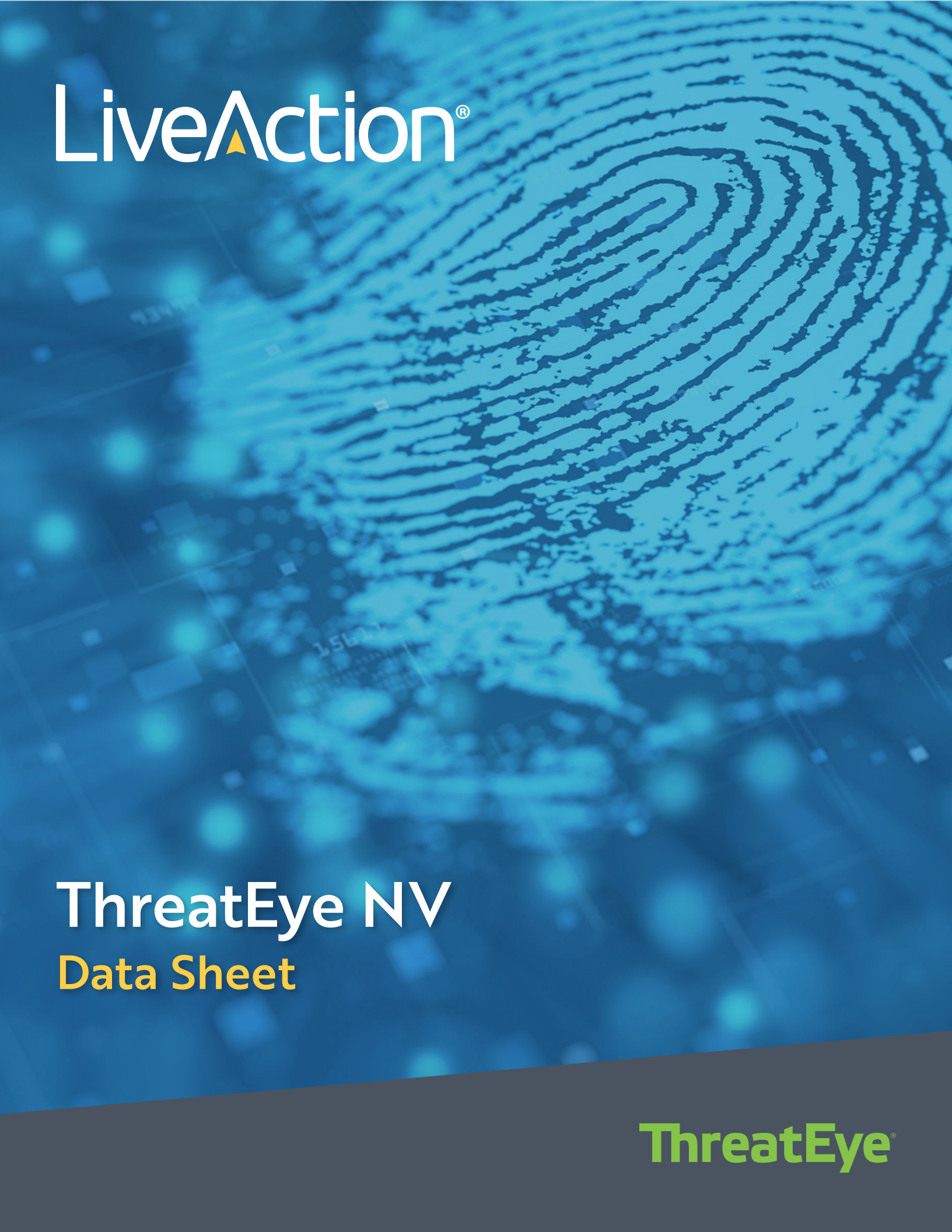

LiveAction®
ThreatEye NV
Data Sheet
ThreatEye®

LiveAction®

ThreatEye NV

Data Sheet

Introduction

Business continuity and operational resiliency are under attack and challenged at an unrelenting pace. Traditional security tools attempt to stop attacks by using deep packet inspection or rules-based monitoring on unencrypted traffic, which is no longer sufficient. In Q2 2021, **91.5% of malware arrived over** an encrypted connection. Attackers are always looking for an advantage to go undetected, hiding activity within encrypted channels to exploit a blind spot or a gap in security architecture. Maintaining visibility has grown increasingly complicated and challenges both NetOps and SecOps teams. While encrypted traffic has been standard practice to drive privacy, its strength and effectiveness has and will continue to evolve, increasing the blind-spot for threat actors to operate within. For organizations to make an immediate impact against adversaries and stay ahead of tomorrow's threats, a different security strategy is needed.

ThreatEye®

Encrypted Traffic Visibility is the Key to Security

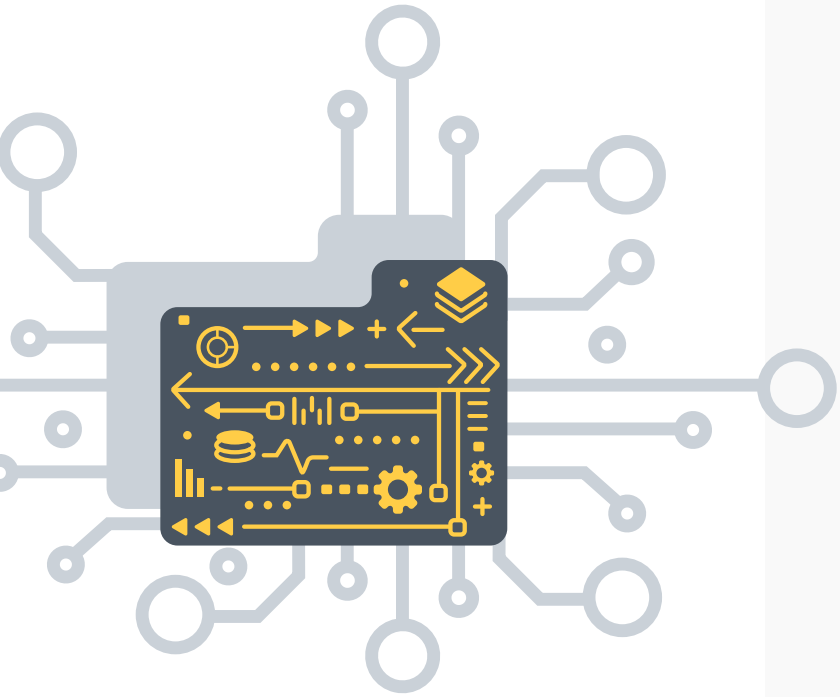
A New Approach: The ThreatEye NV network detection and response (NDR) platform is purpose-built for today's network security environment, combining next-generation data collection, advanced behavioral analysis, and streaming machine learning for threat detection and security compliance. Unfazed by encryption, ThreatEye NV combines network traffic traits and characteristics with streaming machine learning-based analysis. Unlike traffic analysis solutions built on DPI technologies, the ThreatEye platform leverages Deep Packet Dynamics (DPD) to analyze traffic flows. DPD provides high-fidelity flow records with over 150 features for each flow—all without payload inspection. Packet Dynamics, coupled with machine learning, enables unique capabilities for regaining visibility into encrypted traffic.

Key Benefits:

- **Detect Threats and Anomalies Others Miss** – ThreatEye's Deep Packet Dynamics (DPD) is agnostic to packet contents and is used to create a historical inventory of traits and behaviors for profiling and fingerprinting, a technique that works equally well with both encrypted and unencrypted traffic. Machine Learning models are applied to identify advanced behavioral threat actor anomalies.
- **Threat Detection in Real-Time** – Reduce operational outages with faster detection through industry-leading real-time detection analysis. Designed to process millions of events per second, ThreatEye NV's multi-stage analysis pipeline is fueled by analyzers – or models – engineered to analyze network traffic without multiple passes over the data stream. In addition, analyzers are explicitly architected for network security and scale via parallel processing.
- **Eliminate Encryption Blindness** – Increased adoption of encrypted network protocols is causing the erosion of network visibility for security teams. As a result, legacy tools are losing visibility. Encrypted Traffic Analysis, the application of machine learning applied to deep packet dynamics, is the perfect solution for analyzing encrypted traffic without decryption.
- **SOC Enabled** – Decrease Time to Investigate and Respond - ThreatEye NV's multi-stage analysis pipeline correlates and enriches traffic with findings detail, risk scores, and MITRE ATT&CK labeling. Using ThreatEye NV, you can respond in real-time and accelerate triage with integrated packet analysis.
- **Validate End-to-End Encryption Compliance** – ThreatEye NV 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.
- **Secure Your Entire Network** – From Core to Edge to Cloud - The ThreatEye NV solution includes lightweight, easy-to-deploy software sensors available for deployment anywhere and everywhere visibility is needed.
- **Cohesive Response** – ThreatEye NV interconnects seamlessly with existing security tools like SIEMs, SOAR, and Threat Intelligence. Workflow automations with products like Cisco SecureX can take immediate action on security events to quarantine hosts or block threats. SIEM integration can provide correlation with EDR events and malicious activity on previously unseen encrypted channels.

Metadata Enrichment

ThreatEye NV's probe 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. Additionally, 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
- DNS
- OS Fingerprint
- MITRE @TTACK – TTPs

Streaming Analysis

ThreatEye NV is powered by a streaming machine learning engine (MLE) that ingests the high-fidelity metadata generated by its software probes. ThreatEye NV's ML engine 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. Analyzers are architected for specific use cases and scale via parallel processing.

Threat Detection 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

Threat Detection Analyzers

- 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
- Suspicious DNS traffic
- 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
- Keystroke Detection
- Failed/Successful RDP Login
- DNS Tunneling Detection
- 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
- DNS suspicious traffic
- Threat Intelligence – IP Reputation
- Threat Intelligence – Domain Reputation
- Custom Threat Intelligence (Bring Your Own List)
- DNS Tunneling
- 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 NV's SaaS offering includes SOC-enabled dashboards to drive response efficiency. Dashboards are designed to support SOC analyst workflows and are fully customizable to meet any need. ThreatEye NV supports response capabilities to inform and take action. All data is available via Real-Time and RESTful API and integrating key complementary technologies. Custom integrations can be tailored to meet the needs of your organization. ThreatEye NV's powerful integrations can remediate and act based on the client's technology stack.

Investigate and Hunt:

- Integrated continuous packet capture with single-click pivot-to-PCAP SPLT (Sequence of Packet Lengths and Times)

Available Integrations include:

- ElasticSearch
- DataDog
- Azure
- InfluxDB
- Splunk
- Kafka – real-time streaming
- Crowdstrike
- Cisco Secure X
- Cortex XSOAR

Response Actions include:

- email
- webhook
- index
- logging
- slack
- pagerduty

Deployment

ThreatEye NV is a SaaS offering with software sensors deployed as containerized software applications. This containerized approach allows the solution to be deployed either on-premises, in a private or public cloud, or a mixture of both. Regardless of the deployment option, ThreatEye NV's software components scale to ingest network data directly from physical or virtual network taps at wire-speeds up to 40Gbps.

PILOT Inquire today about ThreatEye's POC Program.

PURCHASE ThreatEye software is available via annual subscriptions. Support included.

Minimum Requirements ThreatEye NV hardware recommendations are based on standard internet traffic composition per bandwidth. Therefore, the network traffic mix may affect performance.

BANDWIDTH	SPECIFICATIONS	
1 Gbps	4x Processor Cores CentOS 7 or other Docker compatible Linux OS 16GB memory	4GB storage 2x 1G network interfaces (One for management, one for monitoring)
10-20 Gbps	48x Processor Cores CentOS 7 or other Docker compatible Linux OS 64GB memory	128GB storage Recommended Intel X710 2x10G (SFP+) network interface card and 1x1G for management
40 Gbps	48x Processor Cores CentOS 7 or other Docker compatible Linux OS 96GB memory	128GB storage Napatech SmartNIC 4x10G (SFP+) network interface card, and 1x1G for management

LiveAction®

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

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 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.**