TAG CYBER

WHITEPAPER

# ENGINEERING EFFECTIVE NETWORK DETECTION AND RESPONSE FOR THE ENTERPRISE

DAVID NEUMAN, TAG CYBER

TAGCYBER

WHITEPAPER

# ENGINEERING EFFECTIVE NETWORK DETECTION AND RESPONSE FOR THE ENTERPRISE

DAVID NEUMAN

Security architects and engineers are constantly faced with the challenge of how to best protect their networks from both internal and external threats. This paper addresses areas to consider when evaluating a network detection and response solution, including: 1) outlining the most common challenges faced when utilizing NDR, 2) highlighting how to gain real-time visibility, full-spectrum threat detection and advanced threat-hunting capabilities and 3) discovering how OpenText NDR provides complete visibility to hunt for and defend against threats.

## INTRODUCTION

Network security engineers and architects face numerous challenges in complex enterprises, equipping the security operations center (SOC) with valuable tools to defend against sophisticated cyber adversaries. Network detection and response (NDR) is an important part of network security, and it involves using various tools and techniques to detect, analyze and respond to threats on a network. Some of the most difficult challenges engineers and architects face when deploying NDR include:

**Scalability:** NDR tools can generate a large amount of data that needs to be analyzed in real-time to detect and respond to threats. As the network grows, it can become more difficult to scale and manage NDR tools to handle the increased volume of data.

**Advanced threats:** Attackers are constantly developing new and more sophisticated methods of evading detection. Network security engineers must stay updated with the latest tools, threat intelligence and techniques to detect and respond to these advanced threats.

**Integration:** NDR tools must integrate with other security tools and technologies by exporting data to a unified platform, such as security information and event management (SIEM), to allow for integrated response across the enterprise.

**False positives:** NDR tools can generate many alerts, and not all of them may be actual threats. Choosing a platform that provides a simple method for keeping the solution well-tuned is imperative to minimizing false positives.

The impact of not mitigating these challenges is the increased likelihood that security operations teams will miss intrusion and exploit attempts, resulting in material damage or disruption to a business. When teams lack visibility and fidelity into incidents, they lose the edge to intercept an attacker at the right time and place and with decisive action.

This paper will describe how an NDR helps enterprises gain real-time visibility, full-spectrum threat detection and advanced threat-hunting capabilities. We will also discover how **OpenText™ Network Detection & Response** provides complete visibility to hunt for and defend against threats.

## GAINING REAL-TIME VISIBILITY

The Russian critical infrastructure assaults on Ukraine from 2014 to 2016 were a series of cyberattacks that targeted key systems, including the power grid, financial institutions and government agencies. The attacks were part of a broader conflict between Russia and Ukraine that began in 2014 with Russia's annexation of Crimea and support for separatist rebels in eastern Ukraine. The attacks began in December 2015 with a coordinated power outage that left over 230,000 Ukrainians without electricity for several hours. The attack was carried out by a group of hackers known as Sandworm (Russian military intelligence), who used a sophisticated malware called BlackEnergy to access the control systems of the power grid. The attackers then used the malware to disconnect key power transmission stations, causing widespread disruption. In addition to the power grid attack, Ukrainian banks and financial institutions were also targeted with a series of distributed denial of service (DDoS) attacks in December 2015 and February 2016.

In June 2016, another cyberattack targeted the Ukrainian government, including the country's Ministry of Finance and State Treasury. The attack used malware called Petya, which encrypted files and demanded a ransom in exchange for the decryption key. The attack disrupted government operations and caused significant financial losses.

These attacks demonstrate the deep level of network access threat actors have across many organizations and the freedom of movement to launch these attacks to cause maximum damage. What is more concerning is that Ukraine was not nearly as connected as other countries, making real-time visibility into highly connected networks even more critical.

Threat actors thrive on network blind spots that allow them to blend with normal activity to escape detection and maintain significant dwell times in the highly sensitive parts of an enterprise. Advanced threat actors take a long-time horizon approach to persistent access, and engineers and architects must do the same with solutions for data collection in security operations.

Next-generation NDR solutions need to fuse real-time visibility, advanced detection, analysis, forensics, incident response and threat hunting into a single platform. This is how security teams battling advanced attackers gain complete insight with full context for immediate action. Instead of looking at events in isolation, teams collect all relevant information required for a successful investigation, including all indicators of compromise and detailed information about any other systems or clients—outside the network or within—where a suspected compromised host interacted.

## SMART PCAP

Traditional PCAP provides network insight by collecting all data packets throughout the network for analysis. While this is an important resource, it often leaves security analysts to parse vast amounts of data and alerts to get to the meaningful information they need. Smart PCAP captures the relevant data from packets associated with security events and then correlates that event to other necessary packet capture linked to logs and data to give the analyst historical and real-time information to make decisions. *The converged capabilities described above deliver real-time visibility while effectively using resources, reducing mean time to detect, capitalizing on investment by optimizing other technology stacks and applying the skills of security operating where they are most needed.*

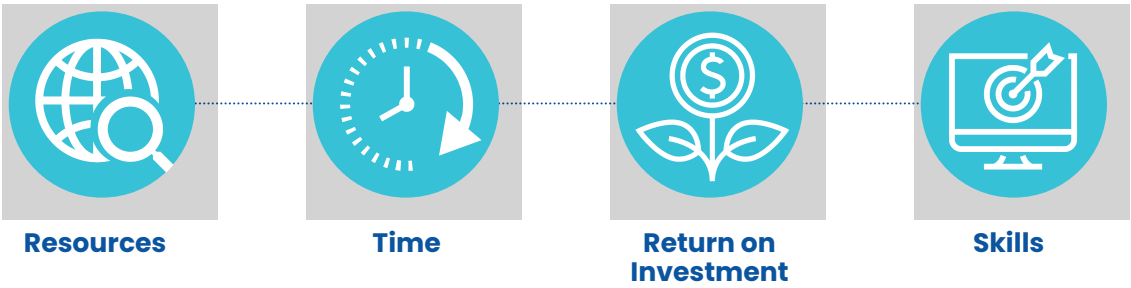


Figure 1: Value proposition to gaining real-time visibility

## FULL SPECTRUM THREAT DETECTION AND ADVANCED THREAT HUNTING

To detect advanced threats, you need to hunt them. These threats move in, out and laterally within an environment, often obfuscating their movements and activities in network blind spots or by hiding in normal traffic. With real-time visibility, a next-generation NDR solution can identify and allow for a rapid and efficient response to threats by focusing analysis on the most relevant traffic. For example, in a critical system that uses non-standard ports or protocols and which may generate seemingly anomalous behavior, an analyst with access to rich network visibility can recognize unexpected traffic based on endpoints, ports and observed applications. In this way, an advanced NDR solution provides the detection of threats that might otherwise go unnoticed in a sea of normal network traffic.

As new threats emerge, an NDR solution must adjust its rules and heuristics to identify relevant traffic, ensuring a team's hunting and detection techniques remain effective and efficient. These capabilities are essential to identify zero-day exploits or unknown, unidentified threats to give security operations advanced threat-hunting and detection capabilities, specifically in the following modalities:

**Threat intelligence:** Integrates with threat intelligence feeds, providing up-to-date information on known threats and attackers. Using full network visibility, indicators of compromise can be curated, tracked and used to engage adversaries.

**Automated response:** Automated response capabilities take action to block or mitigate potential threats as they are detected. For example, a solution may automatically block traffic from an IP address that is identified as a known threat or flag anomalous activity.

**Human expertise:** Advanced threat hunting often involves a combination of automated analysis and human expertise. Next-generation NDR solutions include tools and interfaces so security analysts can easily explore and visualize network data, enabling them to identify potential threats and take swift action to mitigate them.

The hunting and advanced-detection characteristics described above are essential to a security team's ability to observe, orient and act to disrupt adversaries before they can cause major damage to the business or operations. Architects and engineers must consider an NDR platform that empowers the team as a whole to stop the most advanced threats.

## OPENTEXT FOR NETWORK DETECTION AND RESPONSE

TAG Cyber recommends that any organization with network security and resiliency as part of their path to business success considers OpenText's NDR solution. OpenText NDR provides organizations with 360-degree protection, end-to-end visibility, the context for direct answers and powerful insight to take immediate action. The solution provides complete visibility of east-west traffic across network environments in real-time and full-spectrum threat detection that extracts and stores high-fidelity metadata, including an indexed threat-hunting repository.

A multifaceted suite of best-in-breed threat detection allows organizations to inspect network traffic thoroughly from every angle. Users can find unknown, hidden threats to conduct retrospective network traffic analysis and historical data testing to determine if threats infiltrated the environment prior to known indicators being available. They can use meaningful visualizations and flexible network views to see everything in a single view or create custom views for what matters most for their network.

> *"Thanks in large part to [OpenText NDR], we can now detect and correlate events, investigate the data, and notify the client in an average of just 6.5 minutes—less than half our SLA."*
>
> – Jeremy Conway, CEO, MAD Security

## OPENTEXT NDR ELIMINATES SECURITY BLIND SPOTS THROUGH REAL-TIME NETWORK VISIBILITY.

Organizations can see everything on their network via high-fidelity metadata and Smart PCAP, to take advantage of full-spectrum threat detection and reduce noise using multiple detection engines that examine the network from every angle. Users can proactively and with forensic precision investigate detected threats and hunt down unknown threats that did not generate an alert. With seamless response and extensive integrations, organizations can correlate alerts in real-time, enrich existing workflows, automate responses and prevent threats. OpenText NDR is an end-to-end network detection and response platform that allows security teams and the entire enterprise to collaborate better, reduce security risk and solve network problems faster than ever.

## Protect from all sides

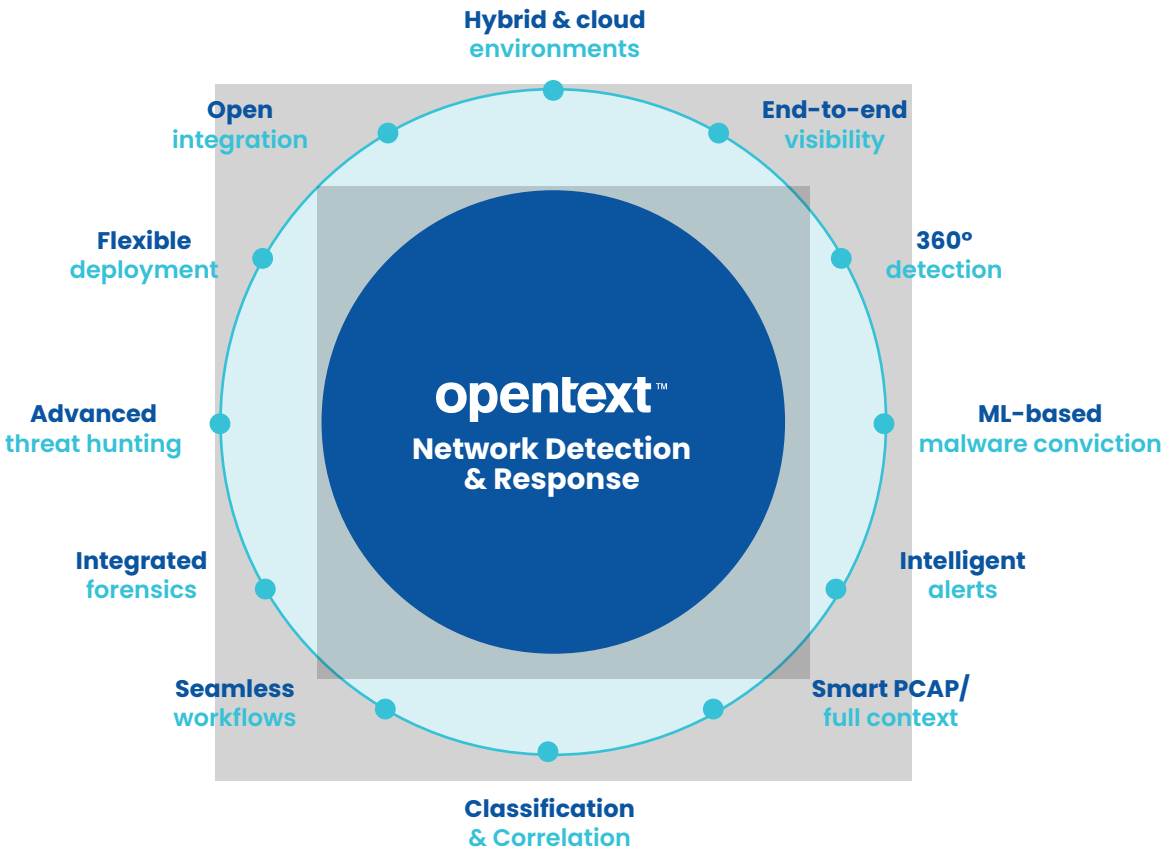


Figure 2: OpenText NDR

## OPENTEXT NDR HAS MANY 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 and deploy smart sensors in just a few clicks to enhance your network.

**Advanced forensics and threat hunting.** Investigate and validate a threat with OpenText NDR's Smart PCAP, which provides enough data to follow the kill chain accurately. Follow a hypothesis to uncover an unknown threat or gain insight into normal operations. Even if you are using full PCAP today, ask the following questions: Is my current PCAP wasting SOC time and storage costs without the desired outcomes? Would we benefit from faster and more accurate threat hunting and incident response? Do I have the capability to identify, replay and solve for previously undetected threats that may return? If the answer is "yes," then you need a Smart PCAP solution.

Network engineers and architects researching an NDR solution should compare the following features:

| 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, 10 Gbps+ in single appliance | X |
| Full-Spectrum Threat Detection | Keep Out | Package inspection | X |
| | | Advanced malware detection (static - ML based) | X |
| | | Network signature (e.g., TALOS, ET Pro) | X |
| | Find Within | Indicator of compromise (i.e., IP, URL or Hash) | X |
| | | Pattern-based anomaly detection (behavior) | 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-tenant data federation (single pane 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 |

Figure 3: OpenText Advantages

OpenText NDR (formerly Bricata) is a "hands-on" network detection and response platform that allows security teams and the entire enterprise to collaborate better, reduce security risks and solve network problems faster and more effectively. "Hands-on" can be interpreted in many ways, but OpenText NDR offers out-of-the-box features and capabilities at scale. In addition, by providing hands-on capabilities, OpenText allows security architects, engineers and analysts to meet mission needs unique to their SOC and the needs of their business. By fusing real-time 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 to protect organizations from material damage.

## ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

**IMPORTANT INFORMATION ABOUT THIS PAPER**

Contributors: David Neuman

Publisher: TAG Cyber, a division of TAG Infosphere, Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Open Text Corporation. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.

Copyright © 2023 TAG Cyber LLC. This report may not be reproduced, distributed or shared without TAG Cyber's written permission. The material in this report is composed of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy or completeness of this report are disclaimed herein.