Magic Quadrant for Network Detection and Response

18 May 2026 - ID G00836320 - 32 min read

By Thomas Lintemuth, Charanpal Bhogal, and 1 more

Network detection and response platforms continuously monitor traffic for anomalies, suspicious patterns and threat indicators, and they complement other threat detection solutions. CIOs and CISOs must make informed decisions about NDR solutions, which are evolving to offer broader threat detection.

Market Definition/Description

Gartner defines network detection and response (NDR) as products that detect abnormal network behaviors by applying behavioral analytics to network traffic data. NDR products continuously analyze raw network packets or traffic metadata within internal networks (east-west) and between internal and external networks (north-south). They include automated responses, such as host containment or traffic blocking, implemented directly or through integration with other cybersecurity products. Vendors deliver NDR as hardware or software appliances for sensors, with some supporting IaaS environments. Management and orchestration consoles are available as software or SaaS.

Organizations rely on NDR to detect and contain postbreach activities such as ransomware, insider threats and lateral movements. NDR complements other technologies that primarily trigger alerts based on rules and signatures by building heuristic models of normal network behavior and detecting anomalies.

Security teams commonly use NDR as a complementary detection and response technology within a broader set of security operations center (SOC) tools. These include security orchestration, automation and response (SOAR), security information and event

management (SIEM), endpoint detection and response (EDR), and other detection technologies.

Mandatory Features

NDR must:

- Deliver physical or virtual sensors in form factors compatible with on-premises and cloud networks to analyze raw network packet traffic or traffic flows, and monitor both north-south (perimeter) and east-west (lateral) traffic.
- Model normal network traffic and highlight unusual activity that falls outside established baselines.
- Provide detection based on behavioral techniques (non-signature-based detection), including machine learning (ML) and advanced analytics, to detect network anomalies.
- Aggregate individual alerts into structured incidents to facilitate threat investigation and enable automatic or manual response to malicious network activity.
- Include traditional detection techniques, such as intrusion detection and prevention system (IDPS) signatures, rule-based heuristics, and threshold-based alerts.
- Automate responses, such as host containment or traffic blocking, either directly or through integration with other cybersecurity products.
- Detect threats using intelligence feeds from internal or external sources.

Optional Features

Optional capabilities for this market include:

- Operating in-line and supporting use cases such as “virtual patching.”
- Monitoring and analyzing traffic in IaaS environments.
- Providing SaaS API connectors to analyze events and user activities.
- Offering log ingestion, investigation and response capabilities that enable SOC analysts to use the NDR console as the primary facility for operational duties and threat hunting, replacing alternative platforms such as SIEM or extended detection and response (XDR).

- Enriching metadata during collection or event analysis.
- Performing retroactive and forensics analysis using network packet flow data and scalable full-packet capture (PCAP) with long-term data retention.
- Utilizing AI-based search assistants to accelerate threat hunting and deliver actionable insights.
- Integrating natively with EDR and SIEM platforms.
- Maintaining a low false-positive rate after initial tuning to provide trustworthy insights and support automated response use cases.

Magic Quadrant

Figure 1: Magic Quadrant for Network Detection and Response

Gartner

Vendor Strengths and Cautions

Arista Networks

Arista Networks is a Niche Player in this Magic Quadrant. Arista NDR is most frequently seen bundled with the vendor's core network switches for a unified infrastructure and security approach. Arista Networks is headquartered in Santa Clara, California; its operations are mostly focused in North America and Western Europe, and the vendor primarily targets customers in the healthcare and media/entertainment industries.

Arista Networks plans to enhance its generative AI (GenAI) capabilities by integrating an agentic AI layer into CloudVision. This will use ChatGPT's large language models (LLMs)

to provide conversational troubleshooting, autonomous intent identification and policy analysis.

Arista Networks declined requests for supplemental information or to review the draft contents of this document. Gartner's analysis is therefore based on other credible sources.

Strengths

- **Product:** Arista NDR offers ease of deployment when deployed in a network that uses Arista Networks' switches, leveraging the native integration between the two.
- **Customer experience:** Customer support is handled across its multiple geographic locations by experienced engineers who are able to assist quickly.
- **Overall viability:** Arista Networks is cash-flow positive with a strong increase in overall sales that can continue to fund the entity.

Cautions

- **Market understanding:** Arista Networks believes its UI is a strength, as it provides more flexibility in working with the product. However, customers have reported that the interface can be cumbersome for analysts to use compared with other offerings.
- **Vertical strategy:** Arista Networks does not support specific verticals in the market. Customers will need to customize the product according to the requirements of their vertical.
- **Marketing strategy:** Arista Networks does not appear to be gaining traction in the NDR market. Gartner clients infrequently inquire about Arista Networks' NDR products.

Corelight

Corelight is a Visionary in this Magic Quadrant. Corelight's Open NDR product is based on the open-source product Zeek, with proprietary extensions to add value. The vendor is headquartered in San Francisco, California; its operations are mostly focused in North America, and its clients tend to be in the public and finance sectors.

Corelight plans to add embedded edge monitoring, enhance detection of evasive threats, and add network performance monitoring to improve its product. The vendor's

longer-term goal is to make network evidence the ground truth for the AI-enabled security operations center (SOC).

Strengths

- **Vertical strategy:** Corelight is adding capabilities for specific markets including energy, healthcare and service providers that cover advanced cyber-physical systems (CPS) and Internet of Things (IoT) detection, and focusing on regulatory compliance.
- **Sales execution pricing:** Corelight provides transparent pricing based on network traffic throughput that is easy to understand and budget, with no hidden fees or data caps.
- **Offering strategy:** All customers receive a free, dedicated, localized technical account manager support to assist with deployment, operationalization and ongoing value creation.

Cautions

- **Product:** Open NDR provides less information on assets that it discovers on the network than most products in the NDR market.
- **Customer experience:** Corelight maintains a limited number of analysts in its support centers outside of North America.
- **Geographic strategy:** Corelight has put forth limited strategies to significantly increase its global deployments. Customers outside of North America likely will find other vendors more represented in their markets.

Darktrace

Darktrace is a Leader in this Magic Quadrant. Its NDR, Darktrace/NETWORK, focuses on providing advanced threat detection and autonomous response capabilities by leveraging its core Self-Learning AI and Cyber AI Analyst. Darktrace is headquartered in Cambridge, U.K.; its operations are focused in North America and Europe, with clients spread across industries including financial services, manufacturing and utilities.

Darktrace's roadmap includes extending its composite and multilayered AI architectures to new use cases, and enhancing the combination of network and other cybersecurity with its wider platform and through third-party integrations.

Strengths

- **Vertical strategy:** The vendor offers thorough coverage across a broad swath of industries, with specific updates for numerous verticals.
- **Geographic strategy:** Darktrace delivers strong customer experience and support through regional sales personnel and regional offices across 29 countries around the world.
- **Innovation:** The vendor continues to develop ways to utilize supervised and unsupervised machine learning. For example, DIGEST, a proprietary machine learning model, is trained on over 1 million incidents to determine whether an incident will continue and become more dangerous.

Cautions

- **Product:** Gartner clients report that it is not unusual for Darktrace's NDR to require additional manual tuning despite using self-learning AI to assist with baselining and autotuning.
- **Offering strategy:** Darktrace has increased its emphasis on go-to-market investments and updated distribution strategies; Gartner believes this emphasis has influenced how some prospective customers assess Darktrace.
- **Operations:** A customer-facing global service status page is not currently available for Darktrace's SaaS services.

ExtraHop

ExtraHop is a Leader in this Magic Quadrant. Its RevealX product is focused on detecting threats with NDR while providing network intelligence with NPM in a single platform. ExtraHop is headquartered in Seattle, Washington; its primary operations are in North America. Its clients tend to be in the financial services, federal government and critical infrastructure industries.

The vendor strives to deliver multiple capabilities using a single platform and an appliance that can support ingesting capacities up to 400 Gbps. It plans to develop AI agents that work in collaboration with products like Microsoft Defender, Microsoft Sentinel, Google SecOps and CrowdStrike to enhance threat detection in a hybrid deployment.

Strengths

- **Product:** ExtraHop RevealX analyzes more than 5,000 data points across OSI Layers 2-7, spanning users, devices, files, applications, flows, sessions and dependency graphs. It collects this telemetry across encrypted and unencrypted traffic at scale.
- **Market understanding:** ExtraHop adds value by displacing current incumbent technologies such as packet capture and intrusion detection system (IDS), delivering a product that offers these capabilities in addition to NPM and NDR.
- **Market responsiveness:** ExtraHop was first to market with native decryption of Transport Layer Security (TLS) and a leader in bringing 100 Gbps ingestion appliances to market. Both of these capabilities are critical for large organizations and useful for organizations of all sizes.

Cautions

- **Operations:** Senior-level leadership turnover has continued through the beginning of 2025, with a transition of the CEO position causing questions about vision.
- Offering strategy: CrowdStrike is the only EDR vendor for which ExtraHop provides out-of-the-box bidirectional integration. Customers using any other EDR vendor will require manual API integration.
- Customer experience: ExtraHop deploys its SaaS status page behind a customer page that requires an account to log in. In addition, the status page has limited information and no drill-down capabilities.

Fortinet

Fortinet is a Niche Player in this Magic Quadrant. The vendor markets two products for NDR — FortiNDR Cloud is the product covered in this research. Fortinet is headquartered in Sunnyvale, California; its operations are geographically diversified and it sells into most verticals.

Fortinet recently updated the deep packet inspection (DPI) engine on its sensors to detect more than 6,000 applications. Fortinet plans to add sensor-level filtering to optimize the capture of network traffic, especially helping small and midsize business (SMB) customers.

Strengths

- **Customer experience:** Fortinet operates a global network of sales offices, each staffed with local support engineers. Customers have multiple options for product support.
- **Operations:** A customer-facing global service status page provides detailed information on services, with drill-down capabilities for additional information.
- **Overall viability:** Fortinet has a diverse set of products covering the networking and network security markets. The company is cash-flow positive, with good sales providing evidence of long-term stability.

Cautions

- **Market understanding:** Fortinet markets two distinct products with different feature sets, diluting the vendor's attention and, possibly, commitment to and investment in each product.
- **Sales execution:** Fortinet's largest sales opportunity generally comes from existing customers. Fortinet commands more than 20% in the firewall market, yet it is rarely seen in the NDR market.
- **Geographic strategy:** Fortinet has not disclosed a specific strategy to sell its NDR product globally. Customers are likely to be introduced only if they are interested in other Fortinet products.

Gatewatcher

Gatewatcher is a Niche Player in this Magic Quadrant. Its product, NDR Platform, is focused on providing an easy-to-use experience through its Decision Center interface. Gatewatcher is headquartered in Paris, France; its two largest markets are Europe and the Middle East, and its customers tend to be in finance, healthcare and manufacturing.

Gatewatcher is developing new technology in passive asset discovery and profiling that will improve asset visibility without relying on active scanning or endpoint agents. This will be helpful in general NDR activities as well as discovery of algorithmic protocols.

Strengths

- **Offering strategy:** The vendor reduces false positives through a focused tuning-support program that is run in Month 1 and Month 6 after purchase.

- **Vertical strategy:** The vendor sells to a broad range of industries, with no vertical representing more than 16% of the customer base.
- **Overall viability:** Gatewatcher invests in marketing and research and development efforts in a manner consistent with growing the business in a profitable manner.

Cautions

- **Geographic strategy:** Gatewatcher has no North American partners to facilitate purchase and deployment. Potential customers in the region must deploy on their own.
- **Customer experience:** Customer support is delivered primarily in English and French from a single support center in France.
- **Operations:** While not generally available during the evaluation period, Gatewatcher has since released a customer-facing global service status for its SaaS services, which was not assessed as part of this Magic Quadrant. Users seeking advanced monitoring capabilities may find its offering insufficient based on the evaluated version of the product.

Jizô AI

Jizô AI is a Niche Player in this Magic Quadrant. Its NDR product, Jizô AI, is geared toward customers that prefer a self-contained deployment option. Jizô AI is headquartered in Paris, France; its two largest markets are in Europe and the Middle East, and it has the largest number of customers in healthcare, manufacturing and government.

Jizô AI has worked to incorporate foundational capabilities into its product over the last several years. The vendor plans to introduce new capabilities including attack path prediction and continuous machine language model retraining.

Strengths

- **Overall viability:** Jizô AI has strong investment in R&D and continues to be cash-flow positive, with a positive operating margin.
- **Vertical strategy:** Jizô AI maintains a focus on the CPS vertical, demonstrated by the addition of ICS/SCADA and medical device capabilities as well as the typical IT capabilities of NDR.

- **Innovation:** Jizô AI plans to bring attack-path prediction capabilities to Jizô AI. This would allow customers to take advantage of proactive defense capabilities that can autonomously generate and test threat hypotheses.

Cautions

- **Geographic strategy:** Jizô AI has few distributors outside of Europe and the Middle East. Customers outside of those regions may have difficulty finding added sales and technical support.
- **Offering strategy:** Jizô AI doesn't offer sensors or an agent option deployed in the network or into the assets. This technical choice can complicate a deployment in a very distributed environment.
- **Customer experience:** Jizô AI has a limited number of geographically concentrated support staff to assist with technical support calls. While the company is closely monitoring support times, some delays could be observed during busy periods.

LinkShadow

LinkShadow is a Visionary in this Magic Quadrant. Its LinkShadow NDR product supports organizations that don't want to share data with a SaaS service. LinkShadow is headquartered in Athens, Georgia; its largest markets are Europe and the Middle East, with government clients representing its leading market segment.

LinkShadow is developing AI SOC agent capability, among other things, to automate tasks like threat intelligence lookups, hash checks and firewall policy checks. This will facilitate quicker information responses from L1 analysts.

Strengths

- **Product:** Storage nodes can be added to LinkShadow NDR to retain PCAP/metadata for more than three years, with tamper-proof audit trails for compliance.
- **Overall viability:** The vendor shows a steady increase in sales, with continued investment in marketing and research and development.
- **Offering strategy:** LinkShadow's strategy is to integrate with partners in adjacent markets. Integration with Nozomi is available in the CPS segment, and LinkShadow is one of the few vendors that can integrate with Alibaba.

Cautions

- **Customer experience:** Customer support is available primarily in English, with some regions supporting Polish, German, Arabic, Hindi or Urdu.
- **Vertical strategy:** The vendor's vertical focus is narrow, with customers in the government vertical representing over 40% of its sales. The vendor will have less expertise to offer in other verticals.
- **Market responsiveness:** LinkShadow plans to focus on addressing a disjointed market in its marketing. This will impact the vendor's ability to focus on product weaknesses or marketing concerns.

NetWitness

NetWitness is a Visionary in this Magic Quadrant. Its NetWitness NDS product is focused on large, complex global organizations that require a full-feature product that includes strong packet capture. NetWitness is headquartered in Boston, Massachusetts; its operations are mostly focused in North America, and its clients tend to be in government, finance and utilities.

Since being acquired by PartnerOne in March 2025, NetWitness has allowed more autonomy versus previous ownership. New leadership at NetWitness includes a new CEO, chief revenue officer (CRO), chief customer officer (CCO), and chief product and technology officer (CPTO). Taken together, these changes seem to be reinvigorating the product.

Strengths

- **Market understanding:** NetWitness has developed a highly flexible and customizable platform that can be deployed in many environments. This allows it to be applicable across many client use cases and requirements.
- **Vertical strategy:** NetWitness sells to a broad range of industries, with no vertical representing more than 16% of customers.
- **Customer experience:** Extremely low turnover among the vendor's account managers creates stability for customers.

Cautions

- **Market responsiveness:** NetWitness was slower to incorporate IDS and operational technology (OT) observability than others in the market, but these capabilities are being addressed.
- **Product strategy:** NetWitness is not designed for SMB environments. Clients with smaller networks will find that other vendors are better positioned to address their needs.
- **Operations:** A customer-facing global service status page is common in this market, but not currently available for NetWitness' SaaS services.

Stellar Cyber

Stellar Cyber is a Niche Player in this Magic Quadrant. Its NDR offering is an NDR-specific licensing option of its unified SecOps platform. Stellar Cyber is headquartered in San Jose, California; its operations are mostly focused in North America and the Asia/Pacific region, and its customers tend to be in the midsize sector, including a high concentration of managed security service provider (MSSP) organizations.

Stellar Cyber is looking to add just-in-time packet analysis, which can avoid always-on inspection costs, and to add systematic noise reduction through prealert checks and contextual tuning.

Strengths

- **Customer experience:** Stellar Cyber offers comprehensive two-tier support with follow-up every six hours until the ticket is resolved. The vendor also reports an excellent time to resolution of 1.5 days for support cases.
- **Market understanding:** Stellar Cyber is focused on human-augmented workflows over opaque, fully autonomous responses, which some vendors are proposing. This aligns with Gartner's view of how NDR will best assist SOC teams.
- **Product:** Stellar Cyber's product offers deployment flexibility that includes the ability for true multitenant operations.

Cautions

- **Innovation:** Stellar Cyber's most cited innovations all are geared toward improving the SOC workflow. This single focus will impact the development of new capabilities.

- **Operations:** Stellar Cyber does not maintain a status page for its SaaS services. Instead, it relies on the infrastructure as a service (IaaS) provider to provide IaaS uptime statistics.
- **Vertical strategy:** The MSSP market, in which third-party organizations provide outsourced management and monitoring of security devices and systems, represents nearly half of Stellar Cyber's sales. Organizations that prefer a direct-sell or reseller model may evaluate this according to their procurement preference.

Trellix

Trellix is a Visionary in this Magic Quadrant. Its NDR product is showing maturity as it has brought several product lines together, yet continues to be one of the few vendors in this market offering in-line deployments for intrusion prevention system (IPS) use cases. Trellix is headquartered in Frisco, Texas; its primary markets are North America and EMEA, while offering a global footprint. Its largest verticals are the critical infrastructure, government and financial sectors.

Trellix is working on expanding protocol awareness of specialized OT protocols with plans to implement additional behavioral models on this data. It also plans to embed complete identity threat detection and response capabilities within NDR.

Strengths

- **Customer experience:** Trellix offers comprehensive three-tier support and has a good time to resolution of three days for support cases.
- **Marketing execution:** Trellix offers a tiered pricing strategy that encourages customers to upgrade from their existing "Essential" products to Core and Enterprise NDR packages. This allows customers to start with lower-cost options and upgrade as required.
- **Innovation:** Trellix's Attack Path Discovery maps assets, associate vulnerability data and risk scores and draws the network topology based on the likely path an adversary can take.

Cautions

- **Sales execution pricing:** Trellix support and maintenance is charged at a higher percentage of total cost than other vendors.

- **Sales strategy:** Trellix does not include basic services such as assisted tuning or certification in the initial cost of its product.
- **Geographic strategy:** Trellix has limited implementation partners in South America, the Middle East or Africa. Customers in these regions should perform due diligence.

Vectra AI

Vectra AI is a Leader in this Magic Quadrant. Its Vectra AI Platform detects malicious activity without the use of agents and provides continuous visibility across IT and OT networks. Vectra AI is headquartered in San Jose, California; it supports sales across all geographic regions, and its three largest market segments are finance, manufacturing and government.

Vectra AI uses adaptive security across networks and identity for the enterprise. Beyond detecting attacks, Vectra AI plans to provide unified observability, proactive defense and compliance evidence across hybrid networks, the IaaS control plane and identity activity.

Strengths

- **Market understanding:** Vectra AI identifies important market trends, including nonhuman identities, the importance of CPS security, incorporating NDR in a proactive defense, and using NDR to enable postquantum readiness.
- **Sales strategy:** Vectra AI has a thorough certification program to train its channel partners to enhance sales and support for its customers.
- **Vertical industry strategy:** Vectra AI has balanced coverage across the spectrum of industries tracked by Gartner.

Cautions

- **Customer experience:** Vectra AI has reported account management turnover that is higher than average for this market. This increases the risk of disjointed contract renewals or escalation of technical issues.
- **Product:** Vectra AI supports current and previous versions of software. Organizations must determine whether they will allow automatic updates to help ensure that the system is on a supported version of software.

- **Offering strategy:** Vectra AI provides minimal initial assistance in architecting the system to capture all network traffic, though partners are able to provide services to verify that the system is capturing the relevant traffic.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Fortinet
- Jizô AI
- LinkShadow

Dropped

- Threatbook
- Trend Micro

Inclusion and Exclusion Criteria

To qualify for inclusion, each provider must:

- Have a network detection and response product that is generally available by 31 October 2025.
- Be primarily marketed as a vendor’s product or service rather than delivered via a managed service provider.
- Have the ability to ingest data via network flows and packet capture

- Have the ability to ingest data at a rate not less than 40 Gbps for network packets

The NDR vendor must also demonstrate scale relevant to enterprise-class organizations. At least two of the following three criteria must be met:

- Have generated $20 million in revenue from the evaluated NDR product between 1 January 2025 and 31 December 2025
- As of 31 December 2025, have at least 70 enterprise customers (each with over 5,000 seats)
- Have at least 4 million devices under paid support as of 31 October 2025

The NDR vendor must also demonstrate relevance to global organizations through:

- Gartner's receiving strong evidence that no more than 85% of its revenue/sales is from a single region (North America, EMEA or Asia/Pacific)

Evaluation Criteria

Ability to Execute

Product/Service

Key areas assessed include administration, platform, threat detection, asset discovery, incident response and CPS security.

Overall Viability (Business Unit, Financial, Strategy, Organization): Financials

Vendor financial health and business unit relevance is evaluated, and the likelihood that investment will continue across multiple areas (e.g., product, marketing, support) to enhance the product and build market share.

Sales Execution/Pricing

Key areas evaluated include growth of the business, how pricing and licensing is offered to customers, consumability, evidence of the ability to build and maintain strong relationships with end customers, and the value of the product for its cost.

Market Responsiveness and Track Record

This criterion assesses the vendor's track record, compared with competitors, in delivering effective and customer-aligned capabilities. It analyzes the demonstrated ability to address the changing market and changing customer demands while overcoming their limitations.

Marketing Execution

We assess whether messaging clarity is free of hype, as well as consider its efficiency and transparency. We also assess investments in marketing and whether these investments are driving interest in the vendor.

Customer Experience

We assess and consider all aspects of the customer experience, including pre- and postsales experience, availability and quality of documentation, technical support and end-user satisfaction with the product.

Operations

We consider whether the vendor sets and meets SLAs and has a stable workforce. Quality of codebase and company evolution are also considered.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High

Evaluation Criteria	*Weighting*
Operations	Medium

Source: Gartner (May 2026)

Completeness of Vision

Market Understanding

This criterion includes the ability to understand and address client needs, as well as like competitors for the vendor's product both now and in the future. Understanding of how the market is changing is considered.

Marketing Strategy

We evaluate whether the vendor shows novel and effective approaches to communicating and differentiating, as well as forward-looking investments in its marketing program and messaging.

Sales Strategy

This criterion assesses how the vendor intends to build out channels, deal strategies, pricing and sales organization, and how these align with customer demands and needs.

Offering (Product) Strategy

We evaluate whether the vendor is delivering in a timely fashion the new features that are relevant to the market and to end users' current and emerging needs.

Business Model

This criterion assesses the design, logic and execution of the organization's business proposition to achieve continued success.

Vertical/Industry Strategy

This criterion includes offering capabilities specific to an industry or a market segment.

Innovation

We evaluate the key planned future innovations across technology, sales, partnerships and features, and how the vendor will bring unique value to the market to address end-user challenges most effectively. We assess whether these innovations provide customer value and are “game changers” to the market.

Geographic Strategy

This criterion looks at the vendor’s delivery, sales and marketing strategies for different geographies, top initiatives for expanding market share, regional compliance localization capabilities and language support. It also assesses the vendor’s plans to increase presence, staff count, customers and channel partners to fill gaps in its geographic coverage.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (May 2026)

Quadrant Descriptions

Leaders

Leaders are vendors with strong momentum in sales and mind share. They have track records of delivering well-integrated NDR products with advanced functionality, as well as a product strategy that aligns with the market trend for providing easy-to-use advanced features and making business investments for the future. Leaders have effective sales and distribution channels for their entire product portfolios, a well-diversified vertical and geographic strategy, and a vision for how NDR products are positioned within the context of organizations' wider security operations.

Challengers

Challengers offer NDR components that may not be tightly integrated or may lack sophisticated features and alignment with the market's direction. They may compensate for this with a strong sales channel, strategic relationships or extensive market visibility. Challengers are often late to introduce new features and lack a complete, unified product strategy. Challengers appeal largely to clients that have established strategic relationships with them.

Visionaries

Visionaries are distinguished by technical and/or product innovation, but lack either the track record of execution and the high visibility of Leaders, or corporate resources such as strong sales channels and strategic relationships. Buyers should expect solid products from Visionaries, but be wary of strategic reliance on them and monitor their viability closely. Visionaries often represent good candidates for acquisition by other vendors. Thus, Visionaries' customers run a slightly higher risk of business disruption.

Niche Players

Niche Players typically offer solid products in terms of one or more discrete NDR capabilities, but are focused on fewer areas (such as technical capabilities, geographic support or vertical industries). Additionally, Niche Players lack the market presence and resources of Challengers and the forward-looking vision and market alignment of Visionaries. They merit attention from the types of buyers on which they focus.

Context

Network detection and response platforms see anomalous traffic, understand the underlying threat behavior and explain the scope of the impact. Beyond ingesting network packets or traffic flow, NDR must ingest and correlate third-party telemetry. This ecosystem includes data from EDR, ITDR, IaaS flow logs, zero-trust network access (ZTNA) network packets and SWG flow logs. NDR products include automated responses such as host containment or traffic blocking, directly or through integration with other cybersecurity tools. NDR can be delivered as a combination of hardware and software appliances for sensors, some with IaaS support.

Data from Gartner surveys and client inquiries indicates that NDR buyers cover the full gamut of user organizations, from small organizations with a nascent security program to very large organizations with an established security program. Most vendors have a preferred set of markets to which they cater.

The NDR market will continue to grow over the next decade, evolving from a niche security product to a critical one. As user behaviors are increasingly obfuscated by encryption and attackers are increasingly hiding their activities in “living off the land” techniques, NDR will be critical in identifying both insider threats and threats that are launched from internally compromised hosts.

Market Overview

Network detection and response (NDR) is the premier option for monitoring network traffic for on-premises locations. In addition, vendors have built solid options for monitoring remote users and IaaS traffic. Increasing monitoring is also available for SaaS environments. Nearly all vendors are increasing their applicability in the CPS/OT market by adding technology to support OT protocols for visibility and detection of anomalous activity.

NDR global market revenue continues to grow by double-digit percentages, registering a year-over-year increase of 17% in 2025 (see **Market Share: Enterprise Network Equipment, Worldwide, 4Q25**). Vendors in the NDR market run the gamut from small startups to some of the largest network security providers. The “sweet spot” is vendors with a primary focus on NDR that have been in the market for more than five years.

The foundation of NDR is detecting malicious activity in network traffic. Yet vendors are quickly adding key capabilities that make NDR much more valuable to the overall market. Key capabilities include signature-based detections and asset visibility.

As part of detection, most vendors provide security analysts with granular details to facilitate forensic analysis. Organizations use this forensic data to enable threat hunting, identify attack paths, and provide long-term use and storage for regulatory compliance.

Other NDR vendors focus heavily on empowering an automated SOC, centering their monitoring dashboards on the explainability of a security incident, streamlining their incident response workflow and optionally sending alerts with context to the SIEM. Organizations with smaller security teams immediately benefit from the improved detection capabilities and are likely to take advantage of automated responses and other mitigations. These easy-to-use, polished products tend to provide a quick return on investment and require little human interaction.

Recent Trends in the NDR Market

Gartner sees that many NDR offerings have expanded to capture new categories of events and to analyze additional traffic patterns. These include:

- **Third-party integrations:** Integrations are critical for thorough analysis and correlation with the primary integration EDR. Integration with identity providers is a strong second, followed by ingesting logs from secure email and IaaS platforms, and integration with SaaS security service edge (SSE) providers.
- **Standard detection techniques:** NDR supports traditional intrusion prevention signatures, decryption on appliance, and including more sophisticated encrypted traffic analysis, such as is provided with JA4.
- **Managed NDR:** Co-management services on top of the NDR product and subscriptions — ranging from proactive notifications from the vendors in case of an incident to co-managed threat detection — are now common across multiple vendors. Many of these single technology management services are increasingly useful to small but growing teams.
- **Evolving architecture:** Newer vendors, looking to accelerate their product development, provide ML analytics only in the cloud. This is limiting, as some use cases require air-gapped deployments.

- **Visibility:** NDR provides immediate identification of all hosts that are connected and communicating on the network. The number of attributes available per device varies, but most vendors can provide a basic asset inventory of devices seen communicating.
- **CPS use cases:** All vendors are enhancing the OT protocols that they can observe and analyze. Some vendors have dedicated products for CPS/OT.
- **AI analysis:** Vendors are expanding the use of AI to predict whether a given incident will expand and become more dangerous. In addition, we see DSLM technology being utilized to assist with local, relevant analysis.
- **MCP analysis:** Vendors are including an MCP server in the product to allow identity and analysis of dangerous MCP traffic.
- **Larger sensor:** Vendors have pushed the starting point of traffic probes to ingest data at the rate of 40 Gbps with the strongest vendors providing 100 Gbps with roadmaps to 400 Gbps.
- **Attack path prediction:** Some vendors can provide a diagram showing the likely hops an attacker will take as they attempt to move laterally through the network.

Vendor Differentiation

Gartner sees three types of vendors in the market:

- Leading NDR vendors build their NDR products with strong NDR foundations. These include ingesting network packets and supplementing with network flows, applying ML analysis, detecting malicious activity and generating an alert that can be actioned directly in the vendor's console.
- The second type of vendor builds a product with a strong detection engine that leverages custom network probes, but is geared toward more general SOC use cases. It prioritizes connections to many third-party security products and looks for threats in general across these sources.
- The third type is the large, established information security vendor that offers NDR as a small component of its overall platform. This vendor likely repurposes legacy technology into what it now markets as NDR.

⊕ Evaluation Criteria Definitions