learning models.

LEARN MORE AT: www.CounterFlowAI.com

CounterFlow ai

About CounterFlow AI, Inc.

CounterFlow AI is addressing the growing network visibility gap created by the rise of encrypted traffic. Its ThreatEye® cloud-native analytics integrate cryptanalysis, packet dynamics, and machine learning techniques to identify patterns associated with network faults, anomalies, and threats in real-time. Unlike subversive SSL decryption methods, ThreatEye's approach preserves privacy and renders deep insights into both encrypted and unencrypted traffic. Offered on a subscription basis, CounterFlow's software is designed for hybrid cloud deployments to easily extend the visibility of network and security operations across an entire enterprise.

CounterFlow AI, Inc.

6181 Rockfish Gap Turnpike, Crozet, VA 22932
info@counterflowai.com