opentext™

POSITION PAPER

What to look for in a Network Detection and Response platform

opentext™

Contents

opentext™

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**

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

opentext™

Comparative Matrix		OpenText NDR
Network Data Capture & Retention	Pure & R	

o ent t

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