KuppingerCole Report

LEADERSHIP COMPASS

By John Tolbert
November 18, 2021

Network Detection & Response (NDR)

This report provides an overview of the market for Network Detection and Response tools (NDR) and provides you with a compass to help you to find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing NDR solutions.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction / Executive Summary

Commercial, government, and non-profit organizations of all kinds increasingly find themselves under cyber-attacks these days. Ransomware, fraud, credential theft, PII theft, and intellectual property theft occur on a daily basis around the globe. IT teams mitigate the risks by employing and deploying a wide array of cybersecurity tools. Many components of security architectures are well-known: firewalls, VPNs, Endpoint Protection Detection & Response (EPDR), Security Incident and Event Management (SIEM), etc. In the last decade, security professionals have pivoted to address how to detect attacks and other malicious activities, rather than focusing solely on prevention. SIEM and IDS (Intrusion Detection Systems) were touted as solutions for detection, but they quickly maxed out their potential usefulness and have been forced to evolve. Endpoint Protection (EPP) has largely merged with Endpoint Detection and Response (EDR), which came to the fore as a means of discovering malicious behavior on desktops, laptops, and servers.

NDR solutions are designed to help security analysts discover evidence on the network and/or in the cloud of malicious activities that are in progress or have already occurred. NDR tools are effectively “Next-Gen IDS”. One of the big differences between NDR and old IDS tools is that NDR tools use multiple Machine Learning (ML) techniques to identify normal baselines and anomalous traffic, rather than static rules or IDS signatures. Given the volumes of network connection data that must be analyzed, using ML algorithms and models is a “must” rather than a “nice-to-have”. Historically, the major drawbacks to IDS were that it was labor intensive to operate, was of limited effectiveness, and could generate high numbers of false positives.

These security tools were created to discover and remediate certain types of attacks. Advanced Persistent Threats (APTs) are often perpetrated by actors from state intelligence agencies for the purpose of gathering intelligence on foreign companies and agencies, copying intellectual property, or sabotage. APT actors may also include well-funded but unscrupulous companies and hacktivist groups. Their goals often require long-terms presence on victims’ properties, hence the use of the term “persistent”. APT groups have historically been the most likely ones to use Zero-Day exploits (those which were previously unseen in the wild), that may give them the advantage of not being detected by EPDR agents. In the last couple of years, cybercriminal groups have begun to use APT strategies and tactics against their victims: gaining access to resources, siphoning out data, then detonating ransomware.

Enter NDR as an additional tool to discover hitherto unknown compromises. Since data exfiltration is usually an objective of attackers, even in contemporary ransomware cases executed by cybercriminal units, properly deployed NDR tools can be better suited at discovering lateral movement from the initial compromised device to other assets within the target organization, use of compromised privileged credentials, and data exfiltration attempts.

NDR tools are also deployed to provide visibility in OT/ICS/IIoT environments where it may not be possible to implement endpoint agent-based solutions. Enterprises often separate OT/ICS and IIoT devices onto their own networks for containment purposes. Such network segmentation is indeed useful, and the control

points between these specialized networks and general-use and back-end networks are logical places to deploy NDR sensors.

NDR tools can also help discover and remediate more common types of attack such as unwanted bot activities, credential theft, and insider threats.

NDR solutions can log all activities from attached networks in a central secure location for both real-time and later forensic analysis. NDR solutions are usually implemented as a mix of appliances, virtual appliances, and IaaS VM images. Appliances and/or virtual appliances deployed on-premises must tap into physical networking gear at all relevant network control points: off switch and router span or tap ports, or off network packet brokers. For example, if your organization still has perimeters (and most do), NDR appliances need to be placed there. Vendors often talk about “north-south” (across perimeters) and “east-west” (lateral movement) deployment points. All directions need to be covered by NDR solutions for maximum coverage.

Alternatively, some NDR virtual appliances can be co-located with firewalls or other perimeter network devices. Other common places to deploy NDR sensors are between network segments, around IoT and/or OT and Industrial Control Systems (ICS) / SCADA networks, and around web-facing properties and Wi-Fi portals. With an irreversible Work-From-Home (WFH) trend in response to the global pandemic, NDRs should be deployed alongside VPNs. NDR VMs can be inserted into your IaaS and potentially PaaS infrastructure as well. Exactly how many appliances or virtual appliances your organization needs and where they should be placed depends on your architecture. Proper design of NDR deployments is necessary to monitor all traffic flows.

A key differentiator for NDR technology is the employment of multiple ML algorithms in the various analysis phases. At a high level, unsupervised ML finds outliers or anomalies in traffic patterns; while supervised ML models categorize possible threats among the outliers, classify malicious activities, domains, and other attributes. Supervised ML is more commonly used by vendors for Encrypted Traffic Analysis. Deep Learning (DL) algorithms and detection models utilize variations of neural networks and are the latest generation of AI/ML technology as applied to the cybersecurity space. Some NDR vendors use DL for Encrypted Traffic Analysis. The most effective solutions utilize several layers of ML-and DL-enhanced processing of all traffic at line speed. Vendor products in this segment typically advertise 10 – 200 Gbps throughput on network sensors, and 1 Gbps for IaaS traffic scanning.

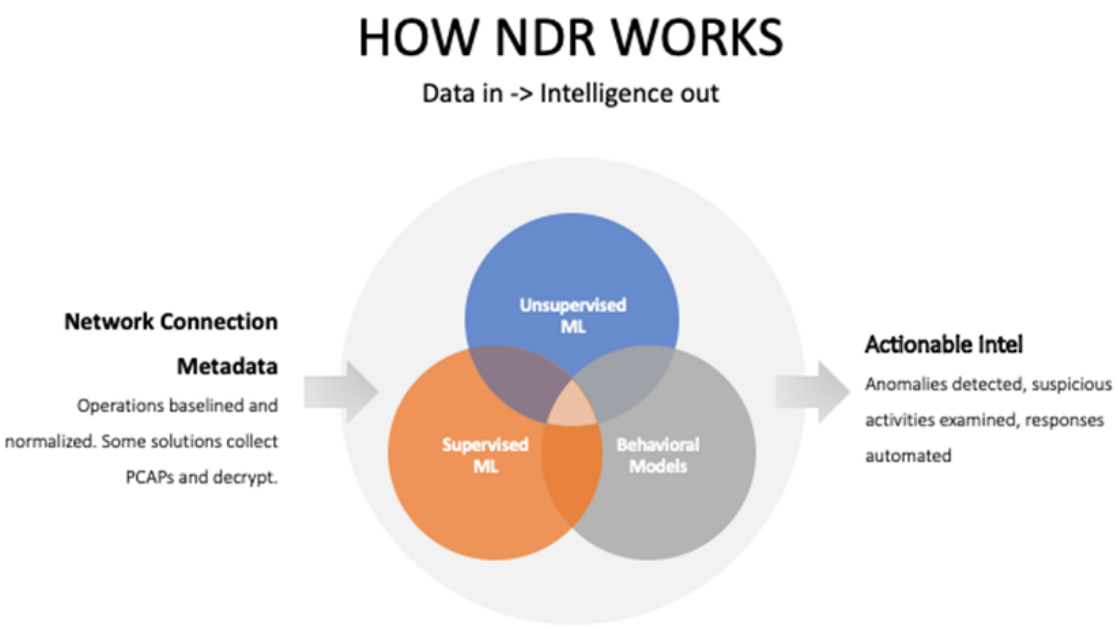


Figure 1: How NDR Works

In terms of responses, NDR solutions can provide dashboards/alerts/reports, display real-time visualizations, allow drilldowns into details, enrich discoveries with threat intelligence, correlate events and provide automated analysis, halt suspicious traffic, isolate nodes, and send event data to SIEMs, SOARs, and forensic/case management applications. In cases where vendor products operate in passive mode, they direct 3rd-party security tools via APIs to execute these responses.

NDR solutions are not usually easy to operate, and in some cases require a dedicated team of one or more analysts (depending on organization size) to make the best use of the capabilities. Knowing this, many vendors provide facilities within their solutions to automate aspects of analysis, including evidence collection, correlation, remediation suggestions, and root cause analysis (RCA). Many of the vendors in the NDR space offer managed services of different types to augment the products. Additionally, many MSSPs can manage an NDR deployment and handle the threat hunting and analysis tasks on behalf of their customers.

There are several good reasons to consider deploying NDR. The typical capabilities outlined above can be of service in discovering malicious activity that your other security tools may have missed.

Endpoint Protection Detection & Response (EPDR) agents are a must for every computing device that can run them. However, sometimes they may not catch every piece of malicious code. There are several reasons why NDR is a needed complement to EPDR and other security solutions:

1. **BYOD bypass:** In permissive environments, some users may bring in infected devices and not know

it because their machines do not have EPDR agents. Business partners and contractors may use their own devices, which may be beyond the control of the hosting organization.

2. **Ineffective EPP:** Some EPP solutions are better at detecting and preventing malware than others. Also, EPP agents need to be updated; even those that use ML-driven heuristics and exploit prevention. If EPP solutions are weak or have outdated signatures or ML models, they are more likely to miss malware. Ultimately, it is not logically possible to design an anti-malware solution that can detect malicious code with 100% accuracy all the time.
3. **Non-traditional endpoints:** Many IoT and IIoT devices can't run EPDR. Operating systems may not support EPDR agents but are still susceptible to hacking. In other cases, IoT devices are simply not user configurable. Enterprises with large numbers of such devices tend to isolate them onto separate VLANs. These environments need security monitoring and detection capabilities that cannot be delivered by standard endpoint security solutions.
4. **Endpoint that cannot run agents:** Some Linux and Windows computing devices have limited builds of operating systems to host specific applications and are not manageable by IT staff. For example, certain medical devices such as MRI machines can't have 3rd-party security software added without invalidating warranties and support agreements. Other examples may include Industrial Control Systems (ICS) and SCADA networks. These environments are known to be targeted by particular kinds of malicious actors and given the highly critical nature of the work they do, must be monitored and protected. As in the IoT environments case, these environments need NDR solutions because other security technologies have no visibility here.
5. **Attack coverups:** Advanced malware can erase application and operating system log entries and suppress security tool reporting. Unauthorized and unaudited use of compromised and privileged credentials may mask attacks. Signs of malicious activity may not make it to the SIEM from endpoints. Therefore, the only place where highly sophisticated attacks may be discovered may be at the network layer.

Organizations today increasingly use the cloud, and key resources may be located in IaaS or in SaaS. Thus, NDR solutions need visibility of cloud environments. Hybrid architectures are common, so many NDR customers need coverage for hybrid architectures.

Even though endpoint-based solutions may not have visibility of all malicious activities, malware communicates on networks: with command and control (C2) servers, to other assets in the environment (lateral movement), to participate in botnets for fraud or DDoS attacks, or to exfiltrate data. Therefore, NDR tools can discover malicious activities that endpoint solutions and SIEMs miss.

NDR solutions can be thought of another block in the foundation of security and monitoring architecture. Therefore, NDR sensors need to be strategically placed at optimum intersections within computing

environments.

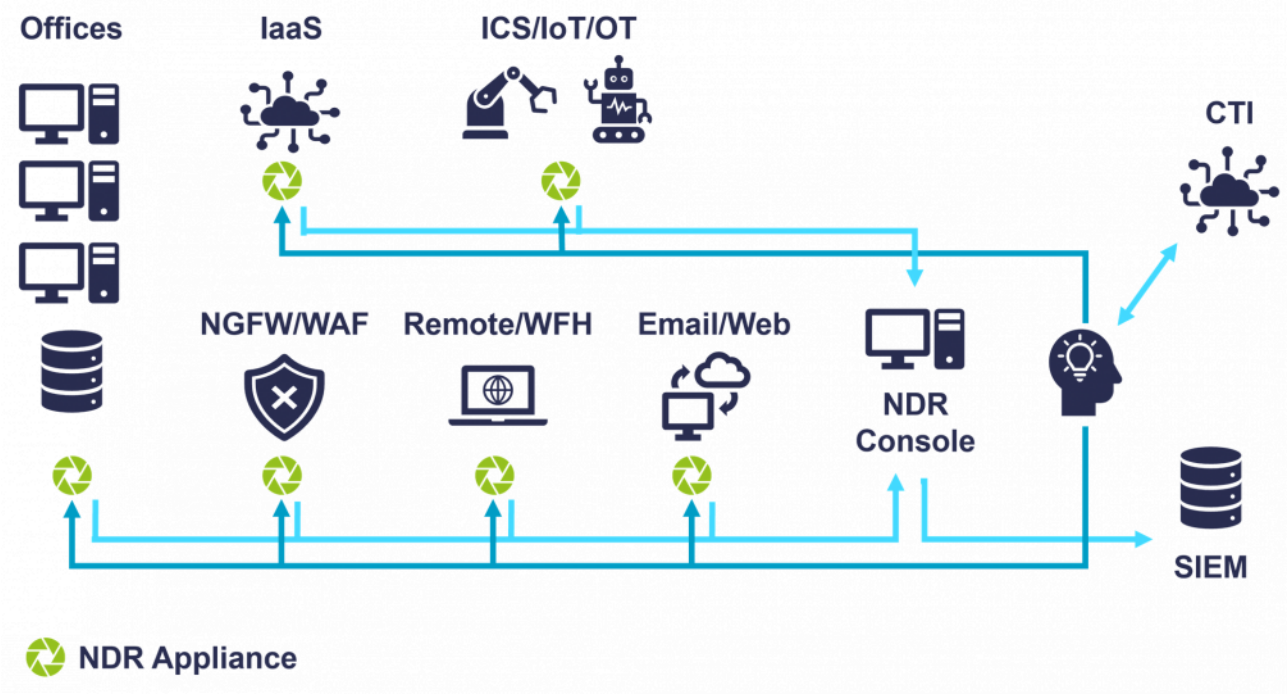


Figure 2: NDR Deployments

1.1 Highlights

The Top Ten findings in this Leadership Compass on Network Detection & Response solutions are:

- The NDR market continues to grow because customers do find value in modern ML-enhanced detection models over legacy IDS/IPS solutions.
- NDR and EPDR cover different kinds of environments, and both are needed in many kinds of organizations. Either type of solution alone may miss anomalies and thus signs of attacks.
- The future of NDR will be XDR, which is NDR + EPDR + User Behavioral Analysis (UBA) + Distributed Deception Platforms (DDP) + Cloud Workload Protection Platforms (CWPP). This market-wide union of product types is probably 3-5 years out, although some vendors have already begun to acquire and consolidate these products.
- Two major deployment paradigms exist in the NDR world: in-line sensors and passive sensors. In-line sensors offer direct response capabilities, while passive sensors rely on integrations. Both types of solutions continue to gain market share.

- Operational Technology Security and Industrial Controls Security are use cases that can be well-served by NDR. A majority of vendors in this report offer varying degrees of coverage for these environments.
- The Response part of NDR is becoming more widely utilized. Early adopters of NDR saw benefits from increased visibility and the ability to detect malicious activities, but many were not ready to allow automated responses. This may have been due to customers not fully trusting the solutions to take actions autonomously, such as shutting down connections and isolating hosts. Some may have felt like the risk of false positives negatively impacting productivity to have been too great. However, with the proliferation of ransomware, more NDR customers are opting to automatically mitigate damage.
- NDR as a managed service is rising. Some vendors offer managed detection and response services, and more MSSPs have NDR as part of their portfolio. NDR as part of an overall MDR (not just EDR) will be appealing to SMBs and some enterprises that need the functionality but do not have the expertise to deploy and maintain it.
- The product leaders in NDR are Arista Networks, Broadcom, Check Point, Cisco, ExtraHop, Fidelis Cybersecurity, Gurucul, NetWitness (RSA), and VMware.
- The innovation leaders in NDR are Arista Networks, Broadcom, Check Point, Cisco, ExtraHop, Fidelis Cybersecurity, Gurucul, and VMware.
- The market leaders in NDR are Arista Networks, Broadcom, Check Point, Cisco, ExtraHop, FireEye, NetWitness (RSA), and VMware.

1.2 Market Segment

The NDR market segment has reached a high level of maturity. Many NDR products offer a fairly complete list of features and deliver real value to their customers. These products are successful at discovering malicious activity and reducing Mean-Time-To-Detect (MTTD) time, adversary dwell time, Mean-Time-To-Respond (MTTR), and data loss from attacks.

There is a good deal of variety in the types of vendors and their products in this market. On one end of the spectrum we find mid-stage startups, progressing through larger, more well-established cybersecurity specialists, to some large IT security stack vendors on the other end. In some cases, the larger vendors have picked-up NDR functionality through acquisitions of smaller vendors. It may be necessary to license multiple, compartmentalized products from the large IT stack vendors in order to achieve full NDR functionality. We describe which components are necessary for each vendor in their chapter 5 entries. If this approach creates a burden on deploying organizations, it is also noted as a challenge in their chapter 5

sections.

In the case of startups and advanced NDR specialists, their products may be easier to deploy, in that, the functional components are generally contained within a smaller number of physical and logical components. For example, a dedicated NDR solution likely comes as a physical appliance, or images that can be installed as virtual appliances and in IaaS environments. The management and analyst consoles may be run on-premises or hosted by the vendor in their cloud as SaaS. If this approach makes it easier for customers to deploy, it is noted in each vendor's chapter 5 entry.

Though the market is maturing and growing rapidly, these two fundamentally different kinds of approaches to product design appeal to different kinds of organizations. Organizations with a large investment in vendor X's security infrastructure may tend to activate NDR functionality and/or add NDR specific modules via licensing with those vendors. Such companies may not publicly tender an RFP. Other companies may prefer to buy a dedicated NDR product from a specialist and run an RFP process that is aimed at such NDR specialists.

This divergence in the approaches taken by NDR customers leads to a lack of awareness among vendors and potential customers of which vendors are actually offering NDR solutions. As a result of this research, we found that some vendors did not know the range of competition in the NDR market. It is likely that organizations looking for NDR solutions may also not realize there are multiple product/service approaches to achieving the technical and business goals that NDR can provide, and that there are a variety of vendors in the space.

As we will see in the report, there is also diversity within the product offerings. The basic capabilities are generally well-met by all vendors. Analysis of real-time traffic flows against historical network connection metadata for the purpose of detecting and responding to attacks is the defining characteristic of this segment. Encrypted Traffic Analysis (ETA) is of particular importance, since the majority of network traffic, both internal to organizations and on the Internet, is encrypted. TLS 1.3 is becoming more widely utilized, which can make ETA more difficult.

Two features are not universally built-in to NDR tools: sandboxing and packet decryption. Not all vendors choose to implement these functions. Packet decryption can require a far more invasive deployment if deployed in-line, but this allows the NDR solution to essentially read all traffic as it passes by. Some vendors offer decryption in an off-line mode that doesn't impact traffic throughput, and some products can selectively decrypt traffic based on features and policy. Sandboxing is not technically feasible unless packet decryption is in place. Products which do not have built-in sandboxes may utilize 3rd-party malware analysis services. KuppingerCole research indicates that the particular market segments that vendors choose to target often has a direct effect on the type of features available in their NDR solutions. Thus, it is likely that those vendors which target government and defense customers are the ones that have full packet decryption capabilities. Private sector organizations that privacy regulatory compliance requirements tend to rely on ETA methods only.

Many NDR vendors argue that full packet decryption is unnecessary because they can reliably figure out if traffic is malicious based on analysis of a number of factors, such as NetFlows, TLS 1.2 handshake characteristics and certificate analysis, HASSH fingerprinting, JA3 and JA3S fingerprinting, SSL deny lists,

session-specific sequencing, etc. Consequently, some vendors who specialize in Encrypted Traffic Analysis techniques may not offer packet decryption. A few vendors argue that sandboxing is not necessary because they are looking for malicious traffic, not trying to uncover the malware itself. The inclusion or exclusion of packet decryption per product is indicated in chapter 5, but it is not a determining factor in whether or not a given vendor solution is considered NDR. Somewhat surprisingly, vendors report an increase in interest and utilization of packet decryption in conjunction with NDR deployments over the last year.

The use of ML is a foundational requirement for NDR and many other security solutions today. It is simply impossible for even large teams of analysts to collect, parse, and analyze the volumes of data that NDR and other tools generate.

The market is evolving as well. While at present the scope of this report has been limited to specialty NDR products and assemblages of NDR components from security stack vendors, increasingly we see signs that other types of security vendors are moving into NDR. Security companies that have agents on endpoints realize that by adding some functionality (code) to those agents, they can effectively turn every monitored node into an eXtended Detection & Response (XDR) fabric. However, products without a dedicated network monitoring capability may lack full visibility into environments that do not have EDR agents installed, such as IoT, IIoT, and some ICS settings.

Thus, NDR specialist vendors are likely to grow and take on additional endpoint security features; and they are likely to be acquired by larger security vendors, particularly endpoint security companies, who are looking to expand from EDR into XDR.

1.3 Delivery Models

NDR products require an on-premises presence for customers who have offices, data centers, factories, and other facilities with their own network infrastructure. Thus, the most common component of NDR solutions is the appliance or virtual appliance that is deployed in-line or plugs into switch/router SPAN/TAP ports or network packet brokers, or is deployed in IaaS. Some vendors provide separate appliances for on-premises management consoles, other vendors deliver integrated sensors and management consoles, while still others provide on-prem components, but telemetry is sent to the cloud for analysis and review via a SaaS-hosted console.

Most NDR vendors offer images for common IaaS environments that allow their solutions to analyze traffic in IaaS and PaaS environments. In addition to agents that allow network metadata collection and analysis for IaaS, many NDR vendors have management consoles that they operate as SaaS for clients. Even in these cases, the data collection and analysis primarily happen on customer premises or in their clouds since it is not feasible to transmit all packets or only metadata to the vendor cloud for examination.

Many vendors in this report offer managed NDR services, which can range from monitoring and alerting on activities that their solutions generate, to ongoing threat hunting, to full incident response options.

1.4 Required Capabilities

We are looking for comprehensive solutions that provide at least 5 of the 7 major areas of functionality areas:

- Support for traditional office, remote access, and data center architectures (LAN/WAN and SD-WAN), across on-premises, hybrid, private cloud, and IaaS environments
- Ability to examine encrypted common IP-based application layer traffic such as DNS, email, web, etc. for threats
- Use of both supervised and unsupervised ML and DL techniques for anomaly detection and categorization of potential threats
- Integration of cyber threat intelligence feeds
- Multi-purpose enterprise management console for alerting, reporting, analysis, and threat hunting for SOCs, security analysts, and Incident Response personnel
- Interoperability via APIs and relevant standards with other components in security architectures, particularly SIEM and SOAR
- Support for customizable playbooks and/or other automated response mechanisms

Drilling down into more detail, this report considers and rates the following criteria:

- Solutions which offer flexible on-premises deployment methods, including appliances, virtual appliances, and VM images to better fit into customer environments.
- Solutions that can be deployed within Amazon AWS, Microsoft Azure, GCP, Oracle Cloud, IBM Cloud, etc.
- Solutions which can draw from both in-vendor-network and out-of-network sources for cyber threat intelligence and effectively use that information for near real-time analysis without impeding customer business (for example, by generating high false positive rates)
- Solutions which can build a baseline of clean, normal network activity over an introductory period and can then compare it in real-time to operational traffic at line speed
- Solutions which can detect attackers' lateral movement within an enterprise
- Solutions which can detect anomalies and attacks including low-level methods such as
    - Unusual DNS queries
    - DNS tunneling and zone transfers

    - Very low volume, intermittent command & control type traffic
    - Unusual HTTP headers and SSL/TLS certificates
    - High or low volume port scanning
    - Unusual RDP traffic and/or remote file execution
    - Web shell usage
    - Network proxy bypass attempts
    - Traffic to/from unusual geo-locations
    - Large volume but slow data exfiltration attempts
    - Attempts to exploit known vulnerabilities
- Solutions which can detect high-level attack types such as:
    - Advanced Persistent Threats by state intelligence or corporate espionage actors
    - PII data breaches
    - Pre-staging of ransomware for later detonation
    - Crypto-mining
    - Fraud
    - Botnets
- Solutions which generate dashboards and reports for customers including the following standard types:
    - Open cases and status
    - Suspicious activities
    - Traffic volume discrepancies or deviations from norms
    - Top threats
    - Forensic investigation capabilities
    - Linked threat intelligence

Additional and related features will be considered as benefits but not absolute functional requirements in this analysis:

- Deployment options for Industrial Controls / Industrial IoT environments, critical infrastructure computing environments, ATM networks, medical facilities, etc.
- Protocol understanding for ICS, IIoT, and IoT environments such as BacNet, CIP, CoAP, LonTalk, ModBus, MQTT, or XMPP.

- Packet decryption. While packet decryption may be required by a small subset of customers, in most cases analysis of TLS traffic is sufficient for identifying anomalous traffic and behavior. Packet decryption can be considered a security risk in itself by some organizations.
- Sandbox integration, either on-premises or in cloud-hosted infrastructure, for detonation and analysis of suspicious code. Third-party malware analysis services are available, and some vendors choose to rely on external services rather than packaging a sandbox within their NDR solutions.
- Network sandboxes which can function autonomously (without constant connection to cloud services) in cases where customers want to deploy the solution on ICS or IIoT networks.
- NDR delivered as a service. Some organizations may choose to employ SOCaaS, MSSPs or vendor provided NDR services.
- Extended Detection & Response (XDR) functions. XDR will be the focus of future KuppingerCole reports.

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

Figure 3: The Overall Leaders in Leadership Compass Network Detection & Response

The Overall Leadership rating provides a consolidated view of all-around functionality, innovation, market presence, and financial position. However, these vendors may differ significantly from each other in terms of product features, platform support, and integrations. Therefore, we strongly recommend looking at all the leadership categories as well as each entry in chapter 5 to get a comprehensive understanding of the

players in this market and what use cases they support best.

Cisco is the leading vendor in this edition of the Leadership Compass on NDR, following by VMware, ExtraHop, Arista Networks, FireEye, Check Point, NetWitness (RSA), Broadcom, and Gurucul. Cisco has an excellent feature set, extensive customer base, global presence, and product innovation. VMware acquired Lastline in 2020 and has continued to expand its functionality and client base. Arista Networks acquired Awake Security and has also continued to build on the good base product and sell to their large customer base. ExtraHop, an NDR specialist, was recently acquired by Bain Capital Private Equity and Crosspoint Capital Partners, which will provide additional GTM opportunities. Check Point and NetWitness (RSA) appear next in the Overall Leaders. Both are global cybersecurity vendors with strong offerings in the NDR space. Broadcom, with its Symantec cybersecurity products, follows closely. Gurucul, a widely respected independent cybersecurity suite vendor, is also an Overall Leader.

The top Challengers for Overall Leadership are Fidelis Cybersecurity, Group-IB, and Plixer. Fidelis Cybersecurity combines NDR, EDR, and DDP features in their Elevate product, providing an example of what next-generation XDR solutions will look like. Group-IB and Plixer each have a differing set of features, market focus, and areas of innovation that are covered in their chapter 5 entries below. Bricata and GreyCortex debut in this edition as Challengers.

Overall Leaders are (in alphabetical order):

- Arista
- Broadcom
- Check Point
- Cisco
- ExtraHop
- FireEye
- Gurucul
- NetWitness (RSA)
- VMware

2.2 Product Leadership

Product Leadership is the first specific category examined below. This view is based on the analysis of product/service features and the overall capabilities of the reviewed solutions.

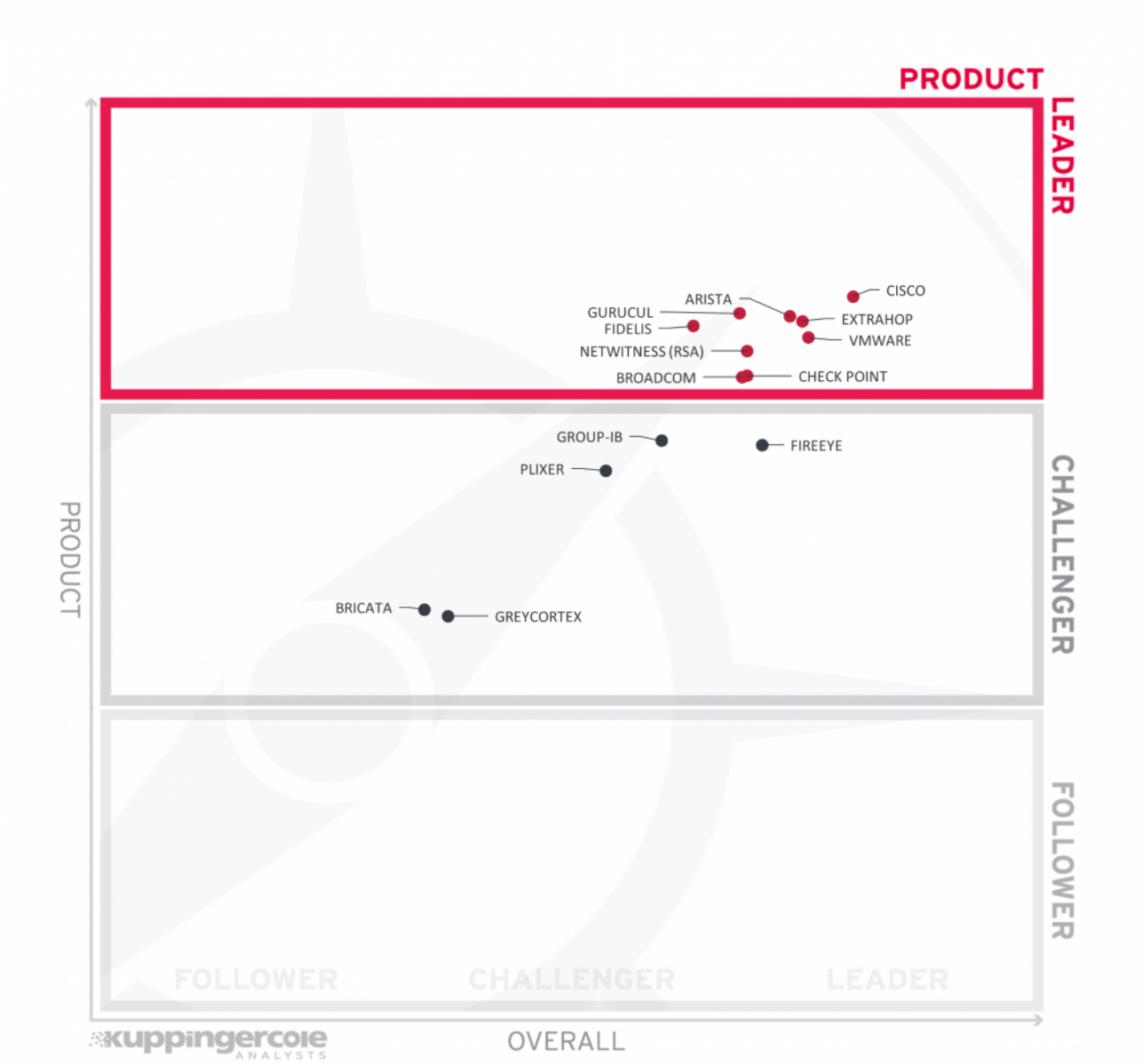


Figure 4: The Product Leaders in Leadership Compass Network Detection & Response

Product Leadership is where we examine the functional strength and completeness of services.

The top tier of Product Leaders includes Cisco, Gurucul, Arista Networks, ExtraHop, Fidelis Cybersecurity, VMware, and NetWitness (RSA). Broadcom and Check Point are also Product Leaders in this updated report. Each of these products meets and, in many instances, exceeds the majority of requirements and use cases for NDR which are defined in chapter 1 above.

Group-IB, FireEye, and Plixer are the top Challengers for Product Leadership. Bricata and GreyCortex appear below the midpoint of the Challenger rank.

The paths taken by these companies to develop or acquired NDR has differed, so the resulting product

implementations can be substantially different. For example, some products recommend MITM deployment in order to decrypt traffic, whereas others use Encrypted Traffic Analysis techniques to achieve satisfactory results for clients. Some products are deployed in-line and can execute playbooks and responses directly, while others operate out-of-band and require integration with SOAR or other security tools. More information is provided below, and a full RFI/RFP process must be engaged before selecting solutions.

Product Leaders (in alphabetical order):

- Arista
- Broadcom
- Check Point
- Cisco
- ExtraHop
- Fidelis Cybersecurity
- Gurucul
- NetWitness (RSA)
- VMware

2.3 Innovation Leadership

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

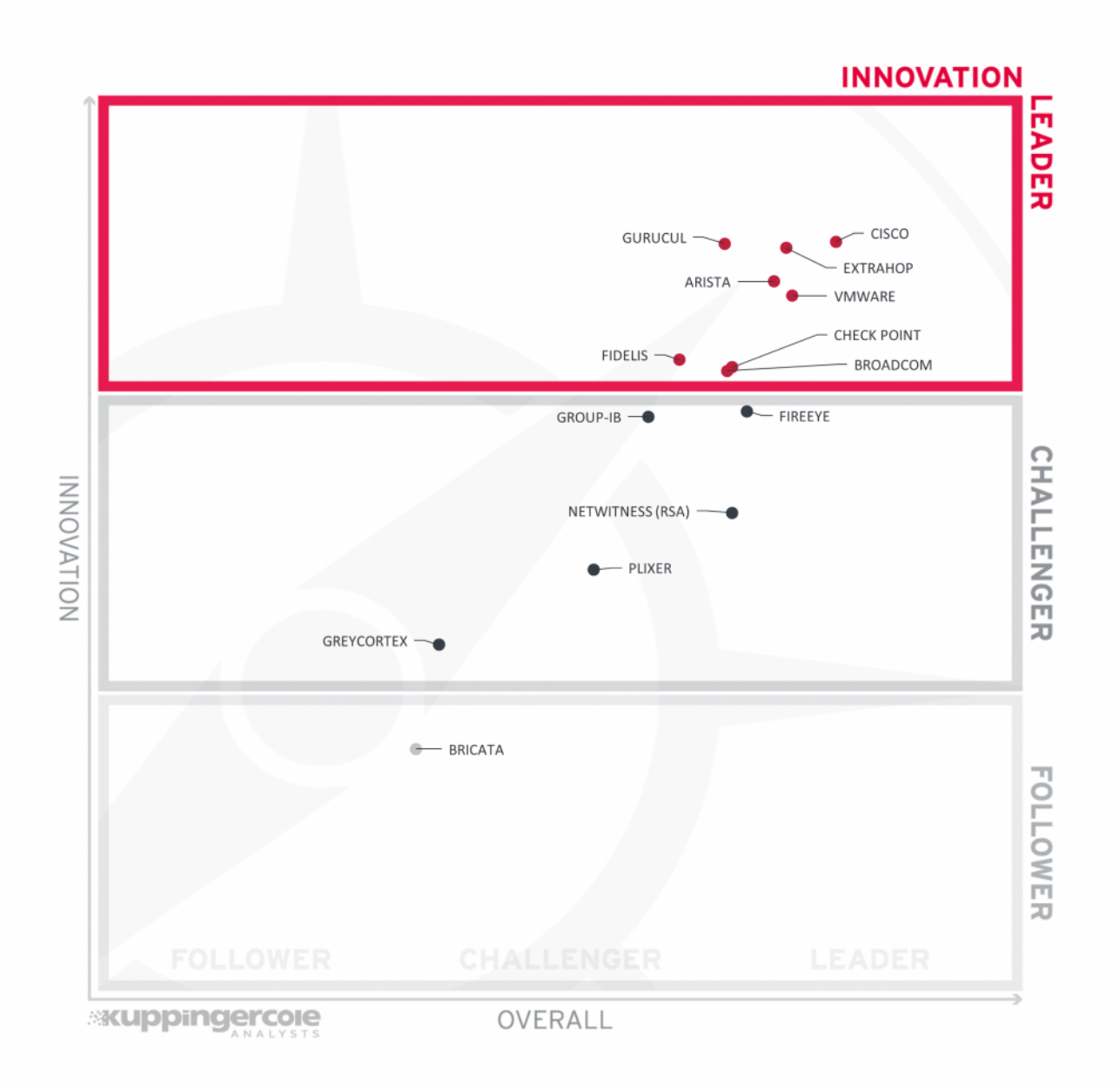


Figure 5: The Innovation Leaders in Network Detection & Response

Innovation in NDR is characterized by emphasis on Encrypted Traffic Analysis techniques, fit-for-purpose use of ML for anomaly detection and classification of possible threats, intuitiveness and utility of the analyst interface, solution understanding of OT/ICS/IIoT protocols, the ability to execute playbooks, and integrations with other security tools.

Appearing at the top of the Innovation Leaders chart in NDR are Cisco, Gurucul, and ExtraHop; followed by Arista Networks and VMware. Above the threshold for Innovation Leadership, we also find Fidelis Cybersecurity, Check Point, and Broadcom. These companies have incorporated the largest number of innovative features as described earlier.

FireEye is at the top of the Challengers on the verge of Innovation Leadership. Group-IB is also near the top of the Challenger rank. NetWitness (RSA) and Plixer are in the middle of the field. GreyCortex is in the lower third of the Challenger area. Bricata is near the top of the Followers section. These vendors have innovative features in the products, but also have ample room for enhancements.

Innovation Leaders (in alphabetical order):

- Arista
- Broadcom
- Check Point
- Cisco
- ExtraHop
- Fidelis Cybersecurity
- Gurucul
- VMware

2.4 Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

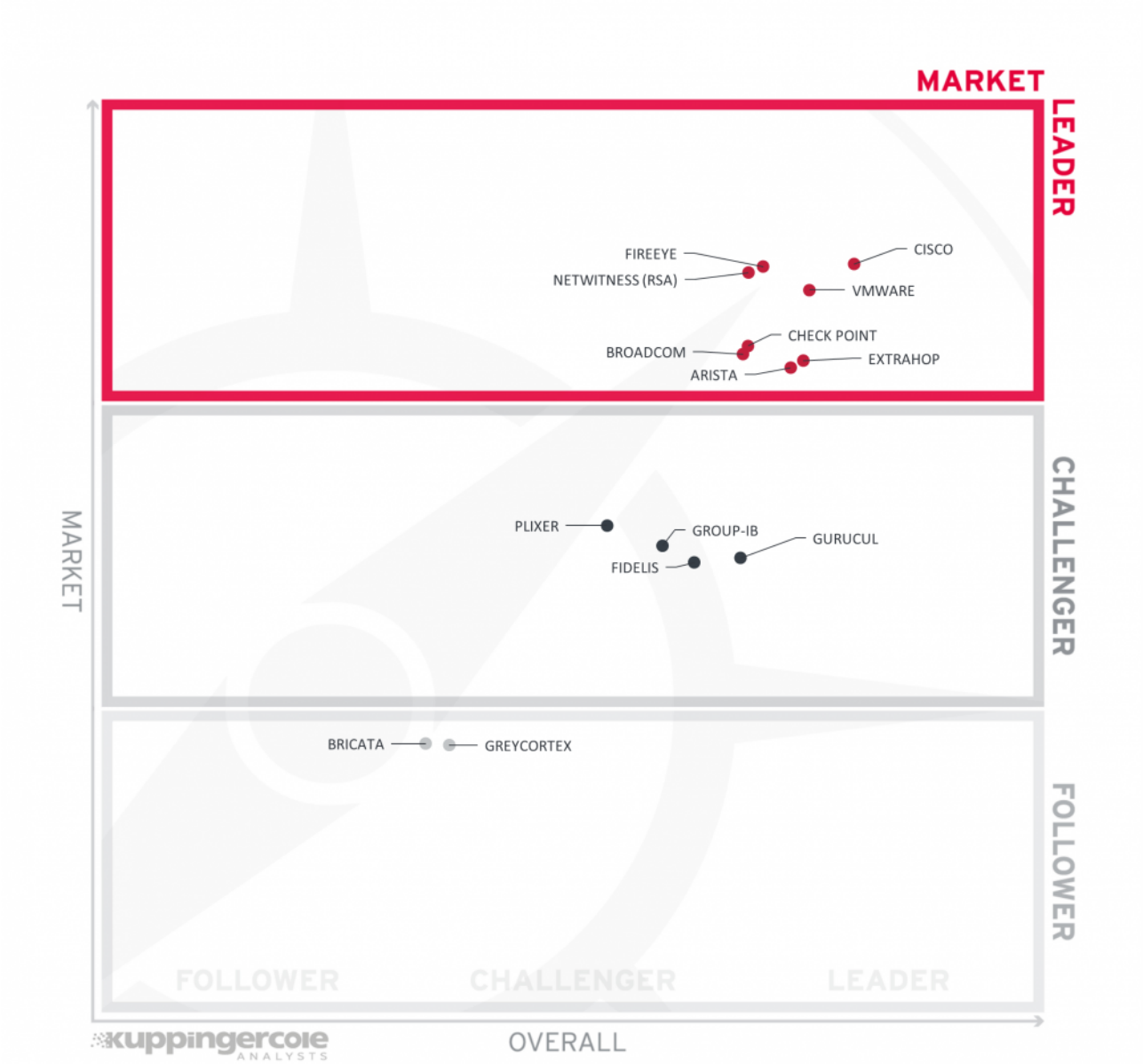


Figure 6: The Market Leaders in Network Detection & Response

Companies in the NDR space have picked up many customers since the first iteration of this report, and in some cases, significantly. Moreover, the number of acquisitions in the field indicates that NDR is a high-growth area within cybersecurity. Additional acquisitions are likely to occur in the next 12-24 months.

The Market Leaders in NDR at this time are Cisco, FireEye, NetWitness (RSA), and VMware; followed by Check Point, Broadcom, ExtraHop and Arista Networks. Market leadership is an amalgamation of numbers and geographic distribution of customers, support base, and financial strength.

Plixer, Group-IB, Gurucul, and Fidelis Cybersecurity occupy the center of the Challenger block.

Bricata and GreyCortex are the top Followers in the market. The NDR market has plenty of room for growth, and we anticipate changes in market positioning in the years ahead.

Market Leaders (in alphabetical order):

- Arista
- Broadcom
- Check Point
- Cisco
- ExtraHop
- FireEye
- NetWitness (RSA)
- VMware

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership.

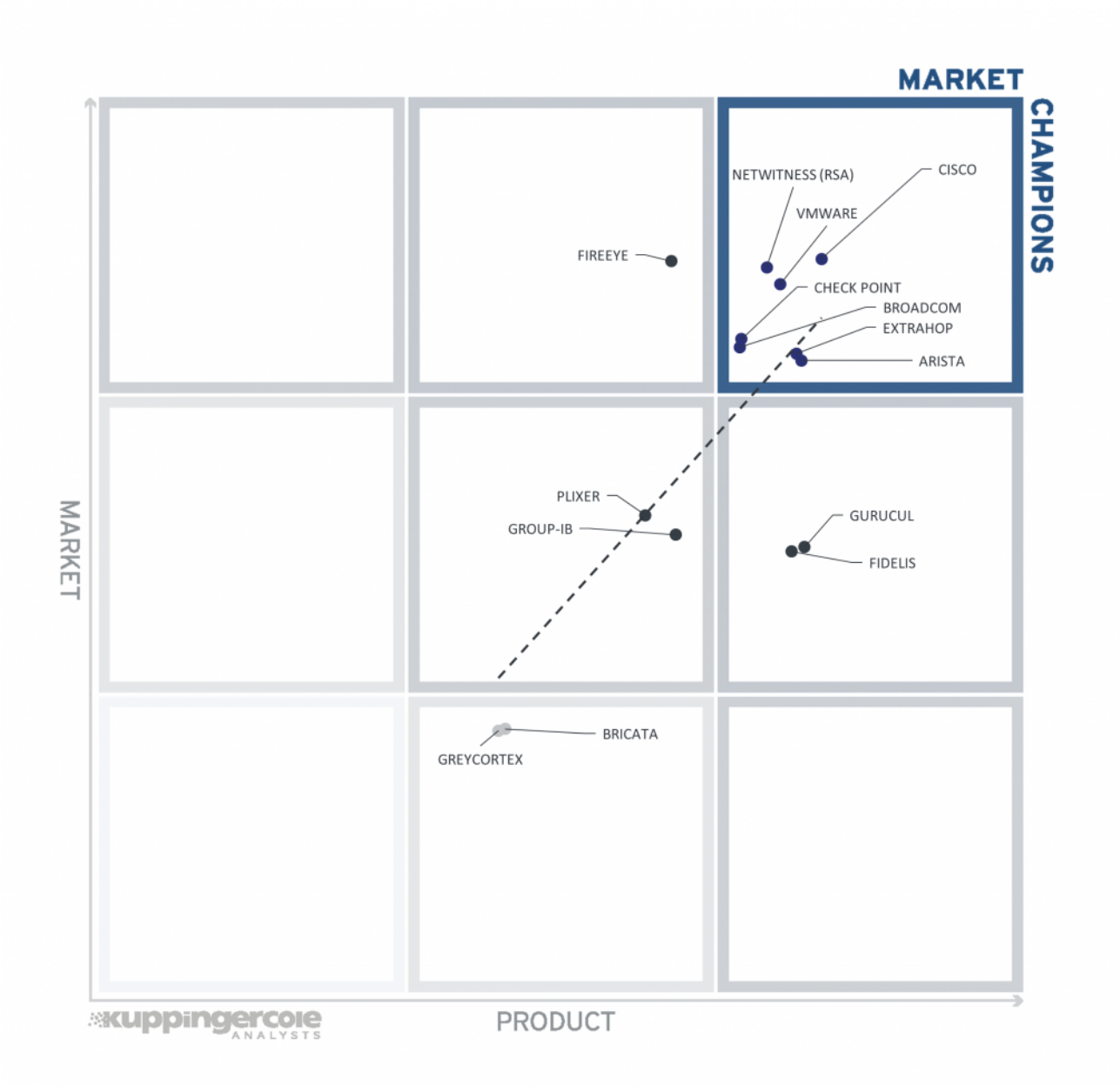


Figure 7: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership. All the vendors below the line are currently underperforming in terms of market share. However, we believe that each has a chance for significant growth.

The Market Champions in the 2021 Leadership Compass on NDR include Cisco, NetWitness (RSA), VMware, Check Point, Broadcom, ExtraHop, and Arista Networks.

FireEye is in the top center, which shows great market position relative to product positioning.

Gurucul and Fidelis are in the center right block. Being below the line shows that their products are better than the market knows at present.

Plixer and Group-IB are in the center section but below the line. They also have good feature sets and the ability to capture additional market share.

Bricata and GreyCortex are in the lower center. Both have room for growth in terms of market and product features.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

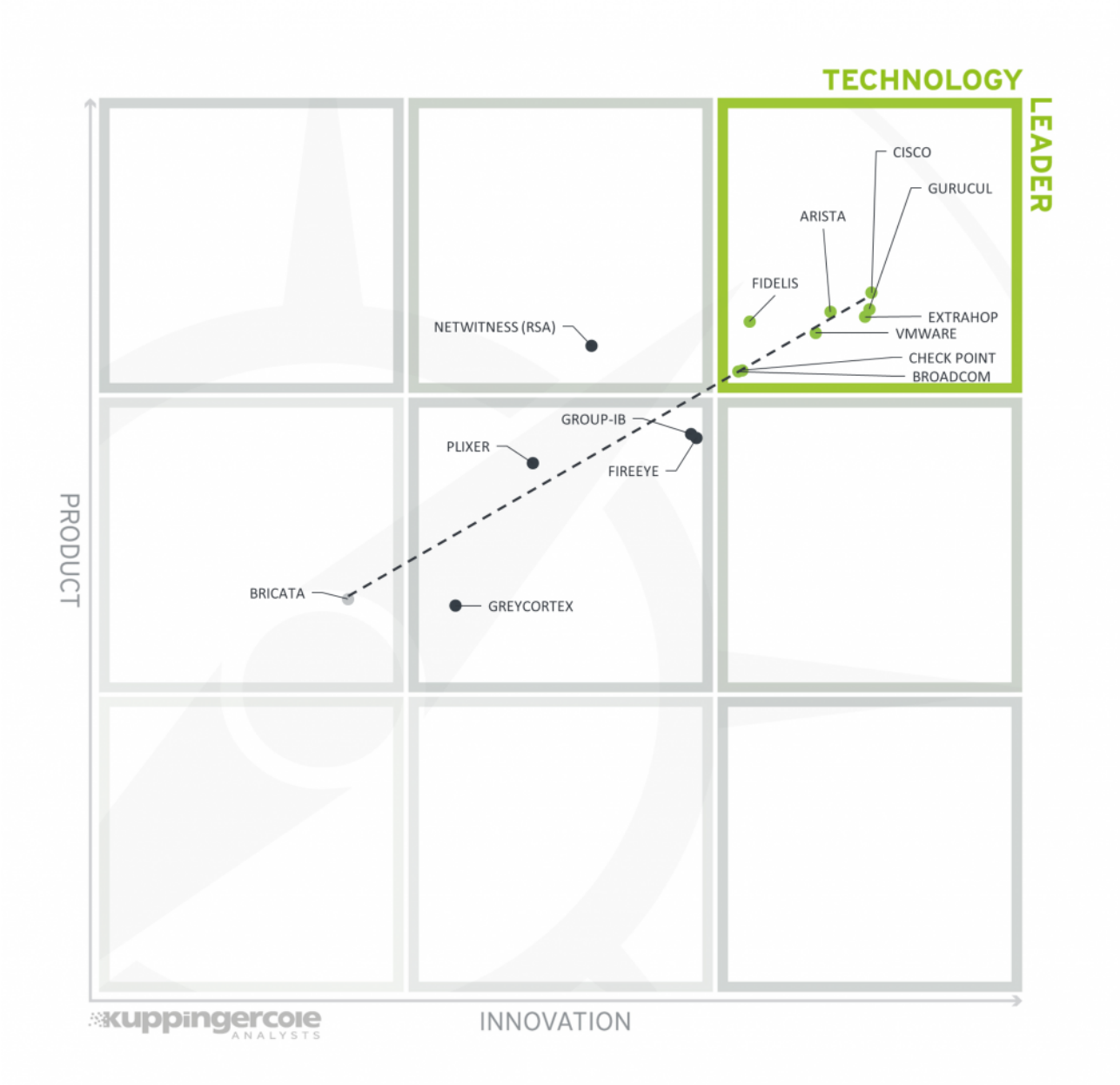


Figure 8: The Product/Innovation Matrix

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Cisco, Gurucul, Arista Networks, ExtraHop, Fidelis Cybersecurity, VMware, Check Point, and Broadcom are the Technology Leaders in NDR.

NetWitness (RSA) is the sole occupant of the top center box with a strong product but less innovation. Group-IB, FireEye, and GreyCortex are in the center section below the line; while Plixer resides above the line.

Bricata is in the left center, with room to expand basic product features and innovations.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

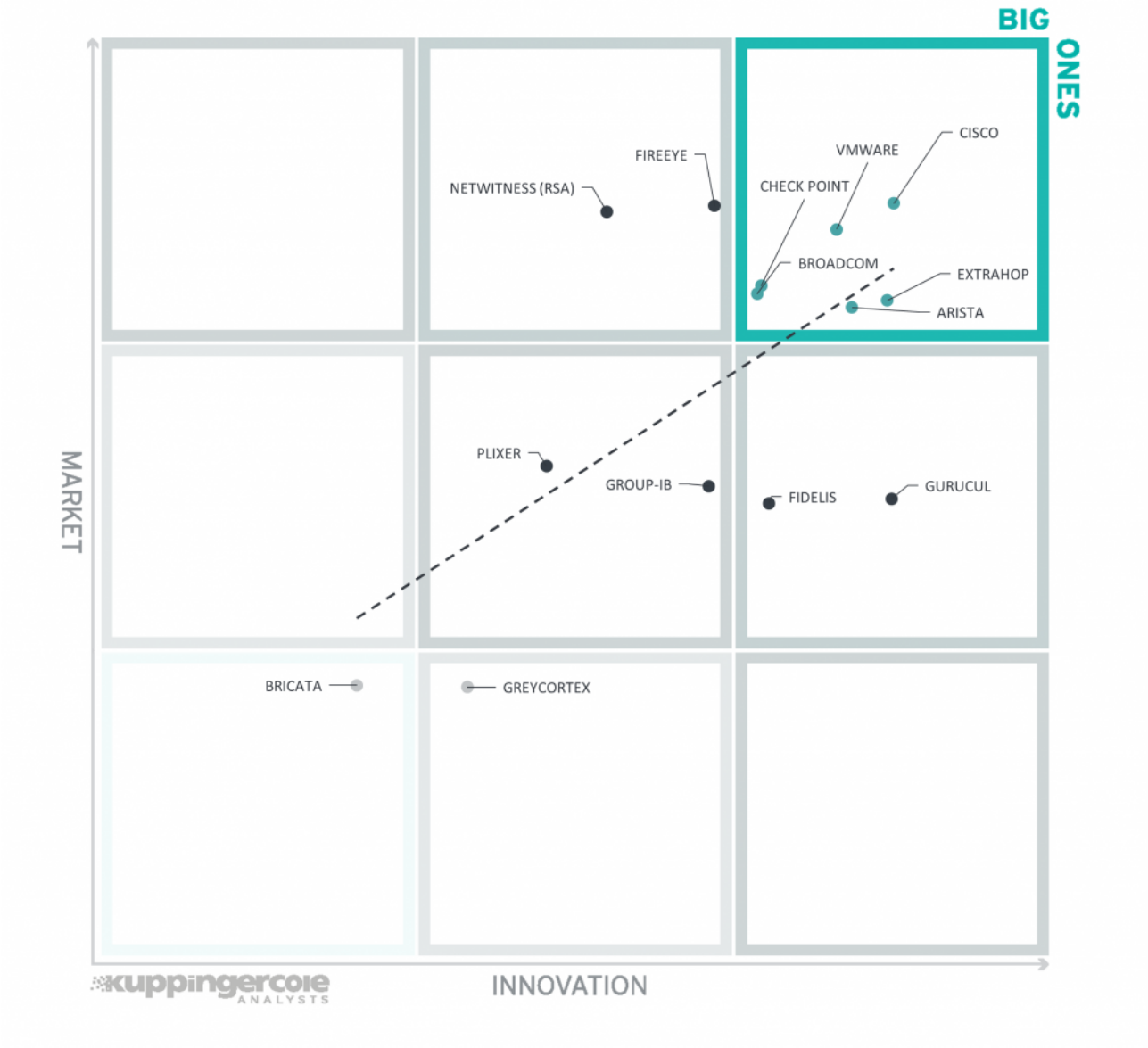


Figure 9: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

Cisco, VMware, Check Point, Broadcom, Extrahop, and Arista Networks are the Big Ones in NDR. Most are above the line suggesting that their innovation has paid off in terms of capturing market share; ExtraHop and Arista Networks are just below the line, showing that their innovative qualities have slightly outpaced the market.

FireEye is in the top center but approaching Big One placement. NetWitness (RSA) is also in the top center.

Both of these companies are doing very well given their investments in NDR development. Gurucul and Fidelis are in the center right, showing a similar degree of innovation as the Big Ones.

Plixer is in the center box above the line; Group-IB is found below the line in the center.

Bricata is in the lower left section, and GreyCortex is in the lower center.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Network Detection & Response products. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Product	Security	Functionality	Interoperability	Usability	Deployment
Arista Networks Awake Security Platform	positive	strong positive	positive	strong positive	strong positive
Bricata Network Detection & Response Platform	neutral	neutral	neutral	neutral	neutral
Broadcom Symantec Secure Web Gateway, Content Analysis, and Security Analytics	strong positive	strong positive	strong positive	positive	positive
Check Point CloudGuard Security and Check Point appliances	strong positive	positive	strong positive	positive	strong positive
Cisco Secure Network and Cloud Analytics	strong positive	strong positive	strong positive	strong positive	positive
ExtraHop Reveal(x) and Reveal(x) 360	strong positive	strong positive	strong positive	positive	positive
Fidelis Cybersecurity Network	strong positive	strong positive	strong positive	positive	positive
FireEye Network Security	positive	positive	positive	positive	positive
GreyCortex Mendel	neutral	neutral	weak	neutral	neutral
Group-IB Threat Hunting Framework	positive	positive	positive	positive	neutral
Gurucul Network Traffic Analysis (NTA)	strong positive	strong positive	strong positive	strong positive	positive
NetWitness Platform	strong positive	positive	positive	positive	positive
Plixer Security Intelligence and Scrutinizer	positive	neutral	positive	positive	positive
VMware NSX Network Detection & Response and Advanced Threat Protection	positive	strong positive	strong positive	positive	strong positive
Legend		critical	weak	neutral	positive	strong positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Arista Networks	●	●	●	●
Bricata	●	●	●	●
Broadcom Inc.	●	●	●	●
Check Point	●	●	●	●
Cisco	●	●	●	●
ExtraHop	●	●	●	●
Fidelis Cybersecurity	●	●	●	●
FireEye	●	●	●	●
GreyCortex	●	●	●	●
Group-IB	●	●	●	●
Gurucul	●	●	●	●
NetWitness (RSA)	●	●	●	●
Plixer	●	●	●	●
VMware	●	●	●	●
Legend	● critical	● weak	● neutral	● positive ● strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass. For some of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC NDR, we look at the following eight categories:

- **Platform Support**
  For on-premises environments, NDR solutions are offered as physical and virtual appliances. These appliances can be deployed in-line, off SPAN/TAP ports of network gear or off network packet brokers, or in some cases out-of-band, relying completely upon other security components for collection telemetry from network devices and execution of responses. Direct access to network traffic and the ability to interdict has advantages. This category includes support for IaaS platforms. Having images for Amazon AWS, Microsoft Azure, Google Cloud Platform (GCP), Oracle, and other IaaS platforms that can collect cloud-hosted network telemetry is essential for many organizations today. The more platforms supported, the better the score.
- **NTA**
  Network Traffic Analysis is often a precursor to being able to perform more sophisticated security analytics. NTA techniques include identification of traffic by application type, association of user identity to traffic flows, file and device fingerprinting, application and site profiling, aggregated network traffic volume analysis, examination of source/destination communication frequencies, host/endpoint to application utilization profiling, and NetFlow/IPFIX collection and analysis.
- **ETA**
  Encrypted Traffic Analysis is becoming the most common approach for detecting network threats. Success with ETA requires that solutions use multiple techniques (HASSH, JA3/JA3S, Mercury, SSLBL, etc.), have a variety of IoC sources, and have the ability to recognize common enterprise network protocols. Higher scores here also reflect more complete utilization of all available ETA methods and better coverage of attributes and protocols.
- **Detection**

In order to detect suspicious and malicious activities on networks and in the cloud, a variety of capabilities are needed. Detection requires visibility, first and foremost. Coverage for all network segments and all IaaS instances is needed. Some solutions use IDS style rules, based on Suricata, YARA or other formats. Full NDR solutions use detection models powered by Machine Learning (ML) algorithms: unsupervised ML for anomaly discovery, supervised for categorization of possible threats, and Deep Learning (DL) for more rapid combination, discovery, and self-sorting to identify previously unknown threats. This rating considers how products utilize ML and DL for higher quality detections and reduction of false positives. Better scores are given for those that use a well-thought-out set of unsupervised and supervised ML and DL algorithms and detection models. Model training methods, sources of data sets, and model update frequency are also considered. NDR solutions should assist with automating the correlation of events, adding threat intel, creating cases for analysts to review, and generating IoCs for analysts to use for threat hunting. This category rates the functionality that enables autonomous detection of suspicious events.

- **Threat Hunting**
  A mix of certain features needs to be in place for analysts to perform threat hunting: CLI and/or GUI query capability; structured or natural language query capabilities preferred, the ability to conduct regular expression searches, the ability to write static rules in YARA, Suricata, or other formats, being able to define or prioritize IoCs and search all assets for them, and the ability to activate recording and playback on suspicious network conversations. Solutions that help the human analyst by assembling relevant events into a timeline and topology map enriched by threat intelligence are preferred. Analysts should be able to use NDR products to conduct threat hunts for malware implantation, botnet and fraud activity, C2 traffic, lateral movement, AD reconnaissance, DNS tunneling, data exfiltration, and other sophisticated TTPs. This category considers the amount and quality of features that facilitate threat hunting.
- **Playbooks & Responses**
  In order for automated responses to be triggered, NDR solutions either must be placed in-line or have good API interoperability with other security tools such as firewalls, VPNs, routers, switches, email gateways, EPDR systems, web proxies, API gateways, SIEM and SOAR systems. Some NDR solutions have packaged connectors for common security tools to make this easier. NDR tools deployed in-line may not need as many connectors for external security tools. A minimum set of automated response includes session termination, node isolation, and forensic evidence collection. Playbooks are essentially scripts that can execute when certain trigger conditions are encountered, either manually or programmatically. Some vendors ship many playbooks with their NDR solutions and allow for easy customization using the analyst interface. Other vendors' playbooks may require scripting or light coding. A few vendors in this Leadership Compass do not support the playbook

concept but can allow API interoperability to build some response capabilities. This category considers the methods used for designing and executing automated responses as well as the number and variety of response actions and playbooks available.

- **Integrations**
  NDR tools must work well with other components in security architectures. Two major approaches exist: the development and support of “integrations” or “connectors” by vendors, and bi-directional accessibility via APIs. Integrations are packages of functionality that can link the NDR system to other security solutions. Integrations are generally installed and require little configuration. Many if not most security tools offer inbound and outbound connectivity through APIs and communication standards. APIs may expose all functions within a management console. In other cases, a subset of functions may be available. APIs themselves must be properly secured to prevent abuse. Using standard communication protocols can be sufficient in some limited cases, e.g., sending event data over syslog to SIEMs. Integrations may allow enhanced features. Examples where integrations are preferred are connections to SOAR systems, which allows more functionality with less customization than invoking APIs.

5.1 Arista Networks

Awake Security was founded in 2014 in Santa Clara, California. In late 2020, Awake Security was acquired by Arista Networks, maker of high-performance switches and other networking gear. Awake had been focused on the North American market but is expanding globally. The sensors are delivered as either hardware or VMWare OVA virtual appliances and are deployed off SPAN/TAP network ports, off network packet brokers, or on Arista DANZ Monitoring Fabric switches. Awake works inside AWS, Azure, and GCP IaaS, and is available in multiple regions. The manager console can be run either on-prem or in the cloud; Arista also hosts customer consoles as SaaS. Arista provides full NDR managed services. Annual licensing is based on average throughput across each customer's networks.

Awake can perform all major Network Traffic Analysis functions. Awake can analyze more than a thousand enterprise IT protocols, streaming protocols, 180 common mobile apps, and dozens of OT/ICS and IIoT protocols. Awake employs a good subset of ETA techniques. Unsupervised and supervised ML and Deep Learning detection models are used to identify malicious traffic. Customers can configure detection models if needed using their Adversarial Modeling Language. Awake claims that EntityIQ, their security knowledge graph, can train and start finding outliers in situ in less than four hours. EntityIQ builds device and application profiles rather than only analyzing traffic flows.

Awake doesn't decrypt traffic or capture malware samples and thus doesn't interface with sandboxes. Awake could be deployed inside a secure enclave where other devices have decrypted traffic. Ava is an automated virtual assistant for analysts, and it performs initial investigations, including event correlation, CTI queries, IoC creation, and case assembly. Awake uses the MISP platform to allow customers to select CTI sources. The analyst interface has map and timeline views, and supports multiple query styles including drop-down lists, regular expressions, and natural language. Analysts can annotate cases and launch playbook actions from the main console.

Awake ships with >100 playbooks which can be used as templates and modified with the graphical model builder. Playbook actions may include full packet capture, terminate sessions, and isolate hosts. Other actions are possible via API integrations with SOAR and other security tools.

Awake supports many relevant standards for communication including CEF, JSON, REST, SNMP, STIX, Syslog, and YARA, which enable SIEM and CTI interoperability. OOB connectors are available for ServiceNow ITSM, Palo Alto XSOAR, and Splunk Phantom. Other connectors can be created using their published APIs. Awake allows for granular admin and analyst roles and supports MFA via SAML.

Arista's Awake Security Platform has the ability to scale to high throughput levels for high traffic environments. Awake has obtained SOC 2 Type 1 but has not yet certified on others such as SOC2 Type 2, ISO 27001/18, or CSA Star. The Arista acquisition means that their customer base will now have the opportunity to easily add NDR functionality and will continue to improve Awake's market position. Awake Security Platform provides excellent coverage in the wide array of domains including enterprise IT, streaming apps, mobile apps, and OT/ICS/IIoT. Their implementation of ML and DL aims to simplify and automate analyst workflows. Any organization looking for advanced NDR solutions that can both scale well

and improve investigation outcomes should give Arista’s Awake Security Platform a look.

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●

ARISTA

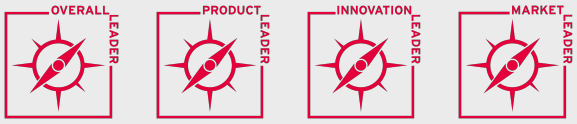
Strengths

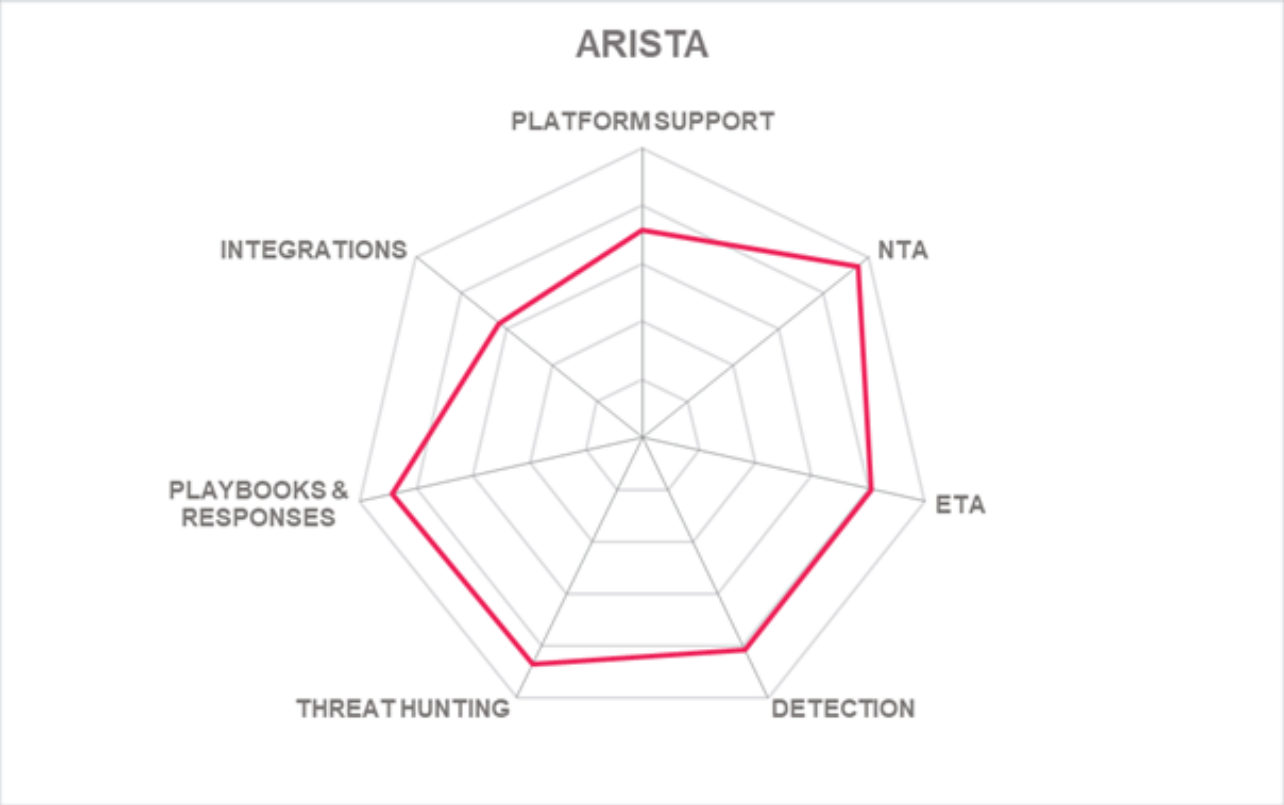
- Sensor throughput up to 100 Gbps
- TLS 1.3 support
- Full coverage for NTA functions
- Broad protocol support for enterprise IT, streaming apps, mobile apps, and OT/ICS/IIoT
- ML and DL detection models are tunable by customers
- Rapid Time-to-Value
- Emphasis on investigation automation

Challenges

- No malware capture and analysis
- Additional ETA methods may be advantageous
- Has not yet achieved some key security and cloud hosting certifications

Leader in




ARISTA
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.2 Bricata

Bricata is an NDR and network traffic analysis specialist startup that was established in 2014 in Maryland, US. Bricata's solution is delivered as appliances or virtual appliances. For on-premises environments, it can be deployed off SPAN or TAP ports or in-line if desired. Cloud images (VMDK, AMI, ISO, etc.) that work in AWS, GCP, and Microsoft Azure are available. Max throughput is up to 20 Gbps for sensors and 1 Gbps for virtual agents. Analyst console can be run from the sensors or in the cloud. Bricata does not host it as SaaS, but they have MSSP and MDR partners. Licensing is by traffic volumes for enterprise customers and by number of analyst users for MSSPs and MDRs.

Bricata uses a few NTA techniques and understands the most prevalent enterprise IT protocols as well as DNP3 and Modbus for OT networks. There is no specific support for mobile apps or streaming protocols. Bricata uses multiple ETA techniques. Support for TLS 1.3 is planned. Static rules, Suricata signatures, and Zeek scripts can be imported and manipulated in the analyst GUI. Cylance's ML-based Infinity Engine is used for static file analysis. Bricata's limited ML detection models are not configurable by customers and are not trained on customer networks. The solution does identify traffic by application and examine files but does not profile apps and hosts and does not consider device or user identity. Bricata looks for common TTPs but the interface is not aligned with MITRE ATT&CK yet.

Bricata sensors don't decrypt traffic, but it can be placed in secure enclaves where other components handle decryption and encryption. It can capture malware samples and dispatch them to 3rd-party sandboxes. Bricata correlates events and assembles them into cases for analysts. Dashboard widgets are customizable, allowing customers to automate CTI queries as right-click options, for example. A narrow list of CTI providers is available OOTB, but others can be added via API. The analyst interface features a standard map and timeline view and has a drop-down list style query builder, but regular expression and natural language searches are not available.

Playbooks are not available, and the solution doesn't recommend actions. If deployed in-line, Bricata can initiate full packet capture, terminate sessions, and block traffic by host/IP. Other actions are possible via integrations with SOAR or other security tools. SOAR connectors include D3, LogRhythm, Microsoft Azure Sentinel, and Siemplify.

Bricata supports CEF, LEEF, REST, SNMP, and syslog as well as email alerting. It can output to any SIEM, and integrations are available for some of the most common. STIX/TAXII support is on the roadmap. No reports ship with the product but customers can create them. Bricata supports role-based access control and integrates with Okta for MFA. Other MFA options are planned for future releases.

Bricata uses FIPS 140-2 crypto components but has not achieved any cloud hosting or other security certifications. The solution is more of an updated IDS/IPS and would benefit from additional development in the areas of ETA techniques and automation. Support for additional standards will increase interoperability and those are planned. Bricata's experience with health care and government customers may give them an edge in those industries.

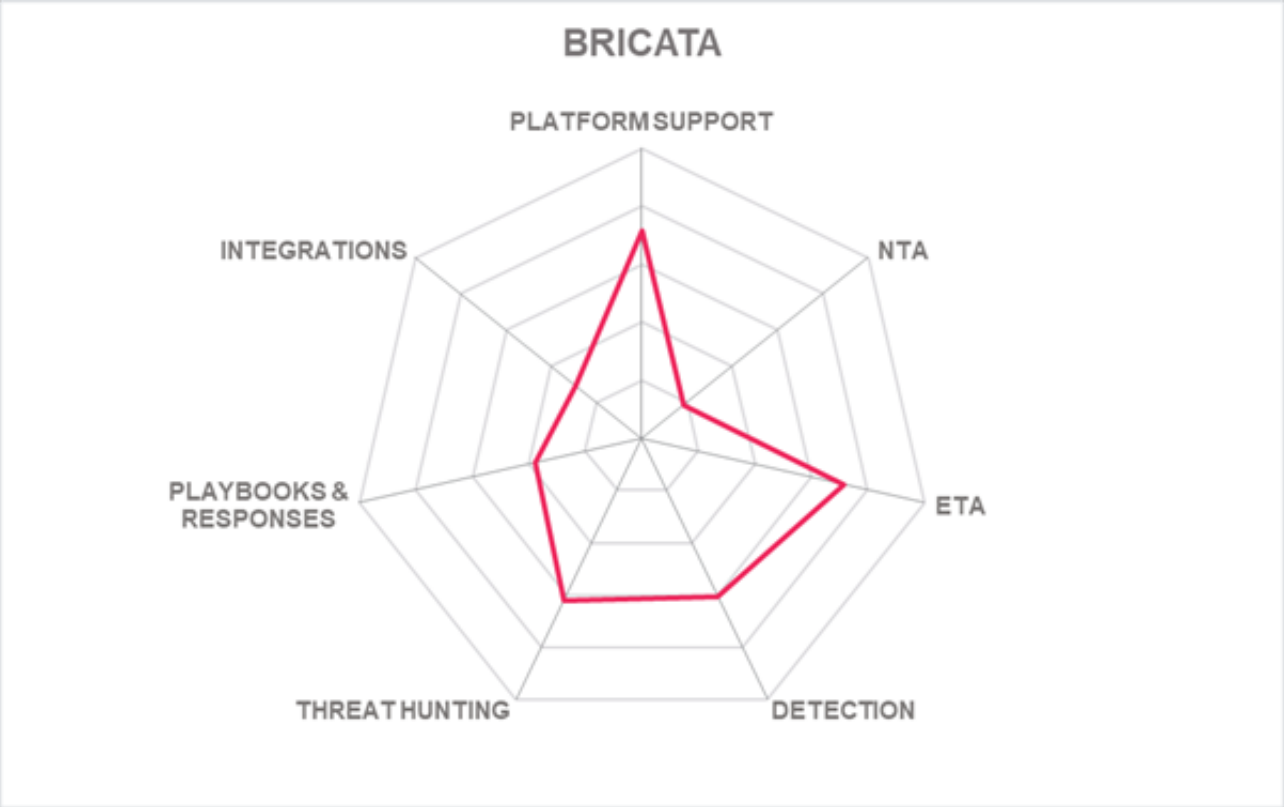
Security	● ● ● ○ ○
Functionality	● ● ● ○ ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ○ ○
Deployment	● ● ● ○ ○

Strengths

- Expertise in protecting health care IT systems
- Smart PCAP model enables customers to keep large amounts of historical data efficiently
- Good selection of ETA techniques employed

Challenges

- MITRE ATT&CK visualization is in work
- Light coverage for OT/ICS/IIoT
- Limited NTA features
- TLS 1.3 not supported yet
- Device/user identity and application to host profiling not analyzed
- Playbooks not supported


BRICATA
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.3 Broadcom Inc.

Broadcom is a large IT vendor with a diverse portfolio of security products, including Symantec Enterprise Security Business, which is maintaining separate branding. Their NDR solution is composed of the three products listed above. The sensors are delivered as on-premises hardware or VMWare ESX virtual appliances and can be deployed off span/tap network ports or off network packet brokers. Symantec SSL Visibility (SSLV) Appliance customers can take advantage of decrypted packet analysis. Sensors can run at up to 10 Gbps individually for full packet capture and analysis, and sensors can be managed in groups of 200. Symantec's solution also works inside AWS, Azure, Google, and Oracle IaaS. The Central Manager (console) can be run either on-prem or in the cloud; Symantec also offers hosted Secure Web Gateway (SWG) for customers as a SaaS with per-user subscriptions. Annual licensing for Security Analytics is based on traffic volumes with charges for additional storage. Symantec partners also provide managed NDR services.

Symantec's product can handle many aspects of NTA. Security Analytics recognizes 3,000 enterprise applications and streaming protocols. For OT and IIoT, it recognizes CIP, CoAP, DNP3, Modbus, MQTT, S7, and some proprietary device types. There is no specific support for mobile apps. Symantec's ETA techniques are less comprehensive than some, as its SSLV appliances do decryption. Symantec uses YARA rules, and a mix of unsupervised and supervised ML detection models trained on public and private datasets, but not on customer data. Models are updated and pushed bi-weekly. Customers can adjust sensitivity of detection models but not other parameters. Detections are not currently aligned to MITRE ATT&CK, although it looks for all TTPs. Device fingerprinting and application-to-host mapping is not performed.

Symantec Content Analysis is the built-in sandbox, and many 3rd-party sandbox integrations are available. The Symantec suite does not perform correlation, automatic enrichment, and case assembly; these tasks are left to SIEM and SOAR integration. Customers can plumb in additional CTI sources. The solution can create IoCs based on observed events. The Central Manager interface features drop-down lists, regexp searches, timeline and map views, annotation, and playbook launching. The analyst GUI needs to be updated, and it is comparatively more labor intensive to operate. All Central Manager functions are exposed via REST API to facilitate integration with SOAR.

Playbooks are not directly available, as the solution relies on external SOAR solutions for advanced functions and responses. The SWG component and Symantec EDR products can terminate sessions, block IPs and hosts, and isolate hosts if directed by SOARs. Connectors are available for all major SOAR products.

Symantec supports CEF, REST API, Slack, SMS, SMTP, SNMP, Symantec Integrated Cyber Defense (ICDx – the backend communication framework), and syslog for comms. STIX/TAXII are not directly supported but can be via Symantec ICDx. There are no integrations for ITSM systems. Many standard reports are available OOTB, and customers can easily define new report types. Symantec has a highly granular role-based and data access control model, which allows master admins to define which categories

of data within the solution are visible to lower-level admins. Various MFA types including OAuth2, Kerberos, LDAP, RADIUS, and CAC cards can be used for authentication.

Broadcom's Symantec NDR suite has an excellent internal security model. It is certified on ISO 15408 and 27001, and SOC 2 Type 1 & 2 for cloud-hosted instances. It can scale to meet high throughput demands. Additional automation for investigations and responses would make it easier for customers without SOARs to operate. Enhancements for the ML detection models would benefit those customers who rely on ETA. Multiple products are needed to achieve full NDR functionality and integration, which may make it more difficult for non-Symantec shops to deploy. Organizations with the need for high security, particularly those requiring packet decryption, will definitely want to consider Symantec's Secure Web Gateway, Content Analysis, and Security Analytics NDR platform.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○

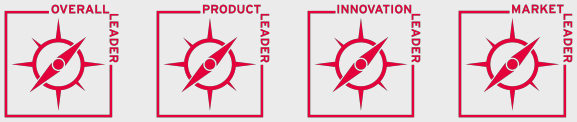
Strengths

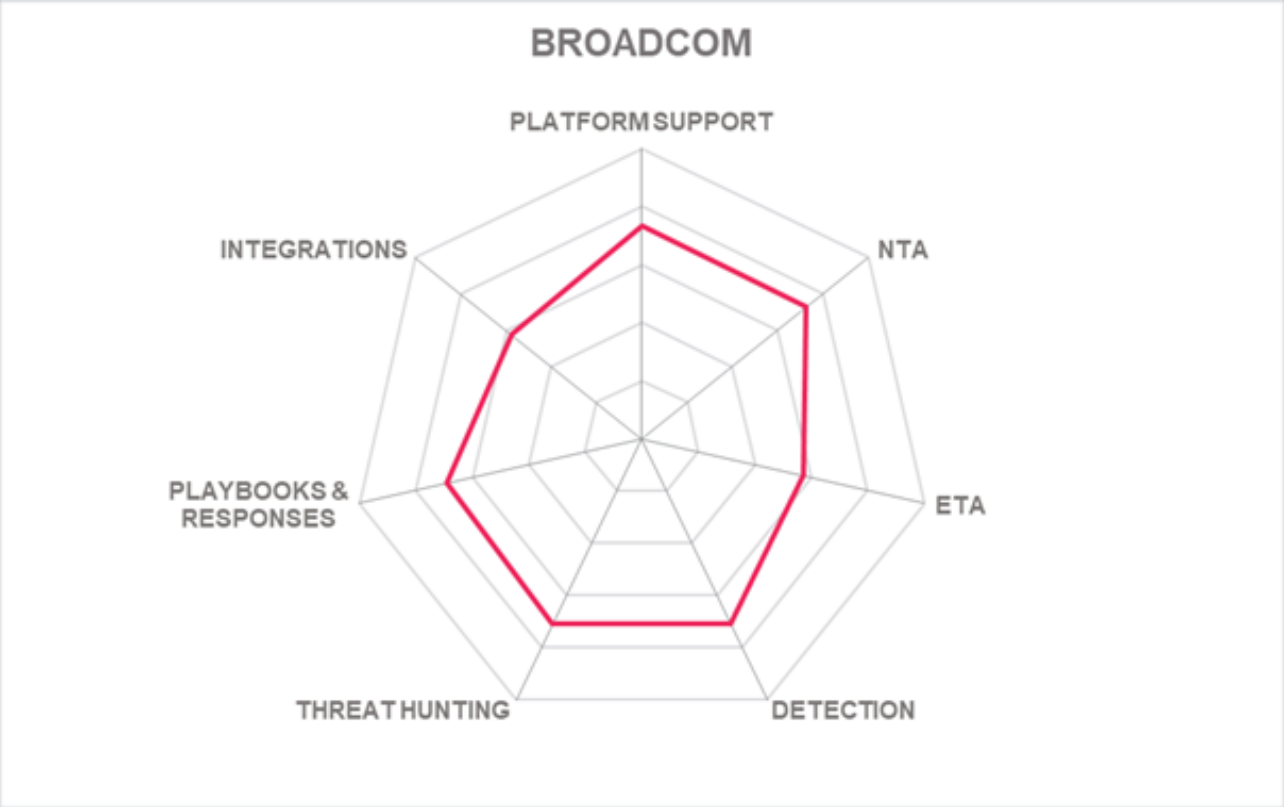
- Thousands of enterprise IT apps analyzed
- Coverage for some common ICS and IIoT protocols
- Built-in sandbox
- Many integrations for most SIEM and SOAR solutions
- Draws upon leading Symantec threat intelligence; Symantec is an affiliate member of Cyber Threat Alliance
- Strong data access control model and multiple MFA options present

Challenges

- NDR solution requires multiple SKUs; a single NDR packaged offering would be easier to adopt
- Emphasis on decrypted traffic analysis rather than ETA
- Investigations and threat hunts need more automation; it is a labor-intensive suite that requires highly skilled staff to operate
- Infrequent detection model updates; models not trained on customer data
- Playbooks not supported

Leader in




BROADCOM
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.4 Check Point

Check Point is a global cybersecurity leader, founded in 1993 in Tel Aviv. Check Point offers next-gen firewalls, edge security solutions, IoT security gateways, VPNs, cloud security solutions, endpoint and mobile security, and complete SOC management solutions The Check Point NDR offering leverages, Check Point CloudGuard Network Security to cover public cloud vendors Alibaba, AWS, Azure, GCP, Huawei, IBM, Oracle, Tencent, and Yandex; private cloud vendors VMware, Cisco, Nutanix, OpenStack, Microsoft Hyper-V and KVM; and Check Point Quantum Security Gateway and Spark SMB appliances and virtual appliances are available for on-premises deployments off SPAN/TAP ports or in-line with fail-open NICs. Max throughput ranges from 1 Gbps for remote offices to 1.5 Tbps for data center and telco/carrier platforms. Licensing costs are based on numbers of appliances and VMs. Check Point offers full MDR services, and many MSSPs use their NDR solution.

Check Point addresses several NTA use cases, and support for the other major ones is on the roadmap. Check Point can identify thousands of enterprise IT, mobile, and streaming applications and protocols. Check Point provides thorough coverage of OT/ICS and IIoT protocols. The solution omits several important ETA techniques. Device fingerprinting is on the roadmap. It uses Snort signatures, YARA rules, and a matrix of unsupervised and supervised ML, and Deep Learning algorithms. Models are maintained by Check Point without customer intervention. Solutions can be tailored by industry for clients. Detections are partially mapped to MITRE ATT&CK.

Check Point can decrypt sessions in-line if so configured. Check Point Harmony EDR can also capture unencrypted data on endpoints and forward for analysis, but this is not required. Suspicious files are detonated by the built-in Check Point sandbox; 3rd-party sandbox integrations are not available. Check Point can correlate events, add relevant threat info, and create IoCs, but auto-generating cases for analysts is not present yet. At first glance, the dashboard seems to be more of an NTA tool, but right-click options offer the full gamut of security investigation actions. Drilling down from the dashboard allows deeper investigations, with multiple query types supported: drop-down lists, regexp, free text queries, etc. Map and timeline views are available.

Playbooks are not supported; this requires the add-on MDR service. Working in conjunction with other tools, some response actions can be executed, such as session termination, blocking IPs/hosts, and DNS sinkholing. Integrations with SOAR include D3 Security, DFLabs, Microsoft Azure Sentinel, and Siemplify. A built-in IoC management facility supports both input and output feeds.

Check Point supports many communication standards: CEF, REST API, SNMP, and syslog; and CyBox, Snort, STIX, TAXII, and YARA formats. It can interface with any SIEM but no ITSMs. Check Point has been evaluated in MITRE ATT&CK exercises and is a charter member of Cyber Threat Alliance. Many reports are available by default, but customers cannot create custom reports yet. MFA for CloudGuard NDR is supported by CheckPoint's Mobile Access solution, which allows for certificates, RADIUS, SecurID, SMS OTP, and SAML.

Check Point has excellent product security and is certified for IEC 15408, FIPS 140-2, NIAPC, UK Cyber

Essentials Plus, US FedRAMP, and multiple other national level programs. Check Point supports the broadest coverage of IaaS providers. For optimal detections, the solution should be able to analyze unencrypted traffic. Check Point needs to enhance their ETA capabilities. With solutions for national government agencies and regional telcos, their performance is unparalleled. Organizations looking for the highest performance NDR that can decrypt traffic should put Check Point near the top of their consideration list.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●●

Check Point®
SOFTWARE TECHNOLOGIES LTD

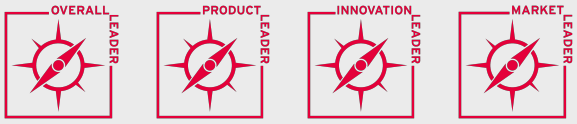
Strengths

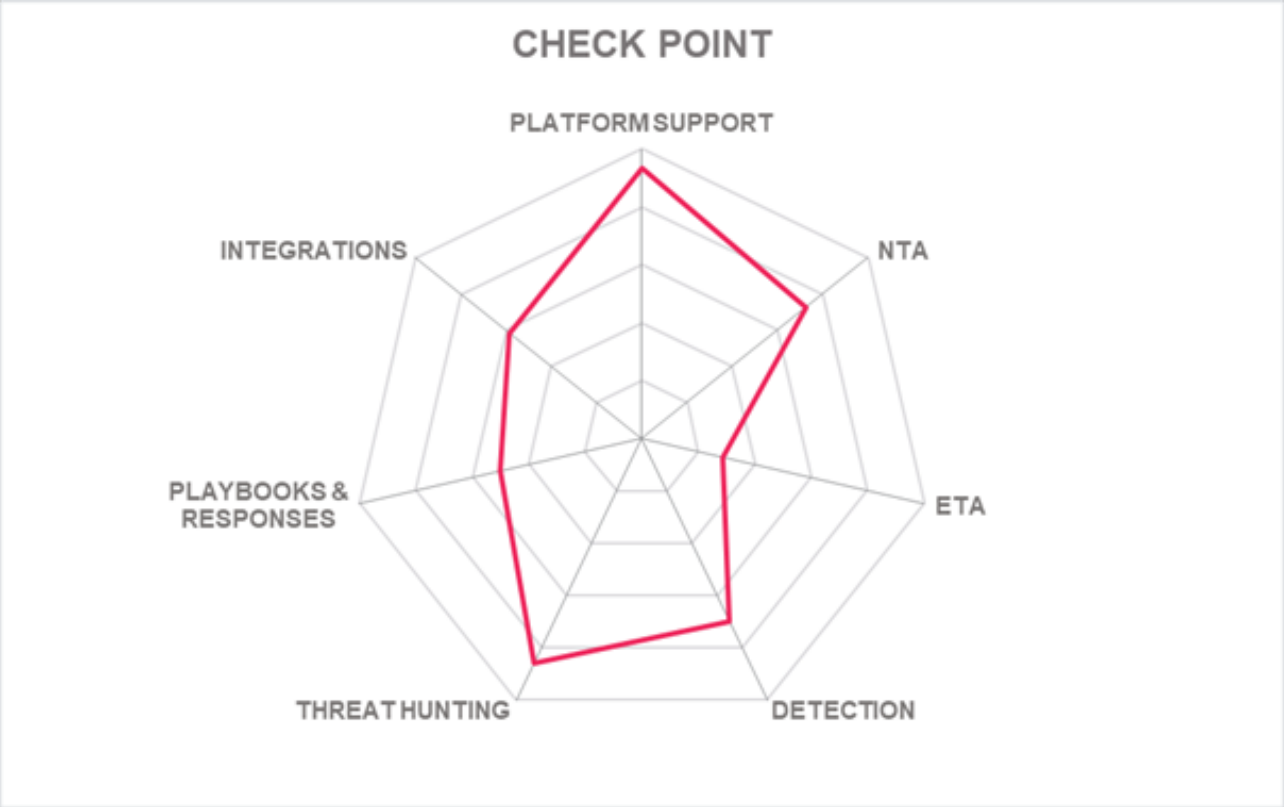
- Highest throughput options ranging up to 1.5 Tbps
- Broad selection of apps that can be identified, including mobile and streaming
- Can work in any cloud
- Built-in sandbox
- ML and DL detection models
- Multiple security certifications
- Cyber Threat Alliance charter member

Challenges

- Missing some NTA and key ETA techniques
- Optimal detection capabilities require access to decrypted traffic
- Does not do device fingerprinting yet
- Case management is a roadmap item
- Playbooks are not supported
- Complex response types require integration with Check Point Harmony EDR
- No ITSM integration

Leader in




CHECK POINT
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.5 Cisco

Cisco is a global network and security leader, founded in 1984, and headquartered in the Bay Area. Cisco is well-known for networking products, and has solutions for mobile, cloud, and IoT. Their NDR entries are Cisco Secure Network and Cloud Analytics, formerly known as Stealthwatch Enterprise and Cloud. The origin of Stealthwatch was Lancope, which was acquired by Cisco in 2015. The Secure Network sensors are delivered as physical or virtual appliances and can be deployed off span ports. ISO images are available for on-premises Kubernetes deployments. The Cloud Analytics component uses native IaaS platform APIs to get Flows from AWS, Azure, and GCP. Additionally, Secure Cloud Analytics also offers Cloud Security Posture Management capabilities. The management console can be run either on-prem or Cisco also hosts it as SaaS. Annual licensing is based on flow rates, with additional charges for physical appliances; SaaS instances can be billed for actual traffic levels. Cisco offers a Managed Detection and Response service.

Cisco addresses almost all NTA/NDR use cases. The solution understands most major enterprise IT, mobile, and streaming app protocols. Cisco recognizes many OT and IIoT protocols including BACNet, CoAP, DNP3, IEC 61850, IEEE 11073, IPMI, Modbus, MQTT, OPC-UA, and XMPP. Network and Cloud Analytics uses multiple ETA methods including their in-house developed then open-sourced Mercury TLS fingerprinting engine. IDS/IPS type rules are not needed as Cisco's NDR suite employs a sophisticated array of dozens of unsupervised and supervised ML detection algorithms. Models are trained on public and proprietary datasets. Updates are pushed as needed after testing. Detection models can be tweaked by knowledgeable customers. Detections are mapped to MITRE ATT&CK.

The NDR product does not capture and test suspicious files, however Cisco SecureX security platform (a cloud-delivered free extension for all customers who purchase a security solution from Cisco) can. For incident analysis, Cisco correlates events, adds threat intelligence from Talos, and assembles cases for analysts. Host Group Automation service allows customers to add other CTI sources if desired. Cisco is a charter member of the Cyber Threat Alliance. The solution supports creation of IoCs. The interface has drop-down list and regexp query builders, global and network maps, and supports annotation, drill down from dashboard to details, and workflow response launch.

Responses are editable in flow-chart format. Eight playbook actions are available and can be orchestrated through Cisco SecureX, but playbook actions are not directly recommended in the analyst console. Response actions can include initiate full packet capture, terminate sessions, isolate hosts, block comms by IP/port, DNS sinkholing, and reconfiguration of IaaS resources. Root cause analysis (RCA) and attribution estimations are supported with confidence metrics. SIEM connectors are available for Rapid7, Splunk, and SumoLogic; others via syslog. Third-party SOAR connections are handled via Cisco SecureX.

Cisco supports REST API, SNMP, Syslog, SMTP, and Webhooks. Webhooks allows integration with ServiceNow ITSM and Slack for alerting and ticketing. STIX and TAXII CTI formats are supported. Many different kinds of reports are present OOTB, and others can be designed by customers. Their platform has been evaluated against MITRE ATT&CK. The console adheres to an extensible RBAC model, and various OTP methods can be used for 2-factor authentication. SAML is supported for administrative federation.

Cisco’s Secure Network and Cloud Analytics solution is a full-featured NDR with excellent interoperability with other security tools as well as good integration with other Cisco products (though licensed separately). The solution is highly scalable and offers some of the highest throughput among the competition. Long default data retention periods increase the usefulness of the solution, particularly for customers facing APTs. Cisco’s commitment to threat information sharing is demonstrated by their role in the Cyber Threat Alliance. Existing Cisco customers will want to consider Secure Network and Cloud Analytics, and other organizations with both high security and high bandwidth needs will want to evaluate it when looking for NDR products.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

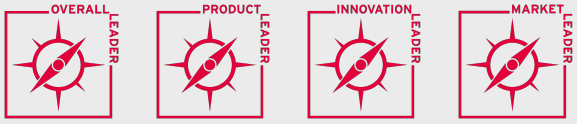
Strengths

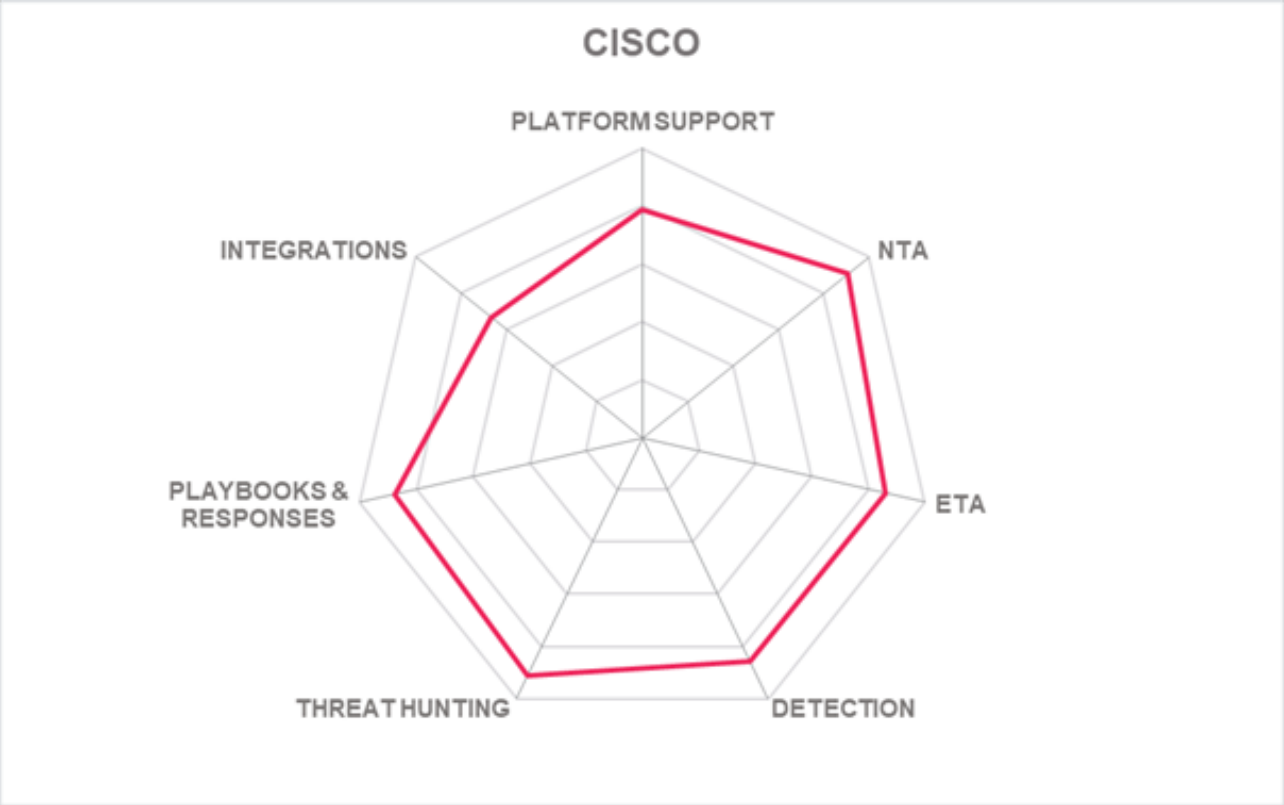
- Up to 80 Gbps throughput for network sensors and 1 Gbps for cloud
- Excellent coverage of OT and IIoT protocols
- Charter member of Cyber Threat Alliance
- Playbook orchestration via Cisco SecureX (no-charge add-on)
- Full range of expected responses, including RCA and attribution theories
- Good support for comm standards enables interoperability with IT and other security infrastructure

Challenges

- Data retention is configurable, but options are complicated and possibly expensive
- Cisco Secure Malware Analytics sandbox service is sold separately

Leader in




CISCO
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.6 ExtraHop

ExtraHop was founded in Seattle in 2007. In June of 2021, the company was acquired by Bain Capital Private Equity and Crosspoint Capital Partners. ExtraHop is an NDR specialist, and their products are Reveal(x) and Reveal(x) 360. Sensors are deployed as physical or virtual appliances off SPAN or TAP ports or network packet brokers. Virtual appliances run on KVM, Hyper-V, or VMware. Cloud sensors work in AWS, Azure, and GCP. Reveal(x) works in Kubernetes and Open vSwitch. Max throughput for a single sensor is 100 Gbps. The management console can run on-premises on the appliances, or in the cloud, with ExtraHop hosting the console as SaaS for those that prefer that option. ExtraHop partners with MSSPs. Licensing is by traffic volume or by number of appliances/VMs installed.

ExtraHop addresses all the common traffic analysis and NDR use cases. Reveal(x) 360 can analyze standard enterprise IT protocols, the RTP streaming protocol, and CoAP, DNP3, Modbus, and MQTT for OT/ICS and IIoT protocols. ExtraHop has an IP analyzer framework that allows customers to design other protocol specific capabilities. ExtraHop employs the full range of ETA techniques and has TLS 1.3 support. ExtraHop utilizes arrays of ML and DL detection models. Customers can configure detection models if needed. Full baselining of customer environments takes about 2 weeks.

ExtraHop recommends that customers set up Reveal(x) 360 to decrypt traffic out-of-band. Malware samples can be captured but sandbox integration is manual. Reveal(x) 360 correlates events, auto-queries CTI sources (including their own) and adds it to cases for analysts. The solution can create IoCs based on observations. The interface has drop-down list and regexp query builders, global and network maps, and supports annotation, drill down from dashboard to details, and playbook launch. Events and console presentation are mapped to MITRE ATT&CK.

Reveal(x) 360 ships with an undisclosed number of playbooks which can be modified by scripting. Response actions require API integrations with SOAR or other security tools. Reveal(x) 360 outputs detection cards that include timeline, MITRE ATT&CK analysis, and context to support analyst conclusions and attribution theories.

Reveal(x) 360 supports CEF, REST API, SNMP, and syslog for infrastructure interoperability. STIX and TAXII formats are understood. ExtraHop can integrate with most ITSM, SIEM, and SOAR solutions. Reveal(x) 360 ships with many basic reports aligned to CIS, MITRE, OWASP, etc. Reports and dashboards are configurable. Admin and analyst access is governed by RBAC and MFA is supported via SAML integration with major IDaaS providers.

ExtraHop's platform is CSA Star Level 1, US HIPAA, and SOC 2/3 attested/certified. ExtraHop has high max throughput rates per appliance, enabling it to scale well. Reveal(x) 360 uses all the main ETA methods but still recommends customers decrypt traffic. This doesn't result in a MITM architecture, but decryption could add risks if appliances are not secured sufficiently. Its out-of-band installation requires 3rd-party interoperability with SOAR or other security tools to effect responses. Playbook editing means scripting, so responses are best orchestrated outside Reveal(x) 360. Organizations that need highly scalable network detection capabilities and already have SOAR for orchestration and response will want to consider

ExtraHop. ExtraHop has special emphasis and features for customers in the financial and healthcare sectors.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○

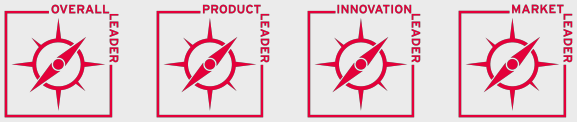
Strengths

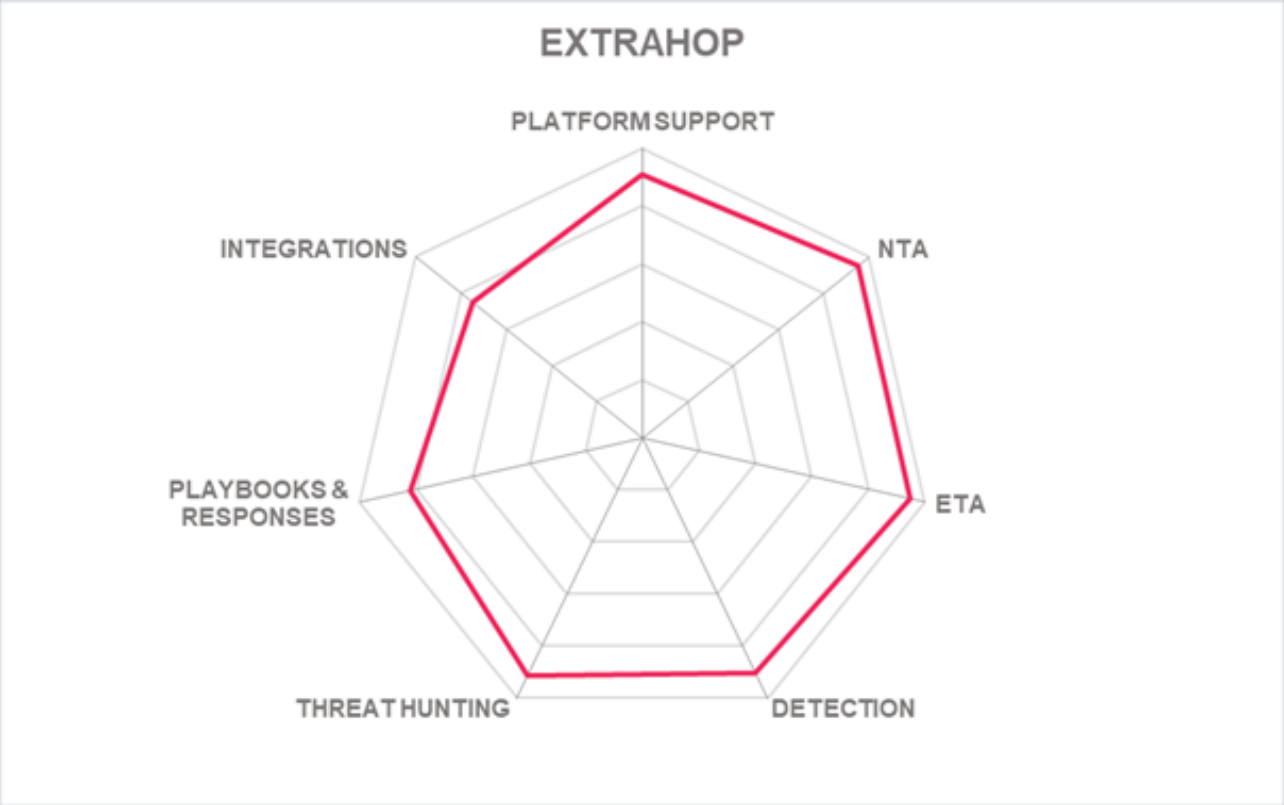
- TLS 1.3 decryption supported
- Excellent per-appliance throughput
- Broad coverage of ETA methods and NTA types
- Good protocol support for healthcare environments; HIPAA certified
- Built-in threat intel plus access to multiple 3rd-party sources

Challenges

- Default data retention period is 90 days
- Playbook editing requires scripting
- Responses require SOAR or integration with other security tools
- Though the solution covers healthcare environments well, OOTB support for other OT & IIoT use cases is light

Leader in




EXTRAHOP
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.7 Fidelis Cybersecurity

Fidelis Cybersecurity was founded in 2002 and is headquartered in Bethesda, MD, outside Washington, DC. They are a privately held company. The sensors are delivered as appliances or virtual appliances (VMware ESXi) and can be deployed in-line, off span ports, or in the cloud. They have images for AWS and Azure. Fidelis Cybersecurity has the capability to decrypt packets for deeper analysis in in-line mode. Each sensor can handle up to 25 Gbps throughput and can be load-balanced. The management console can be run on-prem, in IaaS, and Fidelis Cybersecurity has a SaaS option. Annual licensing is based on aggregate bandwidth used and days of metadata retention required. Customers have the option to purchase hardware (sensor hardware recommended for bandwidths greater than 2Gbps), deploy on VMs or on cloud, based on their needs. Fidelis Cybersecurity offers its NDR product as a standalone offering, or as part of Fidelis Elevate, an Active XDR platform. It is also available as a managed detection and response service via partner and their product is used by other large MSSPs.

Fidelis Network covers all NTA use cases including application/host profiling and mapping, file and device fingerprinting, and traffic volume and frequency analysis. Fidelis Network understands all the major IT protocols and some streaming protocols and mobile apps. There are no specific OT/ICS protocols analyzers, although customers can build limited functionality in this area using Suricata rules. Fidelis Network uses a subset of ETA methods, relying on packet decryption for more thorough analysis. The solution employs a narrow range of unsupervised and supervised ML detection models for outlier discovery and threat classification. Baselining takes about two weeks. The models are tuned in customer environments, and admins can select which models to deploy and tune them in operation.

Fidelis Cybersecurity has its own sandbox for suspicious file detonation. It can correlate events, add pertinent CTI, and build cases for analysts. It supports IoC creation based on observed events for threat hunting. The analyst interface uses drop-down lists and regexp for searches, supports annotation and CTI queries, and has timeline view, network map views, and drill-down from customizable dashboards. Dashboards are aligned with MITRE ATT&CK. Fidelis Network has built-in Data Leakage Prevention (DLP) features such as content analysis, regulatory compliance and policy enforcement, removal of malicious attachments from email, traffic re-routing, and object-level exfiltration prevention.

Fidelis Network has out-of-the-box playbooks for Fidelis Endpoint (EDR) and allows for building custom playbooks as needed, with Fidelis Endpoint or 3rd-party EDR solutions. Playbook development requires template modifications and/or coding. In both in-line or out-of-band mode, Fidelis Network can terminate sessions, isolate hosts, and block IPs. Additionally, in-line deployment enables deny-listing DNS domains. The solution does not propose root causes or attribution theories.

Fidelis Elevate supports CEF, REST API, SNMP, syslog, STIX, TAXII, and YARA standards. A long list of CTI sources can be queried. It interoperates with most SIEMs; and D3 Security, DFLabs, Palo Alto XSOAR, and Splunk SOARs. It does not integrate with ITSMs. It ships with more than 40 pre-packaged reports and allows creation of new report types and modification of dashboards. Google Authenticator, LDAP, RADIUS, OIDC, and SAML can be used for authentication and federation. Various roles with different privileges are

available, and integration with PAMs is possible via LDAP.

Fidelis Network is on the US DoD and US GSA Approved Products List. Fidelis Network is NIAP Common Criteria Certified (EAL2+). Appliances can be load-balanced as needed to achieve desired performance. Fidelis Cybersecurity has a leading-edge architecture enabling it to be considered a full XDR platform, including tight integration with their EDR and DDP products. Moreover, it contains DLP functionality that further differentiates it from competitors. Enhancements to its ML implementation could be beneficial, and more ETA methods may make it appealing for customers who don't want to decrypt traffic. Out-of-the-box playbooks and additional SOAR integrations would improve the response aspect. Organizations that have the highest security needs and are not subject to stringent privacy regulations will want to strongly consider Fidelis Network for NDR.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○

Fidelis® Cybersecurity

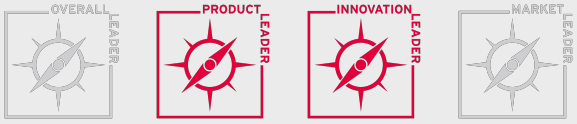
Strengths

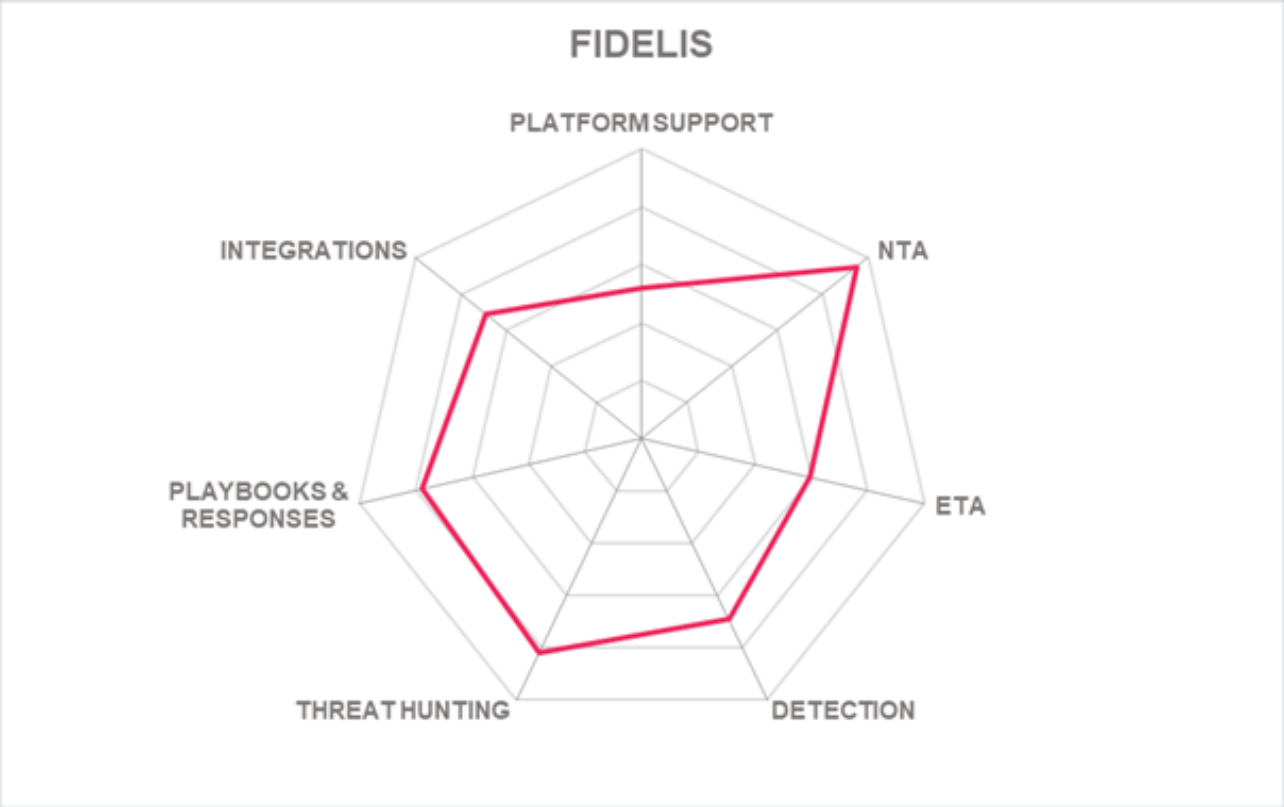
- Integration with Fidelis' EDR agents and Distributed Deception Platform
- Integrated Email and Data/Content Analysis for malware detection and DLP capabilities within NDR platform
- Customer configurable detection engines
- Excellent support for NTA types
- Built-in sandbox
- Interoperability with many CTI sources, 3rd party EDR, SIEM, SOAR, and other security tools
- Multiple certifications demonstrate adherence to the highest security standards

Challenges

- No OOTB coverage for OT/ICS/IIoT
- Playbooks for interop with selected EDR vendors; additional playbooks need to be coded
- Additional ETA methods may obviate the need for decryption
- ML enhancements may be useful

Leader in




FIDELIS
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.8 FireEye

FireEye was founded in 2004 and is headquartered in Milpitas, CA and has offices around the globe. On October 8, 2021, McAfee Enterprise and FireEye announced Symphony Technology Group (STG) had closed its sponsored acquisition of FireEye in an all-cash transaction totaling $1.2 billion. This transaction completed the combination of McAfee Enterprise with FireEye.. Sensors are delivered as physical or virtual appliances running on ESX, Hyper-V, KVM, or as AMIs and Azure instances, and can be deployed in-line, or off SPAN/TAP ports or network packet brokers. Optimal deployment is in-line for full functionality. Full packet capture devices can run at 20 Gbps, hardware sensors that also perform sandboxing run at 10 Gbps, and virtual appliances can run at 1 Gbps. Management console can run on-prem or in AWS and Azure, or as SaaS from FireEye. Their licensing model is based on a combination of per-user, per-appliance, and per-Mbps/year charges. FireEye offers MDR services.

FireEye Network Security covers most NTA use cases, and it understands a large subset of common enterprise IT protocols but omits mobile and streaming apps. For OT, FireEye only recognizes DNP3 and Modbus. No IIoT protocols are covered. The product uses a few common ETA methods, but better support might reduce the need for MITM deployments. FireEye does support Snort and YARA IDS/IPS rules. FireEye uses a basic implementation of unsupervised and supervised ML detection, relying initially on rules and sandboxing. Models are trained by FireEye, are not configurable by customers. Updates are pushed at least semi-annually. Detections are mapped to MITRE ATT&CK and LMCO Kill Chain.

FireEye MVX sandbox is built-in to Network Security, but it can work in conjunction with a few other sandbox services as well. FireEye Network Security can utilize telemetry from their EDR agents if deployed. Network Security console can correlate events, add relevant threat intel from their own service, build IoCs for threat hunting, and create cases for analysts. The analyst console features drop-down list query building, supports drill down from dashboard to start analysis, and has a timeline view. Global and network map views are planned. Cases can be managed within FireEye's XDR platform for analyst assignment, notation, and triage.

FireEye Network Security ships with 400+ playbooks that can operate on more than 200 device types, which can be edited via the GUI in FireEye Security Orchestrator. Playbooks can be tested in a staging mode before being used in production. FireEye Network Security assists with recommending playbook actions, which may include full packet capture, session termination, host isolation, and IP/port/URL blocking. Email, SNMP, and REST APIs can be used for alerting. Incident severity scoring can be encoded in YARA rules. SIEM connectors are available all popular products. FireEye integrates with ServiceNow for ITSM and SOAR, and other ITSM and SOAR connections can be configured as needed.

FireEye supports CEF, REST API, SNMP, STIX, and syslog standards. Executive summaries, alert details and malware activity reports are available OOTB. Limited customization of additional report types is possible. More than two dozen widgets can be configured in the dashboard. FireEye has been involved in MITRE testing. User roles can be mapped to LDAP. Console authentication options include LDAP, RADIUS, SAML, and TACACS. Third-party integrations with SecurID are possible.

FireEye uses FIPS 140-2 crypto and is SSAE SOC 2 Type 1 & 2 and Common Criteria Network Device Protection Profile (NDPP) v1.1 certified. The solution is compliant with UK Cyber Essentials Plus. FireEye Network Security can be tightly integrated with other solutions in their portfolio. The solution includes their sandbox and high-quality threat intelligence. FireEye provides coverage for collaboration systems such as Slack and Microsoft Teams, which are sometimes overlooked data exfiltration and malware infiltration channels. It works best in MITM deployments. Its implementation of ETA and supporting ML need some enhancements, but they are planned. FireEye Network Security bridges legacy IDS/IPS to next-generation NDR, and was designed for traditional network topologies but is expanding to cover more cloud use cases.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○

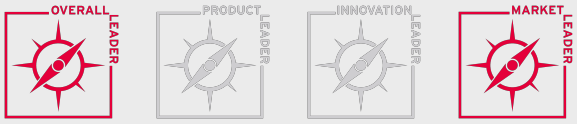
Strengths

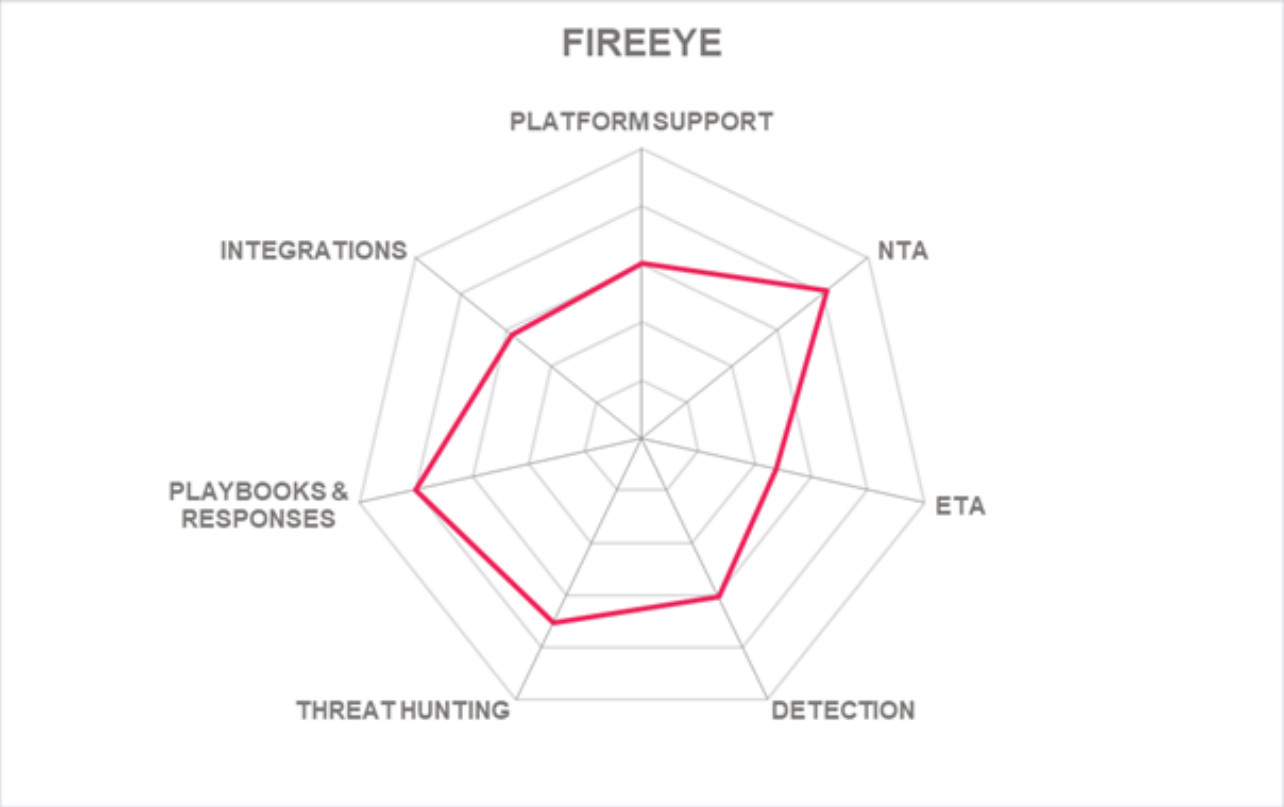
- TLS 1.3 comms
- Long default data retention periods
- API level protection for content within Slack and Microsoft Teams
- Sandbox included
- Access to FireEye CTI sources included
- Network Security offered as a managed service

Challenges

- Additional protocol support for enterprise IT, OT, and IIoT needed
- Additional ETA methods would be beneficial
- Strong MFA options built-in to the solution would make it easier to integrate with customer IAM
- Optimal detection requires MITM deployment

Leader in




FIREEYE
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.9 GreyCortex

GreyCortex is an early-stage startup, founded in Brno, Czechia in 2016. They specialize in NDR. Sensors are delivered as physical or virtual appliances (ISO images). The sensors operate off SPAN/TAP ports or network packet brokers in on-premises networks and virtual instances work in AWS and Microsoft Azure. The top throughput per sensor is currently 40 Gbps, with higher performance models in the works. The management console can run on the appliances, most Linux OSes, and AWS, Azure, and GCP. GreyCortex does not host the solution as SaaS, although they have MSSP partners who do run it for clients. Licensing is by number of appliances or VMs as well by traffic volume.

Mendel performs standard NTA functions and understands a wide range of enterprise IT and streaming protocols. Mendel recognizes many OT and IIoT protocols, including CIP, CoAP, DNP3, Modbus, MQTT, OPC-UA, S7, and more. The product uses most available ETA techniques. Mendel uses Snort and Suricata rules and unsupervised ML detection engines but does not use supervised ML or DL. Customer environment baselining takes about a week.

Mendel can be set up to decrypt traffic if desired. Mendel probes for most MITRE ATT&CK types. It does not capture malware samples and has no sandbox integrations. Few CTI sources are available OOTB. Mendel does correlate events, but does not build cases, add threat intel, or create IoCs for threat hunting automatically. Analysts can manually conduct threat hunts using regular expressions. The interface has a configurable dashboard with timeline and map views. Customers have connected to various SIEMs such as ArcSight, FortiSIEM, LogRhythm, McAfee, and IBM QRadar. Integrations with ITSM and SOAR are possible, but no OOTB connectors are available.

Mendel does not come with pre-defined playbooks, but customers can create them. Any response actions need to be configured over APIs and are constrained by downstream security tools. Root cause analysis and attribution can be facilitated but are not provided by default in the console.

Mendel supports CEF, LEEF, SMTP, SNMP, and syslog for security infrastructure interoperability. STIX and TAXII formats can be utilized. Mendel comes with basic dashboards and reports, and customers can create more if needed. Mendel supports RBAC for admins and analysts, but not MFA or federation.

GreyCortex has not achieved any security certifications yet. The per-sensor throughput is above average. Mendel has advanced IDS/IPS features but does not have a full range of NDR capabilities yet. Enhancements for ML detection models, analysis tools, automated responses, and integrations with other security tools would make the solution more compelling in the marketplace.

Security	●●●○○
Functionality	●●●○○
Interoperability	●●○○○
Usability	●●●○○
Deployment	●●●○○

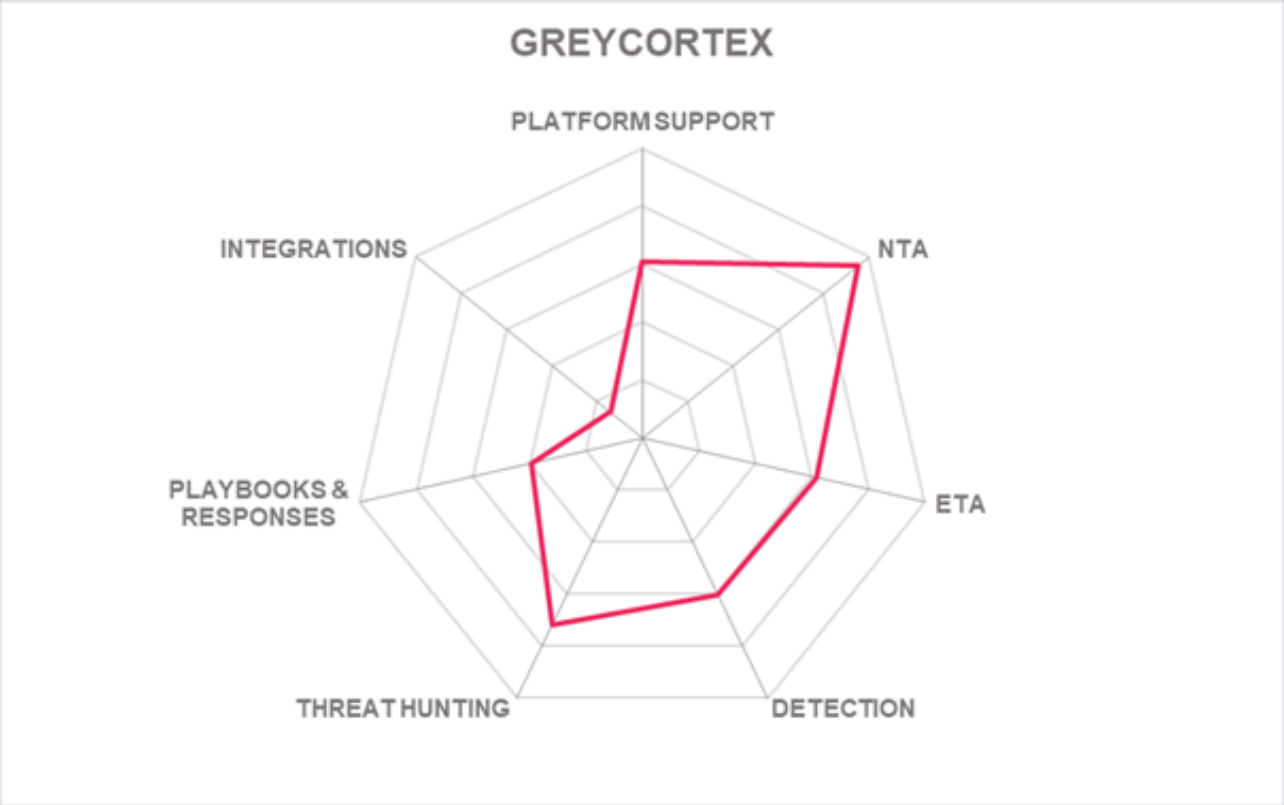
GREYCORTEX

Strengths

- Good support for OT environments
- Coverage for IIoT protocols
- Employs most major ETA techniques

Challenges

- TLS 1.3 not supported yet
- Additional work needed on ML-based detection
- No sandbox and limited CTI connectivity
- More analysis tools would be helpful
- Response automation requires customization
- No OOTB connectors for ITSM or SOAR
- MFA not available yet


GREYCORTEX
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.10 Group-IB

Privately held Group-IB was founded in 2003 in Moscow but now has its global HQ in Singapore, and research centers in Amsterdam and Dubai. Their NDR functionality, packaged as the Threat Hunting Framework (THF), is one part of Group-IB's overall comprehensive solution against complex cybersecurity attacks and APTs. They also offer threat intelligence services, anti-fraud solutions, and brand protection services. The solution can be installed on-premises from an ISO image or delivered as an appliance or virtual appliance. THF can be deployed off network packet brokers or SPAN/TAP ports to perform passive network traffic analysis or configured as an active network defense solution that interoperates with proxy servers (ICAP), email servers (including inline MTA integration and “bcc:” analysis) or file storage systems and other shared resources. Throughput ranges from 10-20 Gbps for appliances and up to 1 Gbps for VMs. It can also be installed in IaaS, but customization is required. Management console can be run on-premises on Ubuntu or hosted in their SaaS. Their licensing model is based on traffic volumes and numbers of appliances deployed. They offer managed service options including full SOC-as-a-service, and THF is used by multiple MSSPs.

THF performs some NTA functions, such as application identification and mapping, file/device fingerprinting, and volume analysis. THF recognizes most of the commonly used enterprise IT protocols but does not cover streaming and mobile apps. THF can examine encrypted Slack communications. The product understands multiple OT/ICS protocols, including CIP, DeltaV, DNP3, IEC 60870-5-104, Modbus, OPC-DA and -UA, and S7/comm/comm+. THF has specific support for TLS 1.3. THF can use Suricata rules and has a sophisticated ML/DL implementation, encompassing unsupervised, supervised, and deep learning models. Models are trained on customer data and are configurable by customers. Baselining takes about a week. Detections are mapped to MITRE ATT&CK.

Packet decryption is possible using their separate THF Decryptor module. Sensor VMs can also be co-located with TLS termination services. THF can also pull data from their associated EDR solution if deployed. THF contains a sandbox for suspicious file detonation. Group-IB THF correlates events, assembles cases, automatically adds threat intelligence context from their CTI service for analysts, creates IoCs and allows customization of IoCs for threat hunting. Group-IB shares CTI with Europol, Interpol, some national CERTs, and other organizations. The analyst interface features drop-down list and regexp query builders, allows drill down from dashboard to details, has timeline and multiple map views, and supports annotation and playbook execution. THF can assist with root cause analysis and attribution theory development.

THF has more than 50 playbooks developed in conjunction with CERT analysts that can be edited by customers. Group-IB can create additional threat hunt playbooks for customers if needed. Responses are limited to host isolation.

THF supports CEF, JSON, REST API, SNMP, syslog, and YARA communications standards. Connectors for many SIEMs are available. Group-IB can interoperate with Palo Alto XSOAR, but other SOAR integrations would require customization. No ITSMs are directly supported. THF has not participated in

MITRE ATT&CK exercises. Basic reports are available, and customers can create other reports in CSV or PDF format. THF can leverage Group-IB's Fraud Hunting Platform capabilities for risk-based authentication for admins and analysts.

Group-IB THF has not obtained any security or cloud certifications. THF has excellent support for enterprise IT and OT protocols, and a good array of various ML and DL detection algorithms as well as support for TLS 1.3. It needs improvements in ETA methods, more SOAR integrations and response capabilities, and coverage for IIoT environments. Organizations that are looking for well-integrated NDR and EDR products, particularly in the APAC and EMEA regions, should place THF on the consideration list when looking for NDR solutions.

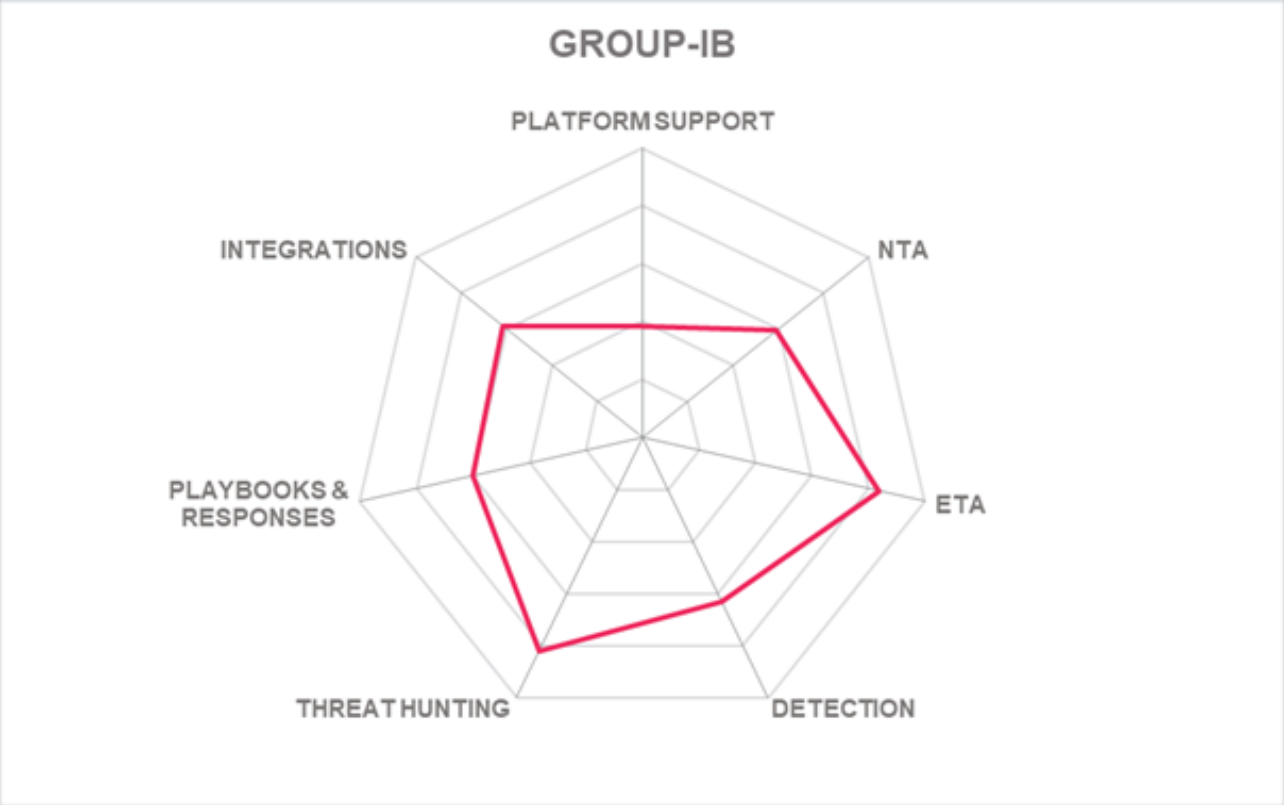
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●○○

Strengths

- Uses TLS 1.3 for sensor to console traffic; TLS 1.3 network comms can be analyzed
- Good support for ICS environments
- Can analyze Slack content
- Built-in sandbox (Polygon) and Threat Intelligence & Attribution service
- Multiple ML & DL detection models
- Risk-based authentication via integration with Group-IB's Fraud Hunting Platform

Challenges

- Complex licensing scheme
- Missing IIoT protocol support
- Playbook functionality and SOAR interoperability is limited
- Few automated responses available
- Security and cloud-hosting certifications should be pursued


GROUP-IB
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.11 Gurucul

Gurucul was founded in 2010 and is a privately-owned company headquartered in Los Angeles. Gurucul has a suite of products and services covering cybersecurity, fraud reduction, and identity intelligence. Gurucul NTA is a log aggregation service, so it is not deployed in-line or off span ports, and throughput isn't measured directly. It can be installed on various flavors of Linux, delivered as an appliance, virtual appliance, or binary that can be installed on customer infrastructure. It can be installed in IaaS via AMI, ISO, or OVA images. Gurucul supports private cloud and hybrid deployment models also. The management console can be run on-premises on CentOS or hosted in AWS, Azure, or their SaaS. Licensing is per node. They offer L1 triage/investigation and model training services.

Gurucul addresses nearly all Network Traffic Analysis use cases and has thorough coverage for enterprise IT protocols. Moreover, Gurucul NTA understands the most comprehensive list of OT/ICS and IIoT protocols, and this functionality is present right out of the box. Gurucul utilizes all ETA methods, obviating the need for traffic decryption in most cases. For static rules, Gurucul supports JSON, Sigma, and YARA formats. Gurucul NTA employs a sophisticated array of multiple unsupervised/supervised ML and DL detection algorithms, including some that are proprietary. Models are trained on public and private datasets as well as while in place at customer sites. Most model maintenance is performed by Gurucul, and models are pushed as needed. Customers can use Gurucul Studio to customize and even generate new detection models. Gurucul Studio's interface allows selection of attributes, model training, setting of prediction thresholds, result categorization, and definition of model arrays. Gurucul looks for all MITRE ATT&CK TTPs, and events are mapped as such in the analyst console.

If traffic capture is enabled and Gurucul NTA is configured with server keys, it can decrypt traffic. Gurucul can leverage endpoint agents, including 3rd-party EDR agents via APIs, to include endpoint telemetry. Connectors are available for a long list of 3rd-party sandbox and CTI services. Gurucul NTA correlates events, adds relevant CTI, and creates cases for analysts to review and IoCs for threat hunts. The console supports drop-down list, regexp, and natural language query building. It has multiple views, including maps and timelines. Case annotation and playbook launch from the console is possible.

Gurucul NTA comes with > 600 playbooks and a visual workflow editor for customization. Gurucul can assist with root cause analysis, attribution, and playbook execution recommendations. Gurucul NTA is part of a full platform including SIEM and SOAR. However, integrations with other vendors' SIEMs and SOARs are also available. Depending on the downstream tools' functions, Gurucul NTA can request actions such as full packet capture, session termination, host isolation, traffic blocking, and DNS sinkholing.

Gurucul NTA supports CEF, REST API, SMTP, SNMP, STIX, syslog, TAXII, YARA formats. Gurucul has integrations for the following ITSMs: BMC Helix, IBM Control Desk, Ivanti, Jira, Micro Focus, and ServiceNow. Gurucul NTA comes with a large number of standard reports, and more can be designed by customers. RBAC and MFA are enabled by integration with Microsoft Active Directory, LDAP, and IDaaS providers such as Duo, Okta, Ping Identity, and SecurID.

Gurucul has obtained most relevant security and cloud-hosting certifications, including ISO 27001/27018

and SSAE SOC 2 Type 2. CSA Star Level certification is in work. National level cyber security certifications are present for Germany, Switzerland, UK, and US. Since Gurucul is out-of-band, typical throughput measurements don’t apply; scaling can be achieved by adding instances. Gurucul has broad coverage for enterprise IT and OT/ICS/IIoT networks. It uses the most sophisticated ML/DL detection arrays in the market. Any organization that is looking for advanced NDR functionality that does not require in-line deployment should put Gurucul near the top of their consideration list.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

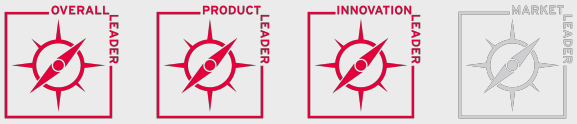
Strengths

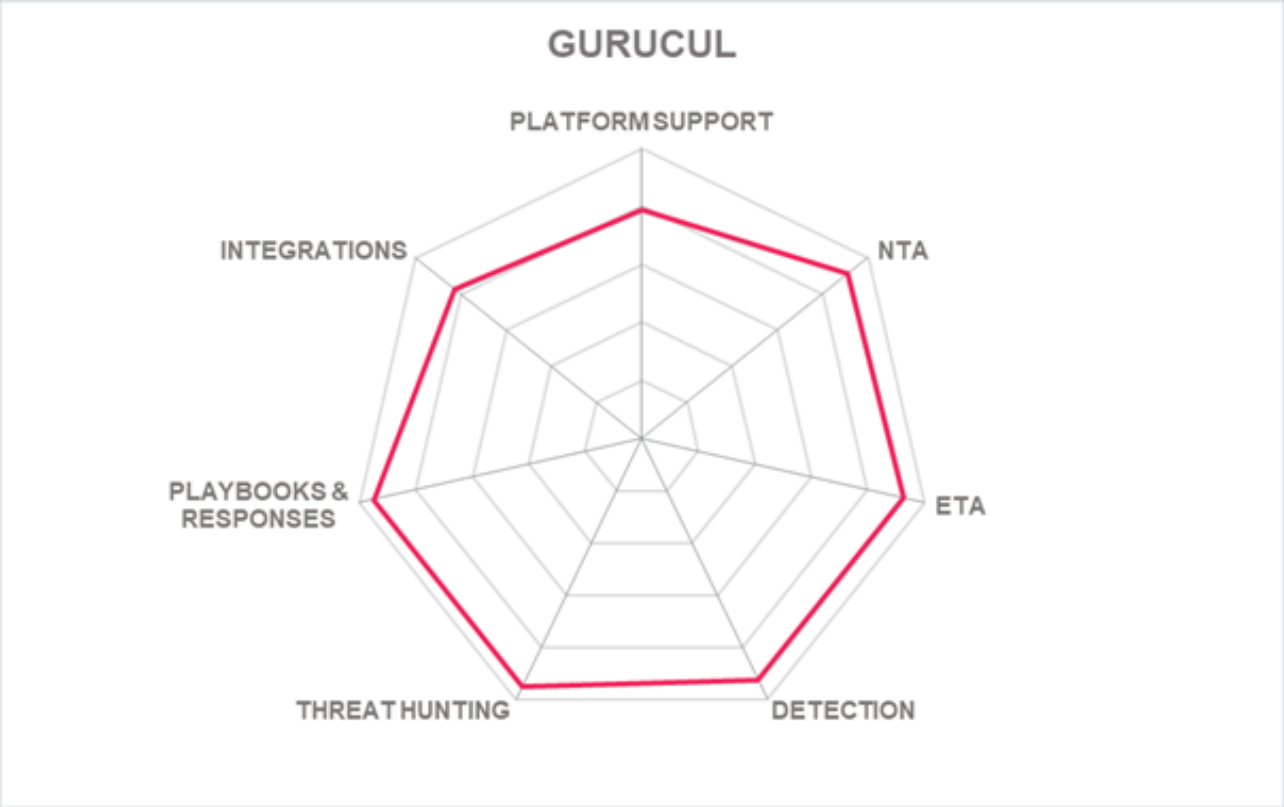
- Excellent coverage of enterprise IT protocols
- Most extensive support for OT/ICS and IIoT environments
- Comprehensive use of ETA techniques
- Excellent array of ML/DL detection models
- Gurucul Studio permits customers to tweak and even create new detection models
- Many relevant security and cloud-hosting certifications achieved
- Interoperable with many security and IAM platforms

Challenges

- No in-line deployment options
- Real-time log aggregation architecture
- Response actions depend on 3rd-party security solution integrations

Leader in




GURUCUL
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.12 NetWitness (RSA)

RSA is a well-known cybersecurity vendor that was acquired by Symphony Technology Group in 2020. Their headquarters is in the Boston area and they have offices around the globe. NetWitness sensors are delivered as CentOS server software, appliances or virtual appliances that can run on VMWare or Microsoft hypervisors and can be deployed off SPAN/TAP ports or packet brokers. Physical appliances can do partial capture up to 40 Gbps, full capture up to 10 Gbps, and virtual appliances and cloud agents can capture at 2 Gbps. Packet decryption is supported. NetWitness images can run in AWS, Azure, and GCP IaaS. Management console can run from the appliance or in the supported IaaS instances, but RSA does not host it as SaaS. Licensing is based on either number of admin/analyst seats, traffic volumes, or numbers of appliances and VMs. UBA options are licensed separately. RSA does not offer MDR services, but they do have approved partners.

NetWitness serves all standard NTA functions, and recognizes all pertinent enterprise IT protocols, however it does not address mobile or streaming apps. Only DNP3 and Modbus ICS protocols are recognized. ETA capabilities may be hampered slightly because a few key techniques are not employed. NetWitness users can write IDS type rules in the Esper Processing Language or YARA. ML detection capabilities are underdeveloped, but improvements are planned.

NetWitness can be set up to decrypt traffic. The separate UEBA and Event Streaming Analytics (ESA) modules help NetWitness detect MITRE ATT&CK TTPs. NetWitness can discover attempts to disable security controls, which is not a common feature in other NDR products. It can capture suspicious files and examine them with NetWitness Malware Analysis or dispatch them to Cisco ThreatGrid. Many CTI sources are accessible via NetWitness Orchestrator (separate module), which can facilitate event correlation, threat intel insertion, and case creation. Orchestrator also enables IoC creation and threat hunting. The analyst interface has drop-down list and regexp querying functions, map and timeline views, annotation, and playbook execution functions.

NetWitness comes with an unspecified number of playbooks that can be edited in flow-chart form and modified as templates. Playbooks can be launched automatically. Response types include session termination, host isolation, block traffic, and DNS sinkholing. Connectors to SIEM and SOAR solutions are available within NetWitness Orchestrator, including Micro Focus ArcSight, Microsoft Azure Sentinel, FireEye, IBM QRadar and Resilience, McAfee, Palo Alto XSOAR, Splunk, and ThreatConnect.

NetWitness supports CEF, Cybox, SNMP, STIX, syslog, TAXII, and YARA protocols and formats. NetWitness has a large number of reports available OOTB, and customers can create more with a visual report editor. Various roles for admins and analysts can be utilized; and MFA options include RSA SecurID and SAML federation.

NetWitness uses FIPS 140-2 crypto and is hardened to IEC 15408 Common Criteria and US DOD STIG guidelines. Other certifications have not been obtained yet. More emphasis on automation of investigations, threat hunting, and responses would be beneficial. Better coverage of ICS and IIoT would make the solution more appealing for industrial settings. The rules-based threat classification engine should be enhanced by

supervised ML and/or DL models. For full NDR capabilities, the licensing scheme requires investment in multiple products (ESA, Malware Analysis, UEBA, and Orchestrator). The packaging of products should be redesigned around NDR use cases. Organizations with other RSA products or who are using NetWitness already for other functions should consider RSA if they are searching for NDR solutions.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○

NETWITNESS

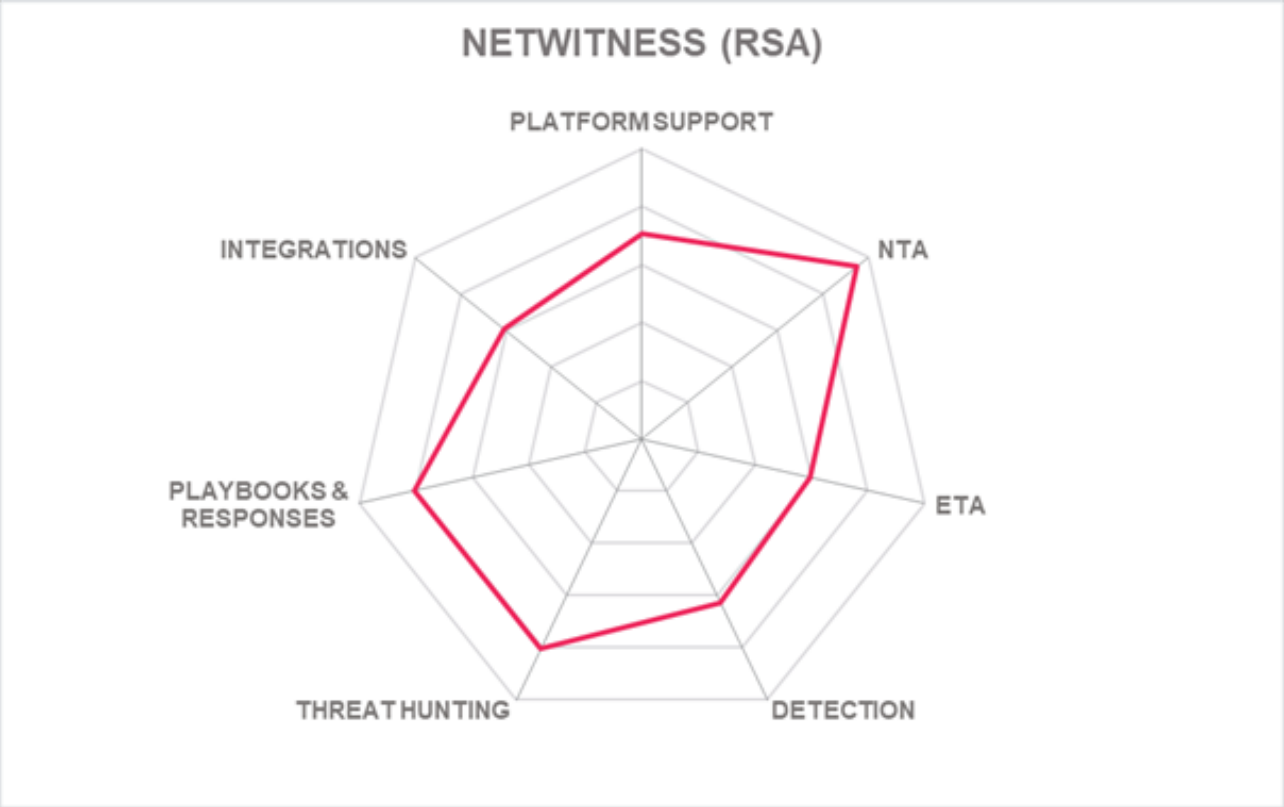
Strengths

- Covers all NTA use cases
- Broad range of attack types discoverable when used with UEBA & ESA
- Extensive list of IoC and attribute types analyzed
- Good selection of auto responses when used with NetWitness Orchestrator
- Hardened to Common Criteria and US DOD STIG standards

Challenges

- Complex licensing arrangements: multiple products needed for optimal functionality
- TLS 1.3 not supported
- Limited OT/ICS/IIoT protocol recognition
- ML-based detection capabilities need to be enhanced
- Additional ETA techniques should be implemented

Leader in


NETWITNESS (RSA)
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.13 Plixer

Plixer is a network and security specialist owned by Battery, a private equity firm. Plixer was founded in 1999 and is headquartered in Kennebunk, Maine, US. Sensors are CentOS-based physical or virtual appliances that can be deployed on Hyper-V, KVM, or VMware hypervisors. The appliances are not installed in-line or off SPAN/TAP ports, rather they gather traffic info via IPFIX or NetFlow. Plixer can take in VPC flows from AWS and Azure. Max ingestion rate is 100,000 flows per second per collector (not counted as throughput in terms of Gbps). The management console can run from the appliances or from the supported cloud services. The pricing model is based on the number of connected flow exporting devices and flow rates, rather than by the number of deployed sensors or by analyst seats.

Plixer handles all major NTA use cases and recognizes most enterprise IT protocols. Plixer does not provide coverage for OT/ICS or IIoT protocols, however. Scrutinizer employs a subset of available ETA methods. Scrutinizer contains a mix of unsupervised and supervised ML detection models to augment rule-based flow analysis. Models train on customer flows and can be updated by Plixer as frequently as warranted. Baselining takes approximately one week. Customers can modify detection models if needed. The solution is not currently aligned with MITRE ATT&CK at present, but it does monitor for the majority of MITRE TTPs. MITRE ATT&CK alignment is planned for 1H2022.

As an out-of-band solution, Plixer does not decrypt traffic, but partners with Gigamon and Ixia for customers who need packet level visibility. Scrutinizer does not capture suspicious files, thus there is no connectivity to sandboxes. External CTI sources are not plumbed in but can be configured. Scrutinizer does event correlation and case assembly and can pull threat info from Security Intelligencer. Analysts can manually build IoCs for threat hunts. The analyst interface features drop-down lists and regexp query facilities, as well as map and timeline views. Analysts can drill down from the dashboard and annotate cases. Advanced investigative functions are not present.

Playbooks are not available out-of-the-box but can be configured by their professional services. Scrutinizer can alert admins via email, SMS, and SNMP. Responses are limited to Webhooks and scripted API actions, such as initiating full packet capture and recommending host isolation. Scrutinizer can interoperate with all major SIEMs, and often is positioned upstream of SIEMs, acting as a filter which only passes on anomalies and alerts. SOAR integrations are planned.

Plixer supports CEF, REST API, SNMP, STIX, syslog, TAXII, and Webhooks formats/protocols. Plixer can interoperate with ServiceNow ITSM, and Qualys and Tenable for vulnerability management. More than 600 canned reports are available, and customers can create new report types if desired. Scrutinizer supports analyst and admin roles, and MFA via SAML.

Since Plixer is not primarily providing cloud-hosted services, they have not pursued certifications in this area. Scrutinizer addresses most all NTA use cases and MITRE ATT&CK TTPs, although the product is not currently aligned with MITRE. Customers can tweak rules and ML detection models as needed. Additional ETA methods would likely be useful. Plixer occupies a slightly different part of the NDR market. The ability to stage Scrutinizer ahead of SIEMs in the architecture can help reduce false positives, alerting, and storage

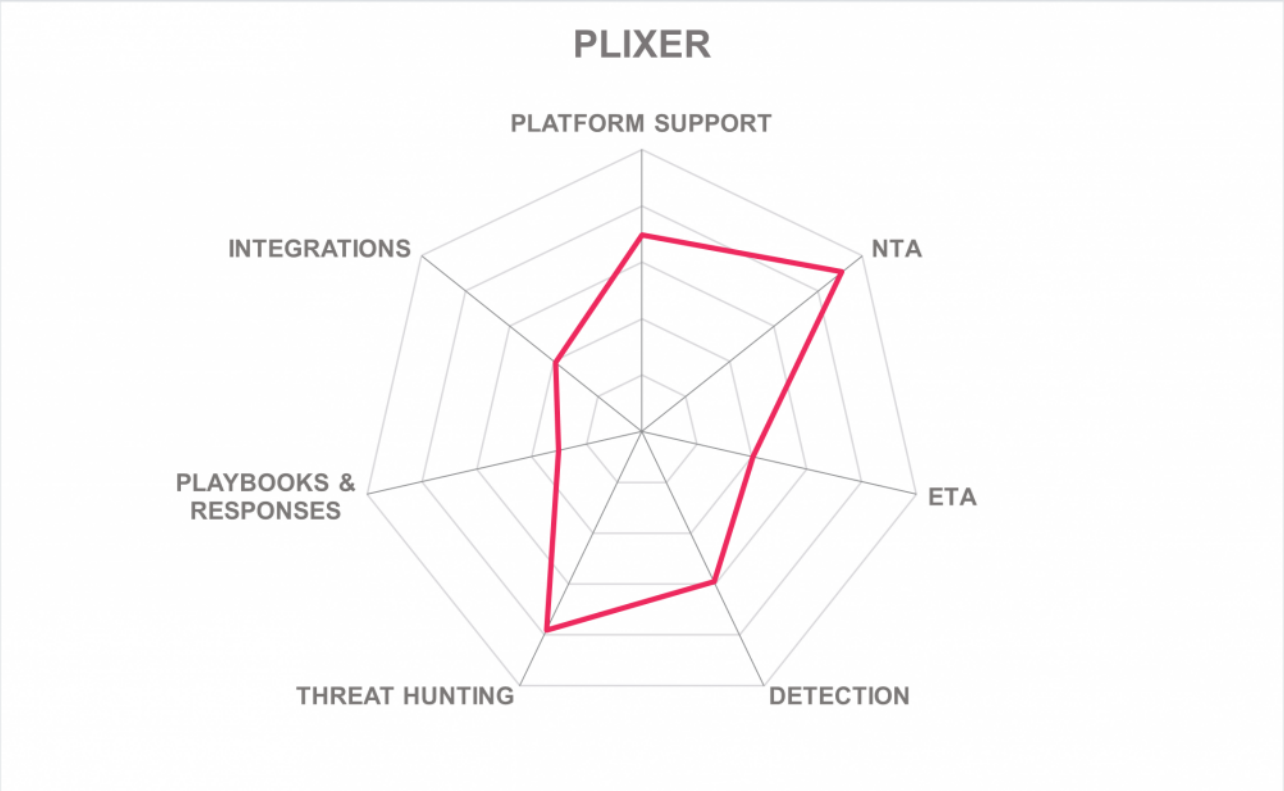
costs within SIEMs. They are targeting enterprises with requirements for strict control over network and security telemetry. Moreover, this design principle allows customers to retain data for longer periods, thereby facilitating investigations of sophisticated attacks such as APTs. Plixer Scrutinizer's out-of-band flow consumption design is appealing to mature organizations that already are capturing such flows and want to add NDR capabilities in a cost-effective manner.

Strengths

- Good NTA use case functionality
- In-situ detection model training; models are configurable by customers
- Many reports available OOTB, and customers can create more types
- Long default data retention periods
- Can serve as a pre-SIEM filter to reduce data storage requirements, costs, and false positives

Challenges

- TLS 1.3 not supported
- Focused on on-premises deployments rather than SaaS
- Additional ETA methods needed
- MITRE ATT&CK mapping on the roadmap
- CTI sources can be integrated and playbooks can be configured by professional services
- More focus on advanced investigations and response automation would be beneficial


PLIXER
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

5.14 VMware

VMware acquired Lastline in 2020. Lastline Defender is the basis of VMware's NSX Network Detection & Response product. Sensors can take the form of appliances, virtual appliances, AWS AMIs, Azure VHDs, and agentless/virtual NICs within the hypervisor. The management console can be co-located within an appliance or VM. Deployment options include in-line, off SPAN/TAP ports, off packet brokers, and through Carbon Black Workloads. In-hypervisor vNIC deployment scenarios are recommended to reduce cost, complexity, and traffic duplication. Max throughput for a single appliance is 10 Gbps, but they can be load-balanced. Pricing is per appliance or per NSX-ATP socket.

NSX NDR performs all standard NTA functions and can examine many enterprise IT protocols and some mobile app traffic. The OT/ICS/IIoT protocols that are understood are limited to DNP3, Modbus, and MQTT. NSX NDR employs the full gamut of encrypted traffic analysis techniques. Customer admins can import or create IDS type rules. NSX NDR utilizes a well-thought-out matrix of unsupervised and supervised ML and DL-based detection models. Detected events are mapped to MITRE ATT&CK. The models are managed and updated by VMware; customers can only adjust alerting parameters. The models are trained on public datasets and in customer environments. Models are updated frequently as needed. Baselining can occur in 1-14 days.

NSX NDR can do packet decryption if desired. VMware Advanced Threat Analyzer is the built-in sandbox. Customers could configure connections to other sandbox services via API. NSX NDR correlates events, adds relevant CTI, and opens cases for analysts to review. The analyst console allows creation and customization of IoCs for threat hunts across the enterprise. Several external CTI sources are integrated, and VMware contributes threat intel with Cyber Threat Alliance. The analyst interface features a built-in query portal which uses their own query language. Elastic-based and regexp searches are also possible. Map and timeline views are present, but playbooks cannot be launched from the console. Dashboard widgets are configurable.

Playbooks have been developed by the community of VMware users. Development of supported playbooks by VMware is planned. Response actions depend on API connectivity to other VMware tools or 3rd-party vendors, and can include session termination, host isolation, full packet capture, blocking traffic by IP/URL, and DNS sinkholing. Email and Slack can be used for alerting. Connectors are available for Micro Focus ArcSight, FortiSIEM, LogRhythm, IBM QRadar, and Splunk SIEMs; and ManageEngine, Micro Focus, Palo Alto XSOAR, ServiceNow, Siemplify, Swimlane, ThreatConnect, and ThreatQuotient SOARs. ServiceNow ITSM integration is available OOTB, and customers can build connections to other ITSMs over APIs.

CEF, JSON, REST API, STIX, syslog, XML, and YARA protocols/formats are supported. Basic reports are present, and customers can extend reporting capabilities using the ELK stack. Three roles are available for admins and analysts, and customers could create more fine-grained roles if needed. NSX NDR does not directly support MFA but does accept SAML assertions.

VMware NSX NDR is only certified for CSA Star Level 1, other relevant certifications for security and cloud-hosting are in work. Although the per-sensor throughput is 10 Gbps, they can be load-balanced to achieve

whatever volumes customers require. VMware NSX NDR has some work to do in the area of playbook development and response capabilities. More support for OT/ICS/IIoT would make the solution more appealing in certain industrial environments. The vNIC deployment option simplifies and lowers costs for customers. NSX NDR has excellent NTA and ETA capabilities. Their implementation of ML and DL-based detection models seems quite sophisticated, aiming to increase the sensitivity of detections while minimizing false positives. Organizations with current investments in VMware will want to closely look at NSX NDR & ATP for NDR; moreover, organizations with extensive public and/or private cloud asset utilization should consider NSX NDR for its architectural advantages.

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●●

vmware®

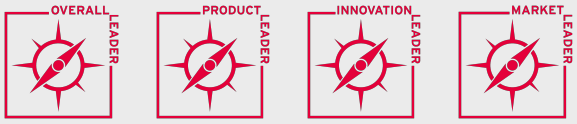
Strengths

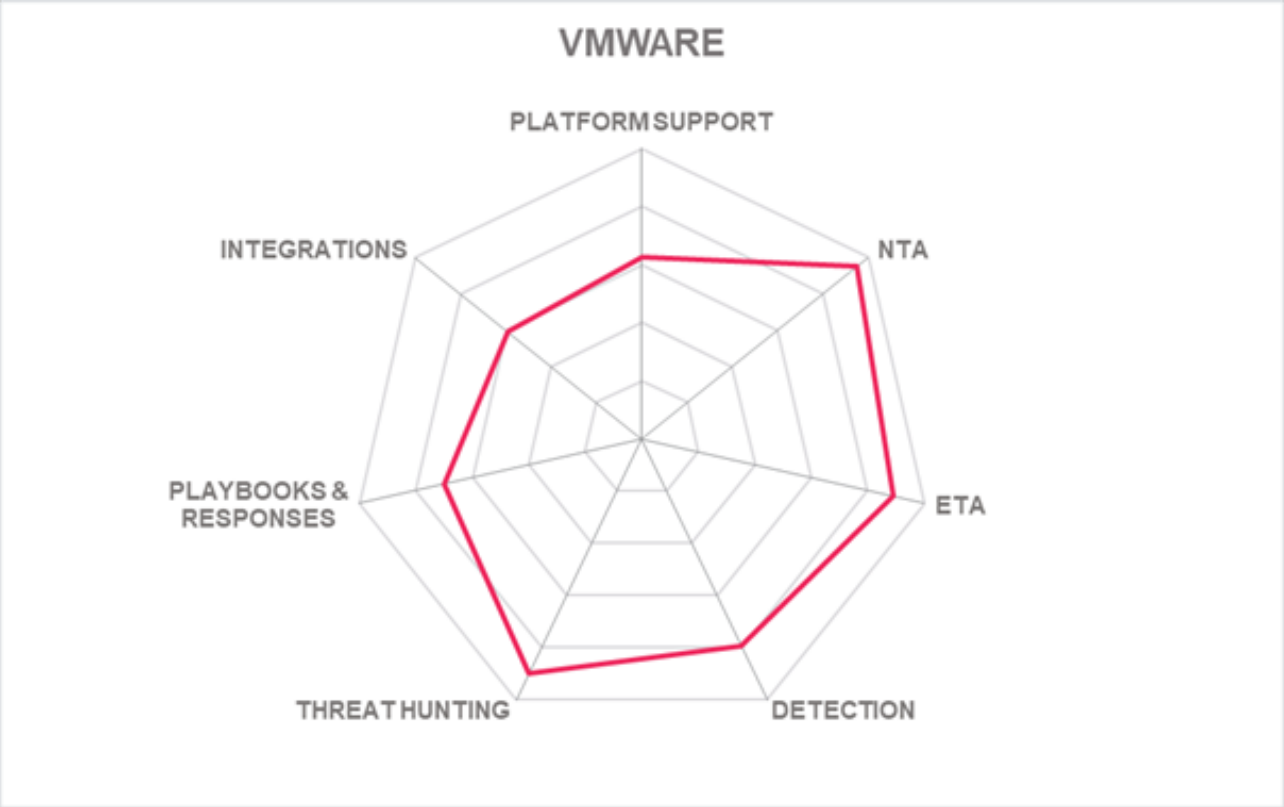
- Agentless vNIC deployment option provides lower cost and complexity
- TLS 1.3 support
- Excellent use of ETA techniques
- Sophisticated array of ML & DL based detection models
- Built-in sandbox
- Contributing member of Cyber Threat Alliance

Challenges

- Coverage for some streaming protocols is not present
- Needs more support for OT/ICS and IIoT protocols
- Response actions and playbook development should be emphasized
- Cloud-hosting and security certifications are in work

Leader in




VMWARE
PLATFORM SUPPORT
NTA
ETA
DETECTION
THREAT HUNTING
PLAYBOOKS & RESPONSES
INTEGRATIONS

6 Vendors to Watch

6.1 Darktrace Enterprise Immune System

Darktrace was founded in 2013 in Cambridge, UK. The software is delivered as virtual or physical appliances and can be deployed off span ports or in the cloud: Darktrace has comprehensive coverage for IaaS and SaaS deployments. Darktrace examines a wide range of network behaviors and protocols and has the ability to learn new protocols as well. Darktrace focuses on understanding “patterns of life” of devices on the network rather than just looking for anomalies and trying to determine if malicious.

Why worth watching: Darktrace was an Overall, Product, Innovation, and Market Leader in last year’s edition of this Leadership Compass on NDR. They were not able to respond to this year’s questionnaire.

6.2 Gigamon ThreatINSIGHT

Gigamon, founded in 2001 in the Bay Area, is a privately owned network traffic visibility and security specialist. Gigamon is well-known for their network packet broker products. ThreatINSIGHT is their NDR solution. It can analyze hundreds of network connection metadata attributes and understands common protocols as observed by their packet brokers. ThreatINSIGHT features multiple ML detection models. Gigamon has expanded the number and types of integrations available to other security tools.

Why worth watching: Gigamon now offers what they call “Guided SaaS NDR”, which is their managed service tailored to customer environments. Given the complexity of NDR deployment at large enterprises, this hybrid deployment and management model should have appeal in the market.

6.3 Kaspersky

Kaspersky is a leading cybersecurity vendor headquartered in Russia with global transparency centers in Switzerland and Spain. Their NDR capabilities are provided by Kaspersky Anti-Targeted Attack, Secure Mail Gateway, and Endpoint Detection & Response. Their solution uses advanced in-house developed ML detection models.

Why worth watching: Kaspersky was an Overall, Product, and Market Leader in last year’s Leadership Compass on NDR. They are focusing on XDR and will appear in future KuppingerCole research on XDR.

6.4 Securonix

Securonix is a late-stage cybersecurity startup renowned for their SIEM solutions. They also have SOAR, UBA, Adversary Behavioral Analytics, and CTI services. Securonix sells passive-mode NDR functionality as an add-on to the SIEM solution. Securonix primarily takes a log analysis approach to NDR, and can also ingest traffic flow data from Gigamon and Corelight. Securonix has strong compliance monitoring features.

Why worth watching: Securonix is widely deployed by MSSPs. Their solution offers advanced security analytics with a strong emphasis on adding identity context. Securonix is moving toward passive-mode XDR, leveraging integrations with other major security tool vendors.

6.5 Sophos

Sophos is a well-respected name in endpoint security, with products and services for endpoint anti-malware, EDR, firewalls, secure web gateways, cloud security. Sophos recently acquired Braintrace, a mid-stage startup focused on NDR.

Why worth watching: Sophos intends to integrate Braintrace's solution into their Managed Threat Response service and XDR products in the first half of 2022. The combination of EDR and NDR will give Sophos an even broader coverage in the XDR market.

6.6 Stellar Cyber – Open XDR

Stellar Cyber is a mid-stage startup founded in 2015 in the Bay Area. Their product, OpenXDR, serves several cybersecurity roles including NDR and SIEM as well as XDR. Stellar Cyber offers their product as both physical or virtual appliances and can be deployed off network devices in on-premises environments. OpenXDR has coverage for common IaaS and SaaS environments. The product also has investigation, threat hunting, and response capabilities which are enhanced by ML. Stellar Cyber Open XDR utilizes SOAR-like integrations with other security tools to collect telemetry and can effect responses in downstream controls.

Why worth watching: Stellar Cyber is focusing on the XDR market and will participate in future KuppingerCole research on that subject.

6.7 Vectra - Cognito

Vectra was established in 2010 in San Jose, CA. Their NDR suite is composed of Detect, Recall, and Stream products. Vectra's strategy focuses on highly tuned ML models that provide a good signal-to-noise ratio thereby making the analysts' jobs easier. Vectra is addressing advanced use cases for IaaS and SaaS app detection and response in a category they call Threat Detection & Response.

Why worth watching: Vectra was a leader in all four categories of the 2020 Leadership Compass on NDR. Vectra declined to participate in this year's report.

7 Related Research

Leadership Compass Network Detection & Response (2020)
Buyer's Compass NDR
Leadership Brief: Do I Need Network Threat Detection & Response?
Executive View: Vectra Cognito
What is XDR? blog

Methodology

About KuppingerCole's Leadership Compass

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- **Security
- Functionality
- Deployment
- Interoperability
- Usability**

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

Strong positive
Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Declined to participate:** Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- **Lack of information supply:** Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will

provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.