DATA SHEET

Encrypted Traffic Visibility and Advanced Behavioral Analysis

A Fundamentally Different Approach to Threat Detection and Response

ThreatEye's AI-powered NDR enables simplified management of the threat investigation life cycle by combining and correlating sets of high-fidelity findings to track the state of an incident.

ThreatEye's workflow capabilities support SOC analyst workflows with integrated packet analysis insights. This allows analysts to collaborate across their teams with an interactive layer. ThreatEye's integrated approach to searching, collaborating, and alerting, all in one place.

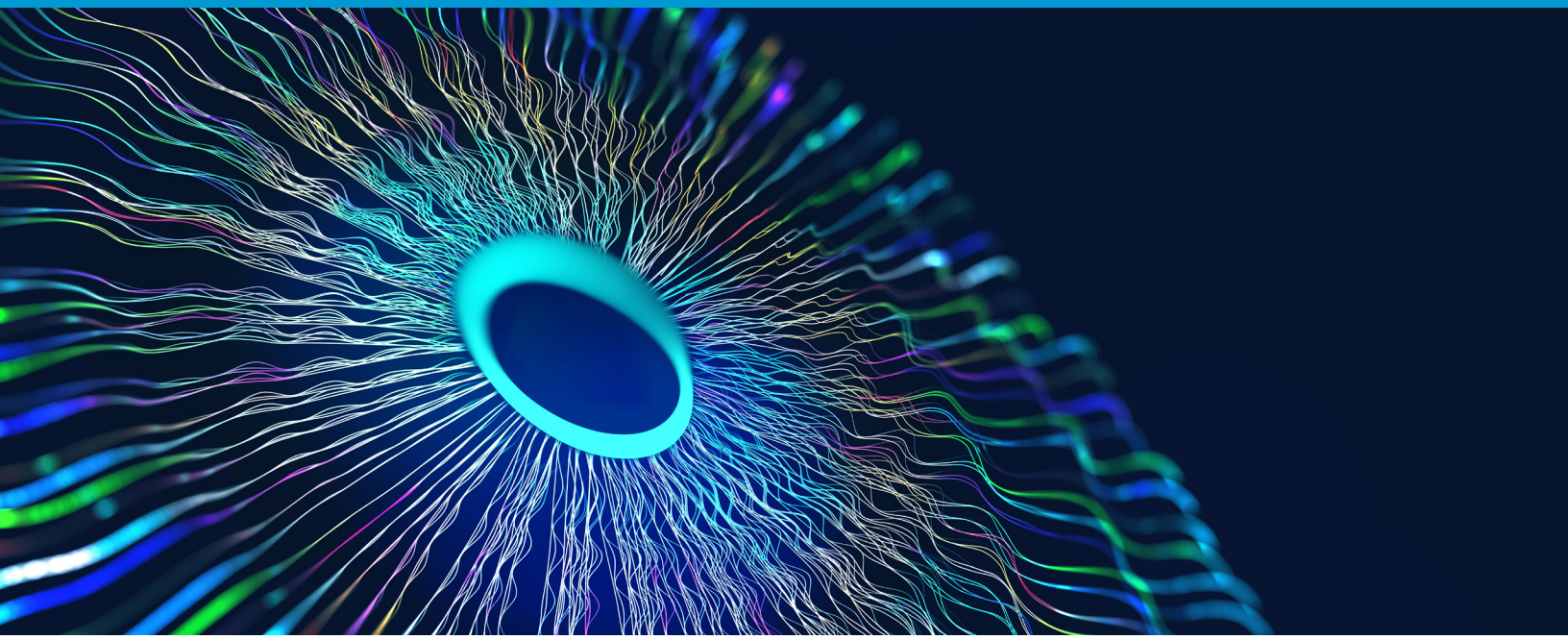
Introduction

Sophisticated threat actors are continually advancing their tactics through phishing and credential theft, social engineering attacks, and exploiting known vulnerabilities to launch cyber-attacks on enterprises. Malware resident on an endpoint is no longer a requirement to breach an organization. With the shift away from signature-based malware used in attacks, strategies focused on leveraging Endpoint Detection and Response (EDR) solutions are increasingly less effective.

SOC Analysts and Network Security Teams need a superior approach to effectively combat cyber-threats. Depth-in-defense strategies will always prove useful, but traditional security staples are proving ineffective to rapidly evolving threat actor methods.

The increased adoption of encryption by enterprises to harden their security posture and protect data has almost killed off the future of Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) solutions.

A different security strategy is overdue for organizations to make an immediate impact against adversaries and stay ahead of tomorrow's threats.



How ThreatEye Works

Supporting the ThreatEye platform is-an AI-powered analysis pipeline, combining data collection, advanced behavioral analysis, predictive threat intelligence, and machine learning to detect threat actors and comply with security regulations. Unfazed by encryption, ThreatEye examines network traffic traits and characteristics with machine learning-based analysis. Unlike traffic analysis solutions built on DPI technologies, the ThreatEye platform leverages Deep Packet Dynamics (DPD) to analyze traffic flows without decryption. DPD provides high-fidelity flow records with over 150 features for each flow—all without payload inspection. Packet Dynamics, backed by machine learning, enables new insights into encrypted traffic.

AI-Powered Advanced Behavioral Analysis

ThreatEye's AI-powered fingerprinting learns how networks operate and how devices interact. ThreatEye discovers anomalies by tracking multiple vectors of information, like Producer-Consumer-Ratios (PCRs) and nth degree social networks, to know when an attacker is active in an environment. ThreatEye creates a historical inventory of traits and behaviors, fingerprinting, mapping, and profiling assets. This technique works equally well with encrypted and unencrypted traffic. Machine Learning models are applied to identify behavioral anomalies indicating threat actor presence.

Key Benefits and Outcomes

Encrypted Traffic Analysis

ThreatEye's Deep Packet Dynamics (DPD) is agnostic to packet contents and is used to create a fingerprint of network flows for profiling and anomaly detection. This technique works equally well with both encrypted and unencrypted traffic. Machine Learning models are applied to individual traffic flows to identify advanced behavioral threat actor anomalies.

Real-Time Detection

Reduce operational outages with faster troubleshooting through real-time detection analysis. Designed to process millions of events per second, ThreatEye leads the industry with its rapid multi-stage analysis pipeline fueled by analyzers or models. These models are engineered to analyze network traffic without multiple passes over the data stream. In addition, these models are explicitly architected for network security and scale via parallel processing.

Key Benefits and Outcomes

Advanced Behavioral Analysis

ThreatEye is continually tracking and updating the behavior of all assets, identifying tools and services usage, inventory of protocols, time of day, asset types, and communication patterns. Threat builds a fingerprint of assets and monitors for change-point detections to identify anomalous usage.

Predictive Threat Intelligence

ThreatEye's threat intelligence feeds are curated by our team to provide up-to-date indicators for active threats in the wild. Included in this feed is predictive threat intelligence and campaign tracking, revealing IPs and domains associated with threat actors before they are activated.

Effective when EDR/IDS/MFA is Bypassed

When attacks occur, changes in the behavior of an assets network traffic is the key differentiator, is in essence the final source of truth, when detecting threat actor behavior after all other layers of the security stack fail to prevent attack escalation. When the attacker is fully authenticated, not using malware, and bypasses EDR, ThreatEye is foundational to the success of stopping the attack.

Decreased Time to Investigate and Respond

ThreatEye's AI-powered NDR enables simplified management of the threat investigation life cycle by combining and correlating sets of high-fidelity findings to track the state of an incident. These findings and enriched metadata provide complete contextual and actionable information needed to resolve incidents faster. Validate Encryption Policy Compliance ThreatEye provides encryption-policy specific alerting and reporting for security compliance. The increased adoption of encryption to secure applications calls for a greater need to ensure all platforms conform to the encryption standards of the enterprise.

Validate Encryption Policy Compliance

ThreatEye provides encryption-policy specific alerting and reporting for security compliance. The increased adoption of encryption to secure applications calls for a greater need to ensure all platforms conform to the encryption standards of the enterprise.

Key Benefits and Outcomes

Auto-Correlated and Enriched Findings with Passive DNS

ThreatEye collects and correlates information from disparate data sources such as geography, passive DNS, MITRE ATT&CK techniques, threat intelligence, risk, and threat scores, and more to aid responders with the best course of action for any investigation.

365 Days of Retention

ThreatEye provides a default retention period of enriched metadata available for 1-year, supporting retrospective Threat Intelligence investigations and Threat Hunting initiatives. The dwell time of threat actors is dependent on their motives.

Asset Tracking and Risk / Threat Scoring

Assets are categorized among two scoring techniques for different workflows. 'Assets by Risk' is a prioritized queue of assets by policy violations that will help security and IT teams evaluate acceptable risk. 'Assets by Threat' provides prioritization of assets by threat activities to aid Network Security Teams and Security Analysts evaluate impact and potential compromise.

Unified Sensor & Intelligent Packet Capture

When attacks occur, changes in the behavior of an assets network traffic is the key differentiator, is in essence the final source of truth, when detecting threat actor behavior after all other layers of the security stack fail to prevent attack escalation. When the attacker is fully authenticated, not using malware, and bypasses EDR, ThreatEye is foundational to the success of stopping the attack.

Deployed in Minutes

ThreatEye is a SaaS platform with physical, virtual, and cloud sensors deployable in minutes. As soon as sensors are enabled, they begin collecting packets and pushing ThreatEye's Deep Packet Dynamics to the AI-Power machine learning pipeline. You'll have access to all ThreatEye's rich metadata, findings, and forensic capabilities within minutes.

Metadata Enrichment

ThreatEye's sensor extracts a rich metadata set of more than 150 packet dynamic features to support threat and anomaly detection, response, hunting, forensics, and compliance validation reporting. Because packet dynamic-based metadata focuses on packet traits and behaviors—not contents—this data collection technique works equally well with encrypted and unencrypted traffic.

Examples of metadata enrichment include:

- Byte Distributions
- SPLT (Sequence of Packet Lengths and Times)
- Jitter
- Producer/Consumer Ratio
- Retransmits
- Connection Setup Time
- Round Trip Time
- Setup Latency RTT
- Per Flow Metrics
- Intra-flow Statistics
- Extended Flow Attributes
- TCP Metrics
- Behavioral Metrics
- L7 Appl. Classification
- Internal Network Labeling
- Country Code
- ASN
- Latitude / Longitude
- Service Provider Type
- JA3 / TLS Fingerprint
- Passive DNS
- OS Fingerprint
- MITRE @TTACK – TTPs

Streaming Analysis

ThreatEye is powered by a streaming machine learning engine (MLE) that ingests high-fidelity metadata generated by its sensors. ThreatEye's MLE is purpose-built for network security. Unlike traditional batch processing, streaming ML is fueled by analyzers —or models— engineered to analyze network traffic without multiple passes over the data stream. These models are architected for specific use cases and scale via parallel processing.

Threat Detection Models & Analyzers

- Unexpected Encryption
- Unexpected Plaintext
- Unassigned Encryption
- New Encryption Detection
- New Encrypted Client Certificate
- New Encrypted Server Certificate
- New Encryption Protocol
- New Encryption Protocol Version
- New Encryption Cipher
- New Encryption Service (network, host)
- New Encryption User
- New SSH Client
- New SSH Server
- New TLS SHA1
- New TLS Version
- Encryption on IANA reserved port
- Encryption on IANA unassigned port
- Encryption Handshake Cache
- TLS Policy –TLS 1.1 vs. 1.2 or 1.3
- Unauthorized DNS server
- Unauthorized TLS version
- Phishing Attempt Detection
- TLS self-signed certificate
- TLS certificate expired
- TLS certificate mismatch
- Malicious JA3 Fingerprint
- Malicious SHA1 Certificate
- TLS with no SNI
- TLS connections not carrying HTTPS
- TLS obsolete version
- TLS weak cipher
- TLS suspicious ESNI usage
- TLS Uncommon ALPN
- SSH/SMB obsolete protocol
- HTTP suspicious user-agent
- HTTP numeric IP host contacted
- HTTP suspicious URL
- HTTP suspicious protocol header
- HTTP Suspicious content
- Malformed packet
- Unsafe protocol used
- XSS (Cross-Site Scripting)
- SQL Injection
- Code Injection/Execution
- Binary.exe application transfer
- Known protocol on a non-standard port
- RDP on a non-standard port
- Risky ASN
- Risky Domain Name
- Desktop of File Sharing Session
- Failed/Successful RDP Login
- Connection-Status
- Unauthorized Application Use
  - DHCP
  - FTP
  - NTP
  - RDP
  - SMB
  - SMTP
  - SSH
  - TELNET
- Allowed Servers (DNS, DHCP, NTP, et al.)
- New Local Server Inference (DNS, DHCP, HTTP, HTTPS, etc.)
- IP Watchlist
- IP TTL Anomaly
- OS Fingerprinting
- Brute Force Attempt Detection (RDP/SSH/VPN)
- Brute Force – Successful Connection After Brute Force Attempt
- Device Producer /Consumer Ratio Change
- Ratio Device Connection Jitter
- Timing Histogram
- Domain Frequency
- Passive DNS Caching
- DOH Detection (DNS over TLS/ HTTPS/QUIC)
- DNS Change Detection
- DGA Domain Detection
- Suspicious DGA domain contacted
- Suspicious DNS traffic
- DNS Tunneling Detection
- Risky Domain Name
- Threat Intelligence – Domain Reputation
- Threat Intelligence – IP Reputation
- Custom Threat Intelligence (Bring Your Own List)
- LOG4J Scanning Detection
- LOG4J Request Detection
- Hands-on-keyboard (Keystroke Detection)
- Lateral Movement
- Degradation
- Data Staging
- Excess Usage
- Excess Interaction
- Data Exfiltration

Inform and Take Action

ThreatEye's SaaS offering, allows customers to always be current on software versions and leverage the latest features through automatic updates. This gives our customers' the ability to effortlessly scale their systems up or down depending on current and future needs.

ThreatEye workflows with integrated packet analysis insights are designed for analysts by analysts to drive efficiency with investigation and combat alert fatigue. ThreatEye supports response capabilities to inform and act. All data is available via Real-Time and RESTful API and integrates with key complementary technologies. Custom integrations can be tailored to meet the needs of your organization. ThreatEye powerful integrations remediate, and act based on your technology stack.

Investigate and Hunt:

- Integrated continuous packet capture with single-click pivot-to-PCAP

Available Integrations include:

- ElasticSearch
- Azure
- InfluxDB
- Splunk
- Kafka - Real-Time Streaming
- Crowdstrike
- Cisco Secure X

Response Actions include:

ThreatEye's simplifed management platform promotes incident escalation and collaboration across teams with an interactive layer. ThreatEye's integrated approach to searching, collaborating, and alerting, all in one place extends with integration to existing security tools such as SIEMs, SOARs and Threat Intel solutions seamlessly.

Deployment

ThreatEye is a SaaS offering with software and scalable hardware sensors with integrated packet capture. This packet and metadata unified approach allows for a simplified solution to be deployed on-premises, in a private or public cloud, or a mixture of both. Regardless of the deployment option, ThreatEye's software components scale to ingest network data directly from physical or virtual network taps at wire speeds up to 40Gbps.

Inquire today about ThreatEye's POC Program.

ThreatEye software is available via annual subscriptions. Support included.

About LiveAction

LiveAction provides end-to-end visibility of network and application performance from a single pane of glass. This gives enterprises confidence that the network is meeting business objectives and offers IT administrators full visibility for better decision making and reduces the overall cost of operations. By unifying and simplifying the collection, correlation and presentation of application and network data, LiveAction empowers network professionals to proactively and quickly identify, troubleshoot and resolve issues across increasingly large and complex networks. To learn more and see how LiveAction delivers unmatched network visibility, visit www.liveaction.com.

LiveAction®

960 San Antonio Rd, Suite 200, Palo Alto, CA 94303 +1 (888) 881-1116