EXTRAHOP®

BUYER'S GUIDE

Network Detection and Response (NDR) Buyer's Guide

Building a Business Case for NDR Adoption in Your Organization

TABLE OF CONTENTS

Introduction

Threat hunters, advanced security teams, and incident responders are all constantly tasked with defending yesterday's infrastructure against tomorrow's threats. As bad actors find new ways to circumvent traditional perimeter defenses like SIEM, endpoints, and logs, organizations must look to new security approaches that leverage network infrastructures as a source of truth - like Network Detection and Response (NDR) solutions.

NDR modernizes cybersecurity by providing **complete network visibility** with a spectrum of techniques to detect activity at every stage of the attack lifecycle, filling coverage gaps left by EDR, SIEM, and logs.

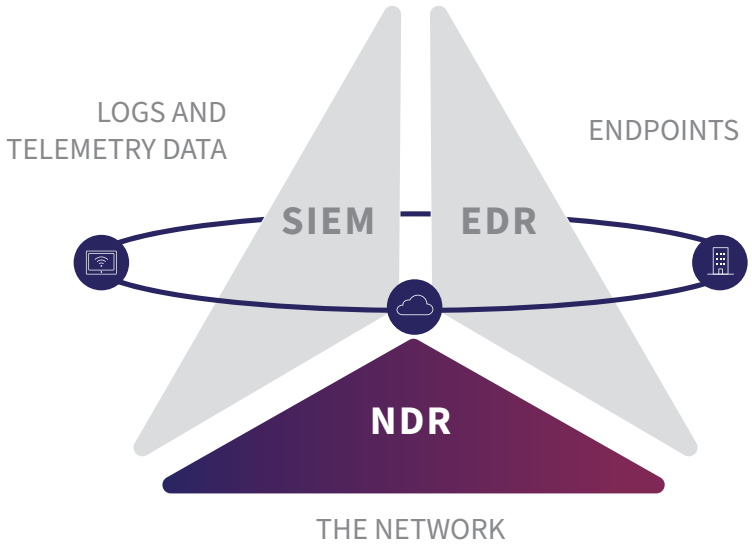
Organizations deploy NDR to gain enhanced visibility into network activity and detect anomalous behavior that indicate advanced threats, particularly those hidden in encrypted traffic, and rapidly respond to potential security incidents by identifying malicious activity early on, often where other security tools miss it.

With a single solution, security analysts can monitor the activity of every device on the network, managed or unmanaged. It's like an eye-in-the-sky helicopter view of all your data in motion, cataloging devices and network conversations that can be inspected for the presence of a malicious actor and their activity.

Deploying an NDR solution is arguably the most significant single step a security team can take to gain complete visibility to understand and monitor what's happening in and on an organization's network. It is important to compare NDR vendors and evaluate how well their solutions will positively impact your security posture.

This guide will walk you through the questions you need to answer to develop a compelling business case for NDR adoption in your organization.

The full visibility that's required for effective security operations demands visibility everywhere



The NDR global market increased

19%

for the period 1Q23 through 3Q23, year over year.[1]

The NDR market will grow at a

14.1%

CAGR by 2028.[2]

Identifying the Challenges for Your NDR Solution

What challenges are you trying to solve or prevent with an NDR solution? Clearly stating the primary reason you are recommending NDR for your organization sets the context for the entire proposal. Common use cases:

Decryption and Deep Packet Inspection

CHALLENGE

Inspecting application protocols to detect malicious files or activity is crucial yet difficult, as over 80% of network traffic is encrypted. You need to first decrypt your applications traffic, then decode it.

NDR SOLUTION

The right NDR can decrypt packets in real time, including complex authentication protocols like Kerberos without impacting performance. You need an NDR solution that understands your business critical applications. With many protocols in use, look for vendors who support at least 90 and use native decryption.

- Ability to perform targeted, out-of-band decryption at speeds nearing 100 gigabits per second, including TLS/SSL 1.3, SMB V3, MS-RPC and other encrypted protocols. Since over 70% of emerging threats leverage encrypted channels, this capability is key.
- Protocol decodes to understand the type of transaction (GET vs. POST or SQL read vs. write) behind the traffic, and the ability to distinguish between normal activity or attacker techniques.
- Comprehensive traffic analysis, including detecting and observing lateral movement by malicious actors penetrating the network and malicious attempts to manipulate network communication protocols.
- Enhanced visibility, moving beyond endpoint sensors to understand the traffic flow that led to the incident detected by the endpoint or other security controls, including the reconstruction of the attackers actual commands executed on compromised systems (like SQL statements executed on Database servers) to see the complete picture.

Ransomware Detection

CHALLENGE

Ransomware attacks are escalating, increasingly sophisticated, and widespread, threatening organizations of all sizes.

NDR SOLUTION

Through early detection of data staging, bulk data exfiltration or lateral data movement, key indicators of ransomware activity are identified, NDR:

- Identifies suspicious traffic patterns quickly.
- Enables rapid isolation of affected systems.
- Supports swift action to prevent ransomware spread.

Asset Discovery

CHALLENGE

An increasing number of unmanaged devices on the network are invisible to endpoint solutions, stemming from remote/distributed teams, IoT devices, guest devices, or other assets that simply can't carry an endpoint agent.

NDR SOLUTION

Using real-time network traffic analysis with machine learning and advanced stream processing, NDR automatically discovers and identifies ALL of the systems and assets that are communicating on the network, providing a continuously up-to-date audit:

- Combines traffic analysis with asset information to provide a comprehensive view of network activity.
- Categorizes all assets on a network and provides deep analytics for device characteristics and behaviors, alerting to devices that may be acting out of the ordinary - like an IoT device randomly connecting to database servers.
- Issues ML-powered alerts so IT analysts can see anomalous behavior and/or flag a device for follow-up.
- Identify and categorize commonly used software like Remote Monitoring and Management (RMM) tools that are increasingly used for malicious purposes.
- Dashboards provide top-level health and security metrics to simplify day-to-day management.

Enabling Zero Trust and Microsegmentation

CHALLENGE

Implementing Zero Trust controls and microsegmentation safeguards can disrupt operations and create complications.

NDR SOLUTION

NDR provides essential context for understanding diverse traffic flows by:

- Understanding traffic flow and access after ZT implementation to gauge effectiveness
- Helping to distinguish between expected traffic and anomalies.
- Identifying infrequent but legitimate device communications.
- Providing continuous monitoring and full visibility.
- Mapping application dependencies to ensure appropriate controls are implemented without disrupting operations.

67%
of malicious traffic is encrypted.[3]

56 DAYS
median dwell time before attackers are discovered.[3]

73% DECREASE IN NET INCOME
within 9 to 12 months after announcing a breach.[4]

Security Tool Consolidation

CHALLENGE

Tool sprawl often overwhelms SOCs as they try to manage and correlate high volumes of alerts from multiple sources. Managing and integrating multiple security tools together is complex and prone to failure.

NDR SOLUTION

Comprehensive NDR platforms consolidate Network Performance Management (NPM), Intrusion Detection System (IDS), packet capture, SSL decryption, and DPI solutions into a single platform that snaps into your EDR/XDR, SIEM, and SOAR infrastructure to complete the SOC triad. This enables:

- NPM functions of availability, performance monitoring, and troubleshooting combined into your SecOps platform.
- Consolidate legacy point solutions into a modern unified platform.
- Streamlined security operations for faster incident detection and response.
- Reduced hardware footprint and associated costs.

Enforcing Immutable Network Security

CHALLENGE

Malicious actors are persistent in innovating their TTPs to evade discovery, covering their tracks by turning off or deleting logs, disabling EDR agents and services on the endpoint, or even passing files using stolen credentials. Enterprise security teams can no longer rely solely on endpoint-based detection tools to look for known threats.

NDR SOLUTION

The right NDR solution gains insights directly from network data, including capturing and analyzing network packets, which cannot be evaded or disabled by threat actors. NDR provides a single source of truth by:

- Monitoring actual network behavior, which cannot be falsified.
- Monitoring all devices on the network, even those without agents or other monitoring solutions.
- Offering detection of unknown threats, beyond log analysis.
- Automatic packet capture and storage with full payload for forensic proof and chain of custody.

Securing DevOps Environments

CHALLENGE

DevOps practices can introduce security risks through increased use of external repositories and untrusted code execution. The increasing use of AI and LLMs in enterprise environments has amplified this attack surface.

NDR SOLUTION

NDR monitors network activity to protect against potential threats by:

- Observing interactions with external code repositories.
- Detecting suspicious behavior from downloaded and executed code.
- Protecting the broader network from potential malicious payloads.
- Monitoring what's on your network and what's allowed to be on your network

Questions For Vendors

Choosing an effective NDR solution demands thorough research across multiple vendors. To identify the provider that best aligns with your organization's requirements, ask the following key questions during your evaluation.

WHAT TO ASK	WHAT TO LISTEN FOR
Does the solution work on-premise and in the cloud?	Confirm support for your specific environment – cloud-native, hybrid, or on-premises. The solution should support both your current infrastructure and your future plans in a single platform in a single UI.
Which cloud service providers are supported?	The solution should seamlessly integrate with your entire IT environment and ecosystem. Verify comprehensive support for your preferred cloud service providers.
Can the system scale with your planned growth?	Ensure the solution can grow with your organization without degrading performance by accommodating increased data volumes, new technologies, and expanding network speed and complexity.
What is the breadth of telemetry support?	Look for a vendor-agnostic platform that can ingest telemetry from a wide range of applications, particularly those critical to your operations. Ensure the platform collects metrics specific to your critical applications; i.e. VOIP metrics for a call center app, SQL metrics for DB apps, HTTP metrics for web apps, etc.
How often are threat models or attack signatures updated?	Seek a provider that offers frequent and prompt updates to their threat intelligence. Understand their update process and how quickly they incorporate new threats into the system.
Does the system perform NetFlow analyses?	Confirm the solution's ability to analyze network traffic patterns, crucial for optimizing performance and defending against certain types of attacks.
Does the platform support full packet capture and deep packet inspection?	Ensure the solution inspects both header and payload. Can the solution do continuous captures as well as trigger based packet captures? The solution should be able to extract malicious files out of packets quickly and easily during an incident or investigation.
Does the solution do full traffic decryption natively?	Does the platform decrypt traffic natively or use a 3rd party? Does it do man-in-the-middle decryption or out of band decryption? Does it decrypt then entire session and payload?
Does the system support file carving?	Assess the solution's forensic capabilities, particularly its ability to recover and analyze files from packets, which is critical for in-depth security investigations.
What percent of MITRE ATT&CK tactics and techniques can the platform cover?	The solution should offer broad coverage across a wide range of TTPs in the framework, offering multiple ways to detect adversary behavior. Pay close attention to TTPs in the Lateral Movement, Command & Control, and Exfiltration stages. Look for vendors with 90%+ coverage of network-addressable MITRE ATT&CK techniques.
What is the use of AI in the system?	Inquire about the AI/ML technologies employed, and their effectiveness in threat detection. Does the system use cloud-delivered ML, which scales out on demand, works globally across all sensors, and is updated continuously, or does it use static onboard ML, which lives on the appliance, rarely gets updated, and cannot scale past that single appliance?
What protocols are supported?	At a minimum, the system should be able to decode SSL/TLS 1.3, SMB v3, MS-RPC, to ensure comprehensive network visibility. The solution should support as many of your application protocols as possible. Make a list of those application protocols (i.e. HTTP, various SQL, DNS, VOIP, etc.) and ensure support for as many as possible.
Does the vendor have experience in my industry?	Are they familiar with the typical infrastructure in use, and the standards and regulations such as PCI-DSS, HIPPA, DORA, NIS, etc.?

Making Your Business Case

Emphasize short and long-term benefits while acknowledging the effort required for NDR adoption. When developing your case, be sure to include the following:

Cost/Benefit Analysis

Discuss the NDR solution that is right for your organization and gather pricing structure information from vendors.

COST SAVINGS

NDR can significantly reduce financial outlay and time investment. Quantify these savings by:

- Calculating the reduction in incident response time
- Estimating the prevention of potential data breaches
- Assessing improved efficiency in security operations
- Determining savings from tool consolidation
- Time-to-value and ROI projections

TOTAL COST OF OWNERSHIP (TCO)

When comparing costs, be sure to include:

- On-premises system expenses, including data
- Cloud expenses, including data
- Energy efficiency – reduced power consumption and data center footprint
- Professional services
- Maintenance and support
- Data egress expenses

Deployment and Implementation

Stakeholders	Identify key roles within your organization who will oversee and support the deployment process. This includes a combination of IT, security, legal, compliance, and executive stakeholders, as well as potential involvement from end-user or application development teams.
Impact on the Status Quo	Evaluate the implementation process by considering factors such as resource allocation, additional hardware or configuration requirements, support, and potential disruptions to your current operations.
Timeline	NDR implementation schedules can vary depending on the size and complexity of the solution. Provide a realistic timeline that includes testing, deployment, onboarding, and training.

Business Alignment

Scalability	Demonstrate how the NDR solution can grow with your organization, accommodating increased data volumes, new technologies, and expanding network complexity without degrading performance..
Initiatives	Explain how the solution aligns with and enhances your current and planned strategic initiatives, such as Zero Trust implementation, cloud-first initiatives, or digital transformation efforts.
Compliance	Include confirmation that the NDR solution will maintain compliance with your specific industry regulations and standards and other relevant compliance requirements (e.g. cyber insurance).
Data Retention	Verify that the tool's data retention capabilities align with your corporate standards.

Third Party Validation

Customer Case Studies	Include reference customers similar in size, complexity, or industry to your organization.
Accolades	Add any industry recognition, analyst insights, reviews, awards, or market share data to bolster the case for your NDR solution provider of choice.

Contact Us

Interested in taking a more proactive approach to security?

Contact ExtraHop at **extrahop.com/contact**, and run your organization at the speed of risk.

1. Gartner Market Guide for NDR, March 2024
2. IDC Worldwide Network Detection and Response Forecast, 2024–2028: The Network Is Talking, Are You Listening?
3. https://www.extrahop.com/products/security/what-is-ndr
4. https://www.extrahop.com/news/press-releases/extrahop-report-finds-73-average-drop-in-net-income-one-year-post-data-breach

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP®

info@extrahop.com
extrahop.com