Market Guide for Network Detection and Response

Published 29 March 2024 - ID G00784755 - 21 min read

By Analyst(s): Jeremy D'Hoinne, Thomas Lintemuth, Nahim Fazal, Charanpal Bhogal

Initiatives: Infrastructure Security; Build and Optimize Cybersecurity Programs; Security Operations

The network detection and response market continues to grow and expand to hybrid network scenarios with IaaS deployments. Security and risk management leaders should reprioritize NDR as a key provider of AI analytics in the context of more automated security operation assistants.

Overview

Key Findings

- Network detection and response (NDR) is commonly used as a complementary detection and response technology as part of a broader arsenal of security operations center (SOC) tools.
- The emergence of "AI-augmented" analytics overlays, in the form of SOC assistants, will benefit the NDR market as a useful source of insights for aggregated and summarized views.
- A handful of NDR vendors capture most of the attention in the market. Higher maturity organizations, often with more specialized detection use cases, often mix these well-known vendors with emerging local players in their shortlists.
- Most organizations value the response capabilities during their NDR provider evaluations, but only deploy very narrowly automated responses past the pilot phase.

Recommendations

To successfully integrate NDR capabilities, security and risk management leaders must:

- Start small. Implement NDR to detect abnormal behaviors and provide investigation capabilities for postbreach activity, extending incrementally across different types of networks.

- Identify how NDR's behavior-based detections, once tuned, might augment your SOC ability to respond to incidents faster and more accurately.
- Compare NDR vendors by defining rationalized metrics and evaluating how these NDR tools positively impact threat detection and incident response.
- Roll out automated response progressively, based on your existing incident response SLA for the type of incident and on the false positive rate of the detection engines.

Strategic Planning Assumptions

By 2029, more than 50% of incidents discovered by NDR technology will come from cloud network activity, up from less than 10% today.

By 2027, the implementation of automated responses to network anomaly detection will remain below 40% of the anomalies detected.

Market Definition

Network detection and response (NDR) products detect abnormal system behaviors by applying behavioral analytics to network traffic data. They continuously analyze raw network packets or traffic metadata within internal networks (east-west) and between internal and external networks (north-south). NDR products include automated responses, such as host containment (through integration) 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. Management and orchestration consoles can be software or SaaS.

Organizations rely on NDR to detect and contain postbreach activity 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. NDR is commonly used as a complementary detection and response technology as part of a broader arsenal of security operation 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, but also services such as managed detection and response (MDR).

NDR must:

- Deliver, via physical or virtual sensors, form factors compatible with on-premises and cloud networks to analyze raw network packet traffic or traffic flows (for example, IP flow information). NDR must also monitor north-south traffic (as it crosses the perimeter) and east-west traffic (as it moves laterally throughout the network).
- 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.

The standard capabilities for this market include:

- Monitoring and analyzing traffic in IaaS environments
- More traditional detection techniques, such as intrusion detection and prevention system (IDPS) signatures, rule-based heuristics and threshold-based alerts
- Alert aggregation of logical security incidents based on multiple factors, not just alert ID and repeated alerts through integration with other SOC tools for richer context
- Automated responses, such as host containment (through integration) or traffic blocking, directly or through integration with other cybersecurity tools
- A low false positive rate, after initial tuning, to become a trustable source of insight and support automated response use cases

Optional capabilities for this market include:

- 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)
- Transport Layer Security (TLS) traffic decryption

- 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

Market Description

Dozens of vendors claim to analyze network traffic (or flow records) and to detect anomalous activity on the network. To be competitive in shortlists, NDR products must provide:

- The ability to gather and baseline activity from raw traffic.
- Metadata enrichment at the time of collection or during event analysis.
- Deployment form factors compatible with on-premises and cloud networks with the ability to deploy their own sensors in the form of physical appliance or virtual machine.
- ML techniques to baseline normal activity and detect abnormal behaviors resulting from compromised assets or malicious insiders.
- Alert aggregation of logical security incidents based on multiple factors, not just alert ID and repeated alerts through integration with other SOC tools for richer context.
- Automated responses, such as host containment (through integration) or traffic blocking.
- A low false positive rate, after initial tuning, to become a trustable source of insights and support automated response use cases.

Technologies are generally excluded from prospective NDR shortlists when:

- They require a prerequisite component — for example, those that require a SIEM or firewall platform.
- They emphasize network forensics over detection functionality, primarily through the storage and analysis of PCAP data.
- They are specialized cyber-physical system (CPS) protection platforms.
- They work primarily on log analysis.

- The vendor/provider lacks market visibility for its NDR capabilities.

Depending on the size of the organization, NDR responsibility, once deployed, extends from the infrastructure to the SOC team, which is in charge of analyzing the alerts and handling the responses that are not automated.

Market Direction

NDR products will evolve into one, or a combination, of these technical platform scenarios:

1. **Hybrid network NDR:** This is the privileged evolution for stand-alone NDR providers. They expand their portfolio to cover new types of networks, often starting with operational technology (OT) and infrastructure as a service (IaaS). They embed in their NDR products new detection techniques to support these use cases. The primary detection telemetry will still come from the analysis of network traffic patterns, but could expand beyond that by adding other types of detection, such as security posture anomalies for cloud infrastructure.

2. **Network defense in depth:** Some NDR vendors integrate signature-based threat detection engines (e.g., Zeek, Suricata), traditionally components of intrusion detection and protection systems (IDPS). As they add more modules, they position the NDR appliance as a "second layer of defense," positioned behind the perimeter controls adding visibility on internal traffic (east-west).

3. **Extended detection and response (XDR):** NDR can contribute to XDR by bringing network event analytics into the mix. Gartner analysts continue to see that a majority of NDR evaluations are for stand-alone deployments today, but this could change in the future. However, by continuing to add other sources of telemetry, such as endpoint and identity and access management (IAM) integrations, NDR could also overlap more with the XDR market.

4. **Augmented NDR:** The emergence and accelerated adoption of large language model (LLM) features in security operation tools might disrupt some of the detection and response market dynamics. NDR provides network visibility, which offers some advantage when trying to offer incident summarization and could compete for being the analytics front end of choice.

For now, stand-alone NDR vendors provide a breadth of network analytics and efficacy not available with multifunction security platforms (SIEM, XDR). Longer term, for the NDR market to succeed, hybrid network NDR vendors must convince organizations with enough network attack surface to invest durably and keep NDR as a stand-alone product, or trust the NDR providers to also become a reasonably good analytics console.

Hybrid Network NDR

Most Gartner client calls on NDR continue to only include network detection use cases, with no or very limited automated response implementations. NDR providers continue to improve their detection capabilities and improve incident response workflows, highlighting the identified root causes of an incident. With this success and confidence, enterprises are experimenting with new NDR features and expanding their coverage to include areas of the network not initially exposed to NDR, especially to see all lateral movement between different types of infrastructure. These include:

1. **IaaS:** Applying a "follow the app" paradigm, NDR sensors are deployed closer to the server workloads, as most organizations now have server farms hosted on one or many of the IaaS platforms. Because the deployment constraints are different, NDR providers are more likely to leverage cloud-native flow analysis APIs and accept their limitations when compared to on-premises networks.

2. **IT/OT convergence:** Organizations engaged in an IT/OT convergence roadmap increasingly consider leveraging the same NDR provider to monitor IT and OT segments. Organizations continue to have stringent requirements when evaluating the technology for the OT networks (see Market Guide for CPS Protection Platforms).

3. **SaaS:** Stretching the definition of network monitoring to its thinnest, NDR providers leverage SaaS APIs to monitor user connectivity to SaaS services, with Microsoft 365 being the most popular example.

4. **Home networks:** A small subset of organizations express their intention to monitor home network connectivity for some key employees (e.g., executives, as well as staff in R&D and sensitive functions operated as "work from home"). To do so, they might deploy a small sensor, but because organizations rarely want to handle the potential legal complexity of monitoring personal networks, they also consider deploying a small software agent on corporate-owned laptops.

Network Defense in Depth

Re-establishing a practice from the early days of network detection and response — 10 years ago — some providers have re-added intrusion prevention system (IPS)-like modules, mixing threat intelligence and more traditional pattern matching to complement behavioral analysis. This creates a potential additional revenue stream for the providers, but also makes NDR a more comprehensive product, detecting a broader set of anomalies. This benefits organizations with smaller teams or fewer infrastructure security tools. This "defense in depth" scenario, leveraging an additional source of threat intelligence and signatures, has a stronger focus on north-south traffic, improving the ability to catch data exfiltration or command and control (C2) communication. This will primarily appeal to large security operation teams in search of a customizable and multipurpose network security sensor.

Conversely, adding intrusion detection system (IDS)-like signatures might negatively impact one of the expected benefits of NDR solutions: be a "turnkey" and "low noise" product, highlighting only critical anomalies.

XDR

NDR technology can contribute to XDR by detecting network-based anomalies and by adding and correlating these events in the centralized dashboard. Most XDR vendors have weak capabilities for native network analysis, leading to an increasing number of integrations with current NDR vendors (see Market Guide for eXtended Detection and Response).

XDR in the market today is primarily a consolidation ("platform") move for vendors with multiple security products. Vendor consolidation trends are driving further adoption of bigger platforms, with less reliance on point solutions. Large network security vendors are also increasingly using the term "XDR" when communicating the value proposition of their existing centralized management and monitoring consoles.

Gartner data continues to show that XDR questions often come as a request to understand the potential for expansion of existing endpoint detection and response (EDR) deployments. Consolidated offers, like XDR, often appeal first to midsize enterprises. These trends are the main drivers for NDR technology to become components of an XDR platform/portfolio in the future. However, when Gartner clients start from an NDR perspective, they generally do not want a dependency on other components that would be part of an XDR deployment. This remains an attractive trait of the NDR market for the larger enterprises, in addition to the more traditional "best in class" versus "best of breed" internal debate.

Augmented NDR

New analytics overlays are emerging, leveraging natural language processing (NLP) and the summarization features of LLMs. They gather events and alerts from existing security controls, including EDR, NDR and SIEM products, and sometimes also pull threat intelligence from separate sources, then present summarized findings.

Although EDR/XDR providers will offer SOC assistants (e.g., Charlotte AI from CrowdStrike), other approaches, like Microsoft Copilot for Security, put the prompt as the main user interface and promise to integrate with multiple sources of events and analytics. NDR providers that are already engaged in hybrid network coverage, and have ML skills and experience, are in a good position to leverage these new AI techniques for incident summarization. But even though they start with an edge when it comes to analyzing behaviors across multiple network environments, they'll struggle to differentiate their solutions from XDR products.

Market Analysis

NDR has shown its flexibility in monitoring network traffic wherever users and workloads exist, as the growing popularity of work-from-home arrangements has shifted on-premises traffic patterns from east-west to north-south. As a consequence, many vendors have accelerated their product development to go beyond the traditional on-premises data center and campus.

Despite strong competition from other platforms, NDR global market revenue continues to grow double digit, registering an increase of 19% for the period 1Q23 through 3Q23, year over year. When the NDR market was nascent, it was composed of a mix of pure-play startups and network monitoring companies expanding to security use cases. As the market grows, it is attracting more and more large platform providers.

One of the benefits of NDR technology is the ability of its management and monitoring consoles to facilitate incident response workflows. Event aggregations and predefined views reduce the learning curve and provide a visibility that small security teams appreciate.

Some vendors prioritize complete transparency in their workflows, allowing expert security analysts to examine granular details that can be used for further scoping and deeper inspection of forensics. Organizations that have the resources, skills and time to work heavily with forensics will appreciate these NDR vendors that focus on hunting, attack frameworks, and longer-term use and storage of network forensics telemetry. The transparency and flexibility of these NDR solutions usually comes at the expense of simplicity and ease of use.

In contrast, 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 will 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:

- **New sensors:** By building or integrating with endpoint sensors, such as EDR, ingesting third-party logs like SIEM, analyzing software/platform/IaaS events through their monitoring APIs, or adding support for OT use cases.
- **New detection techniques:** By adding support for more traditional signatures, performance monitoring, threat intelligence and sometimes malware detection engines. This move toward more detection using multiple techniques aligns well with the use case of network/security operations convergence, but also with midsize enterprises.
- **Managed NDR:** Some of the large vendors have started offering 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. Gartner first observed co-managed service offerings in the SIEM market (see Market Guide for Co-Managed Security Monitoring Services). Many of these single technology management services offered by NDR vendors are recent and supported by small but growing teams.

- **Evolving architecture:** More vendors provide ML analytics only in the cloud now, as the centralized approach facilitates the improvement of ML detections and improves the vendor's ability to scale.
- **Visibility:** NDR is most commonly deployed in large enterprises that have many sources of detection information. When one of these non-NDR signals indicates a threat, SOC teams can dive deep into the asset with the information provided from the NDR product.

Several NDR vendors have built a security portfolio beyond the NDR market and leverage their anomaly detection knowledge in new areas (e.g., SaaS or email security). These vendors are repositioning their value proposition with ML at its core, and network is becoming one of the use cases for this analytical approach.

Gartner continues to observe vendors using alternative approaches to data collection and deployment, such as Cynamics and Netography, differentiating themselves from NDR vendors while competing against them for similar use cases.

"Response" Doesn't Always Mean "Remediation"

When studying NDR shortlists, Gartner notices that the majority of the contenders identify themselves as NDR providers, hinting that the boundaries of the NDR market have solidified over time. Vendors frequently cite SIEM providers as competitors, and security teams see NDR as an improvement over legacy IDS deployments.

Additionally, many NDR vendors identify their products as good tools for threat hunting teams, and include sophisticated search capabilities targeted at incident responders. These characteristics of the "response" component define the NDR technology as much as its detection capabilities.

In many cases, the acceptable use cases for network-based automated response are related north-south traffic patterns (C2 communication, data exfiltration) or ransomware lateral movement. More noticeable improvements are visible through integration with other security controls, on the monitoring dashboards and on incident response workflow automation.

NDR's smart approach to "response" is to support the incident response workflow through event aggregation, workflow automation and contextual awareness. When necessary, it also blocks or contains malicious activity. An individual vendor's ability to provide a low false positive rate and efficient investigation capabilities will encourage customers to adopt the vendor's response capabilities.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

The table below includes a sample list of representative NDR vendors for which Gartner was able to collect and confirm accurate information. These vendors were included because there was sufficient evidence collected that they met Gartner's definition and requirements highlighted in the "Market Description" section.This table also includes information about the availability of physical and virtual appliances for IT and OT environments, and support for the three main global IaaS platforms — Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) — and selected SaaS environments.Please note that the mention of a supported use case does not indicate any specific depth of integration.

Table 1: Representative Vendors in Network Detection and Response

(Enlarged table in Appendix)

Vendor Name	NDR Product Names	Headquarters	IT Sensors (Physical, Virtual)	OT Sensors(Physical, Virtual)	IaaS (AWS, Azure, GCP)	SaaS (API) (M365, Google Workspace, Others)
Arista Networks	Arista NDR	Santa Clara, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, others
Cisco	Cisco Secure Network Analytics, Cisco XDR	San Jose, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	Others
Corelight	Corelight Open NDR Platform	San Francisco, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	–
Darktrace	Darktrace DETECT, Darktrace RESPOND	Cambridge, U.K.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, Google Workspace, others
Exeon Analytics	ExeonTrace	Zürich, Switzerland	Virtual	Virtual	AWS, Azure, GCP	Others
ExtraHop	ExtraHop Reveal(x) NDR	Seattle, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365
Fortinet	FortiNDR,Forti NDR Cloud	Sunnyvale, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	Others
Gatewatcher	Gatewatcher NDR (AIONIQ)	Paris, France	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	–
Hillstone Networks	Hillstone Breach Detection System (BDS)	Santa Clara, California, U.S.; Suzhou, China	Physical & virtual appliances	–	–	–
LinkShadow	LinkShadow Intelligence NDR, Linkshadow Cloud Detection and Response	Athens, Georgia, U.S.	Physical & virtual appliances	–	AWS, Azure, GCP	M365, Google Workspace, Others
MixMode	MixMode Network Detection and Response	Santa Barbara, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, Google Workspace, Others
Muninn	AI Detect,AI Prevent	Lyngby, Denmark	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	M365
NANO Corp.	n.Scope	Paris, France	Virtual appliances	Virtual appliances	AWS, Azure, GCP	–
NetWitness	NetWitness Platform	Bedford, Massachusetts, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, Google Workspace, Others
NSFOCUS	NSFOCUS Network Detection and Response Solution	Beijing, China; Santa Clara, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	–
Plixer	Plixer One Security	Kennebunk, Maine, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	–
Progress	Progress Flowmon Anomaly Detection System (ADS)	Burlington, Massachusetts, U.S.	Physical & virtual appliances	–	AWS, Azure, GCP	–
QAX	SkyEye	Beijing, China	Physical & virtual appliances	–	AWS, Azure, GCP	M365, Google Workspace, Other
Sangfor Technologies	Sangfor Cyber Command	Shenzhen, China	Physical & virtual appliances	–	AWS, Azure, GCP	–
Sesame it	Jizō NDR, Jizō-m	Paris, France	Physical & virtual appliances	Physical & virtual appliances	–	–
Sophos	Sophos NDR	Oxford, U.K.	Virtual	–	AWS	Other
Stamus Networks	Stamus Security Platform	Indianapolis, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	–
Stellar Cyber	Stellar Cyber NDR, Open XDR Platform	San Jose, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, Google Workspace, Other
Symantec by Broadcom	Symantec Security Analytics	San Jose, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	–
Tencent	T-Sec NDR	Shenzhen,Guangdong, China	Physical & virtual appliances	–	AWS, Azure	Other
Trellix	Trellix Network Detection and Response (NDR)	Plano, Texas, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	–
Trend Micro	Trend Vision One – XDR for Networks, Trend Micro Deep Discovery, Trend Micro TippingPoint	Tokyo, Japan; Irving, Texas, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	M365, Google Workspace, Other
Vectra	Vectra NDR	San Jose, California, U.S.	Virtual	Virtual	AWS, Azure, GCP	M365, Other
Venustech	CSA-NTA	Beijing, China	Physical & virtual appliances	Physical & virtual appliances	–	–

Note: AWS = Amazon Web Services, Azure = Microsoft Azure, GCP = Google Cloud Platform

Source: Gartner (March 2024)

Market Recommendations

Enterprises should strongly consider NDR solutions to complement signature-based network security tools and network sandboxes. Many Gartner clients have reported that NDR tools have detected suspicious network traffic that other perimeter security tools had missed.

When evaluating NDR vendors, assess these factors:

- **Pure-play versus NDR as a feature** — Consider cost, deployment requirements, complexity and efficiency of the NDR detections before deciding to implement NDR as a feature from another technology vendor (for example, SIEM or XDR), or investing in a more full-featured, pure-play NDR solution from one of the vendors analyzed in this Market Guide.
- **Hybrid network visibility** — It is more rarely the case that the scope for a new NDR deployment will be only for on-premises IT segments. Each type of network (e.g., OT, IaaS) has its own set of requirements and might face specific threats.
- **Detection** — NDR detections rely on a mix of techniques. Some NDR products are strong because they combine multiple techniques; others primarily rely on a single technique (ML, threat intelligence or signature). Focus on the types of detection, and consider a metric such as "percent of critical incidents detected by NDR" to compare NDR solutions.
- **False positives** — All technologies based on anomaly detection will be prone to false positives. Determine if your vendor of choice has a good track record of helping to minimize false positives through customizable thresholds or fine-tuning of the behavioral biometrics with organizations in your market segment.
- **Response** — Some vendors focus more on automated responses (for example, sending a command to a firewall to drop suspicious traffic), whereas other vendors focus more on supporting incident response workflow or even complement it with threat hunting features.
- **Integration** — When the NDR product senses an issue, must the alert go to its console, or can it be sent to a third-party tool for alerting? Is there an integration with third-party enforcement products, such as an enterprise firewall or network access control product?

Additionally, security and risk management leaders in charge of evaluating and comparing NDR vendors should first define rationalized metrics (for example, "percentage of critical incident," "percentage of false positive," "mean time to categorize as false positive" or "improvement in mean time to detect for ransomware incidents"). These metrics are more relevant for detection systems like NDR that should trigger a lower number of alerts. Leaders should also evaluate how NDR changes the definition of "good enough" for threat detection, SOC productivity and automated response. Examples of such metrics include "percent of critical incidents detected by NDR" or "average reduction in mean time to investigate incidents/false positives."

Document Revision History

Market Guide for Network Detection and Response - 14 December 2022

Market Guide for Network Detection and Response - 11 June 2020

Market Guide for Network Traffic Analysis - 28 February 2019

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Market Guide for Extended Detection and Response

Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 3Q23

4 Ways Generative AI Will Impact CISOs and Their Teams

Table 1: Representative Vendors in Network Detection and Response

Vendor Name	NDR Product Names	Headquarters	IT Sensors (Physical, Virtual)	OT Sensors(Physical, Virtual)	IaaS (AWS, Azure, GCP)	SaaS (API) (M365, Google Workspace, Others)
Arista Networks	Arista NDR	Santa Clara, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, others
Cisco	Cisco Secure Network Analytics, Cisco XDR	San Jose, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	Others
Corelight	Corelight Open NDR Platform	San Francisco, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	–
Darktrace	Darktrace DETECT, Darktrace RESPOND	Cambridge, U.K.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, Google Workspace, others
Exeon Analytics	ExeonTrace	Zürich, Switzerland	Virtual	Virtual	AWS, Azure, GCP	Others
ExtraHop	ExtraHop Reveal(x) NDR	Seattle, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365
Fortinet	FortiNDR,FortiNDR Cloud	Sunnyvale, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	Others
Gatewatcher	Gatewatcher NDR (AIONIQ)	Paris, France	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	–
Hillstone Networks	Hillstone Breach	Santa Clara,	Physical & virtual	–	–	–

	Detection System (BDS)	California, U.S.; Suzhou, China	appliances			
LinkShadow	LinkShadow Intelligence NDR, Linkshadow Cloud Detection and Response	Athens, Georgia, U.S.	Physical & virtual appliances	—	AWS, Azure, GCP	M365, Google Workspace, Others
MixMode	MixMode Network Detection and Response	Santa Barbara, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, Google Workspace, Others
Muninn	AI Detect,AI Prevent	Lyngby, Denmark	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	M365
NANO Corp.	n.Scope	Paris, France	Virtual appliances	Virtual appliances	AWS, Azure, GCP	—
NetWitness	NetWitness Platform	Bedford, Massachusetts, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, Google Workspace, Others
NSFOCUS	NSFOCUS Network Detection and Response Solution	Beijing, China; Santa Clara, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	—
Plixer	Plixer One Security	Kennebunk, Maine, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	—
Progress	Progress Flowmon Anomaly Detection System (ADS)	Burlington, Massachusetts, U.S.	Physical & virtual appliances	—	AWS, Azure, GCP	—

QAX	SkyEye	Beijing, China	Physical & virtual appliances	—	AWS, Azure, GCP	M365, Google Workspace, Other
Sangfor Technologies	Sangfor Cyber Command	Shenzhen, China	Physical & virtual appliances	—	AWS, Azure, GCP	—
Sesame it	Jizô NDR, Jizô-m	Paris, France	Physical & virtual appliances	Physical & virtual appliances	—	—
Sophos	Sophos NDR	Oxford, U.K.	Virtual	—	AWS	Other
Stamus Networks	Stamus Security Platform	Indianapolis, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	—
Stellar Cyber	Stellar Cyber NDR, Open XDR Platform	San Jose, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure, GCP	M365, Google Workspace, Other
Symantec by Broadcom	Symantec Security Analytics	San Jose, California, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	—
Tencent	T-Sec NDR	Shenzhen,Guangdong, China	Physical & virtual appliances	—	AWS, Azure	Other
Trellix	Trellix Network Detection and Response (NDR)	Plano, Texas, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	—
Trend Micro	Trend Vision One — XDR for Networks, Trend Micro Deep Discovery,	Tokyo, Japan; Irving, Texas, U.S.	Physical & virtual appliances	Physical & virtual appliances	AWS, Azure	M365, Google Workspace, Other

	Trend Micro TippingPoint					
Vectra	Vectra NDR	San Jose, California, U.S.	Virtual	Virtual	AWS, Azure, GCP	M365, Other
Venustech	CSA-NTA	Beijing, China	Physical & virtual appliances	Physical & virtual appliances	—	—

Note: AWS = Amazon Web Services; Azure = Microsoft Azure; GCP = Google Cloud Platform

Source: Gartner (March 2024)