CounterFlow ai

ThreatEye® Sensor

Feature Highlights

- Streaming Machine Learning (ML)
- Encrypted Traffic Analysis
- Integration with Threat Intelligence
- Web-based GUI
- Integration with SIEM and firewall solutions
- Supports 1, 10, 20, 40, and 100 Gbps line rates

Product Overview

Machine Learning at the Edge

ThreatEye Sensor enables streaming machine learning (ML) to be deployed at any network vantage point. With versatile deployment options that include hybrid, cloud, and on-premise, it is the cost-efficient software platform of choice for high-performance, wire speed analysis of network traffic. A flexible, open architecture supports rapid deployment of customized ML models and analytics. A RESTful API enables easy integration with other network security devices. Built on Argus, a proven open-source project, ThreatEye Sensor includes enterprise-grade features and performance enhancements to support machine learning and encrypted traffic analysis at line rates.

Comprehensive Data

ThreatEye Sensor provides over 100 network data fields that include flow monitoring, extended flow attributes, packet dynamics, computed statistics, and management records. No need to wait until flow completion before beginning analysis, because flow records are updated incrementally as packets arrive. An open architecture supports the output of both raw data and analyzed results directly to a file, ZeroMQ and/or Apache Kafka easing integration into existing security and automation workflows.

CounterFlow ThreatEye Machine Learning

ThreatEye Sensor provides a full spectrum of analytic capabilities from basic counts and statistics to advanced machine learning models -- all running at sustained 40Gbps performance. An open-box design allows analysts to build trust and confidence in ML, while also enabling them to better understand why a model yields certain results. No more black boxes. Whether using ThreatEye Visualizer or a different visualization platform, ThreatEye Sensor provides analytic insights that go beyond a single score so that humans can easily understand and take action based on the results.

Algorithms and machine learning approaches include, but are not limited to, the following:

- Classification and Regression
- Clustering
- Graph Analysis
- Outlier/Anomaly Detection
- Encrypted Traffic Analysis

Detailed Field Overview

FLOW
- IP (src and dest)
- ports
- protocol
- Total Bytes
- Total Pkts
- Start time
- Duration

EXTENDED FLOW
- Packet payload
- Source and Destination flow details
- Additional networking details (MAC, VLAN, MPLS, ICMP, TCP flags and options)

PACKET DYNAMICS
- Connection Setup Times
- Interpacket Arrival time and Jitter
- Connection statistics (FIN, RST, SYN Window advertisements, Zero windows)
- Bytes and packets per second
- Dropped/retransmitted packet statistics

COMPUTED STATISTICS
- Producer/Consumer Ratio
- App/Byte Ratio
- Key Stroke Count Estimation
- Flow Active Runtime Statistics

MANAGEMENT FIELDS
- Record Cause (Start, Status, Stop, Close, Error)
- Flow Identifier (seq)
- Sensor ID
- Record Type (“flow” or “management”)

ThreatEye Sensor

	ThreatEye Sensor
Form Factor	AMI, 1U
Scriptable Analyzer Interface	LUA Just-in-Time Compiler
Available Output Formats	File, ZeroMQ, Kafka
Line-Rate Processing	1 - 40 Gbps
Management Interface	2 x 1G BT + 2 x 1/10G SFP+
GUI	Yes, WEB based
Redundant PSU	Yes
3 Years Support, Warranty and Updates	Yes
Power Consumption, Approximate Values	Efficiency Class: Platinum Recorder: Rating 2×750W; Idle 477W; Capturing 603W Storage unit: Rating 2×600W; Idle 226W; Capturing 245W Voltage Rating: 100-240V~50/60Hz

ORDER INFORMATION

Scaling from 10 Mbps to 100Gbps, ThreatEye Sensor comes with flexible deployment options including appliances for hybrid cloud deployments. ThreatEye products are sold as appliance images that run on Red Hat certified platforms including physical, virtual and cloud. Physical deployments include an option for a high performance SmartNIC.

Annual Subscriptions options include two technical support levels:

STANDARD SOFTWARE SUPPORT

includes technical support, access to customer web portal, security patches, maintenance updates, and unlimited feature upgrades.

PREMIUM SOFTWARE SUPPORT

includes Standard Software Support plus advanced 24x7 support with a dedicated support engineer.

LEARN MORE AT: www.CounterFlowAI.com

CounterFlow ai

About CounterFlow AI, Inc.

CounterFlow AI is a cybersecurity software company offering an AIOps platform for network forensics. The flagship product, ThreatEye®, integrates advanced security technologies into a streaming machine learning pipeline to identify network faults, anomalies, and threats at wire speed. ThreatEye® is built for hybrid cloud deployments to easily extend customer network and security operations.

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