Gartner Licensed for Distribution

Magic Quadrant pour la détection et la réponse réseau

29 mai 2025 - ID G00808217 - 31 min de lecture

Par Thomas Lintemuth , Esraa ElTahawy , **et 3 autres**

Les plateformes de détection et de réponse réseau surveillent en permanence le trafic à la recherche d'anomalies, de tendances suspectes et d'indicateurs de menace, et complètent d'autres solutions de détection des menaces. Les DSI et les RSSI peuvent s'appuyer sur ces recherches pour prendre des décisions éclairées concernant le NDR, qui évolue vers une détection plus large des menaces.

Définition/Description du marché

Il s'agit de la première version du Magic Quadrant pour la détection et la réponse réseau. Il remplace le **Guide du marché pour la détection et la réponse réseau** .

Les produits de détection et de réponse réseau (NDR) détectent les comportements anormaux du système en appliquant l'analyse comportementale aux données de trafic réseau. Ils analysent en continu les paquets réseau bruts ou les métadonnées de trafic au sein des réseaux internes (est-ouest) et entre les réseaux internes et externes (nord-sud). Les produits NDR incluent des réponses automatisées, telles que le confinement d'hôte ou le blocage du trafic, directement ou via l'intégration avec d'autres outils de cybersécurité. NDR peut être fourni sous la forme d'une combinaison d'appliances matérielles et logicielles pour les capteurs, certaines prenant en charge l'IaaS. Les consoles de gestion et d'orchestration peuvent être logicielles ou SaaS.

Les organisations s'appuient sur NDR pour détecter et contenir les activités post-violation, telles que les rançongiciels, les menaces internes et les mouvements latéraux. NDR complète d'autres technologies qui déclenchent principalement des alertes basées sur des règles et des signatures, en construisant des modèles heuristiques du comportement normal du réseau et en détectant les anomalies. NDR est couramment utilisé comme technologie complémentaire de détection et de réponse au sein d'un arsenal plus large d' outils de centre d'opérations de sécurité (SOC) . Ceux-ci incluent l'orchestration, l'automatisation et la réponse de la sécurité (SOAR), la gestion des informations et des événements de sécurité (SIEM), la détection et la réponse des terminaux (EDR) et d'autres technologies de détection, mais aussi des services tels que la détection et la réponse gérées (MDR).

Caractéristiques obligatoires

Le NDR doit :

- Fournissez, via des capteurs physiques ou virtuels, des facteurs de forme compatibles avec les réseaux locaux et cloud pour analyser le trafic brut des paquets réseau ou les flux de trafic (par exemple, les informations de flux IP). Le NDR doit également surveiller le trafic nord-sud (lorsqu'il traverse le périmètre) et le trafic est-ouest (lorsqu'il se déplace latéralement sur le réseau).

- Model normal network traffic and highlight unusual traffic activity that falls outside the normal range. NDR must also provide detection based on behavioral techniques (non-signature-based detection), including machine learning (ML) and advanced analytics that detect network anomalies.

- Aggregate individual alerts into structured incidents to facilitate threat investigation, and provide automatic or manual response capabilities to react to the detection of malicious network traffic.

- Include traditional detection techniques, such as intrusion detection and prevention system (IDPS) signatures, rule-based heuristics or threshold-based alerts

- Automate responses, such as host containment or traffic blocking, directly or through integration with other cybersecurity tools.

- Detect threats using Intelligence feeds whether internally or externally sourced.

Common Features

Optional capabilities for this market include:

- Monitoring and analyzing traffic in IaaS environments

- SaaS API connectors to analyze events and user activities

- Log ingestion, investigation and response capabilities that enable SOC analysts to use the NDR console as the primary facility to perform operational duties and threat hunting in lieu of alternative platforms such as SIEM or extended detection and response (XDR)

- Metadata enrichment at the time of collection or during event analysis

- The ability to perform retroactive and forensics analysis based on netflow data, but also using scalable full-packet capture (PCAP) with long-term data retention

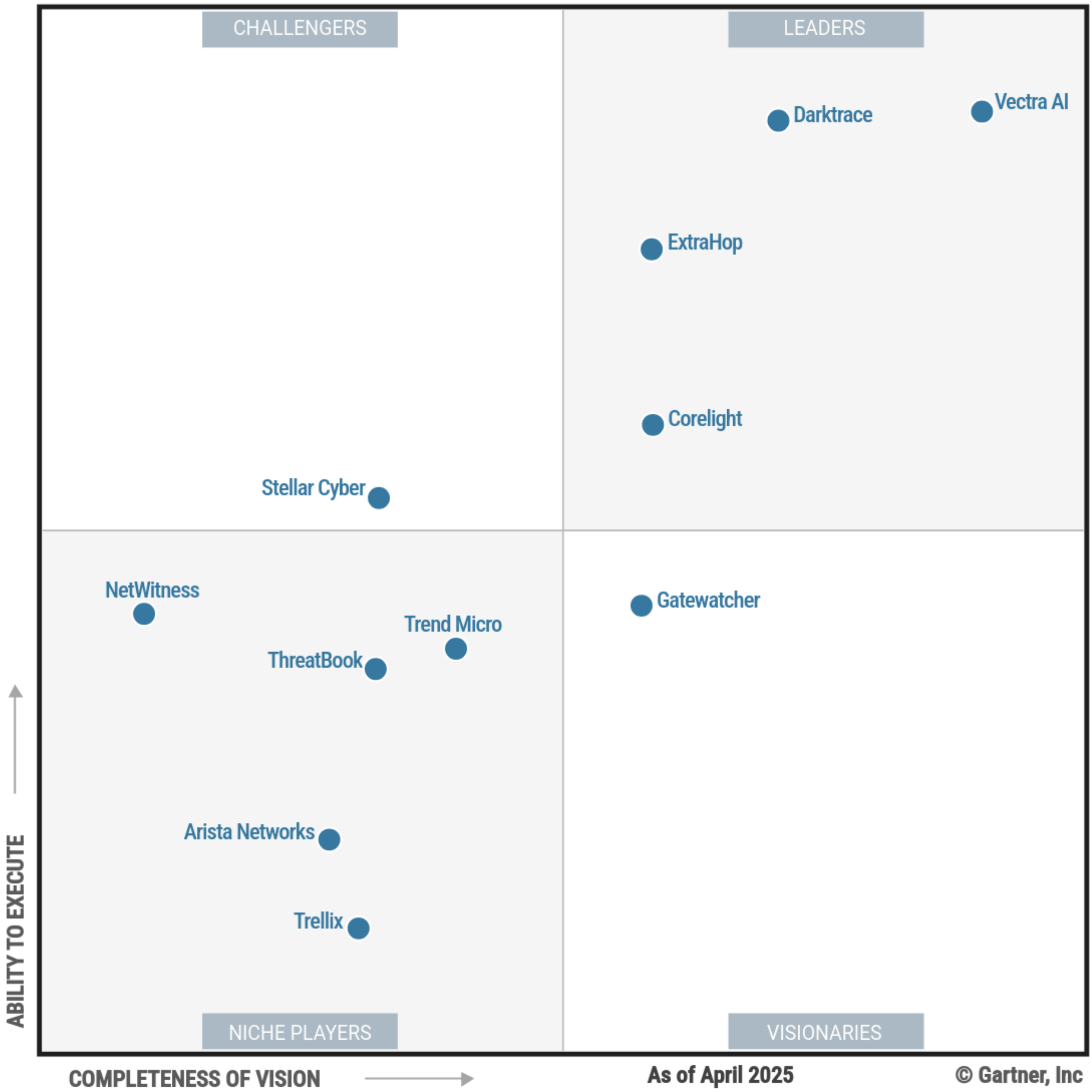
- AI-based search assistants enabling accelerated threat hunting and providing actionable insights

- Native integration with EDR and SIEM

- Maintaining a low false-positive rate, after initial tuning, to become a trustable source of insight and support automated response use cases

Magic Quadrant

Figure 1: Magic Quadrant for Network Detection and Response



Vendor Strengths and Cautions

Arista Networks

Arista Networks is a Niche Player in this Magic Quadrant. Arista NDR is focused on coupling its network detection and response (NDR) with core network switches for a unified infrastructure and security approach. Arista's operations are mostly focused in North America and Western Europe and its top two verticals targeted are healthcare and media/entertainment industries.

Arista is developing encrypted traffic analysis capabilities. When deployed in conjunction with Arista switches, no external test access ports (TAPs) or switch port analyzers (SPANs) are required to ingest network packets into the platform.

Strengths

- **Product:** The product supports encrypted traffic analysis for non-cleartext traffic to provide expansive security. Preconfigured appliances accelerate deployments.
- **Customer experience:** Customers report that the vendor responds quickly to problems, resulting in a lower mean time to resolution and a faster return to steady state.
- **Overall viability:** Arista is a large services provider with many products that appeals to a broad base of customers. Our assessment shows stable growth and higher investment in R&D for NDR, relative to the market.

Cautions

- **Market understanding:** Although Arista provides tight integration with its switches, market feedback indicates that NDR customers do not prioritize this capability. Arista NDR is network vendor agnostic, but buyers must assess the capabilities of Arista's NDR if they do not want to use Arista switches.
- **Vertical strategy:** Arista does not have a program to support specific verticals in the market. Customers seeking NDR tailored to their specific verticals for focused threat detection may not get the product they seek.
- **Market responsiveness:** Gartner sees the vendor focus first on how its NDR product supports platform integration, rather than integration with third-party and mixed vendor environments to support a broader addressable market.

Corelight

Corelight is a Leader in this Magic Quadrant. Corelight's Open NDR product is focused on comprehensive threat detection across on-premises, industrial control systems (ICS)/operational technology (OT) and multicloud environments. The vendor's operations are mostly focused in North America, and its clients tend to be in the public and finance sectors.

Corelight plans to expand its offering by improving the detection of living-off-the-land techniques and integrating advancements in generative AI (GenAI) and large language models (LLMs) to automate and streamline security operations. It also plans to expand into more markets, including the mid- and lower enterprise segments.

Strengths

- **Market responsiveness:** Based on customer feedback, Corelight prioritizes and is continuously delivering new features and updates. Corelight has transitioned from being primarily an on-premises intrusion detection system (IDS) solution to a hybrid NDR offering.

- **Product:** Various sensors are available, including those that can ingest 100 Gbps, while Corelight's Smart PCAP feature enables efficient capture and storage of only the most relevant network packets.

- **Market understanding:** Corelight understands and supports the need to deploy across major cloud service providers (CSPs), expanding its addressable market.

Cautions

- **Vertical strategy:** Historically, Corelight has focused more on the U.S. government and less on other verticals. Potential customers outside the U.S. government should keep this in mind and validate that the threat detection content provided meets their needs.

- **Customer experience:** Gartner views Corelight's user interface (UI) as dated and not intuitive, especially for novice security analysts or those new to NDR.

- **Geographic strategy:** Corelight has few partners available to assist with procurement and deployment, especially outside the U.S. Buyers with in-country channel partner needs or requirements will need to work hard with Corelight to identify a channel partner.

Darktrace

Darktrace is a Leader in this Magic Quadrant. Its NDR, known as Darktrace / NETWORK, focuses on providing advanced threat detection and autonomous response capabilities by leveraging its core Self-Learning AI. Darktrace's largest regions for sales are North America and Europe, with its clients spread across many industries, including financial services, manufacturing and utilities.

Darktrace is looking to promote agentic and investigative AI for security operations center (SOC) workflow transformation to change the SOC dynamics with AI automating Level 1 and Level 2 analyst tasks. Darktrace is advancing its NDR product pushing NDR to take on more preventive and proactive security measures. These include proactive hardening of network security, redefining vulnerability management and prioritization, continuous threat exposure management (CTEM) and breach simulation.

Strengths

- **Product:** Darktrace has a user-friendly and powerful UI, including a large complex detection model library. In addition, all sales include an implementation service to ease the burden on customers to get the product up and running.
- **Market understanding:** Darktrace supports full functionality for air-gapped deployments, eliminating the need for cloud connectivity required by some NDR solutions. This is appealing to buyers with cyber physical systems (CPS) or classified environments.
- **Market responsiveness:** A strong program for collecting customer feedback and incorporating it to enhance the product shows the vendor listens to end users and helps keep the product roadmap fresh as the market evolves.

Cautions

- **Customer experience:** Darktrace's NDR product requires tuning during and after installation to reduce false positives. Based on client and customer feedback, the product is complex to manage in ongoing operations.
- **Operations:** Darktrace does not include a service-level agreement (SLA) in contracts outside the European Union (EU), making it difficult for clients to hold the vendor accountable.
- **Sales execution:** Darktrace prefers selling bundled offerings, rather than itemized proposals, which makes pricing complicated and difficult to understand.

ExtraHop

ExtraHop is a Leader in this Magic Quadrant. Its RevealX product is focused on detecting threats with NDR, while providing network intelligence with network performance monitoring (NPM) in a single platform. ExtraHop's operations are mostly focused in North America and its clients tend to be in the financial services, federal government or critical infrastructure industries.

The vendor is striving to deliver multitool capabilities with a single platform that combines NDR, NPM, IDS and forensics. Its focus is on identifying the attack surface by providing visibility into all assets on the network.

Strengths

- **Product:** ExtraHop RevealX provides patented decryption capability; offers lookback search and packet storage; and delivers an IDS engine for signature-based detection.
- **Market understanding:** ExtraHop delivers network performance, NDR functionality and network performance analysis for small and large networks, with network sensors supporting full line rate ingestion at 100 Gbps. Buyers can use one solution to manage their network health and detect threats, and they can do it across a wide spectrum of network sizes.
- **Market responsiveness:** ExtraHop has implemented GenAI assistant functionality that accepts natural language processing (NLP) to perform queries on network data and security events. This aligns with buyer expectations to reduce manual efforts with the help of AI features.

Cautions

- **Operations:** Senior-level leadership turnover has increased since ExtraHop moved to private ownership in July 2021. Prospective clients should investigate the strategic roadmap and vision of the company during purchasing decisions.
- **Geographic strategy:** ExtraHop has limited reseller options outside North America. Buyers must determine the importance of local sales and product support during the acquisition process.
- **Sales execution:** ExtraHop's proposals typically include a variety of options and products bundled together, making it difficult to determine the costs of specific components. This poses a challenge for customers seeking a customized product.

Gatewatcher

Gatewatcher is a Visionary in this Magic Quadrant. Its AIonIQ is focused on providing an easy-to-use experience through its GAIA technology. Gatewatcher's two largest markets are Europe and the Middle East, and its largest verticals are finance, healthcare and manufacturing.

Gatewatcher is working to produce more extensive asset and user inventory. It strives to analyze both IT and OT network traffic with the intent to identify shadow IT and expose external surface weaknesses.

Strengths

- **Overall viability:** Gatewatcher has a growing customer base, with a clear investment strategy for research and development balanced with sales. Gatewatcher's investment in GenAI functionality and automation align with market direction and will appeal to buyers with limited HR.
- **Vertical strategy:** Gatewatcher can leverage threat intelligence to provide specific rule sets for specific industries.
- **Marketing strategy:** Gatewatcher is targeting the correct buyer personas with a straightforward and simple message on the importance of NDR in the enterprise.

Cautions

- **Geographic strategy:** Gatewatcher has no North or South American partners to facilitate purchase and implementation. This leaves potential customers in those regions to deploy on their own and use virtual support.
- **Customer experience:** Customer support is only available in English or French, and all support is based in France.
- **Marketing execution:** Gatewatcher has not effectively communicated its message to the broader market, reflected in the vendor showing up less frequently in third-party citations.

NetWitness

NetWitness is a Niche Player in this Magic Quadrant. Its Network product is focused on large, complex global organizations that require a full SOC and cybersecurity program. NetWitness's operations are mostly focused in North America, and its clients tend to be in government, finance and utilities.

PartnerOne acquired NetWitness in March 2025. Gartner has no current view on how this will affect the future of the product.

Strengths

- **Geographic strategy:** NetWitness's client base extends to nearly every major continent, illustrating its long-term presence in the NDR market.

- **Market responsiveness:** NetWitness has developed a formal customer feedback and feature request program for taking direct customer feedback on product enhancements and incorporating that feedback into product updates.

- **Product:** NetWitness has a robust and deep forensic capability that enables threat hunting and investigation. Buyers looking for full packet capture forensics and session replay capabilities will find these capabilities in NetWitness.

Cautions

- **Overall viability:** NetWitness's market focus is aligned with government and large enterprise segments that often have advanced users and senior security analysts. Buyers with small or inexperienced security staff may find the solution complex.

- **Customer experience:** The company maintains a smaller ongoing technical support team, which could impact support times going forward. Support is generally available in English, Japanese and Arabic, although other languages may be available on a specific analyst availability.

- **Product strategy:** NetWitness lags behind competitors with support for cloud and complex AI analytic detections or GenAI assistant features. This has forced NetWitness to play "catch-up" to meet hybrid environment needs and deliver AI assistant functionality as it grows in popularity.

Stellar Cyber

Stellar Cyber is a Challenger in this Magic Quadrant. Its NDR product is focused on providing numerous integrations with third parties to function as a central platform for ingesting security threats. Stellar Cyber's operations are mostly focused in North America and the Asia/Pacific region, and its clients tend to be in the midsize sector supporting the government, manufacturing and education segments.

Stellar Cyber is looking to enhance ingesting capabilities using webhooks going forward. Furthermore, it plans to enhance its GenAI by translating natural language questions into precise search queries.

Strengths

- **Operations:** Stellar Cyber is committed to customer success, with strong investment in onboarding and services. Buyers seeking high service delivery and implementation will find that Stellar Cyber stands apart from the NDR market with its offering.

- **Product strategy:** The company has a competitive upgrade program to help new customers migrate from competing products. This makes switching to Stellar Cyber more cost-effective and eases the pain of implementation.
- **Sales strategy:** Itemized proposals and multiyear contracts enable customers to choose the products they need, and to lock in costs full term without year-over-year increases.

Cautions

- **Marketing strategy:** Customers looking for an NDR product could easily miss Stellar Cyber as its marketing and capability focus is on the XDR market.
- **Vertical strategy:** With a focus on the midmarket, Stellar Cyber has limited capabilities for specific industries.
- **Product:** Stellar Cyber's largest sensor only allows ingestion of 10 Gbps of traffic. This will present a deployment challenge for networks with switching infrastructures utilizing multiple 10 Gbps interfaces or larger.

ThreatBook

ThreatBook is a Niche Player in this Magic Quadrant. Its Threat Detection Platform (TDP) is almost singularly focused on detecting threats, with no support for other common uses such as visibility. ThreatBook's operations are focused in the Asia/Pacific region, primarily on the Chinese mainland, and its clients tend to be in finance, education and manufacturing.

ThreatBook plans to grow its product by increasing detection functionality through the use of deception techniques, as well as agents that can be deployed to clients and servers. GenAI will continue to be enhanced to provide more natural language interaction, as well as automating reporting.

Strengths

- **Product:** Detection options include a native, integrated honeypot and an integrated sandbox to enhance the NDR offering.
- **Vertical strategy:** ThreatBook has a notable number of customers across a diverse set of industries, resulting in a broader market share appeal in the regions it targets.

- **Overall viability:** ThreatBook has a high customer renewal rate, and its customer base continues to grow.

Cautions

- **Marketing strategy:** ThreatBook's nearly singular focus on threat detection and response in messaging means there is much less priority on other NDR use cases such as visibility and forensics. This makes its NDR less appealing to organizations looking to satisfy multiple use cases.
- **Geographical strategy:** The vendor has a narrow regional focus. It focuses on midsize and larger enterprises in China and, to a much lesser degree, the Middle East.
- **Customer experience:** ThreatBook's UI is predominantly in Chinese, with some English views. Customers that need an NDR in other languages will need to assess usability in a proof of concept.

Trellix

Trellix is a Niche Player in this Magic Quadrant. Its NDR product builds on its successful IDS detections, adding AI behavioral detections to generate alerts. It is one of the few products in this market still offering in-line deployments for intrusion prevention system (IPS) use cases. Trellix's two primary markets are North America and Asia/Pacific, while offering a global footprint. Its clients tend to be from the government and financial sectors.

Trellix is working on a system to support rapid integration of third-party systems for event collection. In conjunction with this, it is working to use the Open Cybersecurity Schema Framework (OCSF) for event ingestion.

Strengths

- **Product:** The Trellix product delivers strong forensic analysis and search, and includes full IPS capabilities, with the ability to block malicious detections. This gives customers advanced protection directly in the NDR product without integration to take preventative action.
- **Market responsiveness:** Trellix provides specific product enhancements based on feedback from its Design Partner Program. This helps keep the product up to date as the market evolves.

- **Sales strategy:** A simplified pricing model aligns with market expectations, while maintaining value for enterprise customers.

Cautions

- **Sales execution:** Trellix faces challenges with NDR market recognition compared with pure-play vendors. This can be attributed to ownership changes, integration with other companies and previous company names.
- **Product:** Trellix does not offer a SaaS product, which limits its ability to address a part of the market as more companies transition to a hybrid infrastructure model.
- **Innovation:** Many recent product updates have delivered features that are common to the market. Customers may find that the Trellix product does not deliver features that are ahead of the market.

Trend Micro

Trend Micro is a Niche Player in this Magic Quadrant. Its Trend Vision One is focused on a platform approach to threat detection and response, primarily using its own point products while offering some integration with third-party products. Trend Micro's operations are geographically diversified, and its clients tend to be in the financial, government and telecommunication sectors.

Trend Micro is looking to increase the product openness to expand third-party integration. It plans to increase GenAI functionality to make installations faster and easier to accomplish, and to improve navigation and assistance in starting up.

Strengths

- **Product:** The Trend Vision One product offers an extensive threat intelligence library to assist in attribution and context, which is derived from Trend Micro's many other security product offerings, and provides strong visibility across the threat landscape.
- **Marketing strategy:** Trend Micro builds market awareness with strong first- and third-party events that educate its customers and inform the overall market.
- **Market understanding:** Trend Micro offers its NDR capability as a stand-alone product, which is also packaged with its Vision One platform to deliver a holistic solution. Buyers seeking NDR plus packaged adjacent threat detection and response capabilities will find Trend Micro aligns with their needs.

Cautions

- **Sales strategy:** Buyers that want on-premises NDR must confirm that the features they need are included in the stand-alone NDR product.
- **Product:** Trend Micro has limitations on full integration with third-party products, because of its Vision One platform focus. Buyers without a security orchestration, automation and response (SOAR) solution to broker integrations must assess how Trend Micro's NDR will integrate with their environment without the Vision One platform.
- **Customer experience:** Support is primarily available in English and Japanese, while support in other languages is based on the availability of specific support staff.

Vectra AI

Vectra AI is a Leader in this Magic Quadrant. Its Vectra AI Platform is focused on protecting networks from attacks, providing signal clarity, intelligent control and proactive network security posture management. Vectra AI's operations are geographically diversified, and its clients tend to be in finance, government and manufacturing.

Vectra AI plans to bring GenAI principles to the established AI models in use to build smaller, faster models for specific detections, triage and prioritization.

Strengths

- **Product:** Vectra AI's interface is mature, strong and easy to use, and its implementation of AI can assist with triage and prioritization of threats. This simplifies threat detection and response for customers.
- **Product strategy:** Vectra AI offers a program to help new customers migrate from competitors' products, providing organizations with the additional onboarding support needed to move quickly from one solution to another.
- **Sales strategy:** Vectra AI has created an NDR education program to overcome roadblocks specific to the NDR market, such as a lack of customer awareness. This helps customers understand the need for the product and how it fits into their security programs.

Cautions

- **Sales execution:** Vectra AI's customer retention is the lowest among NDR vendors in this research. Potential customers should ensure that Vectra AI can meet their NDR-specific needs.

- **Sales strategy:** Vectra AI does not sell directly, which can be a limitation for organizations that prefer direct dealings with the vendor.
- **Product strategy:** Vectra AI's product has been historically marketed as an XDR product. This may lead to confusion about what it delivers, how focused Vectra is on NDR and whether the company is trying to replace a SIEM.

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

As this is a new Magic Quadrant, no vendors were added.

Dropped

As this is a new Magic Quadrant, no vendors were dropped.

Inclusion and Exclusion Criteria

For Gartner clients, Magic Quadrant research identifies and then analyzes the most relevant providers and their products in a market. Gartner uses by default an upper limit of 20 providers to support the identification of the most relevant providers in a market. On some specific occasions, the upper limit may be extended by Methodologies where the intended research value to our clients might otherwise be diminished.

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, each provider must:

- Have a network detection and response (NDR) product that is generally available by 31 October 2024.
- Offer a stand-alone product that can be deployed without connecting to the Internet, sometimes referred to as “air-gapped.”
- Have at least 30 deployments in Amazon Web Services, Google Cloud Platform and Microsoft Azure.

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 $30 million in revenue from the evaluated NDR product between 1 January 2024 and 31 December 2024.
- As of 31 December 2024, have at least 150 enterprise customers (each with over 5,000 seats).
- Have at least four million devices under paid support as of 31 October 2024.

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

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

Lastly, the NDR vendor must rank among the top 15 organizations in Gartner’s Customer Interest Index for this Magic Quadrant. Data inputs used to calculate the Customer Interest Indicator for NDR included a balanced set of measures:

- Gartner end-user inquiry volume per vendor
- Gartner.com search data
- Gartner Peer Insights competitor mentions
- Google trends data
- Social media analysis

Evaluation Criteria

Ability to Execute

Product/Service

Key areas assessed include: administration, platform, threat detection, network discovery, incident response, cps security and threat hunting.

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 to be evaluated will 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

Messaging clarity free of hype, its efficiency and transparency will be critical. We will also assess investments in marketing, and if these investments are driving customer interest in the vendor.

Customer Experience

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

Operations

Setting and meeting SLAs, having a stable workforce, quality of codebase and company evolution will be considered.

Ability to Execute Evaluation Criteria

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

Source: Gartner (May 2025)

Completeness of Vision

Market Understanding

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

Marketing Strategy

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

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

This includes delivering new features that are relevant to the market and to end users' current and emerging needs, and are delivered in a timely fashion.

Business Model

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

Evaluates the key planned future innovations across technology, sales, partnerships and in features, and how the vendor will bring unique value to the market to address end-user challenges most effectively. We assess if 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

Evaluation Criteria	*Weighting*
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Medium
Innovation	High

Source: Gartner (May 2025)

Quadrant Descriptions

Leaders

Leaders are vendors with strong momentum in terms of sales and mind share. They have track records of delivering well-integrated NDR products with advanced functionality, as v as a product strategy that aligns with the market trend for providing easy-to-use advancec 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

NDR detects abnormal system behaviors by applying behavioral analytics to ingested data. 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 infrastructure as a service (IaaS) support.

Data from Gartner surveys and client inquiries indicates that most NDR buyers are from large to very large organizations with an established security program. More and more vendors, however, are seeing growing opportunities in expanding the market to the midsize buyer segment.

Gartner anticipates that the NDR market will grow over the next decade, evolving from a niche security product to a critical one. As user behaviours 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 are building solid options for monitoring remote users, IaaS and, to a limited extent, SaaS environments.

NDR global market revenue continues to grow by double-digit percentages, registering an increase of 18%, year over year (see **Market Share: Enterprise Network Equipment, Worldwide, 4Q24 Update**). Vendors in the NDR market run the gamut from small startup vendors to some of the largest information 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, some vendors allow security analysts to examine granular details to facilitate deep inspection of forensics. Organizations that have the resources, skills and time to work heavily with forensics appreciate this data to employ threat hunting, attack frameworks, and allow longer-term use and storage of network forensics telemetry. The flexibility of these NDR products comes at the expense of simplicity and ease of use.

Other NDR vendors focus heavily on the threat detection use case, centering their monitoring dashboards on the explainability of a security incident and streamlining their incident response workflow with as much automation as possible. 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 solutions tend to provide a quick return on investment and need less 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:** Integration with endpoint sensors, such as endpoint detection and response (EDR), ingesting logs from secure email platforms, integrating with identity providers and integration with SaaS security service edge (SSE) providers.

- **New detection techniques:** Support for more traditional signatures, decryption on appliance, more sophisticated encrypted traffic analysis and deception.

- **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 — is 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 machine learning (ML) analytics only in the cloud. This is limiting as some use cases require air-gapped deployments.

- **Visibilité :** Le NDR est couramment déployé dans les entreprises disposant de nombreuses sources d'informations de détection. Lorsqu'un signal non NDR indique une menace, les équipes SOC peuvent enrichir l'alerte avec les données fournies par le NDR.

- **Cas d'utilisation OT :** les réseaux IT et OT convergent. Les fournisseurs de NDR ont pris conscience de cette tendance et ajoutent des détections axées sur le matériel et les protocoles OT.

Différenciation des fournisseurs

Gartner distingue trois types de fournisseurs sur le marché :

- Les principaux fournisseurs de NDR construisent leurs produits NDR sur des bases solides. Celles-ci incluent : l'ingestion de données réseau (par paquets ou flux réseau), l'application d'analyses par apprentissage automatique, la détection des activités malveillantes et l'envoi d'alertes avec des options de réponse simples.

- Le deuxième type de fournisseur développe un produit doté d'un puissant moteur de détection qui ne se concentre pas sur le réseau. Il privilégie plutôt les connexions à de nombreux produits de sécurité tiers et recherche les menaces en général sur ces sources.

- Le troisième type est celui des grands fournisseurs de sécurité informatique bien établis qui proposent la NDR comme un petit composant de leur plateforme globale. Ce fournisseur réutilise probablement une technologie héritée pour la commercialiser sous le nom de NDR.

⊕ Définitions des critères d'évaluation

Gartner