BRICATA®

EBOOK

What to Look For in a **Network Detection and Response** Platform

BRICATA.COM | INFO@BRICATA.COM

Introduction

For many of us, 2020 was a year we would like to forget. But from a technology perspective, particularly cyber security, many of the themes that developed will have a permanent place in the way we manage and deploy network infrastructure. Moving forward from the mass migration to remote work, to the dramatic increase in ransomware, or pressures to adopt new cloud based strategies, all organizations will continue to stretch an already resource-constrained security organization into 2021 and beyond.

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

Why is that?

It's all linked to context and visibility. While the landscape may have changed, the requirements on networks and their connectivity remains critically important. Now more than ever, Security Operations need context to understand alerts or investigations quickly and efficiently – and that is the role of an NDR Solution.

An NDR solution is a must-have, but selecting the right tool can be a challenge given the number of vendors and the specific goals or limitations of your environment. This eBook was created to provide some insight into how to simplify the search and target the right features and functions for your business.

The Challenge

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

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

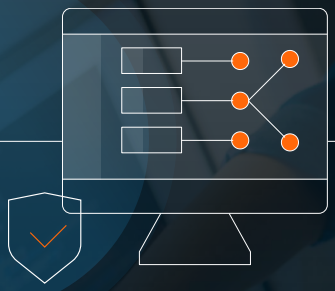
"Hands-on" vs "Hands-off" Approach

The market is already seeing some large divides around two areas: Detection and Visibility. While all offerings deliver both capabilities in order to be classified as NDR, the 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 where 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, as access to information can empower existing security teams, processes or procedures. Organizations with well defined security operations (e.g., teams for SOC, Threat, Incident, Hunting) are craving more data, to eliminate network blinds spots and correlate the network with other critically important data sets such as , endpoint or device logs, etc. Their goal is not only to respond to incidents but to proactively hunt for threats. ML 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.

Recently, Vito Rallo from PWC said "When you don't have network visibility, you are missing a large amount of important security and operational information" when asked about the importance of NDR for his Cyber Threat and Incident Response practice.



The Solution

So, what is NDR? A simple way to describe the capability 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 to NIDS (Network Intrusion Detection Systems) that 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.

BRICATA

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. So what are the best things to consider when reviewing NDR platforms for potential use within your environment? In this section, we will cover the key aspects to consider, starting, as you might expect, with access to information or "network visibility."

1

Network Visibility: Empower your security organization or replace them?

Not all NDR solutions capture raw network packets, some only look at summary data, an example of this would be NetFlow, a set of defined statistics generated by the switch or router providing 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 discard information that is not important to the data science process, the end result is behavioral based detections being generated.

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 every element of the operation with access to live and historical visibility from the network… remembering that the network often holds the ground truth.

What to Look For

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 today you have limited resources, skills or capital to work with. But something is better than nothing. In this case, solutions that are specifically designed to replace the analyst, limit interaction and visibility into the underlying data itself are most likely the right approach.

For those with more established security operations (most likely a defined security team) where investments have already been made in people and processes you 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. In addition (as already highlighted), any detection should be directly linked to the underlying network metadata – not just pertinent to the alert itself – but allow the operator to quickly pivot to broader network history that may not link directly to any specific event.

What to Look For

3

Storage and Retention: here today gone tomorrow?

A key aspect of detection and response, regardless if it's at the endpoint or the network, is access to live and historical information to provide insight into an investigation, often resulting in questions of "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, 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 SIEM.

Retaining information on network transactions has always been one of the hardest challenges to solve given the voluminous amounts of data you can quickly generate from even the most modest networks speeds. As an example, 1Gbps of network traffic can easily generate ½ 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. So, when considering this aspect of your NDR solution ask yourself:

- → How important is network visibility and history for my security processes?
- → Does the solution I'm looking at 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.

What to Look For

4

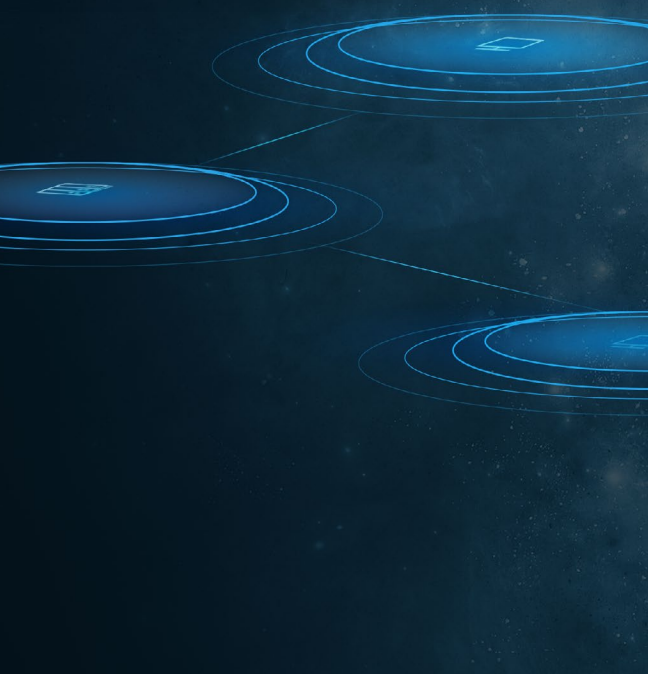
Simplicity of Deployment: Eliminating Blind Spots

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-prem (air-gapped) environments where no data leaves the client's environment, or can it be deployed in the cloud? 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 your 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.

If visibility is a key aspect, ask yourself, "does the solution I'm evaluating truly help me eradicate network blindspots?" Even the most sophisticated security operations making the largest investment in cybersecurity often complain about blind-spots where complexity, cost, or a combination of both force sacrifices on where you instrument the network. Remember, 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.

What to Look For



5

Costs: Understanding TCO

Today, most NDR systems are sold under a subscription. In general, this is a positive change in the overall marketplace, as subscription plans typically include upgrades for software, support and maintenance and in some cases hardware as well. You should inquire on these individual aspects as these can potentially add to the overall cost.

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. As an example; A vendor is likely to 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) however, you may only use a third (⅓) of the links capacity. More than 6Gbps is then paid for but never used.

A growing number of NDR vendors today 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 (pay for what you need). This approach provides a predictable, scalable and future-proof way of investing in a new detection solution such as NDR. 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 (pricebook on a page) will be a major gating factor in any final investment decision.

What to Look For

6

Dipping your toe in the water: Early stage testing

So, you're making progress, the decision to instrument your network has been made and the process to identify and select a technology begins. There is much to be excited about, but one thing hasn't changed: 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, shipping terms and that's before we look at virtual or physical resources to host the technology…

Not to mention the complexities of getting access to the network traffic (e.g., datacenter) or even connecting to the traffic itself (e.g., tabs, spans) or 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 pain free of all of these challenges and allows for security operations to evaluate all the different aspects from visibility, detection, threat hunting, integration, speed and overall efficiencies without paperwork or software downloads – just a web browser.

Competitive Comparison

Another great way to gain insight is to ask your down-selected vendors for their product comparisons: every vendor should have one... You will be surprised to find that most, if not all, follow a very similar format, making it easy to correlate.

There are two key benefits from doing this:

1 It will highlight the key feature/ functions that each vendor believes uniquely differentiate themselves against the competition

2 As the NDR market is increasingly crowded (18+ vendors) 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.

Bricata Comparative Matrix

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

Why Bricata

Bricata is a “hands-on” network detection and response platform. We’re 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 real-time visibility, advanced detection, analysis, forensics, incident response and threat hunting into a single platform, Bricata provides organizations with the most effective tools to find, understand and act on relevant threats.

Bricata 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 intuitive place. Bricata doesn’t replace human analysts. It gives people the power to do what people do best – think, evaluate, discover and decide.

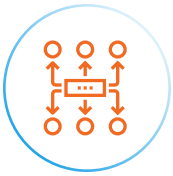
Bricata’s NDR Advantages

End-to-End Visibility & 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 & Powerful Analytics

Multiple threat detection engines give you visibility into the known, unknown, and see the pattern of the unknown unknowns on your network, all while virtually eliminating false positives.



Effective Response & Simple Network Instrumentation

Respond to and correlate alerts in real-time, with frictionless integrations to SIEM/SOC workflows and 3rd party threat intelligence tools. Deploy Bricata’s smart sensors in just a few clicks and easily instrument your network.

Advanced Forensics & Threat Hunting

Bricata’s smart PCAP allows you to investigate and validate a threat by providing enough data to accurately follow the kill-chain. Follow a hypothesis to uncover an unknown threat, or gain insight into normal operations. It’s all at your fingertips.

What Customers Appreciate

"Bricata makes our life easier. It's a truly reliable solution that brings the best of available network forensic, inspection and data visualization technology in one well-orchestrated solution."

– Fortune 500 CISO

With Bricata, you have the right data, at the right time, to get the right answer.

Put Us to the Test

NO PAPERWORK, NO INSTALLERS. JUST A BROWSER

BRICATA®

Launched in September 2020 Bricata.labs delivers prospects a real-time experience of our market leading Network Detection & Response (NDR) platform at the touch of a button.

Individual users of complete teams can request access from 2-hours up to 72-hours at no cost, with no paperwork / agreements and no software installers.

Bricata.labs demonstrates our cloud-enabled capability (with all lab components running in a public cloud) and the simplicity of deployment with the entire process automated, allowing our team to launch an environment(s) at the click of a button in less than three-minutes.

Use cases for Bricata.labs include:

- Early stage assessments of capability (kick-the-tires)
- Team events: Capture the Flag
- Training & Education

BRICATA.labs®

Request Bricata.Labs Account

Contact your account team for more information on Bricata.labs as a next step

ABOUT

Bricata is leading the next generation of advanced network detection and response for the enterprise. By fusing real-time visibility, advanced detection, analysis, forensics, incident response and threat hunting into a single platform, Bricata provides organizations with end-to-end visibility and context for direct answers and powerful insight to take immediate action.

BRICATA.COM | INFO@BRICATA.COM | 888.468.0610 |