

NDR BUYERS GUIDE

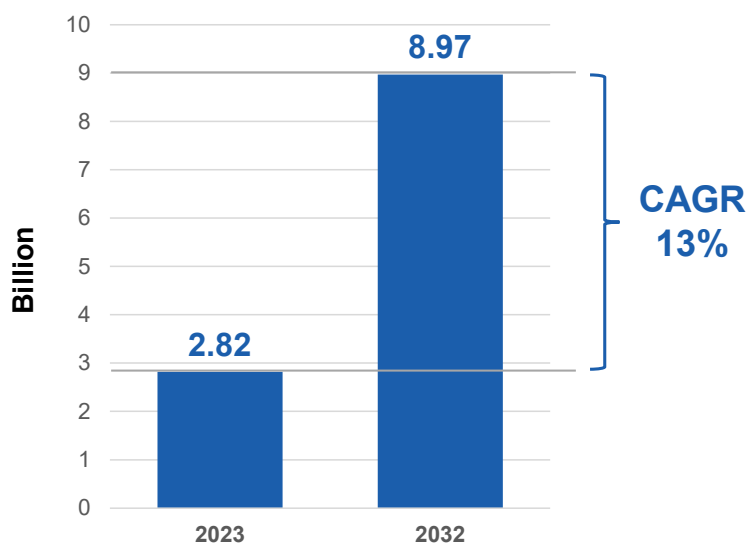




Networks form the backbone of business operations, making them a prime target for cyberattacks.

Threats are increasing in both frequency and sophistication, posing significant challenges to organizations of all sizes. The growing complexity of networks, coupled with the rise of remote work and the proliferation of Internet of Things (IoT) devices, creates conditions where threat actors can easily remain undetected.

A cyberattack can have devastating consequences, jeopardizing an organization's operations, brand reputation, and revenue streams. Often a cyberattack can even cause companies to go out of business due to the aftershocks from the attack, such as fines, legal fees, and the loss of customers who may not feel safe doing business with you anymore.



Global network detection and response (NDR) market size was USD 2.82 billion in 2023 and the market is projected to touch USD 8.97 billion by 2032, exhibiting a CAGR of 13.7% during the forecast period.

Source: <https://www.businessresearchinsights.com/market-reports/network-detection-and-response-ndr-market-101254>

The goal of a cyberattack is often to breach the corporate network perimeter and infiltrate internal systems to gain unauthorized access. Once inside, attackers can steal, modify, or delete data, compromise endpoints, and spread malware, viruses, and other malicious elements.

The speed with which an organization responds to a cyberattack is crucial, yet many businesses lack the necessary resources to handle such incidents effectively. The financial and business consequences of a breach can be insurmountable. No organization is 100% secure, but proactive measures can help mitigate risks and minimize the impact of a successful attack.

The Core Capabilities of NDR

Network Detection and Response (NDR) is a proactive security control that monitors an enterprise's network traffic and helps eliminate network blind spots and detect potential threats before they occur. It does this by continuously monitoring and analyzing a small sampling of network traffic patterns using advanced technologies, such as behavioral analytics, Artificial Intelligence (AI), and Machine Learning (ML), to validate the real-time network behavior against the good operational baseline of normal network traffic behavior. Core capabilities of NDR include:

- Appliance-free and agentless
- Full network coverage (North-South and East-West)
- Pre-trained AI models to analyze network traffic and data, including cloud, SaaS applications, IOTs, POS, legacy, and SCADA data sets
- Monitor traffic at the edge of your network and track users' movement for suspicious activity
- Uncover hidden and unknown attack vectors by utilizing AI and monitoring behavioral techniques to find potential threats
- Modeling that discerns between normal traffic and potentially dangerous traffic
- Dashboards that help security teams investigate and prioritize findings
- AI automation helps security teams sift through alerts and help with attribution

NDR applies AI and ML to detect any deviation from the baseline network traffic pattern and alert security teams of suspicious patterns and the potential threat to their network environment. NDR is completely agnostic to the network's size, scale, and architecture, keeping all networks—whether legacy, public cloud, private cloud, or hybrid—secured and optimized, while uncovering any vulnerabilities, blind spots, or gaps.

Some of the other benefits of NDR include the autonomous discovery of major cloud assets and services and detection of network threats and anomalies/attacks down to the specific server, asset, and service. NDR offers a virtual cyber analyst that provides human-like analysis, continuously monitoring networks and alerting security teams of compromised devices, potential Command and Control (C2/C&C) communication, suspicious outbound communication on mission-critical systems, compromised network assets, vulnerable attack surface, such as insecure protocol in production environment, and others.

Security alerts with context-rich insights are automatically sent to security teams, giving them a full picture of suspicious activity, including a clear attack story, reports, and extensive network-based querying. Organizations can observe active users on their network, their device interactions, and network access locations. This visibility empowers security teams to not just identify threats but to also pinpoint their origins, potential spread, and which users have been compromised.

One of the most important benefits of NDR is its ability to monitor IoT devices, which are especially vulnerable in health care, retail, industrial settings, and any industry that uses devices without screens or endpoints. With NDR, anything connected to the network can be monitored.



More than 50% of companies have implemented AI and IoT in their infrastructures.



Selecting the Right NDR Solution

When selecting an NDR solution, it is crucial to consider the following factors:

Technology Stack:

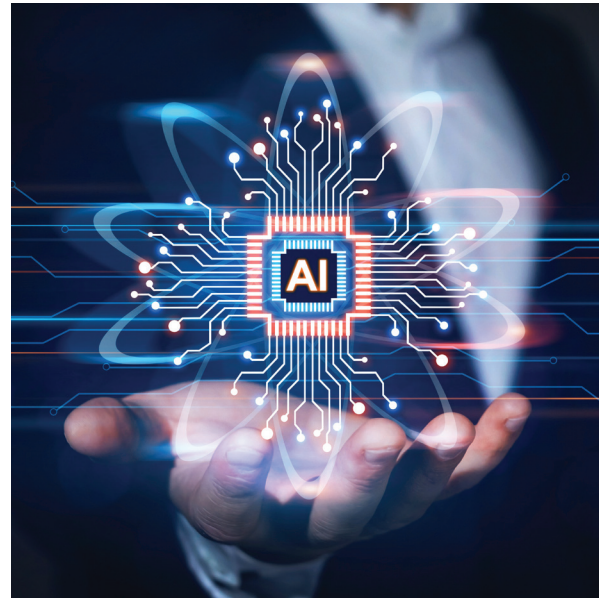
- **Operational—Fast Deployment:** Ready to identify anomalies, detect attacks, and create baselines from day one.
- **AI and ML Capabilities:** Ensure the NDR solution leverages advanced AI and ML algorithms for accurate threat detection.
- **Integration with Existing Systems:** Assess how well the NDR solution integrates with your existing security infrastructure.
- **Network Visibility:** Verify that the NDR solution provides comprehensive visibility across your entire network, including cloud environments, on-premises infrastructure, and IoT devices.

Reporting Capabilities:

- **Real-Time Alerts:** Ensure the NDR solution provides real-time alerts for suspicious activity.
- **Detailed Reports:** Evaluate the quality and depth of the reports that are generated by the NDR solution.
- **Customization:** Assess the ability to customize reports and dashboards to meet your specific needs.

Customization Options:

- **Flexibility:** Determine if the NDR solution can be customized to fit your organization's unique requirements.
- **Integration with Other Tools:** Evaluate the ability to integrate NDR with other security tools, such as Security Information & Event Management (SIEM) or Endpoint Detection and Response (EDR).



Data Residency:

- **Data Storage and Access:** Understand where your data will be stored and who will have access to it.
- **Compliance:** Ensure the NDR solution complies with relevant data privacy regulations.

Service Level Objectives (SLO):

- **Response Times:** Understand the vendor's response times for security incidents.
- **SLOs:** Review the vendor's SLOs to ensure they meet your expectations.

Onboarding Process:

- **Timeframe:** Inquire about the onboarding process and the estimated timeline for its implementation.
- **Support:** Ask about the level of support that is provided during and after onboarding.

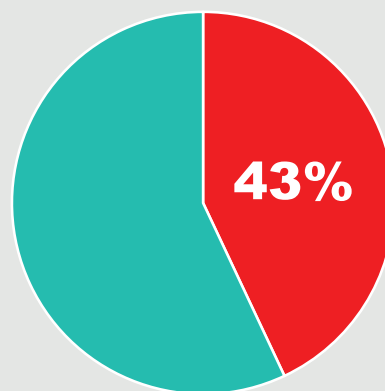
Partnerships:

- **Vendor Relationships:** Understand the vendor's partnerships with other technology providers.
- **Integration Capabilities:** Assess the ability of the NDR solution to integrate with other security tools.

Pricing Model:

- **Cost Structure:** Understand the pricing model and its associated costs.
- **Value Proposition:** Evaluate the value that is provided by the NDR solution in relation to the cost.

By carefully considering these factors, you can select an NDR solution that best meets your organization's needs and helps protect your network from cyber threats.



In two-in-five businesses (43%), some parts of their IoT infrastructure are yet to have any protection.

NDR Buyer's Checklist

- Deployment Method and Operational Availability
- Advanced Threat Detection: Ability to protect against modern threats, especially those that evade traditional signature-based detection
- Behavioral Analysis: Capable of analyzing network behaviors to identify suspicious activities, even if they do not match any known signatures (zero days)
- Real-Time Detection: Detects and responds to threats when they happen; 24/7 capabilities to support your team
- Cloud and Hybrid Environments: Supports both cloud and hybrid environments to ensure complete visibility
- Integration: Integrates seamlessly with existing security tools, like SIEM, EDR, firewalls, etc.
- AI and ML: AI is necessary to improve threat detection and incident response times
- Full Network Visibility: Solution can see all traffic, including to and from IoT devices
- Behavior Baseline: Can establish a baseline of normal network activity and identify deviations that could indicate malicious activity

What to Expect – NDR Operations

Deployment

Customers often highlight ease of deployment as a key advantage of NDR solutions. To ensure a seamless experience in your environment, consider the following:

- **Timeframe:** Your vendor should be able to provide a precise deployment timeline, taking into consideration the solution's wide coverage area.
- **Flexibility:** NDR solutions typically do not require physical hardware agents, enabling deployment across physical, virtual, and cloud environments. Additionally, they should integrate seamlessly with your existing security infrastructure.
- **Shared Responsibility:** Leading NDR vendors offer managed services, allowing you to either augment or outsource security operations. This can be beneficial as it provides access to dedicated platform experts.

Management and Reporting

In today's evolving threat landscape, ease of management and reporting is crucial. Organizations with limited resources or complex, hybrid infrastructures should prioritize AI-driven NDR solutions.

- **Simplified Insights:** AI can streamline the learning process by providing pre-defined views that offer a comprehensive overview of risks across all domains.
- **Intuitive Dashboards:** Teams should be able to easily access and understand relevant views and reports. This functionality is essential for both Security Operations Center (SOC) teams and key stakeholders who need a clear picture of risks and detection decisions.
- **Automated Maintenance:** Some NDR solutions require constant tuning of its analytics and rules. AI-driven technology, supported by expert services, can eliminate the need for manual intervention by continuously baselining normal activity and detecting abnormal behaviors.

User Experience

The effectiveness of an NDR solution lies in its ability to enhance your team's threat detection and response capabilities. Key considerations include:

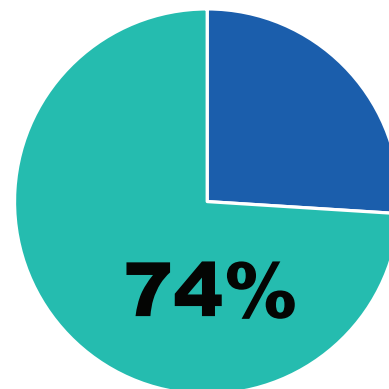
- **Signal Quality:** A powerful NDR solution should focus on identifying attacker Tactics, Techniques, and Procedures (TTPs) throughout the cyber kill chain. It should also prioritize relevant threats by triaging detection patterns unique to your environment, reducing alert noise. Additionally, the ability to categorize threats by severity and impact is essential for analysts to prioritize critical incidents.
- **Intuitive Interface:** The NDR's user interface should be designed to provide analysts with quick and easy access to information. This includes the ability to attribute threats to compromised accounts and users, hunt for threats across attack surfaces, and conduct investigations with context and forensics within the NDR platform.
- **Automated Response:** Understanding how an NDR can automate many manual response and investigation tasks is crucial. Additionally, knowing the available countermeasures for response actions and system remediation will provide insights into the effectiveness of the NDR's response capabilities.

Partnering with Hughes: A Unique Approach to NDR

Hughes Network Systems offers a distinctive approach to NDR, differentiating itself from its competitors in several key areas:

- **Deep-Rooted Cybersecurity Expertise:** With decades of experience in the cybersecurity industry, Hughes possesses a wealth of knowledge and expertise that allows us to provide unparalleled network security solutions.
- **Comprehensive Security Suite:** Hughes offers a comprehensive suite of security services—including NDR, MDR, and EDR—providing a holistic approach to protecting your network.
- **Customer-Centric Focus:** We prioritize our customers' needs and tailor our solutions to meet their specific requirements. Our dedicated team of experts works closely with clients to ensure their complete satisfaction.

- **Innovative Technology:** Hughes invests in cutting-edge technologies to stay ahead of evolving threats. Our NDR solution leverages advanced AI, ML, and behavioral analytics to provide superior threat detection and response capabilities.
- **Global Reach and Local Expertise:** As a global leader in network services, Hughes has a global presence with local experts who understand the unique challenges faced by businesses in different regions.
- **Strong Partnerships:** Hughes has strategic partnerships with leading technology providers, enabling us to offer a comprehensive range of security solutions and services.



According to a survey by SenseON, 74% of SOC teams utilize NDR tools.

Conclusion

NDR solutions offer comprehensive coverage and visibility across your expanding attack surface, providing unmatched signal clarity and intelligent control. AI is a powerful asset in this context, helping teams better understand attacker behavior throughout the cyber kill chain, analyze threats, and prioritize critical incidents. This allows analysts to focus their time on the most important tasks and gain insights that traditional tools cannot provide.

While the specific requirements for threat detection and response may vary between organizations, many teams that have deployed NDR solutions report significant benefits. These include improved SOC analyst efficiency, reduced Mean Time to Detect (MTD), and fewer data breaches.

By carefully considering the information presented in this guide and the accompanying questions, you can identify the NDR vendors that best align with your organization's unique needs and provide the coverage, clarity, and control necessary to protect your assets.

**To request a free demo of NDR services, contact us here:
www.hughes.com/ndr**