Security and Risk Management

SPARK Matrix^{TM}:

Network Detection and Response (NDR), 2022

Market Insights, Competitive Evaluation, and Vendor Rankings

August 2022

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of the global Network Detection and Response (NDR) solution market dynamics, vendor landscape, and competitive positioning analysis. The study provides a comprehensive competition analysis and ranking of the leading NDR vendors in the form of the SPARK Matrix. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

Market Dynamics and Overview

The Network Detection and Response (NDR) technology has evolved out of the need to detect and mitigate threats that can slip past traditional security solutions. The need for such solutions has accelerated following the COVID-19 pandemic and the subsequent spike in remote work. This spike is witnessing different non-secure devices connecting to the organizational networks and endpoints, making them vulnerable to various types of cyber threats, including malware and ransomware attacks. The NDR solutions help alleviate the situation by providing the organizational SOC teams with real-time, advanced management, exposing threats, and response to curb such threats.

Quadrant Knowledge Solutions defines a Network Detection and Response (NDR) solution as “a solution that leverage non-signature-based techniques, including ML and other analytical techniques, to detect malicious and suspicious traffic in the enterprise network. The tools monitor the network and raise alerts for suspicious traffic in the network. Furthermore, the NDR solutions provide automated as well as manual responses to threats. These responses consist of threat-hunting and incident response tools that continuously ingest and correlate large volumes of network traffic and security events across multiple assets and hops.”

An NDR solution provides visibility across all ports and all protocols and bi-directionally scans all network traffic to reveal network and application protocols, files, and content via sensors that can be placed at the gateway, internally, in the cloud, and at both the email and web gateways. Modern NDR solutions conduct real-time analysis of raw network packet traffic and provide contexts for all cyber threats in the network. NDR solutions differentiate between normal and anomalous network and cloud traffic by leveraging machine learning and analytics to detect network traffic anomalies and provide rich metadata that enables retrospective detection and analysis going back up to several months. NDR solutions also profile TLS encrypted traffic based on metadata and certificates, determine human browsing versus machine traffic, and leverage data science models to detect hidden threats and consolidate “Like” alerts and the related context and evidence to accelerate alert triage that helps automate relevant response actions based on what has been detected. It can be deployed on either an enterprise cloud server or on an on-prem device.

Following are the key capabilities of NDR solutions:

- **Threat Detection:** An NDR solution enables the use of non-signature-based techniques to reach a high level of efficacy in identifying suspicious network traffic and threats autonomously and alerting security teams. An NDR solution provides threat detection and intelligence abilities that allow swift identification, protection, detection, response, and recovery from threats at an early stage through hypotheses based on the tactics and techniques used by attackers before the threats can cause any harm to the organizational system. Additionally, the NDR solution allows users to discover anomalous activities, root causes of threats, improve threat detection, analysis, and hunting by leveraging human expertise, technology-assisted techniques, and user behavior analytics. Furthermore, an NDR solution eliminates any blind spots in the network and generates a multi-dimensional stream of events that can be correlated and used for threat hunting and incident investigation.

- **Alert Notification:** An NDR solution provides real-time alerts and monitoring of potential threats lurking in the network while reducing false positives. The solution provides the SOC teams with an automated solution to respond efficiently without attempting to perform triage or validating an alert. An NDR solution performs event triage, as well as exposes and prioritizes threats needing immediate attention automatically. Additionally, the NDR solution offers automated alert prioritization and allocation by leveraging machine learning and algorithmic threat analytics to expose sophisticated cyberthreats in critical IT assets and strategizes the cyber kill chain of those threats to alert the SOC teams when the threat is identified.

- **Threat Intelligence:** An NDR solution automatically identifies and mitigates sophisticated cyberattacks and protects critical information and IT assets. An NDR solution leverages threat intelligence to collect data and information from all types of security threats, including appearance, threat working mechanism, impact, and stops threats and attacks in real-time. The solution identifies and stops emerging threats before they can reach the enterprise IT system and provides meaningful insights into threats and the security landscape in the form of interactive reports.

- **Incident Response:** An NDR solution offers incident response capabilities that enable organizations to identify and respond to threats in real-time. The solution enables users to control an incident and eradicate the threat from the network to recover and restore the organizational data by alerting the incident handling team. Additionally, it reduces the detection time, responds quickly to cyber-attacks and threat actors, and maximizes visibility into the threat landscape. An NDR solution intelligently recognizes advanced cyber-attacks, differentiates between noise and useful reports based on data collected on cyber threats, and converts them into actionable intelligence.

- **Security Monitoring and Analytics:** An NDR solution provides comprehensive visibility into the network, including protocol transactions, flows, and extracted files, along with a clear timeline showing any activity or threats in the network. An NDR solution provides greater visibility into all the IT activities associated with the organization, irrespective of whether these activities occur inside or outside the organizational network. An NDR solution tracks and records data from applications and endpoints, including IoT devices, and analyzes the data to detect inefficiencies or anomalies. Additionally, an NDR solution provides an in-depth analysis of data collected from all endpoints and provides insights through visualization dashboards and custom reports. The solution leverages analytics to track and improve the overall performance and user experience and provides quick access to precise data-driven decisions based on a holistic view of devices and applications.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major vendors of network detection and response (NDR) solutions by evaluating their products, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall NDR market. This study includes an analysis of key vendors, including aizoOn, Arista, Blue Hexagon, Cisco, Corelight, cpacket Networks, Darktrace, ExtraHop, Fidelis Cybersecurity, Gigamon, GREYCORTEX, Hillstone Networks, IronNet, Plixer, Progress, Quad Miners, Stellar Cyber, ThreatBook, Trellix, Vectra AI, Vehere, and VMware.

Arista, Darktrace, ExtraHop, Fidelis Cybersecurity, Progress, Trellix, Vectra AI and VMware are identified as global technology leaders in the SPARK Matrix: Network Detection and Response (NDR), 2022. These companies provide a sophisticated and comprehensive technology platform to protect, detect, analyze, and respond to known and unknown advanced cyber threats throughout the network. NDR improves the effectiveness of threat detection, hunting, investigation, remediation, and incident response processes by integrating with other security technologies, which forms the SOC Visibility framework.

Arista Awake Security offers a unified platform to analyze network communications, autonomously discover profile, and classify every device, user, and application across the user's network to support threat investigation and incident response. Arista Awake Security NDR provides comprehensive visibility into the organization's entire network. It also detects advanced threats by leveraging machine learning (ML) that can be deployed in two modes as per the need of the organization. Furthermore, it allows organizations to easily integrate with SIEM, business intelligence, ticketing and analytics, endpoint detection, and security orchestration tools to isolate compromised devices and mitigate cyberthreats.

Darktrace Enterprise Immune system offers a non-signature-based self-learning unified platform that understands the pattern of threat and prevents future anomalies across user's network. Darktrace Enterprise Immune system provides a comprehensive real-time visibility and investigation capabilities across unauthorized endpoints and remote workers off the VPN. Darktrace Enterprise Immune system interacts with Cyber artificial intelligence (AI) analyst to enable automatic investigation. Additionally, it helps to automatically respond and mitigate cyberthreats across industrial environments, cyber physical systems, and email platforms with the help of the Darktrace Antigena framework.

ExtraHop offers complete visibility by automatically discovering and classifying devices communicating across user's network in real time with its Reveal(x) solution. Additionally, it offers a detailed view of the network without compromising privacy by including the decryption capability. ExtraHop Reveal(x) offers ML-based behavior detection, rules, and custom triggers to comprehensively detect anomalies in the user's network. It provides integration with security tools, including Phantom, Splunk, and Palo Alto to automate investigation and prevent intrusion as mapped by the MITRE ATT&CK framework and CIS Top 20.

Fidelis Cybersecurity offers a unified NDR solution, Fidelis Network, to protect from the cloud and on premises network threats by providing visibility and control across organizational IT environment. Fidelis Cybersecurity Fidelis Network provides integration with Fidelis Endpoint and Fidelis Deception platforms in a centralized Fidelis Elevate (Active XDR platform), which allows users to expose and mitigate cyberthreat across the security infrastructure mapped with the MITRE ATT&CK framework. Fidelis Cybersecurity Fidelis Network provides a comprehensive visibility of bi-directional encrypted traffic with appropriate content for understanding the network along with a unified solution to provide network defense across email, web, IDS, threat, and Data Loss Prevention to expose and mitigate threats comprehensively.

Progress Flowmon ADS offers a complete detection and mitigation of cyberthreat in user's network by adding the network-centric layer with the SOC visibility triad. Progress Flowmon ADS offers ML-powered detection engine, which combines multiple detection mechanisms to reveal malicious behavior, data breaches, and attack against mission-critical applications of the threat lifecycle. Progress Flowmon ADS offers a custom dashboard based on severity rules across levels to prioritize and report security and networking. Additionally, it enables integration with SIEM, big data platforms, network access control, authentication, firewall, and other incident response tools while ingesting data from various sources like AWS, Google Cloud, Progress LoadMaster, and others.

Trellix offers a robust NDR solution, Trellix Network Security, to automatically monitor, detect, and block known and unknown threats across email, endpoints, and other security services. Trellix Network Security offers integration with Trellix Intrusion Prevention System and Network forensics for a comprehensive real time monitoring and visualization of the threats impacting user's organization, respectively. Trellix Network security leverages SmartVision to detect malicious traffic moving between clients and network devices while communicating over Server Message Block.

Vectra AI offers AI-based Cognito Detect to deliver real-time attack visibility and provide contextual attack details for carrying out responses. Cognito Detect offers integration with Cognito AI to automate threat investigation, which facilitates users to respond faster across cloud and enterprises. Vectra AI Cognito Detect offers STIX threat intelligence that provides comprehensive real-time visibility and analyses traffic whether in all directions of the user’s network. Vectra AI Cognito Detect offers Threat Certainty Index to consolidate events and historical context to prioritize incident for response. Vectra AI Cognito Detect provides Privileged Access Analytics that leverages AI to detect and prioritize entities that have privileges and differentiate between approved and malicious uses across cloud, data center, IoT, and enterprise networks.

VMware NSX NDR offers threat correlation and forensics by leveraging AI to efficiently detect malicious activity and block movement of sophisticated threats. NSX NDR allows detection of different advanced threats by collecting threat signals from network traffic analysis, intrusion detection and prevention, and network sandboxing engines VMware NSX NDR offers a Threat Analysis Unit to continuously update NSX NDR in real time with threat intelligence, such as active command and control (C&C) servers, objects with zero-day exploits, toxic websites and malware distribution points, and malware information useful to defend against threats specific to a user's organization.

aizoOn, Cisco, Corelight, Gigamon, Hillstone Networks, and IronNet have been positioned among the primary challengers. These companies provide comprehensive technology capabilities and are gaining significant market traction in the global NDR market. These companies are also aware of the upcoming market trends and have outlined a comprehensive roadmap to tap into future growth opportunities. The other key vendors captured in the 2022 SPARK Matrix include Blue Hexagon, cpacket Networks, GREYCORTEX, Plixer, Quad Miners, Stellar Cyber, ThreatBook, and Vehere.

All the vendors captured in the 2022 SPARK Matrix of NDR are enhancing their capabilities to secure, detect, analyze, and respond to known and unknown advanced cyber threats in the network. Additionally, these vendors help organizations expand their partnership channels and support diverse use cases. Vendors are consistently looking to enhance NDR and expand support for easy deployment options. They continue to enhance their offerings to strengthen the organization's defence-in-depth strategies to significantly improve threat detection and response processes. Additionally, vendors are focusing on increasing their customer base, geographical presence, different industry verticals and expanding their use case support. Vendors are also looking at expanding support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

While most of the leading Network Detection and Response (NDR) vendors may provide off-the-shelf NDR capabilities, good customer experience, seamless integration, comprehensive endpoint management, data and applications management, secure remote access and control, compliance check, patch management, software updating, network security, and analytics & reporting, the flexibility of deployment and the degree of increase in organizational security infrastructure may differ by different vendors offerings. Driven by increasing competition, vendors are increasingly looking at improving their technology capabilities and overall value proposition to remain competitive. Following are some of the key competitive factors and differentiators to evaluate the NDR vendors:

The Sophistication of Technology Platform: Users should evaluate an NDR solution that offers comprehensive capabilities that can support conventional security solutions in customer environments like MDR, EDR, XDR, SIEM, anti-virus software, firewalls, and intrusion detection systems. Cloud providers are undertaking agile deployments, providing more updates, especially for remote worker use cases, where orchestration will increasingly rely on unauthorized network points for response activities. Users should look for NDR vendors providing the ability to integrate via the cloud without added infrastructure, as well as support for an accelerated response via a mobile application. Users should look for vendors who are well-versed with the upcoming opportunities in the NDR market and can devise compelling strategies to overcome unprecedented events. Users should look for a holistic NDR solution with integrated technology, enhancing endpoint security and NDR capabilities to secure networks from cyberattacks.

Maturity of AI and ML: A robust NDR should enable the user to immediately spot anomalies and signs that an undetected attack is imminent. An NDR solution should provide non-signature based techniques like machine learning (ML) or other analytical techniques for detecting unknown anomalies as well as signature based techniques like threat intel fused in-line for alerts to detect known attacks or activities in the network. Both north/south traffic and east/west traffic should be monitored. Traffic in both physical and virtual environments should also be monitored. All data should be collected and stored in a centralized data lake with an advanced AI Engine to detect suspicious traffic patterns and issue alerts. NDR vendors should provide automatic responses to threats such as sending commands to firewall to prevent suspicious traffic or to an EDR tool to isolate an affected endpoint or provide manual responses such as threat hunting or incident responses as a foundation feature to facilitate the SOC teams in strengthening their security infrastructure.

Integration & Interoperability: NDR vendors are increasingly integrating with other security tools like SIEM and EDR to complete the SOC visibility triad, as NDR is only a part of the overall detection and response solution in the security technology stack. An NDR product does not address all security monitoring needs by itself, so organizations need straightforward integration of NDR into their existing tech stack to optimize detection based on the organization's specific needs. Therefore, the NDR product should provide open interfaces that enable straightforward integration with other systems, such as security orchestration, automation, and response (NDR), security information and event management (SIEM), extended detection and response (XDR), and incident response (IR) systems to cover the full spectrum of security infrastructure. An NDR solution should integrate popular open-source projects of threat detection and response, such as Zeek and Suricata. Suricata can efficiently monitor traffic for any anomalies, whereas Zeek delivers large volume of high-quality data to provide comprehensive visibility into the network and provide context. The integration would facilitate users to pivot directly from Suricata alert into any of the Zeek logs to leverage powerful evidence about email, web traffic, SSL, DHCP, DNS, and dozens of other data types inherent to Zeek.

Effectiveness of threat investigation and forensics: An NDR product should provide comprehensive data enrichment. Data enrichment is a critical factor in effective threat detection, threat forensics, and remediation. The addition of enriched data adds event and non-event contextual information to security event data to transform raw data into meaningful insights. So, the data must be collected by the NDR solutions with the process of appending or otherwise enhancing with relevant context obtained from additional sources. The solution should also enrich data in real-time with business and threat intelligence details.

SSL/TLS Decryption: Network traffics are encrypted with new standards TLS 1.2 and 1.3 to provide privacy (using Elliptic Curve Diffie-Hellman Encryption), which creates and ephemeral session key. The ephemeral secret is only used for that conversation and not for private key of either server or the client. While this poses difficulty for hackers trying to steal large databases of intellectual property or credentials, it also becomes difficult for SOC teams to get comprehensive visibility into the network. Therefore, NDR vendors should address the visibility issue of the SOC team by focusing on decryption traffic to and from an organization's public-facing services, such as email, web servers, DNS servers and core infrastructure such as database and Active Directory servers. This approach will facilitate the concerned team to expose and mitigate the cyberthreat while protecting the privacy of the sensitive data.

Extending protection to IoT: Increasing adoption of IoT devices stretches the organizational attack surface. If left unmanaged, endpoints like IoT devices represent a significant and growing risk, as many IoT devices are either too tiny (like the internet-connected thermostats), or too many to manage at scale, or simply too old (in case of manufacturing systems) and simply do not have the ability to run endpoint security software or analytics. Therefore, users should look for an NDR solution that analyzes the network traffic to generate deep insights into the network while providing asset inventory, vulnerability assessment and monitoring threat to improve the security infrastructure of the organization. NDR vendors should provide the capability to protect organizational IoT devices by analyzing their network activity without the overhead of having to manage individual device software.

Mapping with MITRE ATT&CK framework: The MITRE ATT&CK framework is a valuable tool for security teams to identify gaps in their threat detection capabilities. So NDR solution should follow the MITRE ATT&CK framework and provide a dedicated dashboard for the SOC team to see the reports and make necessary changes to their security infrastructure accordingly with endpoint monitoring, activity logs and tactics, techniques, and procedures (TTPs) proving insufficient vendors are now providing the MITRE ATT&CK framework. The NDR solution can integrate with MITRE ATT&CK framework to help security teams fill one of the biggest security tooling and visibility gaps in the network. Therefore, users need to choose an NDR vendor that provides detection and response to modern advanced threats by aligning with the MITRE ATT&CK framework.

Metadata Analysis: Users should look for a solution that provides a metadata analysis feature because it allows observation of network communications at any collection point and provide insights about encrypted communication. However, this is not possible by commonly used deep packet inspection (DPI)-enabled NDR solutions. Although this approach provides detailed analysis, it requires large amounts of processing power and is blind when it comes to encrypted network traffic.

Packet-based visibility into network: Users should look for NDR products that can utilize a packet-based source of data, as these products provide visibility into packets, which allows detection of more advanced attacks such as tunneling. Such products can also provide continuous line-rate packet capture before, during, and after an alert or attack, as compared to common NetFlow-based NDR, which only provides network visibility with a shallow scope.

Ease of Playbook Creation and Customization: Playbook is an essential element for launching effective mitigation strategies. The playbook guides analysts in handling threat alerts and incidents regarding required actions and tools to be used. NDR vendors should provide numerous standard built-in playbooks to help the SOC teams quickly launch mitigation measures. These playbooks can also be customized to suit the organization's unique requirements. NDR solutions' capability regarding ease of playbook creation and customization with low code/no code requirements is amongst the vital technology differentiators. Depending on the vendor's community-building initiative, the NDR solution can support building and expanding the knowledge base with a library of playbooks by providing access to a community of contributors.

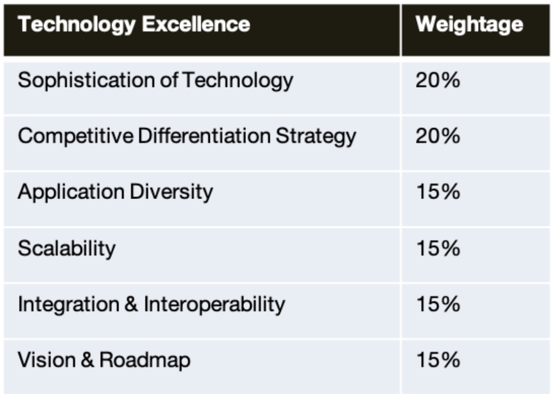
Scalability and Availability: A NDR solution vendor should offer a sophisticated solution that can manage, secure against, and monitor all types of cyber threats. The solution should offer the scalability to fulfill the high demands and workloads while ensuring the best experience for employees and less burden on IT/admin resources. Users should look for vendors providing security event management, security orchestration, incident response and workflow, reporting, and fully operationalized and automated security controls. Additionally, vendors should provide support for full multi-tenancy for large organizations for the deployment of the NDR solution. NDR solution architecture should support both horizontal and vertical scalability to support organizations as they grow and evolve. Enterprise and government organizations often face significant challenges in the case of multiple targeted attacks, politically motivated attacks, and hacktivism trends. During such events, the SOC team may receive an unprecedented surge in alert volumes. The NDR solution should support enterprise-class scalability to improve SOC capacity across the extended enterprise. Users should be able to leverage these services to create a customized security solution to meet their specific business and technology requirements. Users should choose a solution that helps them reduce the risk and protects them from zero-day attacks. Users should look for NDR providers with a history of successful large-scale deployments and carefully analyze the existing case studies of those deployments.

Vendors' Strategy and Roadmap: Users should consider the vendors' capability to formulate a comprehensive and compelling technology roadmap prior to the adoption of NDR. Vendors are investing in digital transformation, catering to specific-use cases, and minimizing risk exposure. Vendors are continuously investing in R&D for their NDR solution to take the lead in providing security. Additionally, some of the vendors are investing in innovating their NDR solution by incorporating AI-powered incidents & alerts management, improved workflow & team collaboration, seamless data ingestion framework, AI-driven operations intelligence aided threat-centric investigation, and a prediction & similarity engine. The vendors are also providing AI-aided playbook generation, action suggestions, connector development, real-time detection and response, tighter integration with security fabric products, threat intel management, and expanded connector coverage with focused integration content packs. Furthermore, vendors are focusing on providing interactive dashboards for easy visualization, data analytics and supporting the convergence of DevOps and SecOps. Vendors are implementing additional technologies with existing SIEM and EDR solutions to build a robust security solution offering protection from these advanced cyberattacks.

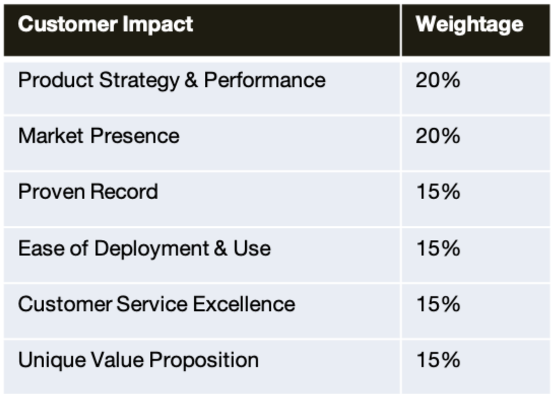
SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions’ SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision makings, such as finding M&A prospects, partnership, geographical expansion, portfolio expansion, and similar others.

Each market participants are analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix.



Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%



Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Evaluation Criteria: Technology Excellence

- **The sophistication of Technology**: The ability to provide comprehensive functional capabilities and product features, technology innovations, product/platform architecture, and such others

- **Competitive Differentiation Strategy**: The ability to differentiate from competitors through functional capabilities and/or innovations and/or GTM strategy, customer value proposition, and such others.

- **Application Diversity**: The ability to demonstrate product deployment for a range of industry verticals and/or multiple use cases.

- **Scalability**: The ability to demonstrate that the solution supports enterprise-grade scalability along with customer case examples.

- **Integration & Interoperability**: The ability to offer product and technology platform that supports integration with multiple best-of-breed technologies, provides prebuilt out-of-the-box integrations, and open API support and services.

- **Vision & Roadmap**: Evaluation of the vendor's product strategy and roadmap with the analysis of key planned enhancements to offer superior products/technology and improve the customer ownership experience.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance**: Evaluation of multiple aspects of product strategy and performance in terms of product availability, price to performance ratio, excellence in GTM strategy, and other product-specific parameters.

- **Market Presence**: The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.

- **Proven Record**: Evaluation of the existing client base from SMB, mid-market and large enterprise segment, growth rate, and analysis of the customer case studies.

- **Ease of Deployment & Use**: The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation and usage experience. Additionally, vendors' products are analyzed to offer user-friendly UI and ownership experience.

- **Customer Service Excellence**: The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

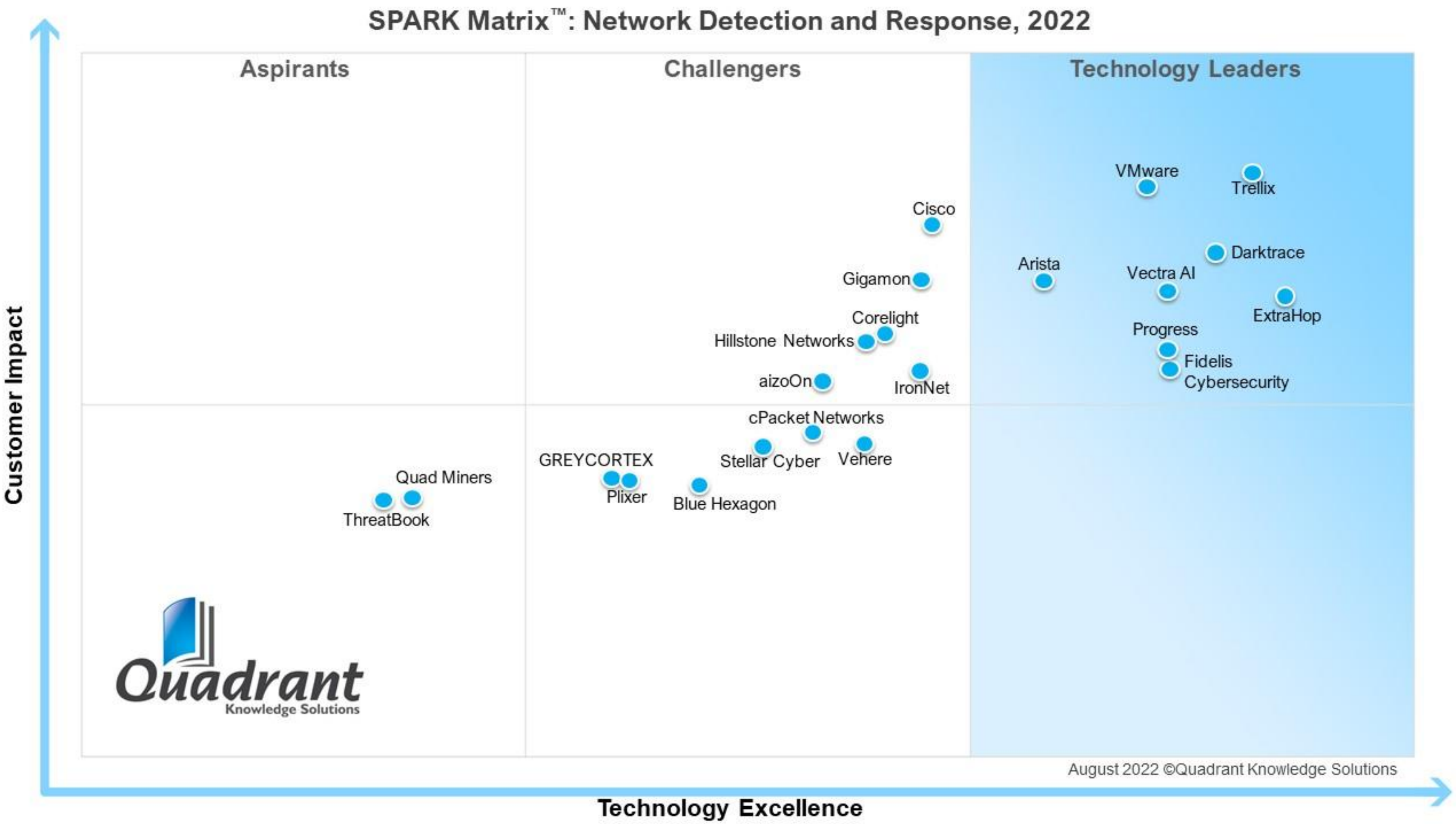
- **Unique Value Proposition**: The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

SPARK Matrix™: Network Detection and Response (NDR), 2022

Strategic Performance Assessment and Ranking

Figure: 2022 SPARK Matrix™

(Strategic Performance Assessment and Ranking)
Network Detection and Response (NDR) Market



August 2022 ©Quadrant Knowledge Solutions

Vendors Profile

Following are the profiles of the leading NDR vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions, regarding NDR and vendor selection based on research findings included in this research service.

Arista

URL: https://awakesecurity.com/

Founded in 2008 and headquartered in California, USA. Arista is the provider of products that use technologies such as their patented CloudVision and Arista EOS to provide security to cloud network for large data center, campus, and routing environments. The company provides 'Arista NDR,' a network detection and response solution that monitors enterprise network traffic and automatically detects, evaluates, and handles risks while providing information that may be used by the SOC team to take appropriate action.

Arista NDR enables organizations to analyze network communications to autonomously discover, profile, and classify every device, user, and application across the user's network—perimeter, core, IoT, and cloud networks by including deep network analysis from sensors that span the user's network Furthermore, it exposes and correlates complex adversarial behaviors to support threat investigation and incident responses.

The Arista NDR platform allows easy integration with legacy and modern industry leading solutions, such as SIEM, business intelligence, ticketing and analytics, endpoint detection, and security orchestration tools. Furthermore, it supports a full API for custom workflows and integrations. Arista NDR facilitates the SOC teams to focus on device profile with associated user(s) and roles, operating system and application details, a forensic threat timeline, and a listing of a similar device(s) for campaign analysis by integrating Arista NDR with SIEM. Additionally, it offers endpoint integrations that allow quarantining of compromised devices or retrieval of endpoint forensic data.

Arista includes AVA Sensors and AVA Nucleus (ensemble machine leaning) that offer comprehensive NDR solutions to mitigate cyberthreats. Arista NDR offers two modes of deployment depending on user's requirements and network architecture: a) All-in-one: In this mode, the AVA Sensor and AVA Nucleus are deployed on a single appliance. This deployment is ideal for users who deploy a single instance of Arista NDR or would like to maintain an isolated view of their deployment. b) Split: In this mode, the AVA Sensor and AVA Nucleus are deployed separately. AVA Sensors can be deployed in a variety of form factors, including on Arista switches, in physical or virtual appliances, and within Amazon Web Services (AWS) or the Google Cloud Platform (GCP).

Analyst Perspectives

Followings is the analysis of Arista's capabilities in the global Network Detection and Response market:

- Arista NDR provides visibility into encrypted traffic using AI to identify network applications, remote control, file transfers, and others. Furthermore, it reduces false positives & negatives by avoiding basic unsupervised learning on IP address data. It requires no agents, manual configuration, or lengthy training periods and can be deployed directly on the network switch.

- Arista NDR offers EnitityIQ to autonomously discover & profile every device, user, and application (managed or unmanaged) in the organization. It also offers Adversarial Modeling that exposes attacks, including insider threats, credential misuse, lateral movement, data exfiltration. Furthermore, it offers Automates triage and investigations through AVA AI, providing a decision support system to SOC.

- In terms of geographical perspective, Arista has a strong presence in North America followed by APAC and EMEA. From an industry vertical perspective, the company holds a strong customer base in automotive, banking, government, healthcare, life sciences, legal, energy etc. From a use case perspective, the company offers comprehensive visibility, securing remote enterprise network, situational awareness, and threat hunting.

- Arista's primary challenges include growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration in small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, Arista is well-positioned to maintain and grow its market share in the Network Detection and Response Market.

- Arista as their roadmap strategy is focusing on enhancing capabilities, increasing the number of number of customers, geographical presence, different industry verticals, and expanding use case support.

Darktrace

URL: https://www.darktrace.com

Founded in 2013 and headquartered in Cambridge, UK. Darktrace is a provider of products and solutions that use AI to offer sophisticated cybersecurity solutions for identifying, preventing, and eliminating insider threats. The company provides 'Enterprise Immune System,' a network detection and response solution that is a scalable, self-learning AI, to understand the digital DNA of an organization and detect cyber-threats at an initial stage of the attack for SOC teams to respond efficiently.

Enterprise Immune System uses non-signature tactics to form a complex understanding of what is 'normal' for the environment as it evolves. Instead of relying on signatures, the Enterprise Immune System understands the pattern of the threat for future anomaly activities across infrastructure – users, devices, clouds, and containers. Furthermore, it allows users to easily ingest telemetry and share Darktrace intelligence by integrating Enterprise Immune System with users' devices and leveraging one click custom template.

Darktrace's Enterprise Immune System combines real-time threat detection, digital visualization, and advanced investigation capabilities in a unified system to mitigate sophisticated cyberattacks. The solution is self-learning, which can identify new threats without relying on historical data of what constitutes "malicious" behavior. Furthermore, it leverages intuitive and easy-to-use graphical interface and threat visualization and investigations to simplify the detection process for the SOC team to respond.

Darktrace Enterprise Immune System offers visibility to the unauthorized endpoint and remote workers off the VPN, while allowing it to analyze real-time traffic of remote workers in the same way it analyzes traffic in the network, correlating a web of connections to develop a robust understanding of workforce behavior. Darktrace Enterprise Immune system provides visibility of suspicious activities occurring from cloud and collaborative tools to the corporate network and remote endpoints of the VPN. Furthermore, it provides integration and custom templates which can ingest new forms of telemetry and share AI insights across established workflows.

Analyst Perspectives

Followings is the analysis of Darktrace's capabilities in the global Network Detection and Response market:

- Darktrace offers advanced network detection and response solution and Enterprise Immune System to detect and mitigate unknown threats in real time. Darktrace Enterprise Immune System leverages scalable and self-learning AI to understand organization's digital DNA and adapts to the unknown that can discover zero-day attacks and provide comprehensive details of attacks.

- Enterprise Immune System interacts with Cyber AI as analysts to enable automatic investigations while compiling security events into an easily understandable report to share with the organization stakeholders. Furthermore, AI can quickly interpret and report on security incidents characterized by innovative attack techniques. Furthermore, Enterprise Immune System provides Darktrace Antigena framework that can automatically respond to self-learning detections and mitigate cyberthreats across industrial environments, cyber physical systems, and email platforms.

- From the geographical perspective, Darktrace has a strong presence in EMEA followed by North America and APAC. From an industry vertical perspective, the company holds a strong customer base in various domains, including education, financial services, government, healthcare, energy, retail, legal, telecom, and manufacturing. From a use case perspective, the company offers Insider Threat and Account Takeover, Attacks on Cloud, IoT, collaboration tools, Zero-Days, Malware, and Ransomware protection.

- Darktrace primary challenges include growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, Darktrace is well-positioned to maintain and grow its market share in the Network Detection and Response Market.

- Darktrace as their roadmap strategy is aiming to expand into proactive security AI and developing Attack path modeling with self-learning AI technology to strength their IT security offerings.

ExtraHop

URL: https://www.extrahop.com

Founded in 2007 and headquartered in Seattle, Washington, USA, ExtraHop provides solutions that apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and providing data-in-flight to expose and mitigate cyberthreats. The company offers 'Reveal(x),' a cloud-native network detection and response (NDR) solution that provides scale, speed, and visibility to the SOC team to detect and respond to threats across hybrid network architectures, containerized applications, and the cloud.

Reveal(x) provides two modes of deployment as their NDR solution: a) Reveal(x) 360: It is a SaaS-based platform that provides comprehensive visibility across on premises and cloud environment, a control panel for unified visibility, and cloud-hosted record store for situational intelligence. b) Reveal(x) Enterprise: It is equipped with self-managed sensors that an organization can deploy, manage and record in the systems.

Reveal(x) offers complete visibility in real time that automatically discovers and classifies devices communicating across the network to help SOC teams understand the network and respond. It analyses the network with decryption capability without compromising the privacy of sensitive data in the network. Furthermore, it offers real time detection that catches threats with cloud scale machine learning and customizable rules-based detections. It facilitates to identify critical assets and compares peer groups to deliver highly accurate detection so that the SOC team can prioritize the threat and respond accordingly.

Reveal(x) offers automated breach detection to detect, contain, and document risky and malicious behavior to take appropriate response actions across cloud native and on premise. Furthermore, it offers audit finding capabilities to validate concerns and vulnerabilities, analyses inventory devices, encrypts audits, and decommissions risky assets.

Reveal(x) offers robust integration with security tools, including Phantom, Splunk, and Palo Alto to automate investigation with convenience and coverage across user's environment. Furthermore, Reveal(x) is mapped with MITRE ATT&CK framework and CIS Top 20 links to help SOC team throughout the attack chain to expose and mitigate cyberthreats.

Analyst Perspectives

Followings is the analysis of ExtraHop capabilities in the global Network Detection and Response market:

- Reveal(x) offers the automated inventory feature by auto-discovering and classifying everything communicating on the network to always keep the inventory up to date. Reveal (x) also decrypts SSL/TLS 1.3 traffic in real time for the user to get details about any threat lurking in its encrypted traffic. Furthermore, it offers automatic investigation while providing risk scoring to expose and mitigate cyberthreats.

- Reveal(x) offers machine learning (ML)-based behavior, rules, and custom triggers to comprehensively detect late-stage attack activities in the organization by automatically detecting new, rogue, and unmanaged devices. It also offers contextual evidence and intelligent response options to expose and mitigate threats across hybrid workforce and enterprises.

- From a geographical perspective, ExtraHop has a strong presence in North America followed by EMEA and APAC. From an industry vertical perspective, the company holds a strong customer base in e-commerce, retail, government, healthcare, financial services, and others. From a use case perspective, the company offers threat hunting and detection, forensic investigation, and vulnerability assessment and compliance.

- ExtraHop's primary challenges include growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small- to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, ExtraHop is well-positioned to maintain and grow its market share in the NDR Market.

- ExtraHop has their roadmap strategy to invest on AI-based detection and response approaches looking at the frequency and severity of advanced threats like software supply chain attacks and ransomware. Furthermore, to increase their presence in government and public sector with specially designed security tools that caters their needs.

Fidelis Cybersecurity

URL: https://fidelissecurity.com/

Founded in 2002 and headquartered in Bethesda, MD, US. Fidelis Cybersecurity is a provider of products and solutions that automate deception, detection, and response across networks, endpoints, and cloud environments. The company provides Network Detection and Response capabilities through the 'Fidelis Network' platform, which provides protection against cloud and on-prem network threats with deep visibility and control over the entire threat framework, from initial compromise through data exfiltration.

Fidelis Network offers contextual intelligence and rapid response tools to proactively detect, neutralize, and protect against network intrusions, malware, and data exfiltration before they damage business operations. Furthermore, it provides a comprehensive analysis of sensitive data through registration and profiling to present sensitive files and match data.

Fidelis Network provides real-time and retrospective analysis without any loss of network, email, and web traffic data by scanning all network traffic, whether east-west or north-south, to expose threats. Furthermore, it offers patented Deep Session Inspection technology that helps the user with contextual metadata analysis across file formats and content across all ports and protocols to reduce response time and provide overall network visibility, validated alerts, incident response workflow automation, and multiple detection techniques. The technology leverages machine learning to expose potential threats which are missed detection by traditional detection methods.

Fidelis Network facilitates the elimination of alert fatigue by automatically validating, correlating, and consolidating network alerts with a unified view across network data, rich content, multiple defenses, security analytics and rules. Furthermore, it unifies network defense and decryption by providing content and context of encrypted traffic to help the SOC teams mitigate the threat. The platform also helps accelerate the threat response by providing group-related alerts to the SOC team to respond efficiently by providing malware analysis, robust threat detection, sandbox, network forensics, DLP, threat intelligence, and automated security rules in a unified solution.

Fidelis Network offers a threat intelligence collector that helps the SOC teams store rich metadata for a long time to gain insights into adversaries and threats along with providing risk assessments and reports which improves SOC team efficiency whenever it is required. Furthermore, it combines comprehensive visibility with contextual threat intelligence and automates alerts based on rules, feeds, and anomaly detection to provide an understanding of the network threats on an enterprise scale.

Fidelis Network can integrate with Fidelis Endpoint and Fidelis Deception platform under the Fidelis Elevate (Active XDR platform) package. This integration offers the SOC team a comprehensive defense strategy by providing contextual visibility and speed to expose and mitigate cyber threats and stop data loss across endpoints (EDR), network (NDR), and cloud applications and services. Fidelis Network is mapped with MITRE ATT&CK framework that provides the SOC team with contextual visibility and deep inspection analysis of the environment to find and eliminate lurking threats and also stop upcoming business attacks.

Analyst Perspectives

Followings is the analysis of Fidelis Cybersecurity’s capabilities in the global Network Detection and Response market:

- Fidelis Network offers content analysis capability that includes collecting metadata attributes for efficient threat intelligence and detecting threats and attacks in their beginning phase through data exfiltration. It provides a comprehensive picture of bi-directional encrypted traffic with appropriate content for an understanding of the network along with a unified solution to provide network defense across Email, Web, IDS, threat, and DLP to expose and mitigate potential threats.

- Fidelis Network provides analysis and inspection of traffic using ports and protocols as an attribute that supports HTTP, SMTP, FTP, DNS, RATs, and Suricata for the user's convenience. Fidelis Cybersecurity works with custom-build decoders for the purpose of analysis, metadata creation, threat detection, and prevention, along with decoding perform at the session level that resembles packets at the TCP layer with the help of patented Deep Session Inspection technology. Furthermore, it provides content analysis that analyses and detects malware and DLP within highly compressed and embedded documents while decoding various file types, email messages and data transfer.

- Fidelis Network offers asset discovery, classification and risk capabilities to identify threat in the network, prioritize them according to their risk level that facilitates the SOC team to monitor for internal or external threat flowing in the network. Furthermore, it can also be integrated with other vendors that does not pass through a Fidelis sensor like EDR solutions, ZScaler, ZIA and Active Director for comprehensive coverage of the user's network.

- Regarding geographical presence, Fidelis Cybersecurity has a strong presence in North America followed by EMEA. From an industry vertical perspective, the company holds a strong customer base in the education, financial services, government, healthcare, energy, telecom, and manufacturing sectors. From a use case perspective, the company offers threat detection and response, data exfiltration, visibility into network data, and threat hunting.

- Fidelis Cybersecurity as their roadmap strategy is strategically investing in MI/AL technology to expand detection, decoding, threat hunting, and sandbox-like analysis to detect even the unknown. Fidelis Cybersecurity is also developing a robust user behavior analytics or UEBA to protect devices across various networks and devices. Furthermore, the company is working on integrating its platforms under one umbrella to provide a complete package of security technologies to expose and mitigate any cyber threats lurking in organizational networks.

- Fidelis Cybersecurity’s primary challenges include the growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are among the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, Fidelis Cybersecurity is well-positioned to maintain and grow its market share in the Network Detection and Response market.

Progress

URL: https://www.progress.com

Founded in 1981 and headquartered in Burlington, MA. Progress provides solutions that simplify the development, deployment, and management of business applications. The company provides a Network Detection and Response solution through titled ‘Flowmon ADS’ that leverages behavior analysis algorithms to detect anomalies concealed within the network traffic to expose malicious behaviors, attacks against mission-critical applications, data breaches, and indicators of compromise.

Flowmon ADS detects and mitigates the cyber threats facing an organization by adding a SOC visibility triad to the organization's network-centric layer. This detects any anomalies hitherto escaping the deployed perimeter and endpoint security products. Flowmon ADS also offers incident visualization in the MITRE ATT&CK framework for a better understanding of the threat. Additionally, the product also leverages AI to reveal unknown threats in the environment while integrating with network access control, authentication, firewall, and other tools for immediate incident response.

Flowmon ADS receives event data from Suricata IDS that allows organizations to cover more attack vectors in the network and mitigate threat with both signature and non-signature approach. Flowmon ADS provides automated pre-defined configurations for a variety of network types that facilitates the SOC team by distinguishing between anomalies and normal traffic to reduce false positives. Furthermore, it provides context-rich evidence, visualization, network data, or full packet traces for forensics to understand and respond to suspicious events.

Flowmon ADS offers custom dashboards based on severity rules at a global, group, or user level to prioritize and report for security, networking, IT helpdesk, or managers. Flowmon ADS also offers automated script-based integration with network or authentication tools to mitigate attacks. Furthermore, it automatically captures full packet when detecting an event that includes network data, even from the period before the attack started which gives a detailed view of the attack to the SOC team. Flowmon ADS also offers custom detection methods with rule-based SQL-like syntax to expose and mitigate unwanted traffic specific to the client's network.

Flowmon ADS offers behavior patterns to detect misuse and suspicious behavior of users, devices, and servers by understanding DNS, DHCP, ICMP, and SMTP. Furthermore, it offers integration with SIEM, big data platforms, incident handling or response tools via syslog, SNMP, email, REST API, or custom scripts to serve as a critical source of information to log management.

Analyst Perspectives

Following is the analysis of Progress's capabilities in the Network Detection and Response Market:

- Flowmon ADS offers deployment of product in the customer network including hybrid networks and monitoring of VPC traffic in public cloud. Furthermore, Flowmon Threat Intelligence which is a cloud-based service that feeds Flowmon ADS with reputation data on malicious IPs or domains to augment the behavior-based detection of the network. Flowmon ADS also leverages an ML-powered detection engine and combines multiple detection mechanisms to reveal malicious behavior, data breaches, and attacks against mission-critical applications to expose and mitigate any cyberthreat.

- Flowmon ADS offers the option to deploy dedicated sensors (Flowmon Probe) in the user's network to gain linear scalability along with the Flowmon Collector for robust analysis of the network to help SOC team with a detailed view of the network. Flowmon ADS also leverages flow (IPFIX) technology which stores a small amount of data compared to traditional packet-based solutions making it highly scalable for enterprises of all sizes along with an option of on-demand full packet capture. Furthermore, it can be integrated with network access control, authentication, firewall, or other incident response tools while ingesting data from various sources like AWS, Google Cloud, and Progress LoadMaster.

- Regarding geographical presence, the company has a strong presence in EMEA, followed by APAC and North America. From an industry vertical perspective, the company holds a strong customer base in e-commerce, retail, government, healthcare, financial services, telecom, education, energy, and manufacturing domains. From a use case perspective, the company offers threat detection, threat hunting, forensic analysis, and active response.

- Progress's primary challenges include growing competition from big vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations as well. However, with its strong research and development projects on encrypted traffic analysis, complex event processing & correlation into high-level incidents, discovery, and assisted configuration that will significantly reduce manual effort to deploy, configure, tune up, and maintain the system and robust customer value proposition, Progress is well-positioned to maintain and grow its market share in the Network Detection and Response Market.

- Regarding future roadmap, Progress is investing in R&D to expand its arsenal of detection methods to cover more security scenarios by leveraging ML along with developing encrypted traffic analysis capabilities to expose threats within the encrypted connections automatically through AI. Furthermore, the company is investing in complex event processing and correlation to infer high-level incidents into actionable intelligence to empower SOC teams.

Trellix

URL: https://www.trellix.com/en-us/index.html

Founded in 2002 and headquartered in Milpitas, California, USA. Trellix is a cybersecurity company that provides the detection and response (NDR) platform to help organizations secure themselves from advanced threats. Trellix offers 'Trellix Network Security,' a network detection and response solution that facilitates the SOC team to focus on attacks, prevent intrusions with robust intelligence, and eliminate the cybersecurity blind spots.

Trellix Network Security provides automatic detection and response of suspicious network activity and attack prevention with non-signature tactics by leveraging artificial intelligence (AI), machine learning (ML), and correlation engines along the lateral movement. Additionally, Trellix Network Security is integrated with Trellix Intrusion Prevention System that detects hidden intruders and keeps the network secure. It enables users to continuously monitor their network for malicious activity and block intrusions with the help of its robust threat prevention capabilities.

Trellix's Network Security offers integration with Network Forensics for deep inspection of the threats impacting a user's organization. Trellix Network Forensics enables user to better quantify the impact of an attack and improve the quality of their response. Also, users can visualize events before, during, and after an attack to keep incidents from continuously taking place. Additionally, Trellix Network Security can increase virtual network visibility to gain east-west network visibility and threat protection across virtualized infrastructure and data centers. Furthermore, it can inspect network traffic decrypt and analyze network traffic with inbound and outbound SSL decryption.

Trellix Network Security leverage ML/AI and correlation engines for retroactive detection, which detects known and unknown threats in real time while also enabling back-in-time detection of threats. It also reduces the post-breach dwell time by detecting suspicious lateral movements that hover over the user's workplace network. Additionally, it provides deployment flexibility to discover and block advanced threats on-premises, in virtual environments, software-defined data centers, and private and public clouds.

Analyst Perspectives

Followings is the analysis of Trellix capabilities in the global Network Detection and Response market:

- Trellix Network Security is a unified NDR platform to monitor, detect, and block known and unknown threats across email, endpoints, and other security services. Additionally, Trellix Network security leverages SmartVision to detect malicious traffic moving between clients and network devices while communicating over Server Message Block.

- Trellix Network Security offers real-time inline blocking that stops attacks instantly with robust intrusion prevention and performs deep inspection of network traffic to detect and protect against malware callbacks and other threats. Furthermore, it provides signature based IPS detection and noise reduction, which helps to eliminate manual tasks. It offers riskware detection and categorization to prioritize response to threats. It also provides contextual information to understand the in-depth information about the attack and the attacker.

- Geographically, Trellix has a strong presence in North America followed by APAC and EMEA. From an industry vertical perspective, the company holds a strong customer base in education, financial services, government, healthcare, energy, retail, manufacturing and others. From a use case perspective, the company offers threat detection, threat hunting, threat visibility and kill chain of malware, and ransomware.

- Trellix's primary challenges include growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, Trellix is well-positioned to maintain and grow its market share in the Network Detection and Response Market.

- Trellix as their roadmap strategy is investing on their R&D to increase their security tools innovation in their primary XDR platform. Additionally, Trellix is focusing on enhancing capabilities, increasing the number of number of customers, geographical presence, different industry verticals, and expanding use case support.

Vectra AI

URL: https://www.vectra.ai

Founded in 2010 and headquartered in San Jose, California, USA, Vectra AI offers products that provide artificial intelligence (AI)-driven threat detection and responses for hybrid and multi-cloud enterprises. The company provides 'Cognito Detect,' a network detection and response (NDR) solution that uses AI to deliver real-time attack visibility and provides contextual attack details for carrying out responses.

Cognito Detect integrates with Cognito AI to automate the manual, time-consuming analysis of security events and solve the threat investigation efficiently to reduce the SOC team's workload, which results in faster response to hidden threats. Furthermore, it identifies, tracks, and scores every IP-enabled device from the cloud to the enterprise.

Cognito Detect offers the STIX threat intelligence capability that detects threats by leveraging threat intelligence and provides real-time visibility into cloud and enterprise traffic by extracting network metadata from packets, enabling protection without breaching privacy. Additionally, it provides visibility across laptops, servers, printers, BYOD, and IoT devices as well as all operating systems and applications. Along with traffic between virtual workloads in data centers and the cloud, even SaaS applications as Metadata analysis is applied to all internal (east-west) traffic, Internet-bound (north-south) traffic, virtual infrastructure, and cloud environments.

Cognito Detect offers the Threat Certainty Index that consolidates thousands of events and historical context to prioritize hosts that pose the most threat. Subsequently, Cognito Detect sends threat alert notifications to the SOC team or a response from other enforcement points, SIEMs, and forensic tools. Additionally, by exposing the connections between hosts across internal detections, external advanced command-and-control detections, and connectivity to shared command-and-control infrastructures, the Attack Campaigns capability within it significantly automates security detections. Cognito Detect provides smooth synchronization, retention and constant coordination between networking, application development, virtualization teams, and the security team with full visibility from cloud to enterprise from remote workplaces.

Analyst Perspectives

Followings is the analysis of Vectra AI capabilities in the global Network Detection and Response market:

- Vectra AI offers Cognito Detect, the artificial intelligence (AI) and machine learning (ML)-based NDR solution to detect and stop cyberthreats in real time. Vectra AI Cognito Detect offers AI-based always-learning behavioral models, which helps organizations to detect and stop unknown and hidden attackers and offers a clear starting point for AI-assisted threat hunting. Cognito Detect offers interoperability with user’s legacy security infrastructure like firewalls, endpoint security, NAC, and other enforcement points, while providing a clear starting point for a more extensive search with SIEMs and forensic tools. Additionally, Cognito Detect also generates syslog messages and CEF logs for all detections and prioritized host scores. This makes it a trigger for investigations and workflows within the user's SIEM solution.

- Cognito Detect offers capabilities that recognize and evaluate interactions between workloads and identities, which facilitates SOC teams to understand how they function in an environment. Furthermore, it provides on-demand access to enriched metadata from captured packets for further forensic analysis that helps SOC teams with the proof and accuracy they need to take immediate, decisive actions. Additionally, it also uses Privileged Access Analytics to automatically analyze behaviors and AI to identify entities with privileges and differentiate between approved and malicious uses that are hidden inside cloud, data center, IoT, and enterprise networks.

- Cognito Detect offers capabilities to identify ransomware campaigns against enterprises and other organizations across all phases of an attack. By monitoring all internal network traffic, Cognito Detect identifies the fundamental behaviors of a ransomware attack as it attempts to take critical assets hostage. In addition to detecting ransomware directly, Cognito Detect exposes ransomware precursors, including command-and-control traffic, network scans, and spreading behavior that ransomware relies on to find and encrypt critical assets.

- From the geographical perspective, Vectra AI has a strong presence in North America followed by EMEA and APAC. From an industry vertical perspective, the company holds a strong customer base in healthcare, financial services, and manufacturing. From a use case perspective, the company offers threat hunting and detection, forensic investigation, vulnerability assessment, and compliance.

- Vectra AI's primary challenges include growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small- to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnerships, compelling customer references, and robust customer value proposition, Vectra AI is well-positioned to maintain and grow its share in the NDR market.

- Vectra AI as their roadmap strategy is investing in their R&D to develop their security offerings to meet the need of the dynamic time. Additionally, it is focusing on enhancing capabilities, increasing the number of number of customers, geographical presence, different industry verticals, and expanding use case support.

VMware

URL: https://www.VMware.com/in.html

Founded in 1998 and headquartered in Palo Alto, California, USA. VMware is a well-known cloud and virtualization service provider. The company offers various software solutions for app modernization, multi-cloud, digital workspace, networking, and security. It also provides network detection and response solutions through its product NSX Network Detection and Response (NDR) that facilitates network security and SOC teams to prevent ransomware, detect malicious network activity, and stop the lateral movement of threats.

NSX Network Detection and Response receives threat signals from network traffic analysis, intrusion detection and prevention, and network sandboxing engines to deliver broad set of threat detection capabilities. Additionally, VMware's NSX offers contextual information to network security and SOC teams to block malicious attacks from the traffic crossing the perimeter and moving laterally across the network.

VMware NSX offers a set of built-in detectors, an AI-based Network Traffic Analytics engine, a signature-based IDS/IPS engine, and third-party threat intelligence feeds to mitigate threat. NSX NDR distributes agentless network sensors to ensure inspection of all East-West traffic and provide threat detection. Additionally, NSX NDR offers threat detection in an encrypted traffic with novel machine learning (ML) models that operate on JA3 hashes and network meta-data. which analyses encrypted files at each host through guest introspection.

VMware allows organizations to use NDR capabilities into vNIC within the hypervisor that provides comprehensive visibility into organizations' network threats and allows to remove any network taps or discrete sensors. Furthermore, NSX NDR adheres to MITRE ATT&CK framework, thus providing coverage and protection across 12 MITRE ATT&CK tactics through network prevention, detection, and response capabilities.

Analyst Perspectives

- Followings is the analysis of VMware capabilities in the global Network Detection and Response market:

- VMware offers a robust NDR solution that increases SOC efficiency and reduces false positives by focusing on threat campaigns rather than just isolated anomalous events unlike legacy security tools. The AI-based correlation engine generates high fidelity, highly accurate alerts that provide authoritative context to speed up forensics. This allows security operations teams to direct their attention on a small subset of relevant events instead of digging through thousands of anomalies.

- VMware NSX NDR ingests signals from detectors within NSX regarding initial access attempts by detecting phishing emails and malicious links that trick the users and evade their defenses. VMware NSX allows organizations to detect phishing emails and malicious links by leveraging signals from detectors within NSX. Furthermore, NSX NDR allows VMware Threat Analysis Unit to continuously update NSX Network Detection and Response in real time with threat intelligence, such as active command and control (C&C) servers, objects with zero-day exploits, toxic websites and malware distribution points, and malware information useful to defend against threats specific to user's organization.

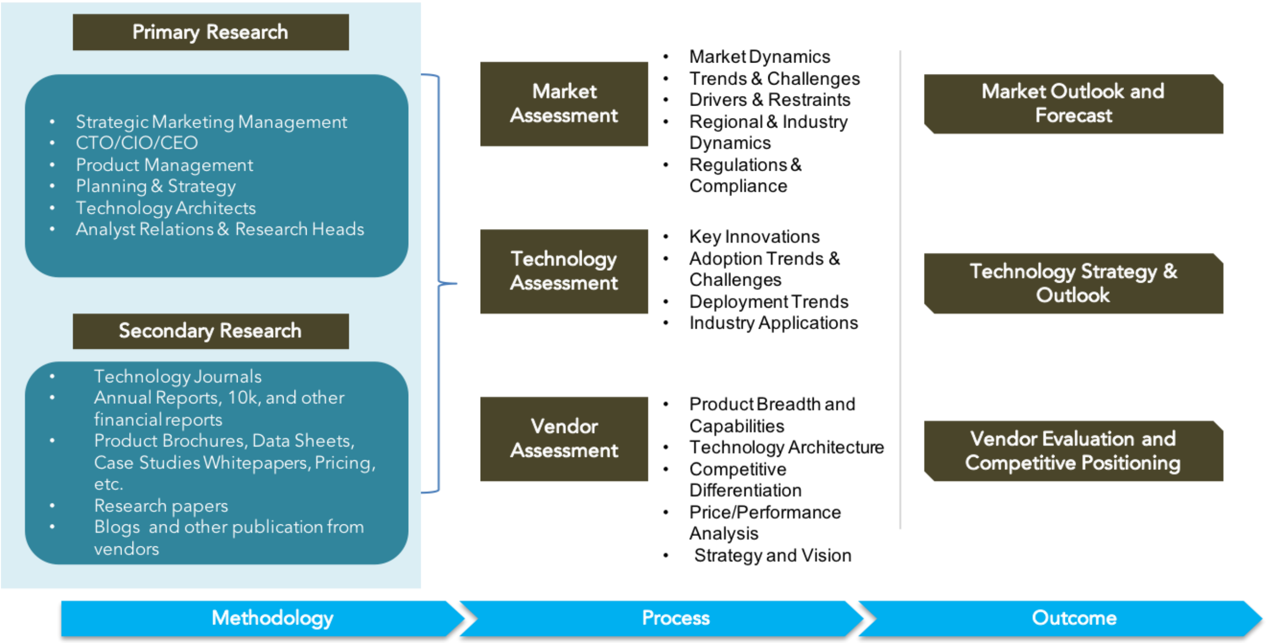
- From the geographical perspective, VMware has a strong presence in North America followed by APAC and EMEA. From an industry vertical perspective, the company holds a strong customer base in education, financial services, government, healthcare, retail, life sciences, and manufacturing with their Network Detection and Response solutions. From the use case perspective, the company can block Lateral Threat Movements, stop Advanced Malware, enable Multi-Cloud Security, and improve SOC Forensics.

- VMware’s primary challenges include growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small- to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, VMware is well-positioned to maintain and grow its market share in the Network Detection and Response market.

- VMware as their roadmap strategy is investing in their R&D to prevent against modern sophisticated malware. Additionally, VMware is focusing on enhancing capabilities, increasing the number of number of customers, geographical presence, different industry verticals, and expanding use case support.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is the brief description of the major sections of our research methodologies.


Primary Research
Strategic Marketing Management
CTO/CIO/CEO
Product Management
Planning & Strategy
Technology Architects
Analyst Relations & Research Heads
Secondary Research
Technology Journals
Annual Reports, 10k, and other financial reports
Product Brochures, Data Sheets, Case Studies Whitepapers, Pricing, etc.
Research papers
Blogs and other publication from vendors
Market Assessment
Market Dynamics
Trends & Challenges
Drivers & Restraints
Regional & Industry Dynamics
Regulations & Compliance
Technology Assessment
Key Innovations
Adoption Trends & Challenges
Deployment Trends
Industry Applications
Vendor Assessment
Product Breadth and Capabilities
Technology Architecture
Competitive Differentiation
Price/Performance Analysis
Strategy and Vision
Market Outlook and Forecast
Technology Strategy & Outlook
Vendor Evaluation and Competitive Positioning
Methodology
Process
Outcome

Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant’s Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists

- Published secondary data on companies and their products
- Database of market sizes and forecast data for different market segments
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team researches with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

Data Analysis: Market Forecast & Competition Analysis

Quadrant's analysts' team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios, economic most accurate forecast scenario for the overall market and its segments.

In addition to market forecasts, our team conducts a detailed review of industry participants to prepare competitive landscape and market positioning analysis for the overall market as well as for various market segments.

SPARK Matrix:

Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis and forecasts, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including market forecast; competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.