Global Network Detection And Response Market To Expand At 10% CAGR During The Forecast Period

The Business Research Company's Network Detection And Response Market Report 2026 – Market Size, Trends, And Global Forecast 2026-2035

The Business Research Company

LONDON, GREATER LONDON, UNITED KINGDOM, July 3, 2026 /EINPresswire.com/ -- "The network detection and response sector has become increasingly vital as organizations seek to protect their digital environments from evolving cyber threats. With cyberattacks growing in both frequency and sophistication, this market is experiencing rapid development, driven by technological advances and shifting security needs.

Network Detection and Response Market Size and Growth Outlook
The network detection and response market has seen substantial expansion in recent years. It is projected to increase from $4.18 billion in 2025 to $4.59 billion in 2026, representing a compound annual growth rate (CAGR) of 9.7%. This earlier surge has been fueled by factors such as the rising number of network-based cyberattacks, limited visibility into lateral network traffic, the continued use of signature-based intrusion detection systems, the growing complexity of enterprise digital infrastructures, and the shortcomings of traditional security tools in providing real-time threat detection.

Download a free sample of the network detection and response market report: https://www.thebusinessresearchcompany.com/sample_request?id=59117747&type=smp&utm_source=EINPresswire&utm_medium=Paid&utm_campaign=Jun_PR

Looking ahead, the market is anticipated to grow even more robustly, reaching $6.71 billion by 2030 with a CAGR of 10.0%. Key drivers for this forecast include the increasing adoption of AI-powered cybersecurity tools, the expansion of hybrid and multi-cloud setups, a heightened need for integrating real-time threat intelligence, broader implementation of zero trust security models, and the escalation in the sophistication of advanced persistent threats (APT). Emerging trends shaping this period involve AI-driven behavioral anomaly detection for immediate threat

identification, machine learning approaches to analyze encrypted traffic uncovering hidden dangers, integration of zero trust architectures with NDR platforms, cloud-native NDR deployments enhancing security across hybrid and multi-cloud environments, and the convergence of extended detection and response (XDR) with network security analytics.

Understanding Network Detection and Response Technology
Network detection and response (NDR) refers to a cybersecurity strategy focused on continuous monitoring and thorough analysis of network traffic to spot unusual or malicious activities inside an organizational network. It leverages methods such as behavioral analytics, machine learning, and threat intelligence to detect anomalies, including sophisticated threats that often evade more traditional security measures. This proactive detection enables faster identification and containment of security risks.

View the full network detection and response market report:
https://www.thebusinessresearchcompany.com/report/network-detection-and-response-market-report?utm_source=EINPresswire&utm_medium=Paid&utm_campaign=Jun_PR

Key Factors Driving Network Detection and Response Market Expansion
One of the primary forces propelling the network detection and response market is the rising occurrence of advanced cyberattacks. These attacks are complex, persistent, and use tactics like ransomware, zero-day exploits, phishing campaigns, and coordinated intrusions to circumvent conventional security defenses and breach organizational networks. The surge in such attacks is influenced by factors including rapid digital transformation, increased cloud adoption, and intensified geopolitical cyber activities. As threats become more persistent and intricate, organizations require cutting-edge security solutions capable of continuous monitoring and real-time threat detection. NDR technologies meet this demand by analyzing network behavior, flagging anomalies, and facilitating swift threat response to prevent escalation.

For example, in October 2025, the European Union Agency for Cybersecurity (ENISA) reported in its Threat Landscape 2025 that between July 2024 and June 2025, there were 4,875 cybersecurity incidents, with ransomware, phishing, and vulnerability exploits being the most common attack methods. This data highlights the growing challenge organizations face and underscores the importance of advanced NDR solutions in combating cyber threats.

Regional Leadership and Market Dynamics in Network Detection and Response
In 2025, North America held the largest share of the network detection and response market. Meanwhile, the Asia-Pacific region is expected to experience the fastest growth during the forecast period. The market analysis includes key regions such as Asia-Pacific, Southeast Asia, Western Europe, Eastern Europe, North America, South America, and the Middle East and Africa, providing a comprehensive view of global trends and opportunities within this evolving cybersecurity domain.

Our latest 2026 market reports provide expanded strategic and visual intelligence with market

attractiveness scoring and analysis, total addressable market (TAM) analysis, company scoring matrix graphics and tables, Excel-based forecasting dashboards, market hotspots infographics, key technologies and future trend analysis, together with updated graphics and tables.

Speak With Our Expert:
Saumya Sahay
Americas +1 310-496-7795
Asia +44 7882 955267 & +91 8897263534
Europe +44 7882 955267
Email: marketing@tbrc.info

The Business Research Company - www.thebusinessresearchcompany.com

Follow Us On:
• LinkedIn: https://in.linkedin.com/company/the-business-research-company"

Oliver Guirdham
The Business Research Company
+44 7882 955267
info@tbrc.info
Visit us on social media:
LinkedIn
Facebook
X
