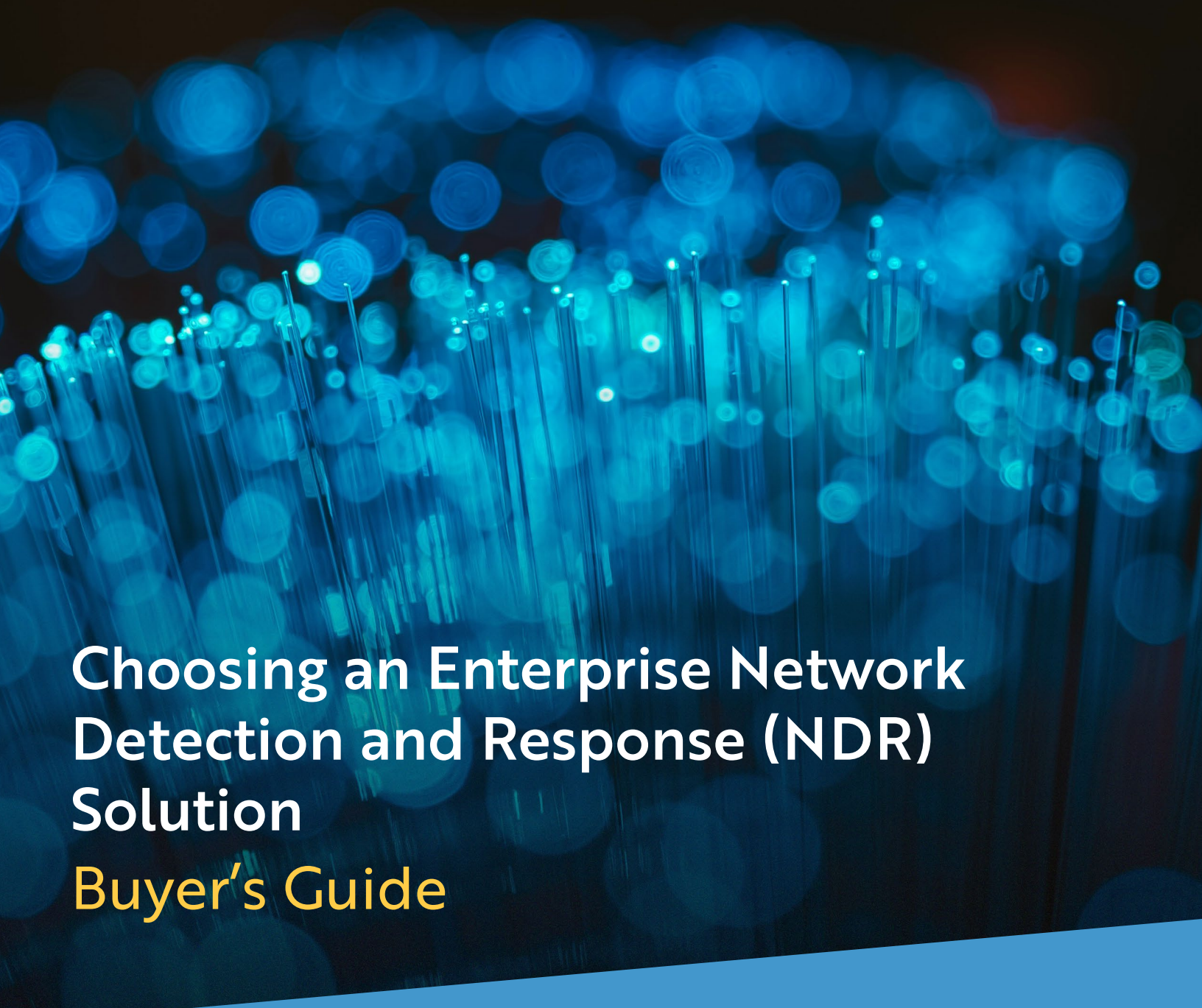
LiveAction®



Choosing an Enterprise Network Detection and Response (NDR) Solution

Buyer's Guide

Table of Contents

Five Criteria for Choosing an Enterprise Network Detection and Response (NDR) Solution

Organizations worldwide have invested billions of dollars in solutions and technologies intended to keep adversaries out of their networks. Despite increased spending by 12% year to year, attacks on organizations have increased by 40% annually, resulting in even more significant damage. Despite more cybersecurity spending to prevent network attacks, CISOs and CIOs reportedly are 58% less confident in their ability to detect and respond to cybersecurity threats in 2021 compared to 2020. Executives have a reason for concern, as the number of network attacks in Q1 2022 was up 25% compared to Q1 2021.

One of the reasons attackers continue to find their way around perimeter defenses and gain access to a targeted network is that they hide malicious activity within encrypted traffic. Unfortunately, organizations that continue to use legacy NDR solutions lack the visibility and detection capabilities to find anomalous activity in real-time encrypted network traffic. These legacy solutions may be capable of detecting known malware with signature-based detection on clear text data. However, these solutions lack the capabilities to analyze encrypted traffic and flow records in real-time, utilizing machine learning to identify normal versus anomalous behavior.

Organizations' IT and cybersecurity staff not only have their work cut out for them to prevent attacks but also must select the best cybersecurity tools for their organization. To help determine best practices for NDR solution selection criteria, Apprize360 conducted a primary research study by interviewing CISOs, CIOs, and heads of IT security from organizations with more than $250 million in annual revenue. The research study collected data to answer the following questions:

1. What strategies do enterprises deploy for NDR today?
2. What current NDR challenges are they experiencing?
3. What NDR goals are emerging for IT organizations?
4. What factors should large enterprises consider when evaluating NDR solutions?
5. Which vendors best meet large enterprises' NDR requirements?

Interviews were conducted with IT security leaders of enterprise organizations actively using one or more of six NDR solutions: LiveAction ThreatEye, Vectra Cognito Detect, ExtraHop Reveal(x), Darktrace Immune System, Corelight Zeek, and Cisco Secure Network Analytics (formerly Cisco StealthWatch).

Apprize360's research discovered that 65% of the interviewed CISO and IT security decision-makers lacked confidence in their companies' current NDR solutions to detect and prevent attacks. Only 5% expressed complete confidence.

Enterprise IT security leaders consistently reported five factors to consider when evaluating future NDR solutions. These reported criteria included the following:

1. Can the solution ingest a broad number and type of rich data sources?
2. Does the solution support modern data science and analytics?
3. Can the solution support a broad number of deep threat protection use cases?
4. Does the solution enable security operations center (SOC) to respond more rapidly and remediate threats?
5. Does the solution support a cohesive response to threats?

PART 1:

Factors to Consider When Selecting an NDR Solution

If your organization is experiencing challenges and a lack of confidence regarding NDR or is considering one of the six vendors included in the study, you may want to utilize these five factors as part of your evaluation process.

QUESTION 1

Can the solution collect a broad number and type of rich data sources?

What types of data are included and excluded from the collection? Does the solution offer metadata enrichment?

Data are a critical component of any successful NDR platform. Network activity and traffic data provide essential data that can be analyzed to identify anomalous and potentially malicious activity versus abnormal but safe activity. Unfortunately, half of the decision-makers interviewed reported that a lack of confidence in their legacy NDR platform originated from an overreliance on NetFlow ingestion. For example, according to the head of IT security at a large Midwestern food distributor service provider, the company's legacy solution has limited visibility and detection of modern attacks because of its overreliance on NetFlow data alone.

Our CIO knows my position. It isn't "if" but "when" an attack is going to happen. Because we haven't been able to secure the budget for a more modern NDR solution, we're using an older platform that primarily analyzes NetFlow data. This has significant limitations because the solution only has visibility of port and IP addresses but can't identify threats embedded within encrypted network traffic.

The interviewed decision-makers acknowledge the importance of collecting a broad amount of network data. Interviewees reported that data collection was critical for a solution to offer visibility and support for accurate and timely threat detection elements. Decision makers indicated that the breadth and depth of data was an essential foundational evaluation factor they would consider when assessing future solutions. Decision makers specifically highlighted the following factors in their assessment of data ingestion capabilities:

- **Ability to collect and inspect deep data packets:** This includes the ability to collect packet data contents, traits, and behaviors.
- **Ingestion of metadata:** Ingestion of metadata from network flow, data packets, device activities, fault information, and alerts.
- **Enrichment of collected metadata:** The ability to enrich metadata with information to help with rapid anomaly and malicious threat detection.
- **Network flow data collection:** The ability to collect network flow data with other important network data sources.
- **Network traffic:** The ingestion of complete network traffic, including network logs, net flow, alerts from other systems, intrusion detection, or other data subsets.
- **User Behavior:** User entity and behavior analysis.

QUESTION 2

Does the solution include modern data science and analytics?

Does the vendor's platform leverage machine learning to correlate data collected across the network to identify threats and prevent malicious activity?

The interviewed decision-makers reported that it was critical to separate data collection from analysis to highlight the importance of the two factors. Decision makers acknowledge that an NDR platform should support deep data science and analytics capabilities to analyze the collected network data. IT security decision-makers made it clear that accuracy was pivotal in identifying legitimate threats to reduce noise and false positives. According to a CISO from a mid-sized financial services software company:

> *NDR solutions promote their machine-learning capabilities, but you have to look carefully into how their machine learning contributes to accurate threat identification within the network. It does no good to create dozens of alerts a day that are false positives, which creates extra work for the security team and negatively impacts the user experience. That's why I'm looking for NDR solutions with machine learning that can correlate activity across network devices, user behavior, and applications and automate this analysis accurately with a low percentage of false positives.*

According to the interviewed decision-makers, part of the evaluation process for this select factor is to determine machine learning capacities for the following:

- Anomaly detection capabilities
- Signature and non-signature-based techniques
- Data normalization
- Device profiling
- DNS analysis

QUESTION 3

Can the solution support a broad number of deep threat protection use cases?

Does the NDR solution support encrypted traffic analysis? Does the NDR solution provide long-term user behavioral analysis? How many specific threat protection use cases does the NDR solution support?

NDR solutions that support multiple, specific-use threat use cases enable security teams to improve the speed and accuracy of threat detection and prevent adversaries from executing successful disruptive and damaging cyberattacks. IT security decision-makers reported the top 10 critical threat detection use cases that should be supported:

- Encrypted traffic analysis (ETA)/encryption blindness
- User behavior analysis
- Incident and network forensics
- Threat hunting
- Financial fraud detection (including ransomware)
- Zero trust
- Detect known attacker tactics, techniques, and procedures (TTPs)
- Retrospective detection
- Advanced persistent threats (APTs)
- Lateral movement

The interviewed decision makers highlighted the importance of NDR solutions supporting ETA. The increased adoption of encryption in network traffic creates challenges by preventing network visibility for security teams. Encrypted protocols used to protect user privacy have the unintended side effect of providing cover for malicious actors. ETA can restore lost visibility while protecting user privacy by combining traditional traffic analysis with deep packet dynamics, cryptoanalysis, and machine learning. This combination can provide additional insights into network traffic and regain the edge of network defenders. According to a director of cybersecurity at a consumer financial payments mobile application:

> *I'm finding that our NDR solution doesn't support ETA, and we're missing advanced threats hidden within encrypted traffic. One command-and-control malware threat was hidden within encryption for seven days before it became executable, allowing complete access to our payments database. It was by luck that we caught it. Right now, we're looking for new vendors that can support next-gen firewall protection and NDR solutions with deep ETA.*

QUESTION 4

Does the solution enable security operations centers (SOC) to respond to and remediate threats more rapidly?

Does the solution support a scalable incident response workflow so SOC analysts can prioritize multiple simultaneous threats?

Decision makers told Apprize360 that accurate detection and alerts are a critical part of a modern NDR solution. However, solutions must also support the organization's SOC to prioritize multiple threats and reduce remediation time. Interviewed decision makers highlighted wanting an NDR platform with native workflow and triage capabilities to meet the complex needs of an IT security organization. For example, according to a CISO from a large B2B marketing software company:

> *Our IT team has only a few dedicated cybersecurity analysts, so it's critical that they work together intelligently and collaboratively. In addition, they need a platform that can help them prioritize threats and provide guidance on how to remediate specific threats.*

Other requirements reported by decision-makers as essential included the following:

- Intelligent alerts and notifications to inform SOC specialists or on-call technicians.
- Workflow to support triage and response and collaboration on packet analysis.
- Dashboards and insights to support the prioritization of MITRE ATT&CK labeling, risk scores, and incident details for faster responses.

QUESTION 5

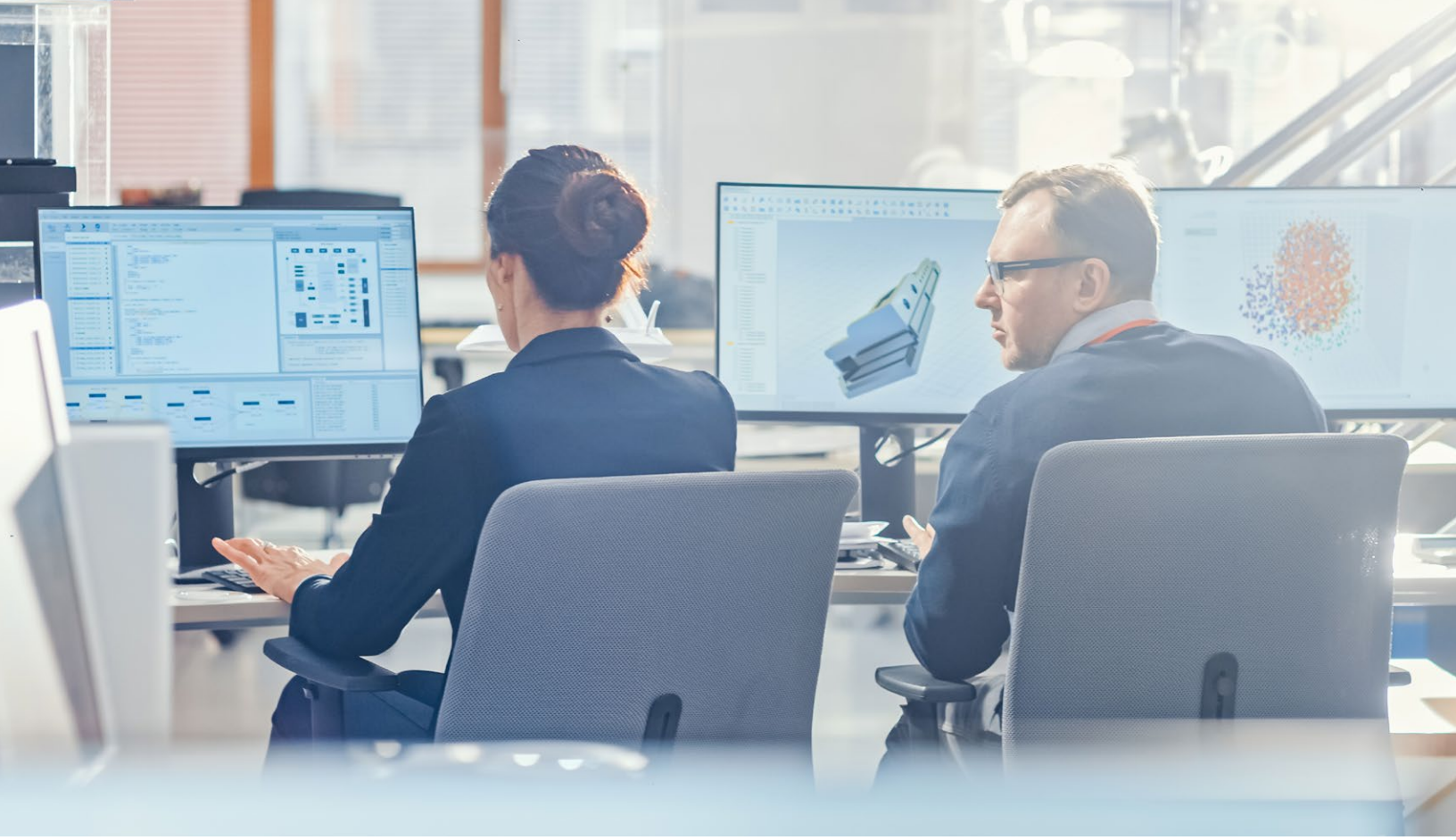
Does the solution support a cohesive response to threats?

Does the solution seamlessly integrate with existing security tools like SIEM, SOAR, and Threat Intelligence? Can the solution integrate and work with network performance management (NPM) solutions?

Organizations evaluating NDR solutions should ensure that the solution interconnects seamlessly with existing security tools, such as SIEMs, SOAR, and Threat Intelligence. Workflow automation should be able to integrate with products that can take immediate action on security events to quarantine hosts or block threats. SIEM integration can correlate with EDR events and malicious activity on previously unseen encrypted channels. In addition, native integration with an NPM solution can support a more integrated approach to NDR with NPM.

A head of IT security told Apprize360 that the quality and breadth of integrations are important to avoid creating more disparate security solutions.

> *The last thing we need is another tool that collects data and works separately from any detection system. NDR systems should work as a puzzle with other solutions, whether an EDR, SIEM, or malware solution. I firmly believe that a best practice is that NDR systems should work hand in hand with NPM solutions for access to network data and to respond more quickly to remediation tasks.*



PART 2:

NDR Vendor Considerations

The second part of the study focused on evaluating specific NDR vendors. Apprize360 asked IT security decision makers about their existing NDR solutions' perceived strengths and weaknesses and how they plan to assess future vendors. Apprize360 also asked interviewees to rank their deployed solutions among the five selection factors to analyze how their deployed solutions were measured against their selection factors.

QUESTION 1

Can the solution collect a broad number and type of rich data sources?

LiveAction's ThreatEye solution was ranked as one of the highest solutions for this selection factor due to the depth and breadth of the data collection. ThreatEye buyers reported that the solution provides detailed visibility and insights because of the solution's ability to capture 100% of all generated packets with other critical data, including the following:

- High-fidelity data (HF flow data packet dynamics)
- Network flow data collection and network traffic
- User entity and behavior analysis
- Other device and application property data

One ThreatEye customer, a director of information security for a financial services company, spoke about the company's behavior analysis capabilities as an advantage:

> *I am excited about ThreatEye's new behavior analysis capabilities because it collects all behavior data for analysis to identify changes in the baseline and identify baseline anomalies. Data is the foundation of strong security. Without the ability to ingest data from multiple sources, you're blind to threats. Behavior data capabilities are a major step ahead and an advantage.*

Another advantage that decision-makers highlighted was ThreatEye's metadata enrichment capabilities. ThreatEye collects rich metadata of more than 150 packet dynamic features and enriches that data with over 25 enrichment attributes, such as per flow metrics, TCP metrics, behavioral metrics, MITRE ATT@CK – TTPs, and OS fingerprints.

QUESTION 2

Does the solution support modern data science and analytics?

Many NDR and cybersecurity vendors promote their machine learning capabilities but struggle to highlight the concrete advantages of their algorithms. Simultaneously, machine learning is often applied to platforms to learn what "normal" looks like and then alert users about events that are "different" from the analyzed "normal" baseline. Unfortunately, this strategy confuses "different" with "threat" and allows experienced hackers to create complex attacks to evade detection. This results in missed critical threats and a great deal of irrelevant noise.

Interviewed decision makers who were ThreatEye customers reported two main advantages of ThreatEye's machine learning capabilities: streaming machine learning analytics and deep packet dynamics.

- **Streaming machine learning:** Users of ThreatEye highlighted the platform's "streaming machine learning engine" as an advantage. The streaming machine learning engine ingests high-fidelity metadata generated by software probes. The streaming machine learning is fueled by "analyzers," purpose-built to analyze network traffic without multiple passes over the data stream. Threat analyzers are built to support over 100 security and visibility use cases, such as unexpected encryption, new encryption protocol, domain reputation, lateral movement, and TLS self-signed certificates.

- **Deep Packet Dynamics (DPD):** ThreatEye's Deep Packet Dynamics (DPD) is agnostic to packet content and is used to create a historical inventory of traits and behaviors for profiling and fingerprinting both encrypted and unencrypted traffic. DPD technology analyzes high-fidelity flow records, analyzing more than 150 packet traits and behaviors across multi-vendor, multi-domain, and multi-cloud network environments. This helps accelerate real-time threat detection, eliminates encryption blindness, validates encryption compliance, and allows teams to secure better the entire network and coordinate responses with other security tools such as SIEM and SOAR.

QUESTION 3

Can the solution support a broad number of deep threat protection use cases?

An effective NDR platform must detect and respond to hundreds of threats. The interviewed decision makers acknowledge that ETA is a growing challenge that security teams face. According to a director of information security from a financial services platform:

> *We call it "eliminate encryption," where we can't see into the encrypted data streams to support user privacy. The downside is that attackers can hide their malicious payloads within encrypted traffic, avoiding detection. We evaluated a few players promoting ETA capabilities, but those solutions didn't have advanced capabilities. These solutions use simplistic network traffic analysis and certificates to match signatures, which modern attackers easily defeat. We selected ThreatEye in part because of its advanced ETA capabilities, leveraging the platform's advanced machine learning that analyzes deep packet dynamics to identify complex bad actors.*

ThreatEye also supports hundreds of threat-use cases, including:

- → Encrypted traffic analysis/encryption blindness
- → Incident and network forensics
- → Threat hunting
- → Financial fraud detection
- → Financial latency measurement
- → Policy management

QUESTION 4

Does the solution enable security operations centers (SOC) to respond to and remediate threats more rapidly?

Companies need not only a robust detection and response solution but also one that can support the SOC team, create scale, and promote collaboration. Decision makers highlight ThreatEye's workflow capabilities supporting a multi-stage analysis pipeline that correlates and enriches traffic with threat and incident details, risk scores, and MITRE ATT&CK labeling. According to the director of information security for a financial services platform:

> *ThreatEye's dashboards are designed to support SOC analyst workflows with integrated packet analysis insights. Our analysts can tag captured files and collaborate across the team with this interactive layer. I love the integrated approach to searching, collaborating, and alerting in one place.*

Other reported advantages of ThreatEye's SOC support include the following:

- → Workflow to support triage and response and collaboration on packet analysis
- → Integrated continuous packet capture with single-click pivot-to-PCAP
- → Integrations with third-party vendors for remediation and automation of workflows
- → Configurable response actions, such as email, webhook, logging, Slack, and PagerDuty

QUESTION 5

Does the solution support a cohesive response to threats?

Another factor that elevated ThreatEye's ranking among the platform's customers was its supported integration capabilities. ThreatEye interconnects seamlessly with existing security tools, including many SIEMs, SOAR, and Threat Intelligence. ThreatEye also supports integrated workflow automation with products such as Cisco SecureX, so analysts can take immediate action on security events to quarantine hosts or block threats.

Another factor that ranked ThreatEye positively was the integration with LiveAction's NPM solution.

> *I'm a firm believer that disparate IT management tools create holes of visibility in your network performance. We're moving to what I think is the best practice of treating network management as a single strategy, integrating NPM and NDR together. This is where I believe ThreatEye and LiveAction have an advantage. They're both best-of-breed tools for NDR and NPM, respectively. But together, it will allow us a combined performance and security management strategy that will enable us to address threats quickly while enabling the high performance of our network.*

The final category of the study included quantitative vendor assessment. Apprize360 asked interviewees to rank their currently deployed solutions using a 5-point measurement scale to determine the strengths and weaknesses of their deployed NDR solution. The following table provides a comparative assessment of vendor-specific capabilities based on interviews with decision makers using one or more sized studied solutions.

CATEGORIES OF ASSESSMENT	LIVEACTION ThreatEye NV	VECTRA Cognito Detect	EXTRAHOP Reveal(x) 360	CORELIGHT Zeek	CISCO Secure Network Analytics	DARKTRACE Darktrace
Broad, Rich Data Sources						
Rich Number of Data Sources • Network flow and Traffic data • Deep data packets • Metadata • User behavior	●	◕	◕	◑	◑	◑
Enrichment of Metadata • Metadata enrichment	●	◕	◕	◔	◔	◑
Complete Packet Capture • 100% packet capture	●	◕	◕	◔	◔	◕
Data Science and Analytics						
Advanced Anomaly Detection & Correlation • Machine learning algorithms to identify anomalous behavior from raw data	●	◕	◕	◑	◕	◑
Deep Packet Dynamics (DPD) • Creation of a historical inventory of traits and behaviors for profiling, fingerprinting, and advanced behavioral analysis	●	○	○	○	○	○
Streaming Analytics • Ingestion of high-fidelity metadata analyzed for specific use cases	●	◑	◑	○	○	○
Deep Threat Protection Use Cases						
Encrypted Traffic Analytics (ETA) • Monitors network packet metadata to detect malicious traffic	●	◕	●	◑	◑	○
Support for advanced threat use cases, such as: • User behavior analysis • Incident and network forensics • Threat hunting • Retrospective detection	◕	◕	●	◑	◑	◑
Enable Security Operations Centers (SOC)						
Alerts & Notifications • Intelligent alerts and notifications to inform SOC specialists or on-call technicians	◑	◕	◕	◑	◕	◕
Workflow & Collaboration • Workflow to support triage and response and collaboration on packet analysis • Dashboards and insights to support prioritization	◕	◕	◕	◔	◑	◑
Application & Asset Detection • Automated detection of unauthorized applications and assets	◔	●	●	◕	◕	◔
Cohesive Response						
Integration With Security Platforms • Integrations with third-party SIEM, SORE, and threat intelligence platforms	◕	◕	◕	◕	◕	◑
Native Integrations With NPM • Ability to integrate natively with NPM solution	●	◔	◕	◕	◔	◔

LEGEND ● Full Present (100%) ◕ Partial Functionality (~75%) ◑ Half Functionality (~50%) ◔ Minor Functionality (~25%) ○ Fully Absent (0%)

Note: This assessment was based on interviews with current customers of each solution and was not a statistically significant quantitative study. The opinions, vendor rankings, and reported solution strengths and weaknesses can change without notice based on newly released vendor features, improved functionality, and changing customer perceptions.

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.

LiveAction®

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