Buyer's Guide:
Network Detection and Response (NDR)

Choosing a Network Detection and Response (NDR) platform that is the best fit for your organization will improve your ability to detect and quickly respond to threats that are often missed today—and to ultimately attain a stronger security posture.

Introduction

Organizations worldwide have collectively invested billions of dollars in solutions and technologies intended to keep adversaries out of their networks. Nevertheless, tenacious attackers are still able to find their way around perimeter defenses to gain access to a targeted network. Once that foothold is established, the attacker could go unnoticed for months, putting data assets at high risk of theft or corruption.

Consider the unfortunate case of Marriott International, Inc., which discovered in September 2018 that a breach had occurred and 500 million customer records had been compromised. An in-depth forensic analysis showed that the attackers were in the company's network since July 2014—a full four years that their activity went completely unnoticed.[1]

More recently, consider the December 2021 ransomware attack on Kronos public cloud that took down payroll systems and led to data breach disclosures for many of its high-profile customers. In fact, in time we saw many government entities and organizations also discovered that they were victims of the same data breach. Thus, the real concern lies in the fact that organizations still do not have the security posture to detect the early warning signs of attacks like these on their network.

Legacy point-in-time preventative solutions tend to focus on signatures of known malware. Such solutions are still necessary, but they aren't enough for comprehensive security coverage. Solutions providing real-time detection and response to suspicious activity are now a necessary complement to traditional security tools and network detection and response (NDR) is at the forefront of this market.

In its February 2019 Market Guide for Network Detection and Response, Gartner described the technology as using "a combination of machine learning, advanced analytics and rule-based detection to detect suspicious activities on enterprise networks. NDR tools continuously analyze raw traffic and flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect abnormal traffic patterns, they raise alerts. In addition to monitoring north/south traffic that crosses the enterprise perimeter, NDR solutions can also monitor east/west communications by analyzing network traffic or flow records that it receives from strategically placed network sensors."[2]

Security experts profess that enterprise organizations must assume their network is already compromised. When it comes to threat detection and response, understanding network behavior matters. Cyber-attacks use network communications for malware distribution, command and control, and data exfiltration. Integrating security at the network layer presents a unique vantage point to identify security threats right from inception. With the right tools and network oversight, security professionals should be able to uncover malicious activity[3] and take prompt action to mitigate it.

This Buyer's Guide is to help the reader understand the important features and characteristics to look for in a security-focused Network Detection and Response solution, what to discuss with vendors when evaluating products, and how to test them.

---

[1] *Kate O'Flaherty, Forbes, Marriott CEO Reveals New Details About Mega Breach, March 11, 2019*

[2] *Gartner, Inc., Market Guide for Network Traffic Analysis, February 2019*

[3] *Jon Oltsik, CSO Online, Network traffic analysis tools must include these 6 capabilities, July 18, 2019*

Critical Criteria

Here's a look at the critical criteria that matter most to enterprise customers.

TEST CASES

IoT Visibility and Threat Detection

IoT devices, or any of the many things in the internet of things, are nonstandard computing devices that connect wirelessly to a network and have the ability to transmit data. IoT involves extending internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over both the intranet and internet, and they can be remotely monitored and controlled. Thus, a device can be made to perform malicious behaviors.

Test Considerations

How would the NTA solution detect when an IoT device connects to an external server (attacker controlled) and uploads data to a destination server? Would this work if the compromised device was already in the network before the NTA solution was deployed?

Lateral Movement Detection

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos authentication is currently the default authorization technology used by Microsoft Windows, and implementations of Kerberos exist in Apple OS, FreeBSD, UNIX, and Linux. Kerberos requires trusted third-party authorization to verify user identities.

Test Considerations

Can the NTA solution deeply parse authentication protocols like Kerberos as well as application protocols like SMB and Microsoft Remote Desktop Protocol? If not, how would the solution detect threats such as credential abuse and lateral movement?

Data

As the lifeblood of any NDR platform, activity data tells the story of the traffic on the network—where it originates, where it's going, who the sender is, what device it came from, and so on. The broader and deeper the data collected, consumed, and analyzed – including current and historical data – the better it tells a more complete and contextual story.

Legacy NetFlow-based solutions are limited in their depth of visibility (just port and IP address information along with the protocols) and lack the context to identify modern devices or threats. To understand the true attack surface and preempt modern threats, getting access to real-time, ground-truth data about the network devices' state and, if required, the raw packets is paramount.

Look for a solution that provides deep visibility into network traffic – the full stack (rather than just metadata), network logs, net flow, alerts from other systems, or other subsets of data. Looking at data from the full network stack helps uncover a broader set of threats, especially those that blend in with business-justified" activity.

The tool should also deliver a broad array of visibility, including devices, users, applications, and organizations, rather than just IP addresses. This enables resolving the relationships among these entities and helps to uncover threats within north-south and east-west communications with low false positives and negatives.

Additionally, the ability to monitor IoT traffic, protocols, devices, etc., is an up-and-coming need that will grow more important as more companies connect more types of "things" to their network and the threat surface grows ever larger. The best NDR platforms will support a broad set of use cases rather than forcing the need for specific solutions focused on IoT security, etc.

Another factor that can be important to some companies, including highly regulated ones, is organizational data privacy. This pertains to where an NDR stores and analyzes the customer data. Some vendors take the data off-premise and into the vendor's cloud, resulting in regulatory non-compliance for those companies that must maintain their data on-premise or in their private cloud.

Key questions to ask vendors

- What data sources are used as input to the NDR solution?
- What level of network visibility does the platform provide?
- Is data taken out of the customer's environment for any reason?
- How far along is the organization in its cloud, mobile, and hybrid workspace adoption?

Data Science and Analytics

Data science and analytics deliver the ability to obtain insights and information from the data collected across the network. An NDR solution uses various scientific methods, processes, algorithms, and analytical systems to extract these insights from structured and unstructured data.

The intent is to develop sufficiently detailed information about a genuine threat so that an automated response can be taken and a security analyst can be assigned to delve into the situation.

It's one thing to process the data as individual data elements. Still, it is more useful to look at the data and determine who is talking in the network and to understand the context—i.eWhat are the devices, the users, the applications, and how are they interacting with each other? Look for an NDR solution that automates this correlation and analysis.

This is important because humans don't think in terms of IP addresses. For example, consider what is more important for a security analyst to know: that IP address 10.1.2.3 did something unusual, or that the user Joe, who is in Marketing and uses a Windows PC, accessed an application typically used by Finance employees.

A second key characteristic to look for is "features" in machine learning jargon. A feature is an individual measurable property or characteristic of a phenomenon being observed.

Features help provide context to a scenario. For example, contrast these scenarios: "Device A is uploading a lot of data to the cloud." vs. "Device A is uploading a lot of data to Dropbox, and the source of that data is a Python script." It's easy to see which alert would be more beneficial to a security analyst.

Therefore, look for a solution that provides a significant number of security-specific features because that, in turn, enables high fidelity threat detection with a low number of false positives.

Key questions to ask vendors

- Describe how the product correlates individual observations to build context around flagged behaviors or activities.
- Describe the number and assortment of security-specific machine learning features used to detect threats.
- Recognizing that not all anomalies are malicious and not all malicious behavior is anomalous, describe how the system is trained to recognize genuine threats worthy of follow-up.

Use of Machine Learning

Another important characteristic of an NDR solution is the type(s) of machine learning it uses. Unsupervised learning is the training of an artificial intelligence (AI) algorithm using information that is neither classified nor labeled and allowing the algorithm to act on that information without guidance. Supervised learning is a system in which both input and desired output data are provided and labeled for classification to provide a learning basis for future data processing.

TEST CASES

Data Exfiltration

DNS data exfiltration is a way to exchange data between two computers without any direct connection. The data is exchanged through DNS protocol on intermediate DNS servers. During the exfiltration phase, the client makes a DNS resolution request to an external DNS server address. Instead of responding with an A record in response, the attacker's name server will respond back with a CNAME, MX or TXT record, which allows a large amount of unstructured data to be sent between attacker and victim.

Test Considerations
Does the NTA solution inspect DNS at a granular enough level to uncover such a threat or is the attacker able to fly under the radar by taking advantage of a common blind spot given how prevalent DNS traffic is?

Living off the Land Detection

An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.

In this test case, a malicious insider "lives off the land" and uses common system administration tools to enumerate the network and gather sensitive data from SMB shares. The attacker then stages all the stolen data onto popular cloud service provider infrastructure.

Test Considerations
Can the solution detect malicious activity by someone inside the organization that appears to follow acceptable behavior? How would this be done?

Some NDR solutions only use an unsupervised learning model. They study the customer's environment for a few weeks or longer, and then if something changes in the environment after that, it is flagged as an anomaly. This is a one-dimensional approach to machine learning that can lead to excessive false positives or the need to retrain the algorithms.

For example, consider the scenario where an organization deploys a new cloud-based data backup utility. Suddenly many users are sending excessive amounts of data to the cloud, and the NDR system labels this as anomalous behavior because it's different behavior than was originally learned.

This causes two problems. One, an analyst will waste time investigating this anomalous (but not malicious) activity, and two, the NDR system needs to be retrained to understand the new behavior patterns. This latter situation must be factored into operational costs if the system needs weeks, once again, to model all the entities' behaviors.

An ensemble approach that includes both unsupervised and supervised learning reduces the level of effort for the human analysts after something has been flagged as bad behavior.

TEST CASE

Man in the Browser Detection

With an ever-increasing amount of business duties fulfilled through the usage of the web browser – e.g. email, CRM, collaborating etc. – having a program or a malicious actor being able to intercept and manipulate that data is a large risk for an enterprise. Browser extensions are increasingly the attacker's tool of choice, since these are easy to create (unlike advanced malware), can be installed on the machine easily through social engineering and have unfettered access to everything the victim user has access to in the browser.

Test Considerations

Does the NTA solution have the ability to detect data theft originating from a malicious Chrome extension that uploads data to an external server for later access?

Supported Use Cases

Many security tools are built around use cases or scenarios likely to be found in customers' environments. The more use cases a solution can support, and the more specific those cases are to security practitioners, the better value and quicker return on investment (ROI) the tool can provide for the security team.

There are two aspects to the breadth of use cases a solution can provide. One is to help an organization with its current security needs, and the other is to help as the security program matures, e.g., to perform functions like digital forensics and threat hunting.

Here are some of the most important use cases that a good NDR tool should support.

Detect Known Attacker TTPs

Historically, most threat detection has occurred through indicators of compromise (IOCs). However, these days attackers are smart enough to keep changing those indicators, so a more effective way to detect threats is by modeling an adversary's tactics, techniques, and procedures (TTPs).

For example, instead of searching for a particular domain, which an attacker can change quite easily, look at the infrastructure behind the domain. Where is it registered? Where is it being hosted? What is the autonomous system number (ASN) for the host network? How long has the domain existed?

These are things an attacker can't change quite as easily. An effective NDR solution provides these types of adversarial models out of the box but also allows a customer to customize or build its own models for TTPs that are specially custom to their organization.

Threat Hunting

An effective NDR platform must be able to automate threat hunting. Security analysts need information that has already been correlated and distilled to point them in the right direction of the security incident. Security teams with access to vital contextual data, historical forensics, and AI-driven threat hunting capabilities are able to speed up both time to detection and time to remediation.

By building threat hunting into the NDR platform and even into the network switching infrastructure itself, organizations can deploy a deep packet-inspection security analytics solution as part of their network fabric.

Retrospective Detection

Whenever a new attacker TTP emerges, organizations should investigate whether that TTP has unknowingly occurred in their environment in the past. This necessitates the ability to search back in time to automatically surface relevant behaviors and visualize the entire lifecycle of the attack

For example, an intelligence service might issue information about a type of attack that has been lurking in the network but is newly disclosed publicly. The organization can look back in time to see if there are any signs of that attack in the network over a historical period of time.

Encrypted Traffic Visibility

More and more network traffic is getting encrypted, and organizations are increasingly hesitant to decrypt it due to the policy and privacy implications involved. Attackers are attuned to this hesitancy and are increasingly using encrypted traffic to evade network detection.

Encrypted traffic analysis solutions enable the identification of the applications that are communicating and the nature of the traffic that is going over the wire, among other aspects—because context is everything.

For example, it might not be of concern when an encrypted file is transferred over a Zoom meeting session, but if that file is transferred from a PowerShell script to a Dropbox account, which is unusual, it might be more concerning.

An effective NDR product will offer means for analyzing encrypted traffic without needing to inspect the actual content of the traffic to determine if it is suspicious. In addition, NDR solutions should not require agents to be installed for performing such analysis.

Incident Response and Forensics

Security threats that are not instantly blocked by preventative security tools eventually turn into incidents that must be detected, and then human security specialists need to intervene to respond.

Network traffic can show exactly who and what is active on the network over any time interval. The NDR platform should enable building endpoint profiles from network communications to quickly present investigators with the information required to close security issues.

Key questions to ask vendors

- Give examples of specific use cases that the NDR solution can support out of the box
- Does the solution provide the means to create and automatically hunt for threats custom to the organization?
- How effectively does the solution support the security operations workflow, from network visibility to detection, investigations, incident response, and digital forensics?

Company Background

When it comes to an advanced solution like Network Detection and Response, there is no substitute for deep subject matter knowledge and expertise; i.eThe solution vendor should have "security DNA" and an understanding of hybrid networks to the device level. It's important to consider the company background, financial stability, and how much experience they have in establishing security at the network layer specifically as opposed to other aspects of network traffic processing, e.g., network performance management. This is important since it often reflects in the product user experience and who the workflows actually target.

Key questions to ask vendors

- Has this platform been purpose-built to focus on the security aspects of the network?
- Is the platform built to scale demands from hybrid networks of today?
- What kind of security education/experience/threat research expertise does the team (including executives and company advisors) possess?
- If the product is pivoting from a related space, what level of effort and threat research has gone into making sure the workflows are effective for security practitioners?

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062

Checklist for Security-Focused Network Traffic Analysis Solutions

Security threats that are not instantly blocked by preventative security tools eventually turn into incidents that must be detected, and then human security specialists need to intervene to respond.

DATA FEATURES, CHARACTERISTICS AND CAPABILITIES		
Deep visibility – the solution looks at the full stack of network traffic, Layer 2 on up	☐ Yes	☐ No
Broad visibility – collects data about devices, users, applications and organizations rather than just IP addresses	☐ Yes	☐ No
IoT, OT and cloud network support – ability to monitor IoT, OT and cloud traffic, devices, protocols	☐ Yes	☐ No
DATA SCIENCE AND ANALYTICS		
Data points are automatically correlated and analyzed in context of the entities on the network rather than IP addresses	☐ Yes	☐ No
A significant number of security-specific "features" that enable high-fidelity threat detection with low false positives	☐ Yes	☐ No
An ensemble of machine learning models	☐ Yes	☐ No
USE CASES		
Detects known attacker TTPs by enabling adversarial modeling	☐ Yes	☐ No
Allows retrospective detection of signs of attack	☐ Yes	☐ No
Provides visibility into encrypted traffic without requiring decryption	☐ Yes	☐ No
Allows customer to customize or create own use cases and detection models	☐ Yes	☐ No
Enables incident response, forensics and threat hunting	☐ Yes	☐ No
DEPLOYMENT AND EXTENSIBILITY		
Provides comprehensive network coverage without the need for excessive numbers of sensors	☐ Yes	☐ No
Sensors can be physical or virtual, as needed	☐ Yes	☐ No
Solution is a platform that operates well with other security tools	☐ Yes	☐ No
Endpoint software agents are not necessary for any part of the analysis	☐ Yes	☐ No
Can the solution scale to accommodate the security needs of hybrid networks?	☐ Yes	☐ No
COMPANY BACKGROUND		
Platform is purpose-built for security analysis	☐ Yes	☐ No
Solution provider has deep security experience and expertise	☐ Yes	☐ No
Solution provider can build security at the network layer	☐ Yes	☐ No

Glossary of Terms

Advanced Persistent Threat (APT): NIST defines an APT as an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization, or positioning itself to carry out these objectives in the future.

The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

East/West traffic movement (also Lateral Movement): East/west or lateral movement is a technique used by cybercriminals to systematically move through a network in search of data or assets to exfiltrate. It is a means to an end, a technique used to identify, gain access, and exfiltrate sensitive data.

The attacker will use different tools and methods to gain higher privileges and access, allowing them to move laterally (sideways; between devices and apps) through a network to map the system, identify targets and eventually get to the organization's crown jewels. For example, suppose if the attacker can secure administrative privilege, malicious lateral movement activities can be extremely difficult to detect as they appear as "normal" network traffic to security pros that lack the tools to differentiate or are overwhelmed by a flurry of alerts.

Insider Threat: An insider threat is a security risk to an organization that comes from within the business itself. It may originate with current or former employees, contractors or any other business associates that have – or have had – access to an organization's data and computer systems. Because it originates from within and may or may not be intentional, an insider threat is among the costliest and hardest to detect of all attack types.

Network Detection and Response (NDR): Network detection and response is a security solution category used by organizations to detect and prevent malicious network activity, investigate and perform forensics to determine root cause, and response and mitigation strategy. NDR solutions parse network data at a much deeper level and use an ensemble of machine learning approaches rather than relying on unsupervised learning (anomaly detection) that is prone to high false positives and negatives.

These platforms support a broad set of use cases from situational awareness and detection to incident response, threat hunting, and digital forensics.

With protection against non-malware threats, including insider attacks, credential abuse, lateral movement, and data exfiltration, NDR solutions give organizations greater visibility into what is actually on the network as well as all activity occurring. This, in turn, enables security teams to identify and stop suspicious network activity rapidly and thus minimize impact.

North/South traffic movement: With north/south movement, traffic comes into and out of the network into Internet space, i.e., in and out of edge firewalls and/routers.

Threat Hunting: Threat hunting is the process of an experienced cybersecurity analyst proactively using manual or machine-based techniques to identify incidents or threats that currently deployed automated detection methods didn't catch.

To be successful with threat hunting, analysts need to know how to coax their toolsets into finding the most dangerous threats. They also require ample knowledge of different types of malware, exploits, and network protocols to navigate the large volume of data consisting of logs, metadata, and packet capture (PCAP) data.