SANGFOR

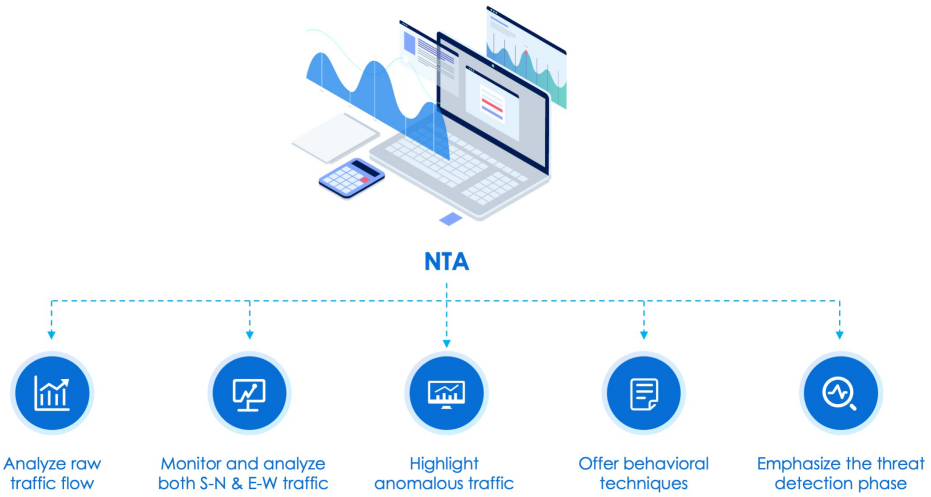
Sangfor
Cyber Command Positioning

Cyber Command Positioning

Cyber Command NDR is an intelligent threat detection and response platform that significantly improves customer security detection and response capabilities.

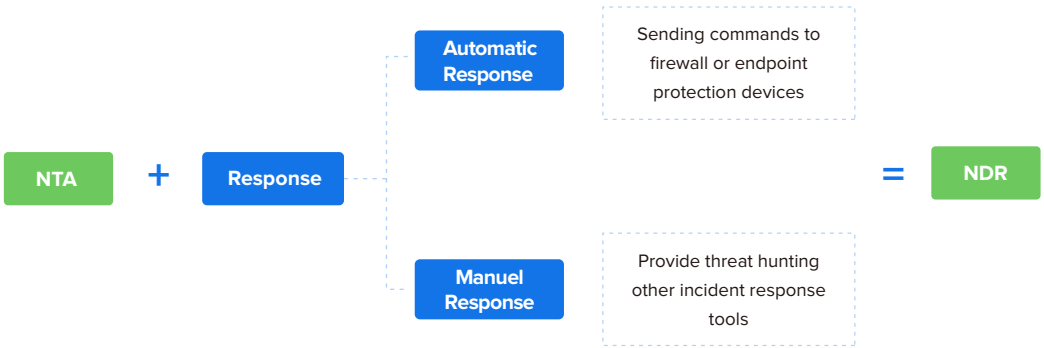
What is NDR (Network Detection and Response)

Network Detection and Response (NDR) was previously referred to as Network Traffic Analysis (NTA) by Gartner.



In 2019. Gartner publish the first NTA market guide, determining that NTA must include the following criteria:

- Analyze raw network packet traffic or traffic flows (for example, NetFlow records) in real-time or near real-time
- Have the ability to monitor and analyze North/South traffic (as it crosses the perimeter), as well as East/West traffic (as it moves laterally throughout the network)
- Be able to model normal network traffic and highlight anomalous traffic
- Offer behavioral techniques (non-signature-based detection), such as machine learning or advanced analytics, that detect network anomalies
- Be able to emphasize the threat detection phase, rather than the forensics — for example, packet capture (PCAP) analysis — phase of an attack



In 2020, Gartner change the “NTA Market Guide” to the “NDR Market Guide.” In the past year, all NTA vendors began adding more automated and manual response features to their solutions. So NTA plus response, became an NDR category.

Why NDR?

Gartner states that, “Applying machine learning and other analytical techniques to network traffic is helping enterprises detect suspicious traffic that other security tools are missing.”

Detect the 1%

There are more than 500,000 new malware variants created daily, and while your existing security solutions may be able to block 99% of them, there are still thousands of new malware variants that can bypass your security devices and cause damage.

AI vs. AI

AI technology has been used by the hackers to weaponize with increased sophistication. Legacy security system has limited AI threat detection functions, meaning it takes AI to defeat AI.

100% visibility in your network

NDR has the ability to monitor and analyze North/South traffic, as well as East/West traffic. It is the fastest and most efficient way to find threats in your cloud, data center, enterprise network, and IoT devices.

Why Cyber Command?

More Comprehensive Detection Capabilities

While other NDR products only emphasize behavior detection engines, Cyber Command enables multiple detection engines. Cyber Command can detect threats using signature-based detection engines and Threat Intelligence, and detects anomalies using AI engines. In this way, Cyber Command provides a low false-positive rate and high detection rate results.

Simpler Threat Hunting Model

Currently, a lot of NDR products are hard to use. Once an organization subscribes the NDR, they must also subscribe the reporting functions. It hard for the security team to use the product directly. Cyber Command provides a built-in threat hunting model, including an impact analysis model, timeline view for entry points, and attack patch recovery, which allows security personnel to conduct fast and easy threat hunting.

More In-depth Correlated Response

While other NDR vendors are improving their response capabilities by integrating with 3rd-party security vendor by open API, or self-developing simple response features like TCP reset, Cyber Command directly correlates with Sangfor NGAF, IAG and Endpoint Secure, to provide comprehensive and automatic response.

The Difference Between NDR and SIEM

	NDR	SIEM
3rd-party Integration	• Focus on Response (Using Open AI for Automatic Response) • Integrate with Security products	• Focus on Security Event Correlation (Using logs normalization) • Integrate with large ranges of IT assets (Server, Router, switch, Security devices)
Key Scenario	• Focus on Security (Detect the threats that others solutions are missing) • Mid-sized Enterprise security operation center -- Using sensor to detect the entire network traffic and Correlate response with endpoint and network security solutions.	• Logs Management • Regulatory Compliance report (HIPPA, HIPAA, SOX, PII, NERC, COBIT 5, FISMA, PCI, etc.) • MSS/Large Enterprise Security Operation Center – Build for vast logs collection (running security analytics on top of huge data sets. Needs lots of resources for operation)
Key Technologies	• AI Detection Engines (Machine learning /Big data) • Raw traffic analysis • Built-in Investigation and Threat Hunting Tools	• Logs Collectors (Standardize API) • Logs Normalization • Correlation Engines (Associated statistics of security events, Vulnerability information, monitoring lists, asset information, network information and historical information)
Technical Trend	• Anomalies Detection Engines • Simplify Threat Hunting • Simplify Threat Investigation • Automatic Response (Using Open API)	• Integrated UEBA engines • Integrated SOAR (Using open API)