opentext™

POSITION PAPER

What to look for in a Network Detection and Response platform

opentext™

Contents

opentext™

Executive summary

From a technology perspective, particularly cyber security, many of the themes that developed in 2020 will have a permanent place in the way we manage and deploy network infrastructure. The mass migration to remote work, the dramatic increase in ransomware and other pressures are driving the need for innovation in already resource-constrained security organizations.

During this global uncertainty, technology sectors like Network Detection and Response (NDR) not only weathered the storm but demonstrated unprecedented growth.

Why? While the landscape may have changed, the requirements on networks and their connectivity remain critically important. Now more than ever, Security Operations need context to understand alerts or investigations quickly and efficiently.

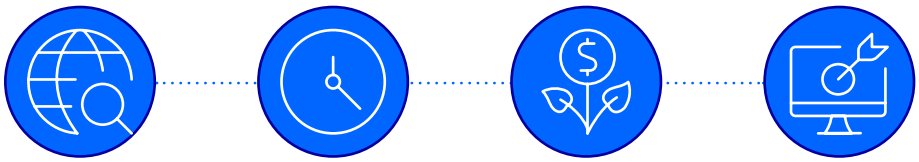
An NDR solution is a must have, but selecting the right tool can be a challenge, given the number of vendors and the goals and limitations of your environment. This guide provides insight into how to simplify the search and target the right features and functions.

opentext™

The challenge

While NDR is seeing high demand, it has become a saturated market with many vendors and approaches. When you compound all these choices with your own internal struggles (resources, time, return on investment, skills) the biggest challenge is determining which tool to evaluate before a purchasing decision is made.

Adding to the challenge, NDR is still in its infancy and trends are still developing, in particular, the balance between whether vendors' solutions provide more of a hands-on or hands-off approach.



"Hands-on" vs "hands-off" approaches

The market is already seeing some large divides around two areas: detection and visibility. While all offerings must deliver both capabilities to be classified as NDR, each solution's approach is defined by which of these principles it is founded upon.

The hands-off approach is founded on detection. Tools of this kind are most often machine learning (ML) based. The data's primary role is to train a model over time, and the machine then prioritizes what is retained and reported against. To date, this approach is by far the most popular, as it can often provide critical insight into your environment and act as a substitute for the analyst you are struggling to find or support. If your organization has a small security operation and the team is wearing multiple hats at once, this approach is a strong alternative to the common route of outsourcing to a managed security services provider (MSSP).

In stark contrast, the hands-on approach most often is founded on visibility first, with access to information empowering existing security teams, processes or procedures. Organizations with well-defined security operations (e.g., teams for security operations center, threat, incident, hunting) are craving more data to eliminate network blind spots and correlate the network with other critically important data sets, such as endpoint or device logs. Their goal is not only to respond to incidents but to proactively hunt for threats. Machine learning can still be found in the hands-on approach, however, all data and multiple detection techniques are often used to empower the security operation overall.

When asked about the importance of NDR for his cyber threat and incident response practice, Jeremy Conway from MAD Security said, "We're offering our clients greater protection against cyber threats and helping them respond to attacks faster."[1]

1 OpenText, MAD Security protects sensitive government data against advanced cyber threats. (2022)

The solution

True NDR is the perfect balance between threat detection and network context. When combined, these capabilities allow human analysts, machines or processes (e.g., SOAR platform) to quickly and effectively identify or respond to threats discovered on the wire. NDR is the natural replacement for NIDS (Network Intrusion Detection Systems), which relied heavily on known indicators (or signatures) to be effective and provided little to no context. NIDS were often referred to as "barking dogs" or "alert cannons," with each system generating thousands of alerts that overwhelmed even the largest, most proficient security operation.

While false positives will never be removed entirely, today's NDR platforms help the user prioritize, tune and respond to threats found traversing the network. Many platforms offer multiple detection techniques and user workflows to support incident response, event triage or even proactive threat hunting.

What to look for

NDR has a lot to offer, but it will also ask a lot of your organization, infrastructure, skills, applications and systems. This section will cover the key aspects to consider when reviewing NDR platforms for potential use within your environment.

1. **Network visibility:** Empower your security organization or replace them?
2. **Detection:** Is it all about behavior or should I look for more?
3. **Storage and retention:** Here today, gone tomorrow?
4. **Simplicity of deployment:** Eliminating blind spots
5. **Costs:** Understanding TCO
6. **Dipping your toe in the water:** Early-stage testing

1) Network visibility: Empower your security organization or replace them?

Not all NDR solutions capture raw network packets. Some only look at summary data, like NetFlow, that uses a set of defined statistics generated by the switch or router to provide a high-level summary of traffic profiles/activity. Other systems will briefly inspect and classify traffic flows to assist with the training of unsupervised machine learning models, but then discard information that is not important to the data science process. The result is behavioral based detections.

A growing portion of the NDR market is focused on supporting the analyst and not replacing them. An NDR solution will generate meaningful metadata (and even record the raw packets themselves) on every connection or flow regardless of any initial detection or behavior being flagged for analysis. By providing this level of visibility and not restricting access to the data for an algorithm or detection process, many security organizations can quickly empower staff across the organization with access to live and historical visibility from the network.

opentext™

2) Detection: Is it all about behavior or should I look for more?

Networks can be used to generate a wide variety of alerts, from the most commonly 'known' indicators (such as network signatures) to behavioral analytics capabilities that look for outliers crossing thresholds (or baselines) resulting in alarm bells ringing. Regardless of the technique, you should ask yourself, "what am I looking to achieve?"

For some, having any form of "eyes-on" may be the right solution since something is better than nothing and they have limited resources, skills or capital to work with. In this case, solutions specifically designed to replace the analyst and limit interaction and visibility into the underlying data are most likely the right approach.

Those with more established security operations (most likely a defined security team) where investments have already been made in people and processes are more likely to look beyond one layer of detection (e.g., automated behavioral analysis) and focus on empowerment of the analysts and systems in place. That means leveraging tried and trusted known indicators that get updated frequently every day, along with other advanced techniques, such as advanced malware detection (which requires the NDR platform to extract and analyze files) and behavior or pattern-based detection capabilities all in the same sensing platform. Any detection should be directly linked to underlying network metadata and allow the operator to quickly pivot to broader network history that may not link directly to any specific event.

3) Storage and retention: Here today gone tomorrow?

A key aspect of detection and response, either at the endpoint or the network, is access to live and historical information to provide insight into an investigation. Such data can answer questions like: "who else did this host connect with?" or "did I see this type of traffic or file content hours, days, weeks ago before I knew of the threat?" Today, only a fraction of NDR providers deliver storage or retention of PCAP (raw packets), alerts or network metadata. This forces the end-user to invest in their own data-lake or develop an integration into other solutions, such as a security information and event management (SIEM).

Retaining information on network transactions has always been one of the hardest challenges to solve, given the voluminous amounts of data quickly generated from even the most modest network speeds. For example, 1Gbps of network traffic can easily generate half a Terabyte (500GB) of metadata in a 24-hour period. When you consider many security teams are looking for weeks or even months of historical data, this results in data repositories growing out of control.

When considering this aspect of your NDR solution ask yourself:

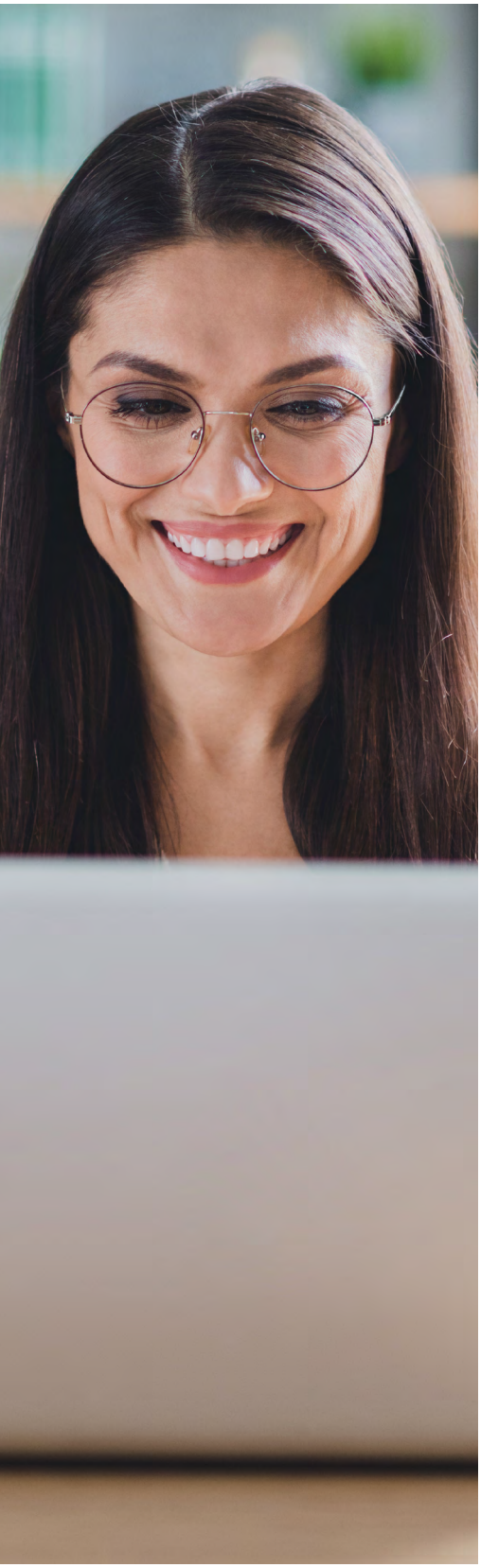
→ How important is network visibility and history for my security processes?

→ Does the solution offer onboard metadata, file or even PCAP retention or do I need to build my own data facility?

→ Is my only option a SIEM? If so, how easy is it to integrate?

→ How flexible is the solution, can it be customized to limit what is retained/exported?

For many organizations, network metadata (or PCAP) retention is a must. Without access to the ground truth, it is almost impossible to quickly and effectively investigate alerts generated by the NDR platform.



4) Simplicity of deployment: Eliminating blind spots

When you consider the deployment aspect, always verify if your NDR solution is suitable for your environment (either SMB or Enterprise). Does your NDR solution support on-premises (air-gapped) environments where no data leaves the client's environment, or can it be deployed in the cloud? It's important to note whether or not your NDR solution also permits its management console and sensors to be easily deployed in a private cloud environment. This provides security analysts with anywhere, anytime access for administering sensors and defending against threats across on-premises and cloud environments.

An NDR solution that is available both on-premises and in the cloud offers flexibility to enterprises migrating to the cloud or managing hybrid environments. Although it might sound strange, not all NDR providers have developed solutions that work with the native capabilities of the public cloud providers. This forces you to invest in additional tools to gain access to traffic flows.

Is the NDR solution software based or a black box? Black-box solutions increase the cost of the overall deployment and force YAD (yet another device) into already complex data center environments. Look for solutions that can operate at scale within your environment, using virtualization, or with your trusted server OEM (e.g., Dell, CISCO or HPE) to remove the burden of YAD or the complexity involved in replacing failed components. Not all solutions require black boxes or require complex per device pricing structures. Gaining total coverage can be a lot easier than you first thought.

5) Costs: Understanding TCO

Today, most NDR systems are sold under a subscription. In general, this is a positive change as subscription plans typically include upgrades for software, support and maintenance and in some cases hardware as well. Be sure to inquire about how these individual aspects are covered by the subscription you're considering.

Subscription plans can vary based on the charging metric being used. The variance in approach to pricing is a major focus area for many organizations, particularly those with defined selection teams (or committees). One of the most common approaches is appliance-based pricing, which can often penalize the end-user by generating unnecessary expense and limiting the scale/size—and ultimately effectiveness—of the deployment itself. A vendor may sell you a hardware appliance rated for a particular interface type (e.g., 10Gb/E) where the price is based upon consumption of the entire line speed (e.g., 10Gbps) when you may only use a third (⅓) of the link's capacity. That's more than 6Gbps paid for but never used.

A growing number of NDR vendors use COTs (commercial off the shelf) solutions, allowing the user to build out their own hardware at standard system costs while purchasing a subscription plan that matches their exact network monitoring throughputs. This approach provides a predictable, scalable and future-proof way of investing in a new detection solution.

When you discuss pricing with your chosen vendor, dig into their price book and explore how many charging vectors are leveraged for a deployment, large or small. Often the simplest models will be a major gating factor in any final investment decision.

opentext™

6) Early-stage testing: Dipping your toe in the water

Time and resources are critical factors, particularly as you try to prove out solutions.

Should you expect the same age-old demonstration and evaluation process when you engage with the vendor(s) you select? Engaging in lengthy demonstrations, arduous legal exchanges and shipping terms before even looking at virtual or physical resources to host the technology. Then there are the complexities of getting access to the network traffic (e.g., datacenter), even connecting to the traffic itself (e.g., tabs, spans) and the time some tools need to train their AI/ML models.

The proving ground doesn't have to be hard… a handful of vendors offer hands on access to an environment that is free of all of these challenges and allows security operations to evaluate visibility, detection, threat hunting, integration, speed and overall efficiencies in a web browser without paperwork or software downloads.

Competitive comparison

Ask your down-selected vendors for product comparisons. Every vendor should have one, and you will be surprised to find that most follow a very similar format, making correlation easy.

Doing this provides two key benefits:

1. It will highlight the key feature/ functions that each vendor believes uniquely differentiate themselves.
2. As the NDR market is increasingly crowded, it is not possible to create an easy visual comparison against all participants. Asking for the comparison, without stating who you are looking at, will let you see who that vendor views as their major competition. You'll also be able to identify their "hands-on" or "hands-off" approach to the problem.

opentext™

Comparative Matrix			OpenText NDR
Network Data Capture & Retention		Full Network Recording (First In First Out – FIFO)	X
		Smart PCAP recording (alert based retained for long periods)	X
		Network metadata long term retention (Data Nodes)	X
		High speed (low-cost) sensor option 18Gbps+ in single appliance	X
Full Spectrum Threat Detection	Keep Out	Package inspection	X
		Advanced Malware detection (static – ML based)	X
		Advanced Malware detection (dynamic – sandbox)	X
		Network signature (e.g. TALOS, ET Pro)	X
	Find Within	Indicator of Compromise (e.g. IP, URL or Hash)	X
		Pattern based anomaly detection (behaviour)	X
		Threat hunting workflows (non-alert driven) in product not via SIEM	X
Threat Prevention		Intrusion prevention (inline) option	X
		Customizable signatures and scripts (bring, build or modify)	X
		Automated tagging & tuning of alerts (assignment, prioritization, severity)	X
		Multi-Tennant Data Federation (single pain of glass)	X
		Cloud based management & data retention options (not sensor)	X
		Customizable export options (Syslog, ECS, Netflow/IPFIX, JSON)	X
Deployment		Consumption based pricing (pay for what you use)	X
		Cloud protection option (Google, Amazon, Microsoft)	X
		Software only solution option – bring your own hardware (at any speed)	X

OpenText™ Network Detection & Response advantages

End-to-end visibility and meaningful visualization

See high-fidelity metadata to know in real time how users, devices, systems and applications are behaving on the network.

Advanced 360 detection and powerful analytics

Gain visibility into the known, unknown and pattern of unknown unknowns on your network with multiple threat detection engines, all while virtually eliminating false positives.

Effective response and simple network instrumentation

Respond to and correlate alerts in real time with frictionless integrations to SIEM/SOC workflows and third-party threat intelligence tools. Deploy smart sensors in just a few clicks and easily instrument your network.

opentext™

Security
OpenText Blogs

Threat Detection and Response
OpenText Solutions

Advanced forensics and threat hunting

Investigate and validate a threat with OpenText NDR's smart PCAP providing enough data to accurately follow the kill-chain. Follow a hypothesis to uncover an unknown threat or gain insight into normal operations.

Why OpenText NDR?

OpenText Network Detection & Response (formerly Bricata) is a "hands-on" network detection and response platform. It's the only NDR platform that allows security teams and the entire enterprise to collaborate better, reduce security risk and solve network problems faster than ever before. By fusing realtime visibility, advanced detection, analysis, forensics, incident response and threat hunting into a single platform, OpenText provides organizations with the most effective tools to find, understand and act on relevant threats.

OpenText NDR bridges the gap between "alert cannon" and "black box" network security solutions, offering signature inspection, stateful anomaly detection and machine learning-powered malware conviction in one place. It does not replace human analysts, it gives people the power to do what people do best: think, evaluate, discover and decide.

What customers appreciate

"It's a truly reliable solution that brings the best of available network forensic, inspection and data visualization technology into one well-orchestrated solution."
– Fortune 500 CISO

- Consumption-based pricing: only pay for what you need
- Seamless integration with other security tools and processes
- Smart PCAP, for forensics and remediation
- Robust threat hunting and forensic analytic capability
- Easy to implement, immediate impact and easy to tune
- Hardware agnostic and software-based

With OpenText Network Detection & Response, you have the right data, at the right time, to get the right answer.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact