Progress® Flowmon®

Network Detection and Response (NDR) Buyer's Guide

BUYER'S GUIDE

This buyer's guide provides a robust Network Detection and Response (NDR) market overview. It also showcases key features to consider in an NDR solution and critical considerations for selecting the right platform to enhance your organization's security posture.

Introduction

As cyberthreats become increasingly sophisticated, traditional security solutions such as firewalls, antivirus programs and intrusion detection systems (IDS) aren't enough to protect enterprise networks. Cybercriminals are adept at evading perimeter defenses and moving laterally within the network, undetected for extended periods. Organizations require advanced solutions that provide continuous monitoring, detect anomalies, and respond to network-based threats in real time.

**Find Out More:
Analysts Share Their 2025
Cybersecurity Predictions**

The Network Detection and Response (NDR) market is experiencing significant growth, driven by the increasing sophistication of cyber threats and the need for advanced security solutions. In 2024, the global average cost of a data breach reached $4.88 million, marking a 10% increase from the previous year and the highest total ever recorded. This escalation underscores the urgency for organizations to adopt robust cybersecurity solutions.

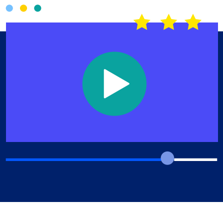
In 2024, it took organizations an average of 204 days to identify a breach and an additional 73 days to contain it, totaling a breach lifecycle of 277 days. This prolonged detection and response period significantly contributes to the overall cost of breaches.

NDR solutions play a critical role in addressing this challenge by providing continuous monitoring and analysis of network traffic to detect and respond to anomalies and potential threats. The market for NDR is expanding rapidly, with projections indicating a compound annual growth rate (CAGR) of approximately 13.7% from 2024 to 2033, potentially reaching $10.2 billion by 2033.

NDR: The Next Frontier in Proactive Network Security

NDR is an advanced cybersecurity solution that detects and responds to network-based threats that may otherwise go unnoticed by traditional security solutions. NDR helps organizations provide timely responses to mitigate threats by leveraging machine learning, advanced analytics and non-signature-based detection methods to identify suspicious behavior across the network while monitoring internal and external communications.

Watch Webinar:
Network Detection and Response Explained



Why NDR Is a Game-Changer in Threat Detection and Incident Response

- **Advanced Threat Detection:**
  Uncover threats that traditional security tools often miss, such as lateral movement, insider threats, zero-day and ransomware.

- **Real-Time Visibility:**
  Gain real-time network traffic analytics, giving security teams full visibility into internal (east-west) and external (north-south) traffic.

- **Behavioral Analysis:**
  Leverage behavioral analytics and machine learning to establish a baseline of normal network activity and identify anomalies that may indicate a potential threat.

- **Rapid Incident Response:**
  Enable automated response capabilities, such as blocking malicious IPs or isolating compromised devices, reducing the time it takes to mitigate an attack.

- **Detection of Encrypted Traffic:**
  Analyze encrypted traffic that is often overlooked by traditional security tools and ensure that threats hiding behind encryption are detected and mitigated.

- **Improved Incident Investigation:**
  Help security teams investigate incidents efficiently with contextual data including information about affected devices, users, severity and more.

- **Integration with Other Security Tools:**
  Integrate seamlessly with other security solutions like SIEM, SOAR and EDR, enhancing the overall security ecosystem and erasing blind spots.

- **Compliance Support:**
  Provide more secure network monitoring, visibility, alerts, and reports to maintain compliance with industry regulations (e.g., GDPR, NIS2, HIPAA).

- **Scalable for Growing Networks:**
  Scale easily to accommodate organizations of any size, from small enterprises to large corporations with complex, hybrid or multi-cloud infrastructures.

- **Reduced Costs:**
  Detect threats earlier in the attack lifecycle to reduce the financial impact of data breaches, including recovery costs, legal fees and reputational damage.

- **Proactive Security:**
  Shift your security posture from reactive to proactive, enabling you to detect and respond to threats before they cause significant harm to the organization.

> Security and risk management leaders should reprioritize NDR as a key provider of AI analytics in the context of more automated security operation assistants.
>
> *Source: Gartner Market guide for NDR 2024*

NDR Deployment Recommendations

- **Start Small:**
  Begin with detecting abnormal behaviors and providing investigation capabilities for post-breach activities. This initial focus helps avoid overwhelming security teams and allows for the gradual expansion of NDR's capabilities across different network segments.

- **Evaluate Behavior-Based Detection:**
  Identify how behavior-based detection can augment the ability of your Security Operations Center (SOC) to respond faster and more accurately to incidents. This is especially important as NDR platforms increasingly rely on machine learning and behavioral analytics to detect threats.

- **Compare NDR Vendors Using Rationalized Metrics:**
  Evaluate solutions based on rationalized metrics such as detection accuracy, false positive rates and incident response times. Assess how each platform will positively impact your threat detection and response effectiveness.

- **Roll Out Automated Responses Gradually:**
  While automated responses can greatly enhance security, they should be implemented progressively. First, maintain your NDR system's accuracy is fine-tuned to reduce false positives. Gradually introduce automated responses based on the Service Level Agreements (SLAs) for your organization's response times.

- **Conduct a Proof of Value (PoV):**
  Before fully deploying an NDR solution, consider conducting a Proof of Value (PoV) or pilot test to assess its effectiveness in your network environment. This confirms that the selected solution meets your organization's specific needs and security requirements.

Make Your Case for Management

When presenting the value of an NDR solution to leadership, it's essential to highlight how the investment strengthens security while delivering significant cost savings and operational efficiencies.

01. Price to Value

An effective NDR solution can drive substantial reductions in both financial and time-related costs, ultimately providing a high return on investment. Key areas where these savings can be measured include:

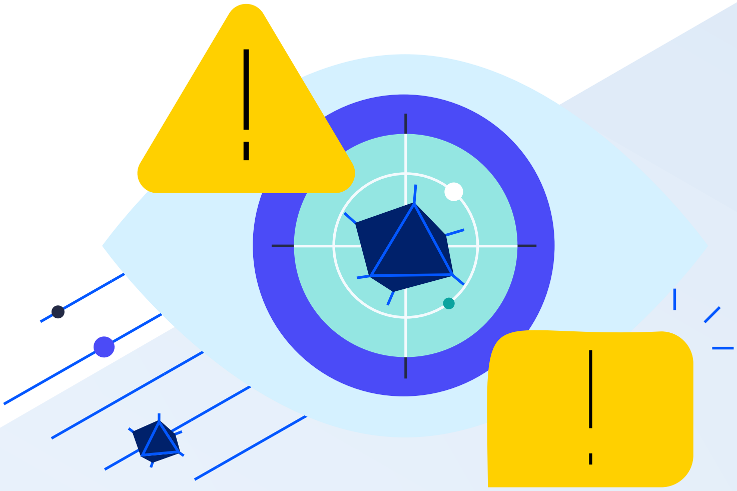
- **Reducing incident response time** and minimizing the duration of security events.
- **Estimating the prevention of costly data breaches** before they escalate.
- **Improving operational efficiency** in security processes and workflows.
- **Identifying savings** from consolidating multiple security tools into one solution.
- **Calculating time-to-value** and projecting **return on investment (ROI)** over time.

02. Total Cost of Ownership (TCO)

When evaluating an NDR solution's total cost of ownership, it's important to look beyond the initial purchase price. Consider the long-term costs associated with deployment, maintenance and operational efficiency, and how they align with your organization's overall security budget.

Key components of TCO include:

- **Initial Setup and Licensing Costs:** Include the costs associated with purchasing the solution, including hardware, software and any licensing fees.
- **Ongoing Maintenance and Subscription Fees:** Consider the recurring costs for updates, patches and renewals and any subscription fees for cloud-based solutions.
- **Integration and Deployment Costs:** Account for the time and resources needed to integrate the NDR solution into your existing security ecosystem, including personnel training and potential consultant fees.
- **Operational Overhead:** Evaluate the cost of managing the solution over time, including administrative effort, support costs and any additional staffing requirements.
- **Upgrades and Scalability:** Consider any future costs related to scaling the solution as your organization grows, including expanding capacity and upgrading to advanced features.
- **Opportunity Cost:** Assess the potential cost savings from tool consolidation and improved efficiency, factoring in both direct and indirect benefits of streamlined operations.



Checklist for Evaluating NDR Solutions

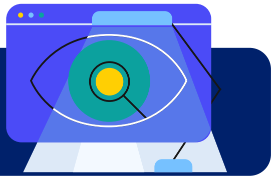
This checklist will guide you through any NDR solution must-have's essential features and capabilities, making your evaluation process clear and straightforward.

Core Capability	Check (✓) When Evaluated
Real-Time Network Visibility (Internal and External Traffic)	
AI, Machine Learning and Behavioral Analytics	
Anomaly Detection (Behavior-Based)	
Encrypted Traffic Analysis	
Automated Response Capabilities (e.g., Blocking, Isolation)	
Seamless Integration with SIEM and SOAR	
Low False Positive Rate	
Incident Investigation and Contextual Data	
Retrospective Analysis and Forensics	
Scalability for Growing Infrastructure (Cloud/Hybrid/On-Premises)	
Compliance and Reporting Features	
Ease of Deployment and Management	
Vendor Support and Training Resources	

Make the Right Choice: Unlock Advanced Flowmon Threat Detection and Response

The cutting-edge Flowmon Network Detection and Response (NDR) solution empowers organizations to gain real-time visibility into network traffic, detect sophisticated threats and respond swiftly to mitigate risks. Designed to enhance network security in both traditional and modern infrastructures (cloud, hybrid and on-premises), the Flowmon solution delivers AI-powered detection and advanced analytics to uncover hidden attacks that traditional security tools often miss.

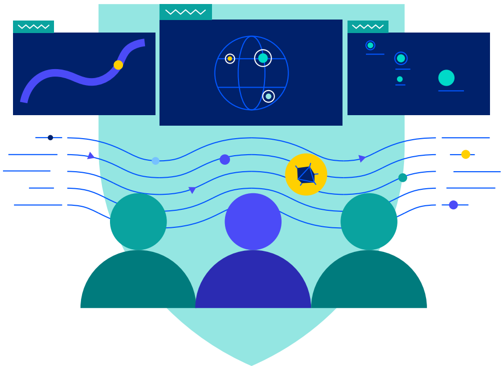
EXPLORE FLOWMON PLATFORM



Empower Your Security Team

Whether defending against ransomware, insider threats, zero-day exploits or lateral movement, Flowmon security helps IT teams stay ahead of evolving cyberthreats.

- **Minimize Breach Impact -** Detect and contain threats in real-time to limit breach damage and help prevent escalation.
- **Efficient Threat Hunting -** Use AI/ML and behavioral analytics to proactively identify and investigate advanced threats.
- **Faster Incident Response -** Automate response actions to quickly isolate compromised devices and block malicious traffic.
- **Enhanced Visibility -** Gain full network visibility across both internal and external traffic to spot hidden threats.



Start Your Journey Today

Take the first step toward strengthening your network security and see the Flowmon solution in action.
Request Free Trial

About Progress

Progress (Nasdaq: PRGS) empowers organizations to achieve transformational success in the face of disruptive change. Our software enables our customers to develop, deploy and manage responsible AI-powered applications and experiences with agility and ease. Customers get a trusted provider in Progress, with the products, expertise and vision they need to succeed. Over 4 million developers and technologists at hundreds of thousands of enterprises depend on Progress. Learn more at www.progress.com

Progress

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA 01803, USA
Tel: +1-800-477-6473

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
progress_sw_