vehere

WHITEPAPER

Choosing the Cybersecurity Champion: Network Detection & Response vs Extended Detection & Response

In today's world, we inhabit two realms: the physical one we navigate daily and the cyber network where our data resides. Amidst the relentless battle against cyber threats, navigating through the maze of evolving technology and terminology can be daunting. Security analysts, along with their brightest teams, often find themselves lost in a sea of similar acronyms.

However, understanding the nuanced disparities between Network Detection and Response (NDR) and Extended Detection and Response (XDR) is crucial. This paper aims to demystify NDR vs. XDR, empowering you to make informed decisions for your security operations.

The Definitions: NDR and XDR

Network Detection & Response (NDR), extends beyond traditional security tools like SIEM and EDR by analyzing Layer 2 to Layer 7 network data, including both north-south and east-west traffic. Using advanced behavioral analytics and machine learning, NDR solutions swiftly uncover and address hidden threats.

Extended Detection & Response (XDR), integrates data from various sources like endpoints, networks, servers, and email, providing a comprehensive security view. By analyzing this data, XDR empowers teams to swiftly detect and respond to threats across the organization.

NDR vs. XDR – A Brief Comparison

Network Detection & Response (NDR) and Extended Detection & Response (XDR) as components within a unified security framework, enhance network security effectively. Despite being modules within the same security stack, they differ in their functionalities and monitoring capabilities.

Point of Difference	Network Detection & Response	Extended Detection & Response
Data Source	Network tap, traffic mirror, or AWS flow logs (on premises, virtual, hybrid, or public cloud).	Combination of endpoint agents analyzing host process behavior, NGFW appliances analyzing network traffic, and potentially other data sources.

Point of Difference	Network Detection & Response	Extended Detection & Response
Installation Site	Deployed without agents. Positioned out-of-band in cloud environments, data centers, and remote locations.	Endpoint agents and NGFW appliances are deployed on each endpoint and at network boundaries for enhanced visibility.
Performance Considerations	No negative performance impact.	Potential performance degradation when monitoring lateral network traffic.
Deployment Strategy	Best in class: Purpose-built NDR for passive monitoring of L2-L7 network data that leverages ML and is natively integrated with threat intelligence data, EDR, and SIEM to avoid vendor lock-in.	Single vendor: XDR platforms are typically vendor-specific, limiting 3rd party integrations to data enrichment such as threat intelligence feeds.
Data Privacy	In case of data privacy as top priority, the limited data scope of NDR is extremely beneficial.	XDR collects data from various sources across one's IT infrastructure, which can raise data privacy concerns in some industries or organizations.
Focus on specific threats	For organizations facing specific network-based threats as a major concern, such as lateral movement within the network or targeted data exfiltration attempts, NDR's deep visibility into network traffic can be highly valuable.	With data collected from various sources, XDR may not prove to be beneficial for having focused attention on those specific threats.
Cost-effectiveness	The lower upfront cost of NDR can be a major advantage for budget-conscious organizations.	Due to its comprehensive integration and higher implementation costs, XDR is not considered cost-effective.

Choice Matters: What is the right cyber defender for you?

XDR holds promise for analysts with streamlined analysis and forensics yet hinges on open interfaces for optimal integration.

Meanwhile, NDR stands as a vital security element, tapping into network data for unparalleled threat coverage. Unlike EDR or XDR, NDR zeroes in on packet analysis, offering unparalleled reliability. Afterall, packets don't lie, making them the best source for reliable, accurate, and comprehensive insights. Coupled with SIEM and EDR, NDR combats blind spots, fortifying network security and fostering seamless collaboration.

Vehere AI Network Security

Vehere AI Network Security is a unified solution of Network Detection & Response and Network Forensics. Being an AI activated software, Vehere NDR ensures lossless packet monitoring, real-time threat detection, threat hunting for emerging threats, support for millions of IOCs & IOAs. With comprehensive network forensics, Vehere NDR enables organizations to intercept attacks at their inception, preventing breaches before they occur and saving time for decision makers.

vehere