

Feature Highlights

- Full line-rate packet recording
- Sustained 40 Gbps capture-to-disk
- Federated Search
- Nanosecond timestamp precision
- Ultra-fast data retrieval
- Berkeley Packet Filters (BPF)
- RESTful API
- Web-based GUI
- Integration with SIEM and firewall solutions
- Supports 10, 20, 40, and 100 Gbps line-rates
- Retrospective DPI and threat analytic

Product Overview

Accelerate Time to Resolution

ThreatEye Recorder is the cost-efficient software platform of choice for ultra-fast, highly reliable, real-time capture of network traffic. With flexible deployment options that include on-premise, hybrid, and cloud. Connectivity options are available for 10, 20, 40, and 100 Gbps line rates. Storage capacity scales to retain petabytes of data with advanced indexing and search features. A RESTful API enables easy integration with other network security devices.



Demand Network Visibility

Quickly access critical data with 100% accuracy and no packet loss. Empower analysts with an efficient packet analysis workflow. Tag captured files and share links to notes and comments, facilitating easy collaboration across teams of analysts. Correlate a security alert with the raw packet data that triggered it and leverage retrospective threat analytics to understand the structure and timeline of a compromise or attack.

Advanced Indexing for Faster Results

An indexing scheme based on 5-tuple and layer 2-4 protocols returns accelerated search results. Use federated search features to query across multiple recorders in a group, either co-located or geographically distributed.

CounterFlow ThreatEye Recorder Applications

Network security analysis is only as good as the data it's based upon. ThreatEye Recorder provides total recording confidence and fast, easy access to retained data for applications in security, performance, or compliance. Proven use cases include, but are not limited to, the following:

- Incident Response
- Threat Hunting
- Compliance
- Network Monitoring
- Financial Fraud Detection and Latency Measurement

	ThreatEye Recorder Flex	ThreatEye Recorder 20
Form Factor	2U + 2U per storage unit	2U
Storage Capacity	120TB - 1PB	28TB
Capture-to-Disk Performance	10 - 40 Gbps	20 Gbps
Capture Connectivity Options	<ul style="list-style-type: none"> • 4 x Dual-rate 1/10 Gbps SFP/SFP+ • 2 x 40 Gbps QSFP+ • 2 x 100 Gbps QSFP28 	<ul style="list-style-type: none"> • 4 x Dual-rate 1/10 Gbps SFP/SFP+ • 2 x 40 Gbps QSFP+ • 2 x 100 Gbps QSFP28
Management Interface	2 x 1G BT + 2 x 1/10G SFP+	2 x 1G BT + 2 x 1/10G BT
GUI	Yes, WEB based	Yes, WEB based
Redundant PSU	Yes	Yes
3 Years Support, Warranty and Updates	Yes	Yes
Power Consumption, Approximate Values	Efficiency Class: Platinum Recorder: Rating 2x750W; Idle 477W; Capturing 603W Storage unit: Rating 2x600W; Idle 226W; Capturing 245W Voltage Rating: 100-240V~50/60Hz	Rating 2x750W; Idle 312W; Capturing 374W 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



Copyright © CounterFlow AI 2019. All rights reserved. CounterFlow AI is a trademark used under license by CounterFlow AI, Inc. All other logos, trademarks and service marks are the property of the respective third parties.

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

