KuppingerCole Report

LEADERSHIP COMPASS

By John Tolbert

June 10, 2020

Network Detection and Response

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

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 (EPP), 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 Detection and Response (EDR) 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 (previously unseen in the wild), which may give them the advantage of not being detected by EPP agents. Enter NDR as a tool of last resort to discover hitherto unknown compromises. Since data exfiltration is usually an objective, 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 combat botnet activities and to provide visibility in IoT/OT/SCADA environments where it may not be possible to implement endpoint agent-based solutions.

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 real-time and later 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, 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 effectiveness.

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 you need and where they should be placed depends on your architecture. Proper design of NDR deployments is necessary to capture 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; while supervised ML models categorize possible threats among the outliers, classify malicious activities, domains, and other attributes. Supervised ML is also used by some vendors for encrypted traffic analysis. The most effective solutions utilize several layers of ML-enhanced processing of all traffic at line speed. Vendor products in this segment typically advertise 5 – 100 Gbps throughput.

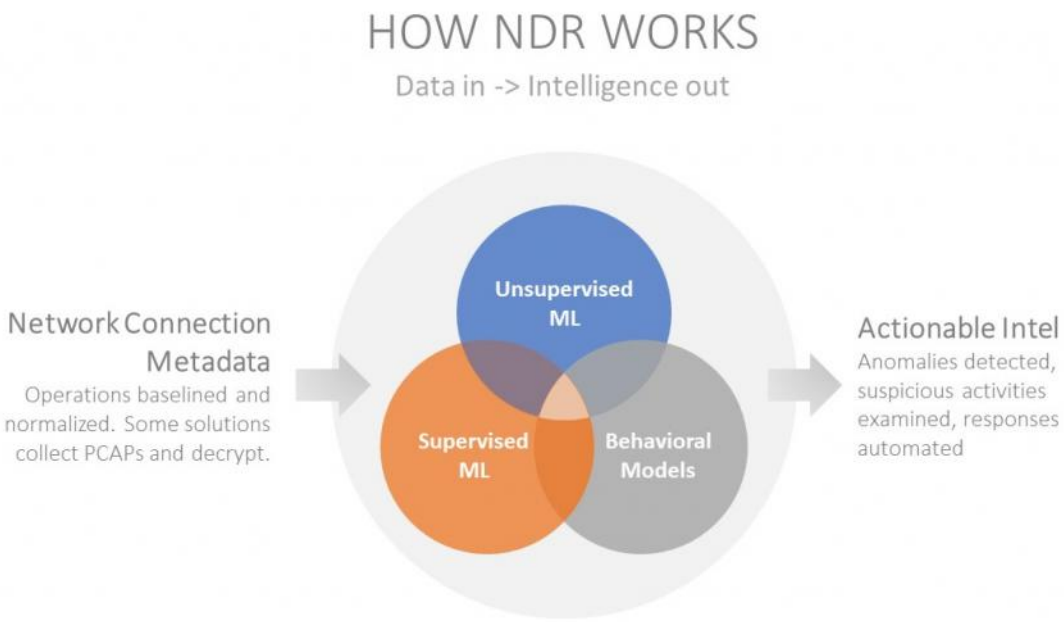


Figure 1: How NDR Works

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.

Though many security pros tend to ignore trends that seem overhyped by vendors, there are some 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 (EPP) 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 this happens:

1. BYOD bypass: In permissive environments, some users may not have EPP and may bring

in infected devices. Business partners and contractors may use their own devices, which are typically 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.
3. Many IoT devices can't run EPP. Operating systems may not support EPP 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. 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 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. 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.

In most of the above IoT/OT scenarios, enterprises segregate these kinds of 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.

Even though endpoint-based solutions may not have visibility of all malicious activities, malware generally 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.

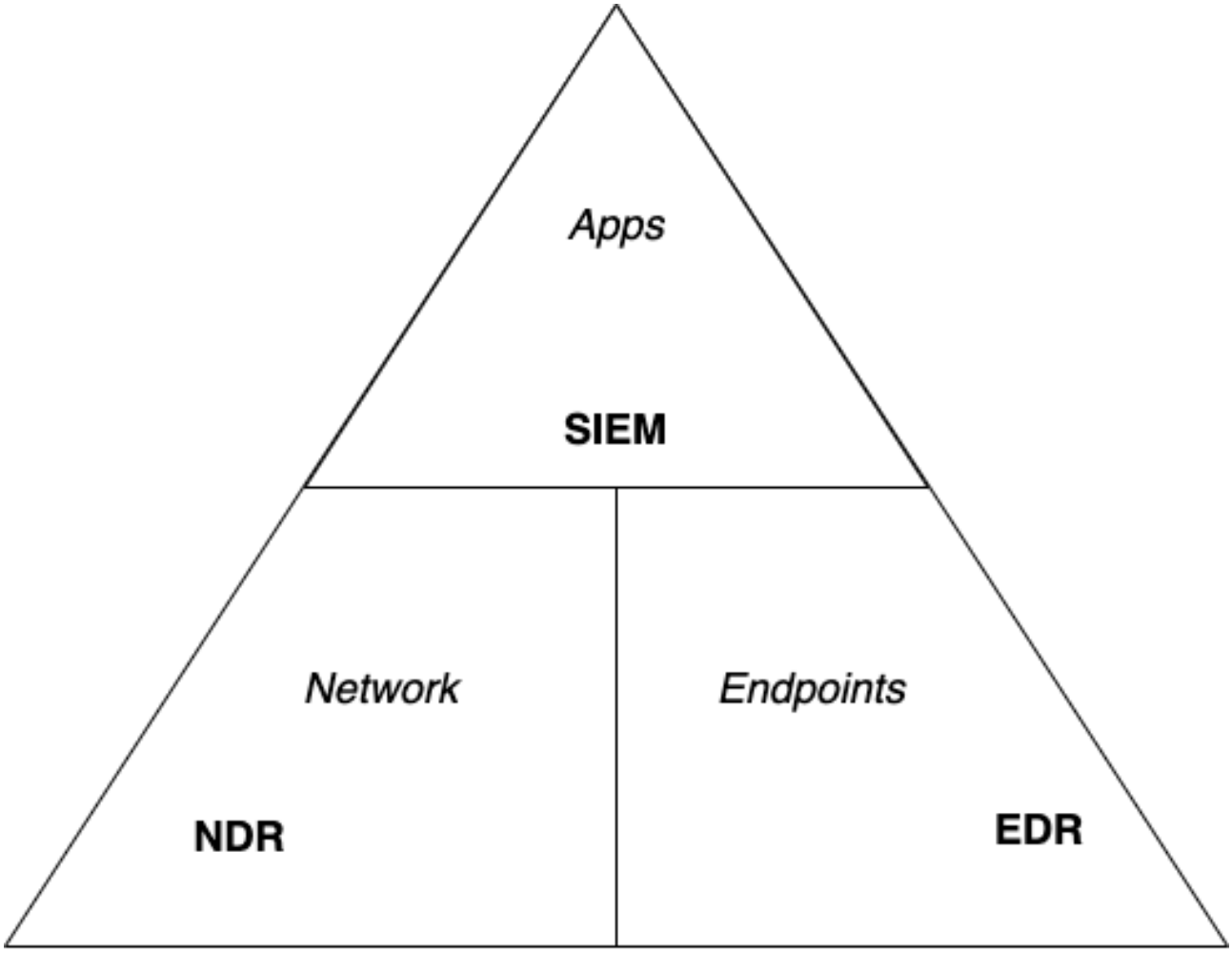


Figure 1: Security Monitoring Pyramid

1.1 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, reducing adversary dwell time, Mean-Time-To-Respond (MTTR), and data loss from attacks.

There is some variety in the types of vendors in this market. On one end of the spectrum we find startups, progressing through larger, more well-established 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 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. Differentiators are vendors which offer two features especially: sandboxing and packet decryption. Not all vendors choose to implement these functions. Packet decryption requires a far more invasive deployment, allowing the NDR solution to essentially read all traffic as it passes by. Sandboxing is not technically feasible unless packet decryption is in place. Furthermore, 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.

Some vendors argue that decryption is unnecessary because they can reliably figure out if traffic is malicious based on analysis of network connection metadata. Consequently, these vendors' products do not offer packet decryption. Other 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 and sandboxing is represented in this report, but it is not a determining factor in whether or not a given vendor solution is considered NDR.
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 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.

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

1.2 Delivery Models

NDR products require an on-premise 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 ports/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 in 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.

1.3 Required and Optional Capabilities

In this report, we are looking for comprehensive solutions that provide at least 7 of the 9 major areas of functionality detailed below. These are typically the requirements that customers pose to prospective vendors in RFPs. NDR products and services can have a wide range of functions. The major required features are:

- Full packet capture and analysis
- Use of unsupervised and supervised ML algorithms and models for detection and analysis
- Traffic metadata analysis to yield baselines
- Anomaly detection in traffic patterns

- Analysis of anomalies to detect threats
- Ability to generate automated responses based on policies or playbooks
- Integration with other security solutions such as SIEM and SOAR
- Packet decryption (optional)
- Sandbox detonation of suspicious code (optional)

Full packet capture and analysis does not necessarily mean that encrypted packets are decrypted prior to analysis. Not all NDR tools offer packet decryption. The ability to decrypt packets for full in-the-clear inspection generally requires in-line deployment of NDR sensors, with the NDR sensors essentially acting as a Man-in-the-Middle. Many NDR vendors have avoided this technical path for two major reasons: this approach makes NDR an explicit target for attackers, and not many customer organizations request it or choose to use it. Packet decryption enables collection and detonation of possible malware payloads, so vendor products that don't decrypt don't have sandboxes. Some organizations deploy NDR in special segmented network zones where multiple security tools have access to decrypted data. In these cases, it is possible for NDR solutions to examine all decrypted traffic without having to be set up in-line and holding the pertinent encryption keys.

In lieu of packet decryption, some vendors use the JA3 and JA3S methods of fingerprinting and analyzing SSL/TLS encrypted communications. These techniques can be useful because there are a limited number of libraries and extensions for SSL/TLS Hello processes. Researchers discovered that fingerprints or profiles could be built that would identify clients and servers. This method has been widely used in the last few years, but there are gaps. It is best-effort open source project, which is not updated as frequently as necessary. This leads to occasional new permutations of browsers, clients, and servers which are not easily identified. Also, if an attacker uses proprietary encryption libraries, it will succeed in being undetected for a while. The JA3/S method is essentially a signature detection technique, which suffers from the same kind of failure scenarios that signature-based anti-malware solutions do: new threats have not been fingerprinted, so there are no corresponding signatures to detect, thus there is an inability to detect new threats until signatures are developed.

Other vendors take a slightly different approach. Realizing some of the limitations of JA3 and JA3S, they have developed proprietary methods for analyzing encrypted traffic to determine if it is indicative of malicious behavior. In these cases, vendors do not provide a lot of technical detail on how this is done because they consider this kind of technology to be their intellectual property and competitive advantage.

NDR products that are not deployed in-line passively examine traffic flows from the span/tap ports or from network packet brokers. They do not have the built-in ability to take response actions such as isolating nodes or blocking traffic. They accomplish this by using network

enforcement devices APIs (firewalls, email/web gateways, VPNs, etc.).

2 Leadership

Selecting a vendor of a product or service must not be only based on the comparison provided by 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.

2.1 Overall Leadership

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

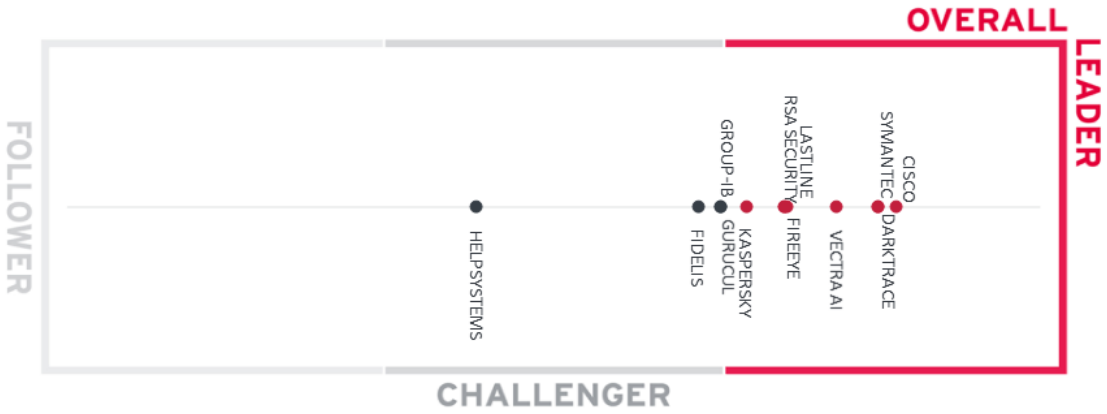


Figure 3: The Overall Leadership rating for the Network Detection and Response market segment

The Overall Leaders in NDR are Cisco, Darktrace, FireEye, Kaspersky, Lastline, RSA, Symantec, and Vectra. Many of these are IT security juggernauts with decades of experience in designing, acquiring, and integrating various security technologies into their overall stacks. Cisco added security to their portfolio of network solutions very early and continues to leverage their size and placement to help defend customer environments. FireEye, Kaspersky, RSA, and Symantec have had security as a focus since they were established and have developed a robust suite of interconnected security solutions including NDR. Darktrace, Lastline, and Vectra are specialists in the detection and response field. They have grown considerably in terms of product capabilities and installed base in a relatively short period because of the value their customers perceive.

The upper half of the Challenger area is quite crowded, with Fidelis, Group-IB, and Gurucul found here. Most of these companies are dedicated XDR expert solutions, where the "X" = NDR + EDR. In the second half of the Challenger box we find HelpSystems.

Overall Leaders are (in alphabetical order):

- Cisco
- Darktrace
- FireEye
- Lastline
- RSA
- Symantec
- Vectra

2.2 Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

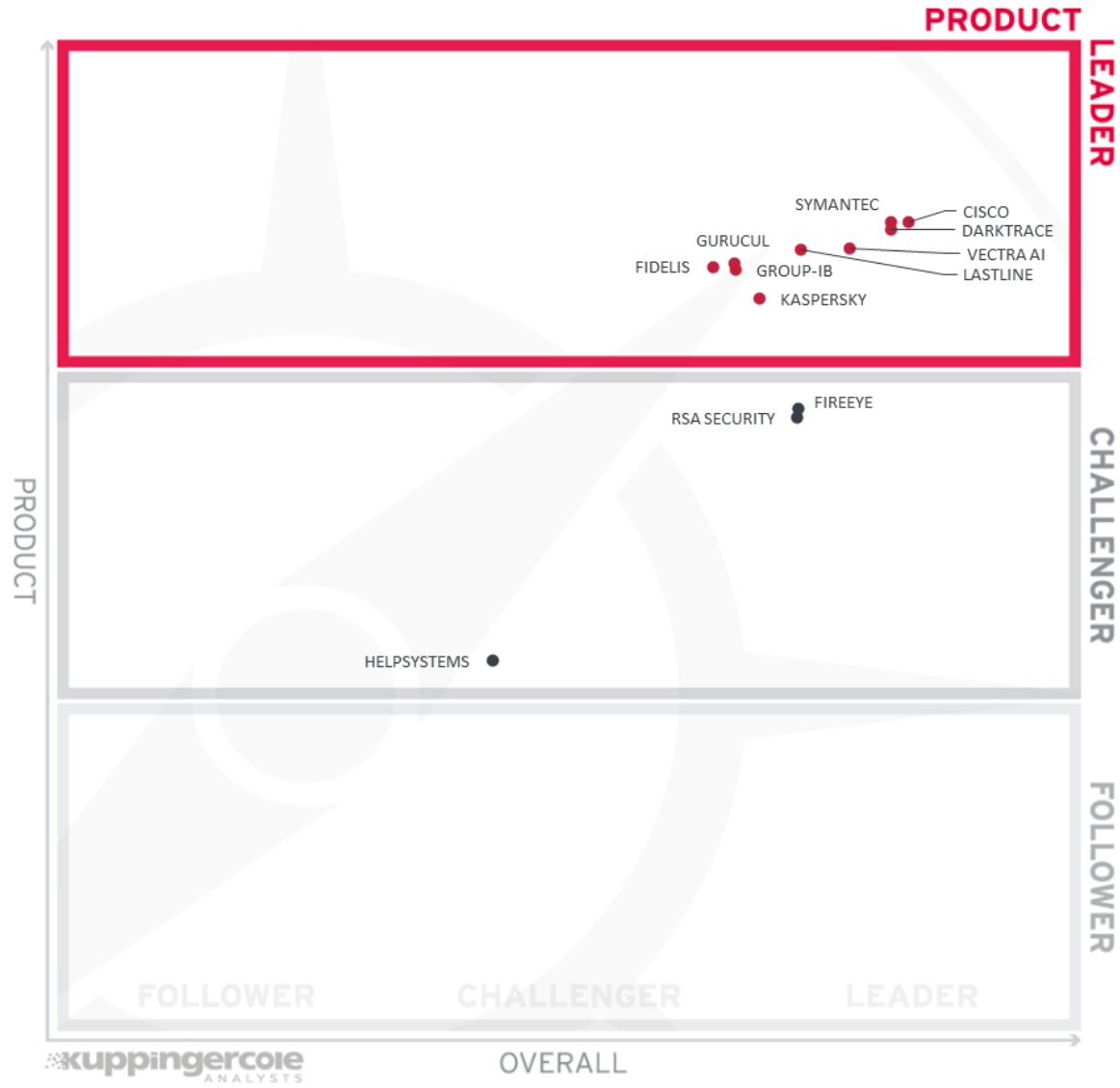


Figure 4: Product Leaders in the Network Detection and Response market segment

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

We have a large selection of products in the Product Leader chart. Many are large security vendors but there are some rather focused VC-backed startups in the list as well. Cisco, Darktrace, Fidelis, Group-IB, Gurucul, Kaspersky, Lastline, Symantec, and Vectra are all leaders. It is interesting to note, as you see in more technical detail in chapter 5, how these vendors approach NDR from different perspectives and yet all have made it into the Product Leadership category.

Near the border on the Challenger side we see FireEye and RSA. Both of these solutions are quite strong overall but missing a few key features.

HelpSystems is lower in the Challenger chart. These products have particular strengths or may be emphasizing specific feature sets for their target customers. They are missing the complete feature list for NDR that we expect but may perform well for certain use cases.

Product Leaders (in alphabetical order):

- Cisco
- Darktrace
- Fidelis
- Group-IB
- Gurucul
- Lastline
- Symantec
- Vectra

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 cutting-edge features, while maintaining compatibility with previous versions.

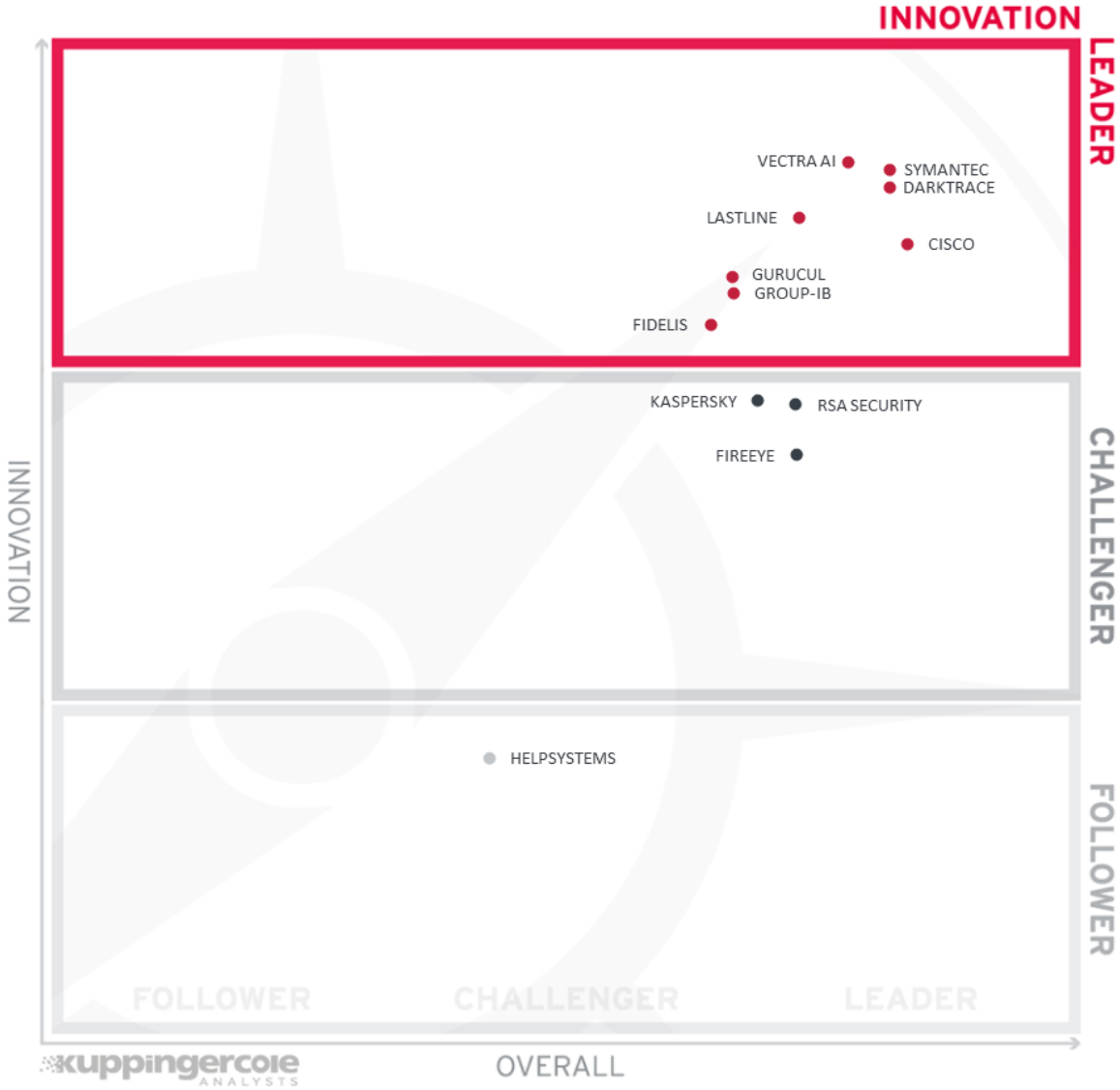


Figure 5: Innovation Leaders in the Network Detection and Response market segment

Among those surveyed in this field, many are innovators. Innovation leadership is especially important in cybersecurity because attackers are constantly innovating as well. Tracking how malicious actors are modifying their tactics and even learning to anticipate their next moves is essential for environments that require excellent cybersecurity posture.

In the top third we see Cisco, Darktrace, Fidelis, Group-IB, Gurucul, Lastline, Symantec, and Vectra. Most of these are NDR or XDR specialists.

Kaspersky and RSA are just below the Innovation Leaders. FireEye is in the center of the Challenger block. HelpSystems is near the top of the Follower region.

Innovation Leaders (in alphabetical order):

- Cisco
- Darktrace
- Fidelis
- Group-IB
- Gurucul
- Lastline
- Symantec
- Vectra

2.4 Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of managed appliances or instances, ratio between customers and managed 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.

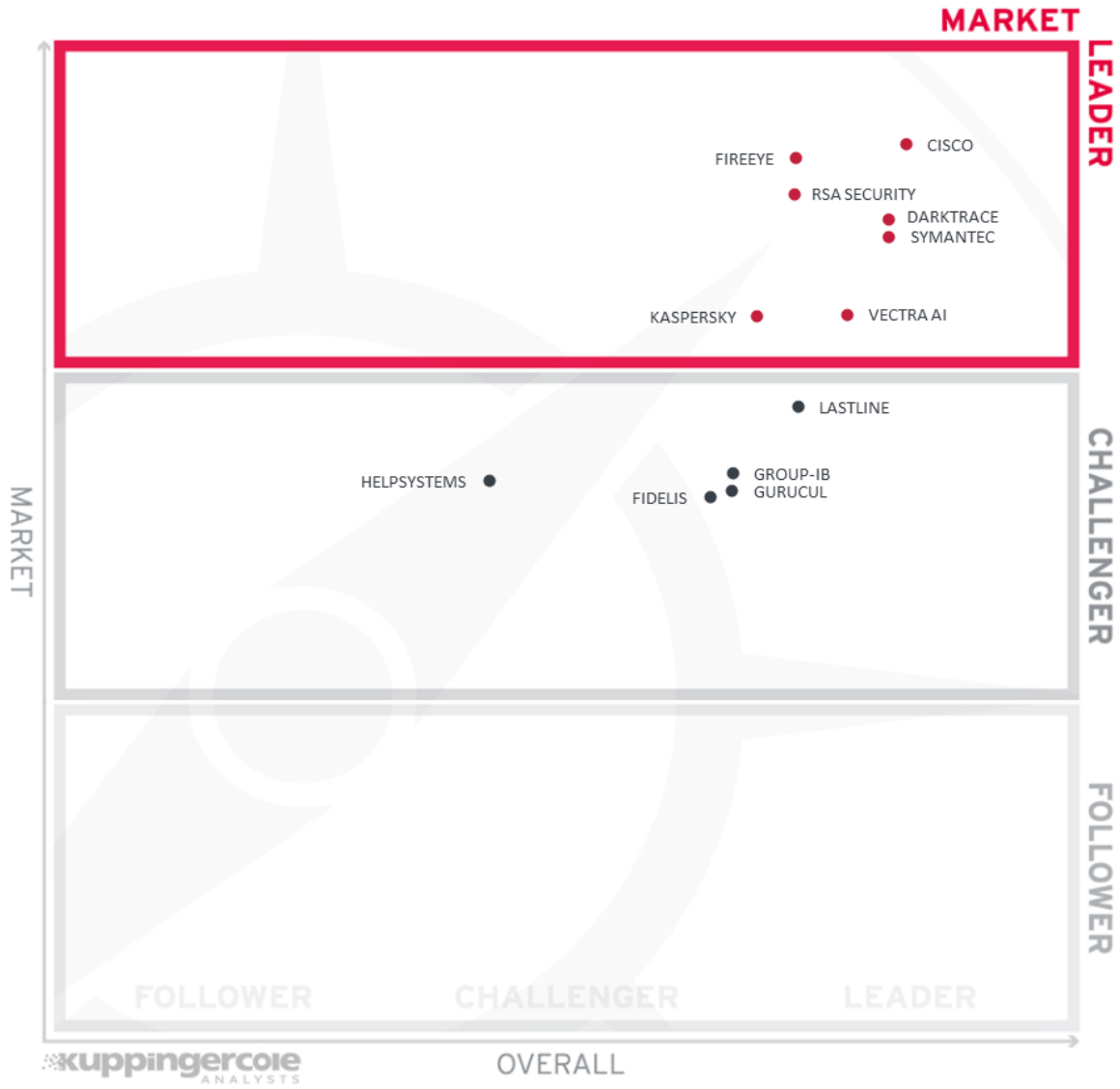


Figure 6: Market Leaders in the Network Detection and Response market segment

Cisco, Darktrace, FireEye, Kaspersky, RSA, Symantec, and Vectra are the Market Leaders. Although it is not surprising that some of the large vendors are at the top, it is important to note that this rating is influenced by the number and size of reported active customers of NDR solutions.

Lastline is almost in the market leader section. With the announced acquisition by VMWare, they will certainly move to market leader when the deal closes. Across the remainder of the Challenger section we see Fidelis, Group-IB, Gurucul, and HelpSystems.

Market Leaders (in alphabetical order):

- Cisco

- Darktrace
- FireEye
- RSA
- Symantec
- Vectra

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.

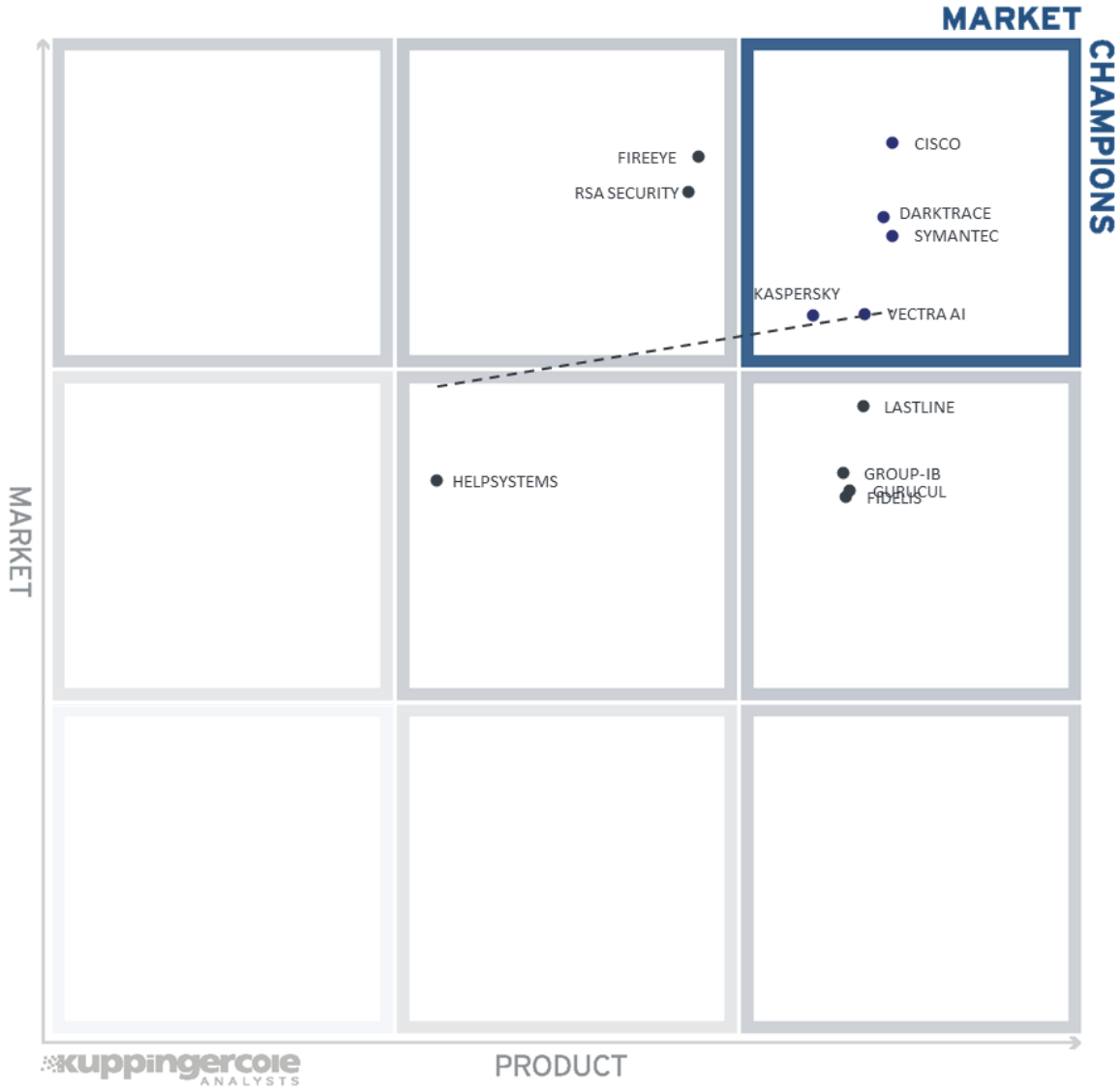


Figure 7: The Market/Product Matrix

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.

Cisco, Darktrace, Kaspersky, Symantec, and Vectra are the Market Champions, with a dominating lead in both product vision and market share. Just to the left in the top center we see FireEye and RSA, also with significant market position and respectable product completeness.

A large concentration of products is in the right center box: Fidelis, Group-IB, Gurucul, Lastline. These vendors have excellent NDR solutions but haven't captured the market share that their products merit yet.

HelpSystems is in the center box above the line, with an average amount of market and product capabilities.

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. This distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

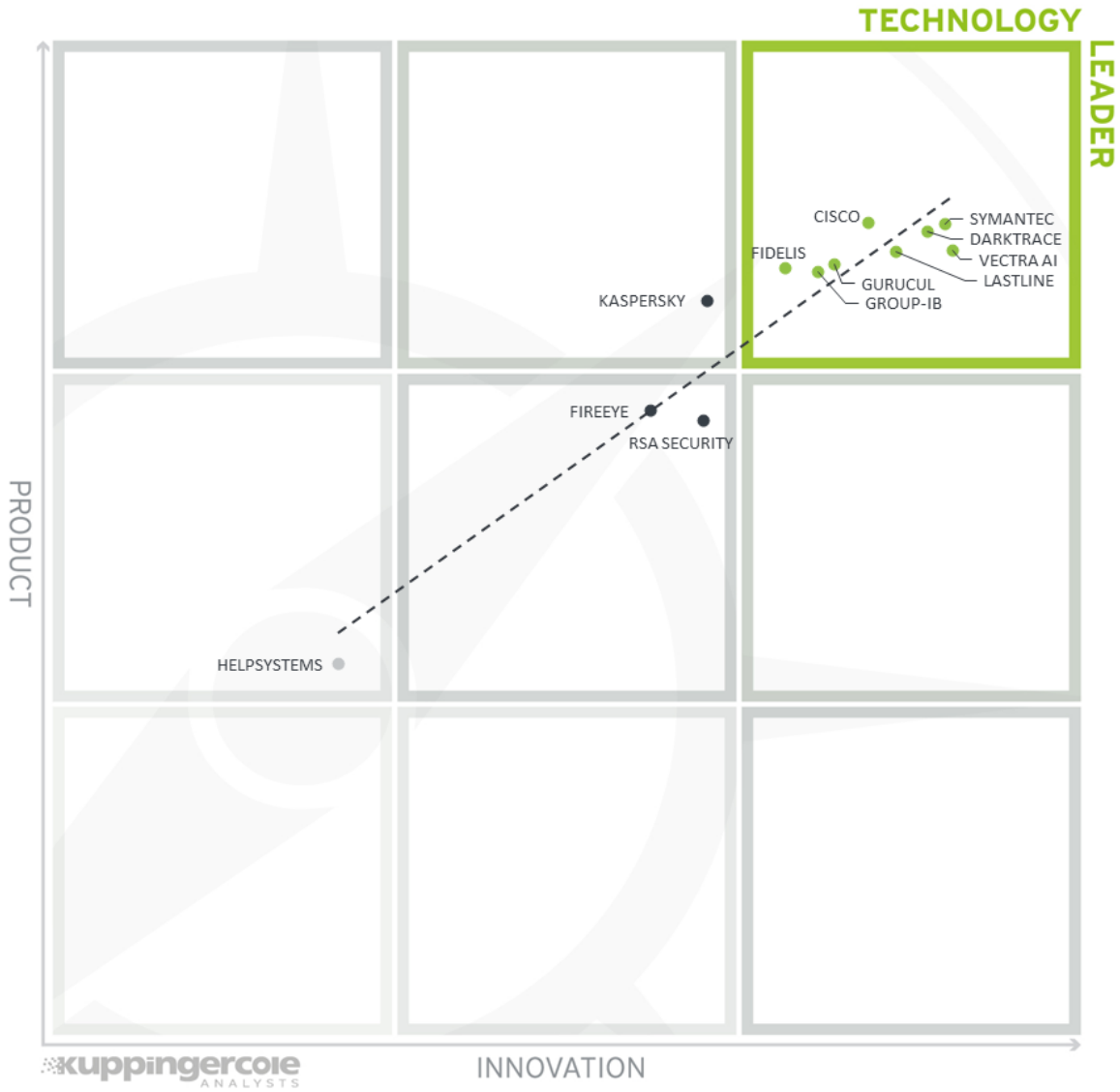


Figure 8: The Product/Innovation Matrix

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

The Technology Leaders box has a large number of entrants: Cisco, Darktrace, Fidelis, Group-IB, Gurucul, Lastline, Symantec, and Vectra AI. Kaspersky is found in the middle top box, with a strong product but slightly less innovation. FireEye and RSA are in the center but near the Technology Leaders. HelpSystems is on the line in the left center square. The relative positioning close to the line shows that there is a correlation between innovativeness and product vision; therefore, the strongest products in this space are the most innovative.

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.

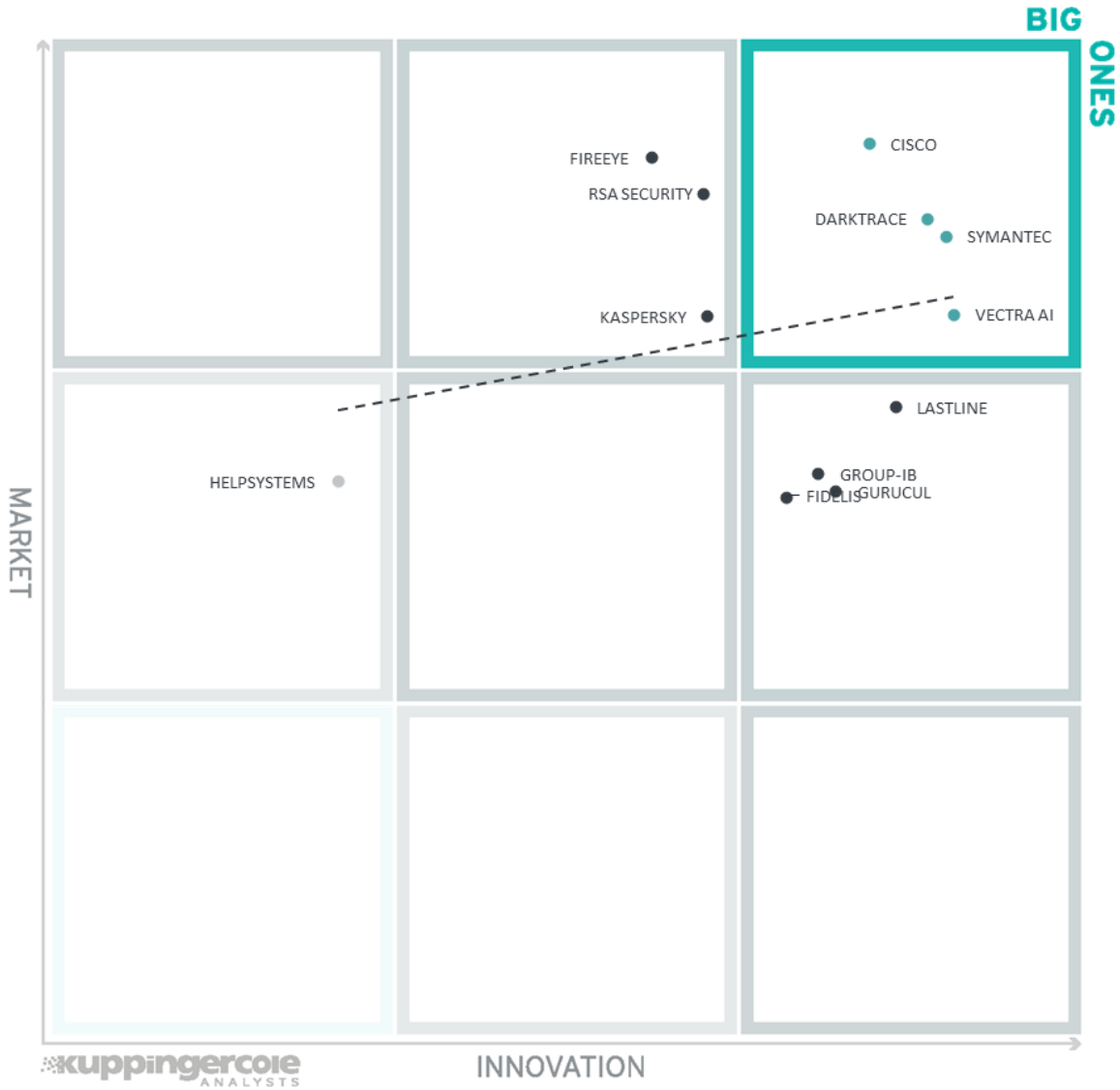


Figure 9: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating; while vendors below the line show an ability to

innovate, and thus the biggest potential for improving their market position.

Cisco, Darktrace, Symantec, and Vectra are the Big Ones in NDR. Their positioning shows that innovation is needed for success in the NDR market, and that their customers believe that their leading-edge security technologies deliver as expected.

FireEye, Kaspersky, and RSA are in the top center, exhibiting sufficient innovation leadership and benefiting from good market share.

In the right center, we find Fidelis, Group-IB, Gurucul, and Lastline. These products are highly innovative, but since they are below the line, there is much growth potential for their products in this market. HelpSystems is on the line in the left 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 and Response. 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.

4.1 Ratings at a Glance

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	Integration	Interoperability	Usability
Cisco Stealthwatch	●	●	●	●	●
Darktrace Enterprise Immune System	●	●	●	●	●
Fidelis Network	●	●	●	●	●
FireEye Network Security	●	●	●	●	●
Group-IB Threat Detection System (TDS)	●	●	●	●	●
Gurucul Network Traffic Analysis (NTA)	●	●	●	●	●
HelpSystems Core Network Insight	●	●	●	●	●
Kaspersky Network Threat Detection	●	●	●	●	●
Lastline Defender	●	●	●	●	●
RSA NetWitness Platform	●	●	●	●	●
Symantec Network Threat Detection	●	●	●	●	●
Vectra Cognito	●	●	●	●	●
Legend		● critical	● weak	● neutral	● positive ● strongly positive

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
Cisco	●	●	●	●
Darktrace	●	●	●	●
Fidelis Cybersecurity	●	●	●	●
FireEye	●	●	●	●
Group-IB	●	●	●	●
Gurucul	●	●	●	●
HelpSystems	●	●	●	●
Kaspersky	●	●	●	●
Lastline	●	●	●	●
RSA Security	●	●	●	●
Symantec	●	●	●	●
Vectra	●	●	●	●
Legend	● critical	● weak	● neutral	● positive	● strongly positive

Table 2 requires some additional explanation regarding the "critical" rating.

In Innovativeness, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in that analysis, like support for multi-tenancy, shopping cart approaches for requesting access, and others.

These ratings are applied for Market Position in the case of vendors which have a very limited visibility outside of regional markets like France or Germany or even within these markets. Usually the number of existing customers is also limited in these cases.

In Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base but is also based on some other criteria. This doesn't imply that the vendor is in a critical financial situation; however, the potential for massive investments for quick growth appears to be limited. On the other hand, it's also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no or a very limited ecosystem with respect to numbers and regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that growth and successful market entry of companies into a market segment relies on strong partnerships.

5 Product/Service Evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many 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 Network Detection and Response, we look at the following six areas:
Deployment models The major deployment models are in-line, usually residing on a gateway device such as a firewall; or in passive mode off a span or tap port from a network device, or off a network packet broker. In this category, more flexibility yields a higher score.

- **Cloud support**
  Having AMIs or VHDs for AWS, Azure, Google Cloud, Oracle, and other IaaS platforms is essential for many organizations today. The more platforms supported, the better the score.

- **Packet decryption**
  This category is primarily a "yes/no". A few organizations require packet decryption for NDR, but most do not. A positive value here serves as an indicator for those who may be looking for this feature.

- **Sandbox**
  Malware detonation sandboxes are not part of every NDR solution. Generally, only those systems that can do packet decryption have sandboxes. NDR sandboxes can be useful for finding malware that other solutions may have missed, so it is measured here. Higher scores are given for products that support both vendor-cloud-hosted sandboxes and on-premise sandboxes. The rationale is that, some of the most at-risk environments are those which may not have constant internet connectivity, such as ICS and SCADA networks.

- **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, ability to write static rules in YARA 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 with suspected RCA enriched by threat intelligence are preferred.

- **Detection**
  NDR is like IDS but requires proper implementation of ML algorithms and models to be effective. This rating considers how products utilize ML for higher quality detections and reduction of false positives, based architectural descriptions given by vendors. Better scores are given for those that use a well-thought-out set of unsupervised and supervised ML and DL algorithms and models. Model training methods and update frequency are also considered. Success in detection also requires that solutions have a variety of IoC sources, have the ability to understand many network metadata attributes and network protocols, and employ multiple methods for analyzing encrypted traffic. Higher scores here also reflect diversity of threat intel sources, better coverage of attributes and protocols, and encrypted traffic forensics.

- **Automated 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, web proxies, API gateways, SIEM and SOAR systems. Some NDR solutions have packaged connectors for common security tools to make this easier. A minimum set of automated response includes session termination, node isolation, and forensic evidence collection. This category considers the methods used for executing automated responses as well as the variety of response actions available.

- **Max throughput**
  This is a simple metric based on max throughput reported by vendors. 10 Gbps is the median.

The spider graphs provide comparative information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas, while being strong in other areas. These might be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on Network Detection and Response.

5.1 Cisco Stealthwatch

Cisco's entry in NDR is Stealthwatch, the former Lancope, which they acquired in 2015. The sensors are delivered as VMWare virtual appliances and can be deployed off span ports. Cisco's solution also works inside AWS, Azure, and Oracle IaaS. Manager console can be run either on-prem or Cisco also hosts customer consoles as SaaS. Annual licensing is based on flow rates, with additional charges for appliances; SaaS instances can be charged for actual traffic levels. Cisco offers a Managed Detection and Response service.

Stealthwatch analyzes hundreds of network connection metadata attributes and performs protocol-level analysis using NetFlow telemetry. Suspect files can be analyzed by Cisco Threat Grid sandbox, which is an add-on service. Stealthwatch utilizes Cisco Encrypted Traffic Analytics (ETA), which reportedly can detect malware in encrypted payloads. Stealthwatch forwards ETA data to a cloud-based Cognitive Threat Analytics engine for analysis. Cisco uses an impressive array of unsupervised and supervised ML algorithms for continuous baselining, anomaly detection and classification, and threat analysis, which can be supplemented with UBA from add-on Information Centric Analytics product. Models are selectable and tunable by customers and are updated every 1-2 weeks.

Cisco can send alerts via email, REST API, syslog, and SNMP. All console functions are addressable over APIs. Many pre-defined reports are available, and customers can build their own. Playbooks are not defined but Cisco can consult with customers to develop their own. Stealthwatch leverages Cisco Identity Services Engine to automatically isolate nodes, block traffic by port or protocol, and can command IOS routers to block external IPs. Cisco provides connectors to interoperate with a large number of 3rd-party tools, allowing automated responses that are initiated by Stealthwatch to be executed by downstream security controls. Cisco is launching SecureX in summer 2020 which will serve as the central information collection point and orchestrator for automated responses. Stealthwatch today generates risk and confidence levels for analysts; threat hunters can use their Stealthwatch Flow searches and define Custom Security Event logic in the console.

Cisco has its own threat intelligence and IoC sources and their solution is enriched with multiple external sources as well. Cisco is a charter member of the Cyber Threat Alliance. Cisco supports CyBox, STIX, and TAXII. APIs permit interoperation with SIEM and SOAR apps such as QRadar and Splunk.

Their platform has been evaluated against MITRE ATT&CK. There are limited options for admin MFA and SAML federation can be configured for admins. It can use 3rd-party PAMs to lockdown admin or service accounts. Granular role-based and delegated administration are supported.

Cisco's Stealthwatch is a mature NDR with excellent interoperability with other security tools as well as good integration with other Cisco products (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 Stealthwatch, and other organizations with both high security and high bandwidth needs will want to evaluate it when looking for NDR products.

Security	●●●●●
Functionality	●●●●●
Integration	●●●●○
Interoperability	●●●●●
Usability	●●●●●

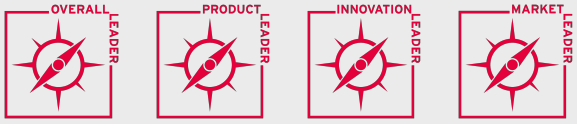
Strengths

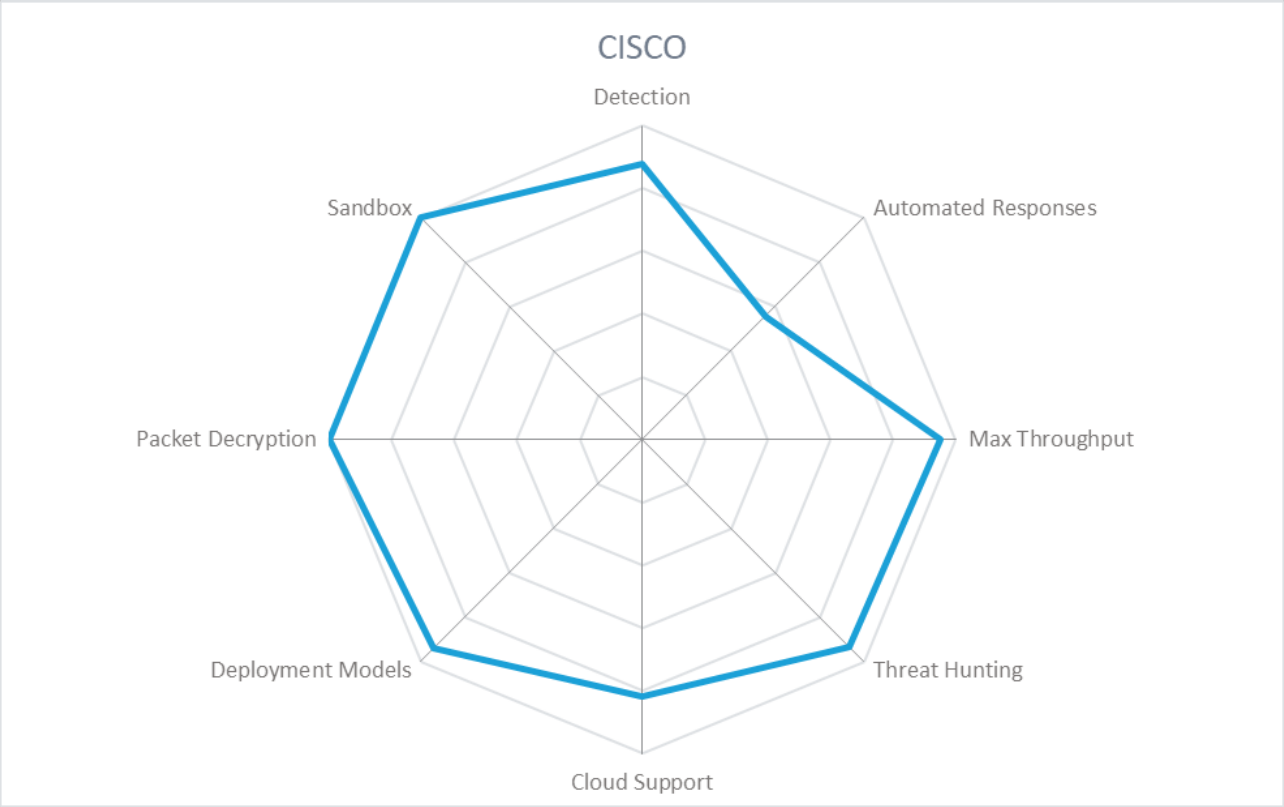
- Up to 80 Gbps throughput on largest unit
- Highly scalable
- Good integration with Cisco products
- Multi-year data storage plans available
- 30-45 day activity recording for enhanced investigations

Challenges

- Professional services needed for playbook and IR development
- Better admin MFA options needed
- Complex licensing model, requires multiple components for full functionality

Leader in




CISCO
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.2 Darktrace Enterprise Immune System

Darktrace was founded in 2013 in Cambridge, UK. They are a late stage venture backed company with thousands of deployments and offices around the world. 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 can decrypt packets if configured with keys, but this approach is not recommended. Management console can be run in a Darktrace cloud instance or on-premise probe. Annual licensing is based on the size of the customer, the distribution and scope of their deployment, which includes such factors as peak sustained throughput, maximum unique internal devices, and maximum connections per minute. Darktrace offers several service options around their product.

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. This is essentially a continuous baselining process. Packet decryption is possible but not used often. Darktrace uses JA3/S methods for fingerprinting and analyzing encrypted comms. Darktrace' implementation of ML is sophisticated, using competing unsupervised ML algorithms orchestrated by master models to produce the best results. The supervised ML models in their Cyber AI Analyst service are trained on input from human analyst responses, rather than just positive diagnostics. Model update rates vary between daily and nearly continuously as needed. Darktrace has a model editor enabling customers to design their own. Baselining is continuous and initial baselining takes on average one week.

Alerting is possible via email, ActiveMQ, Darktrace Mobile App, HTTP, JIRA, and Syslog. Canned and customized reports are available. Antigena can respond automatically to known and unknown threats so there is no need for conventional playbooks. The solution generates risk and confidence levels for analysts; threat hunters can use free text query functions. Through API integration with firewalls and network enforcement tools, Darktrace can automatically terminate connections, isolate nodes and/or block traffic by port or protocol. Fine-grained responses for cloud services include re-writing permissions, terminating sessions, temporarily disabling user accounts, restricting file sharing, and more.

Darktrace doesn't require IoCs, instead it focuses on learning and discerning behavior in customer environments. However, customers can configure external feeds, and Darktrace supports STIX and TAXII. Darktrace Inoculation is an add-on service that allow customers to benefit from shared data about cyber-threats detected across their customer base. APIs, CEF, LEEF, and syslog are used for interoperating with other security applications such as ArcSight, Demisto, LogRhythm, QRadar, ServiceNow, and Splunk.

Darktrace detections can be mapped to the MITRE ATT&CK framework if desired. Admin

authentication is over LDAP, so 2FA is possible. and it can use 3rd-party PAMs over LDAP to lockdown admin accounts. Role-based and delegated administration are supported.

Darktrace promotes their solutions as AI, and their ML implementation is superior in the marketplace. This leads to benefits to customers in terms of decreased labor and false positives, and increased reliability for automated responses. Their coverage for cloud-based solutions, including many SaaS apps as well as the full range of IaaS environments, makes their solution a top consideration for NDR RFPs.

Security	●●●●○
Functionality	●●●●●
Integration	●●●●○
Interoperability	●●●●●
Usability	●●●●●

DARKTRACE

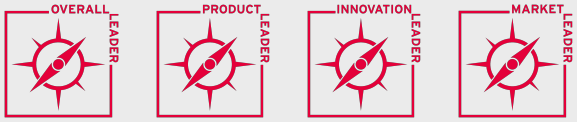
Strengths

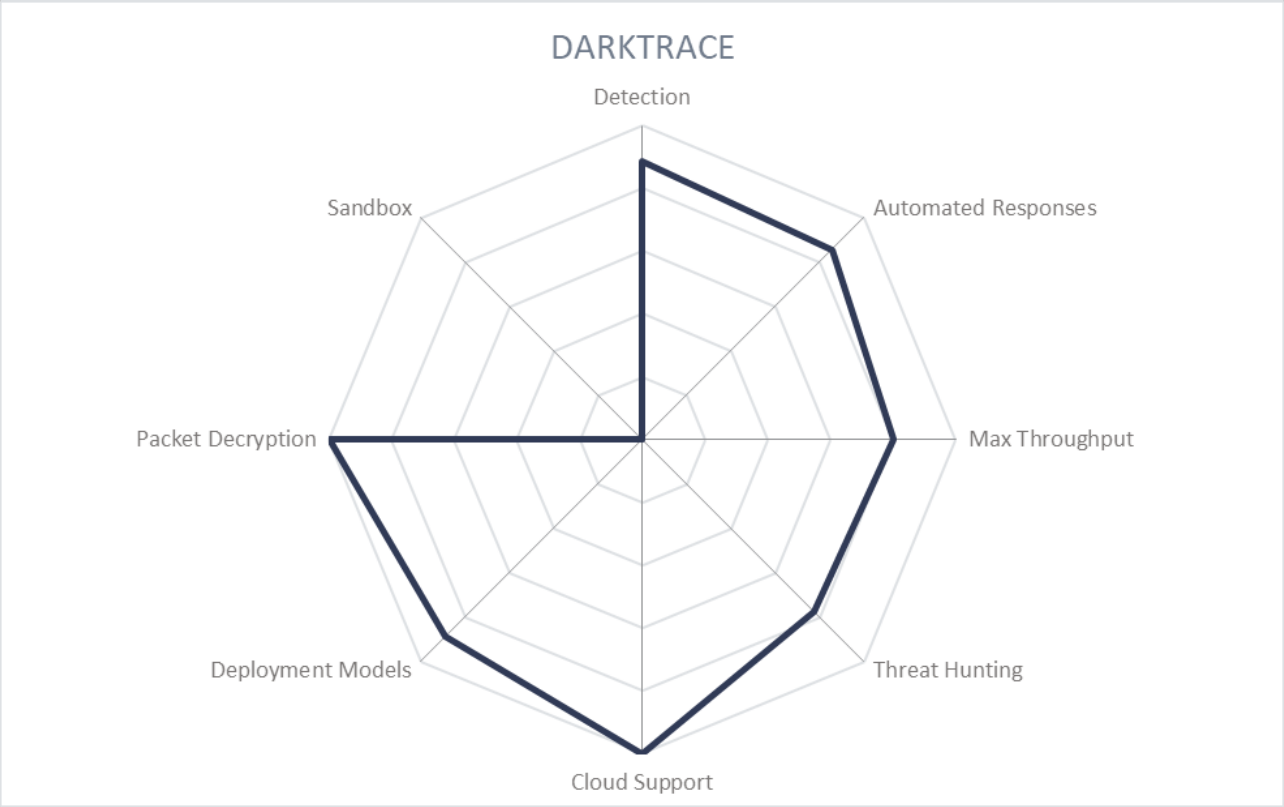
- Most coverage for IaaS and SaaS
- Average 6-9 month data retention
- 40 Gbps per device max throughput, and expandable with Endace
- Excellent ML implementation, and customers can design their own detection models
- Mobile manager app
- Wide range of automated responses including in-cloud actions

Challenges

- Longer term storage of PCAPs requires Endace (3rd -party)
- Threat intelligence integration is available at no extra charge, but is not enabled by default
- More MFA options and SAML federation support needed

Leader in




DARKTRACE
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.3 Fidelis Network

Fidelis was founded in 2003 and is headquartered in Bethesda, MD, outside Washington, DC. They are a privately held company. The sensors are delivered as appliances or virtual appliances and can be deployed in-line, off span ports or in the cloud. They have images for AWS and Azure. Fidelis has the optional abilities to decrypt packets for deeper analysis in in-line mode. Throughput ranges from 10-20 Gbps depending on appliance type. The management console can be run on-prem, in IaaS, and Fidelis has a SaaS option. Annual licensing is per appliance and additional charges for storage and aggregate bandwidth used. Fidelis offers a managed service in this area.

Fidelis analyzes the standard set of network metadata and protocols as described by MITRE ATT&CK, but also can perform application layer content level inspection of data objects if decrypted. Fidelis' Deep Session Inspection® then also performs as a network layer Data Loss Prevention (DLP) system, for example looking at unstructured data files for unauthorized flows of PII or confidential information. Fidelis has a malware detonation sandbox. Fidelis uses a hierarchy of unsupervised ML algorithms for outlier detection. Supervised ML models run in parallel to classify threats by type. Model update rates vary between daily and bi-weekly as needed. Customers can fine-tine or augment models using Fidelis Policy Delivery Infrastructure. Baselining is continuous and initial baselining takes on average 1-2 weeks.

Alerting shows up on the dashboard and can be piped into ticketing systems. Canned and customized reports are available. Fidelis Network supports playbook development, from which automated responses are generated, such as node isolation, port blocking, and session termination. More elaborate app-specific actions are possible within the Web and Email sensors. Fidelis does not have recording/playback or natural language query search functions.

Fidelis supports STIX and TAXII and pulls from a long list of high-quality threat intel sources. Customers can configure more external feeds. Fidelis can send to SIEMs via syslog, and connectors for Demisto and Splunk are available.

Fidelis is NIAP Common Criteria Certified. Authentication is limited to LDAP and RADIUS. SAML federation is supported as well. Role-based and delegated administration are supported.

Fidelis Network and associated add-ons provide a depth of coverage that surpasses the competition in some ways, particularly in terms of application layer content analysis. Organizations that have the highest security needs and are not subject to stringent privacy regulations should take a look at Fidelis for NDR. The product would benefit from built-in MFA methods and a few more threat hunter facilities such as a natural language query interface.

Security	●●●●●
Functionality	●●●●○
Integration	●●●●○
Interoperability	●●●●○
Usability	●●●●●

Fidelis® Cybersecurity

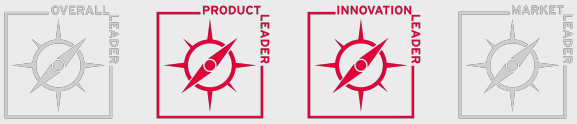
Strengths

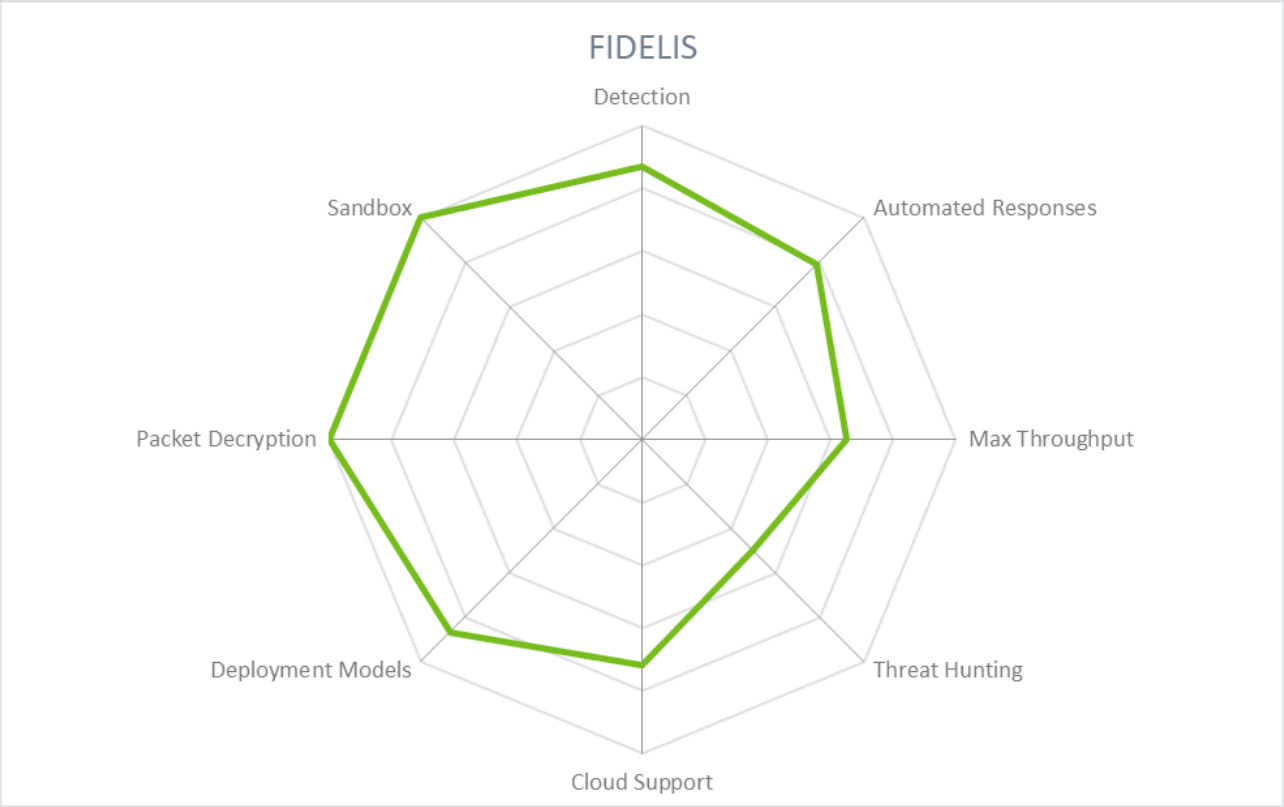
- Email and web decryption options
- Malware detonation sandbox
- Deep Session Inspection® does application layer content analysis on the network at line speed (10-20 Gbps)
- NIAP CC certification

Challenges

- 30-day data storage but can be extended
- More strong MFA options needed
- Support for NL queries would increase usability

Leader in




FIDELIS
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.4 FireEye Network Security

FireEye was founded in 2004. The company is headquartered in Milpitas, CA and have offices around the globe. Sensors are delivered as physical or virtual appliances running on ESX, KVM, or as AMIs, and can be deployed in-line, 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, and hardware sensors that also perform sandboxing run at 10 Gbps. Management console can run on-prem or in AWS, or as SaaS from FireEye. Their licensing model is based on a combination of per-user and per-Mbps/year charges. FireEye offers MDR services.

FireEye performs deep analysis on DNS, FTP, HTTP(S), and SMB protocols. FireEye has a malware detonation sandbox that can be deployed on-prem and/or use their cloud version. FireEye uses both unsupervised and supervised ML but did not provide details. ML models are updated semi-annually. Customers can write their own YARA rules but ML model configuration and tuning is done by the vendor. Baselining takes about one week.

Email, SNMP, syslog, and web are the alerting methods employed. Basic reports are provided, and customers can write their own. FireEye Helix SecOps is where event information is enriched with threat intelligence and playbooks are built. TCP reset/session termination, port blocking, node isolation, and evidence collection are examples of automated responses that can be executed either from Helix, directly from the FireEye network products, or via APIs for other vendors' products. Recording/playback of both sessions and full-packet streams are available. Enterprise-wide searches are available but natural language queries are not supported.

Customers get the benefit of FireEye/Mandiant's renowned threat intel, and FireEye Packet Capture (PX) (but not Network Security directly) supports STIX and TAXII. FireEye interoperates with a long list of other security vendor tools including ArcSight, CyberArk, Demisto, McAfee, Palo Alto, Panorama, QRadar, Splunk, etc.

FireEye Network Security has been evaluated against MITRE ATT&CK and contributes to the Cyber Threat Alliance. The console supports SAML federation; and LDAP, RADIUS, and TACACS for authentication. Role-based and delegated administration are supported.

FireEye Network Security meets expectations with regard to essential features. The solution needs some updates in terms of broader IaaS support, admin authentication, and ML detection model usability.

Security	●●●●○
Functionality	●●●●○
Integration	●●●●○
Interoperability	●●●●○
Usability	●●●●○

FIREEYE™

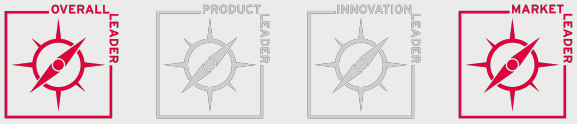
Strengths

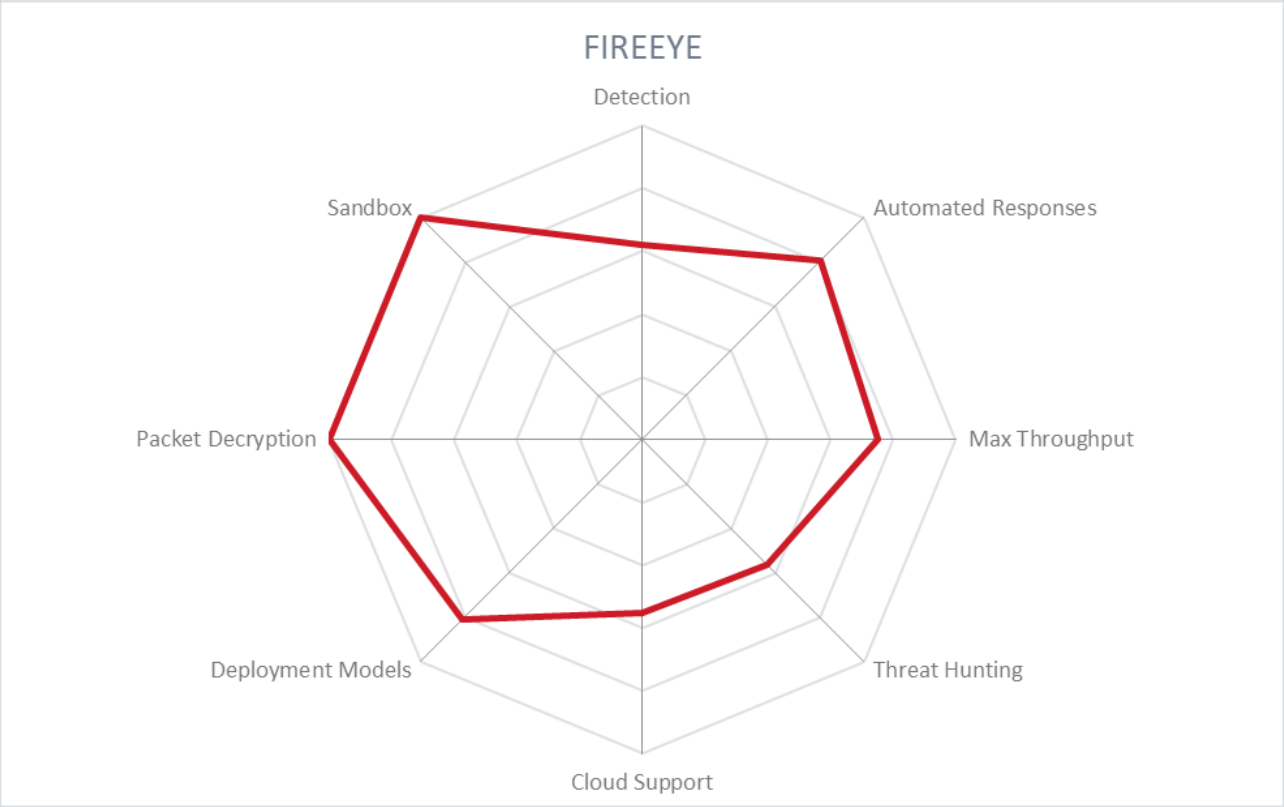
- Packet decryption and sandboxing
- Up to 20 Gbps for packet capture; 10 Gbps for sandboxing
- Long default data storage periods
- Excellent threat intel (FireEye/Mandiant)
- Highly interoperable with other security solutions

Challenges

- Support for more IaaS environments needed
- ML models updated infrequently and cannot be configured by customers
- More strong MFA options needed

Leader in




FIREEYE
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.5 Group-IB Threat Detection System (TDS)

Privately held Group IB was founded in 2003 in Moscow but now has global HQ in Singapore. NDR functionality 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 ISO-image with their own *nix based OS, and delivered as an appliance or virtual appliance. It can be deployed off network packet brokers or span/tap ports, or installed on file, proxy, email, and other servers. Packet decryption is possible using their separate TDS Decryptor module. Throughput ranges from 10-20 Gbps for appliances. It can also be installed in IaaS, but customization is required. Management console can be run on-premises on nixOS or hosted in their SaaS. Their licensing model depends on multiple factors. They offer managed service options including full SOC-as-a-service.

TDS analyzes all the common protocols and supports ICS and SCADA traffic. Packet decryption is available in a separate module, and the solution has a sandbox for malware detonation, which can be deployed on-site or use their cloud version. Their sandbox can detect multi-flow attacks, which are techniques designed specifically to evade sandboxes. Customers can integrate other security tools with the TDS sandbox using APIs. TDS uses signatures and anomaly detection algorithms (such as DGA analysis), unsupervised ML models to find lateral movement and covert C2 comms, and supervised ML models for malware analysis and ICS topology changes. Group-IB claims baselining for topology may take as little as an hour. Customers can activate/deactivate ML models as needed, but tuning is restricted to Group-IB. Models are updated frequently.

Group-IB's CERT team can alert customers by email/phone/SMS, syslog, and tickets. Pre-defined reports are available, and customers can build their own. If deployed with Group-IB's Huntpoint module (EDR), TDS can terminate processes and sessions, and isolate nodes. Other playbook actions can be carried out via API integration with 3rd party tools. Integration with NGFWs is on their roadmap, which will allow automated responses such as port blocking there. The solution generates risk and confidence levels for analysts. With EDR and NDR integrated, analysts can use Apache Lucerne syntax for comprehensive threat hunting. A range of reports is available OOTB and customization is possible. Customers can trigger activity recording and playback.

Group-IB is a provider of high-quality threat intel, which is also used by their products as well as shared with Cyber Threat Alliance, global CERTs, Europol, Interpol, etc. CyBox, STIX, and TAXII are supported. Interoperability with SIEM, SOAR, and other security tools is achieved by broad support for syslog, CEF, JSON, and APIs. TDS can interoperate with any security tool that understand these relevant standards.

Their platform is aligned with MITRE ATT&CK. In lieu of token-based 2FA, Group-IB applies their Secure Portal anti-fraud technology for admin authentication, considering device health and

fingerprint, User Behavioral Analysis (UBA), and behavioral biometrics for each interaction with the admin console. TDS doesn't require privileged accounts, therefore TDS does not support PAM integration.

Group-IB's TDS is one of the most feature-rich NDR solutions in the market. It exceeds expectations for NDR functionality. Though their main market presence has been in Russia/CIS, Eastern Europe, and the Middle East, they are expanding globally. Organizations that need a full range of NDR capabilities, especially for industrial applications, should consider Group-IB TDS.

Security	●●●●●
Functionality	●●●●●
Integration	●●●●●
Interoperability	●●●●○
Usability	●●●●●

GROUP IB

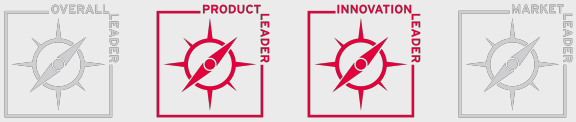
Strengths

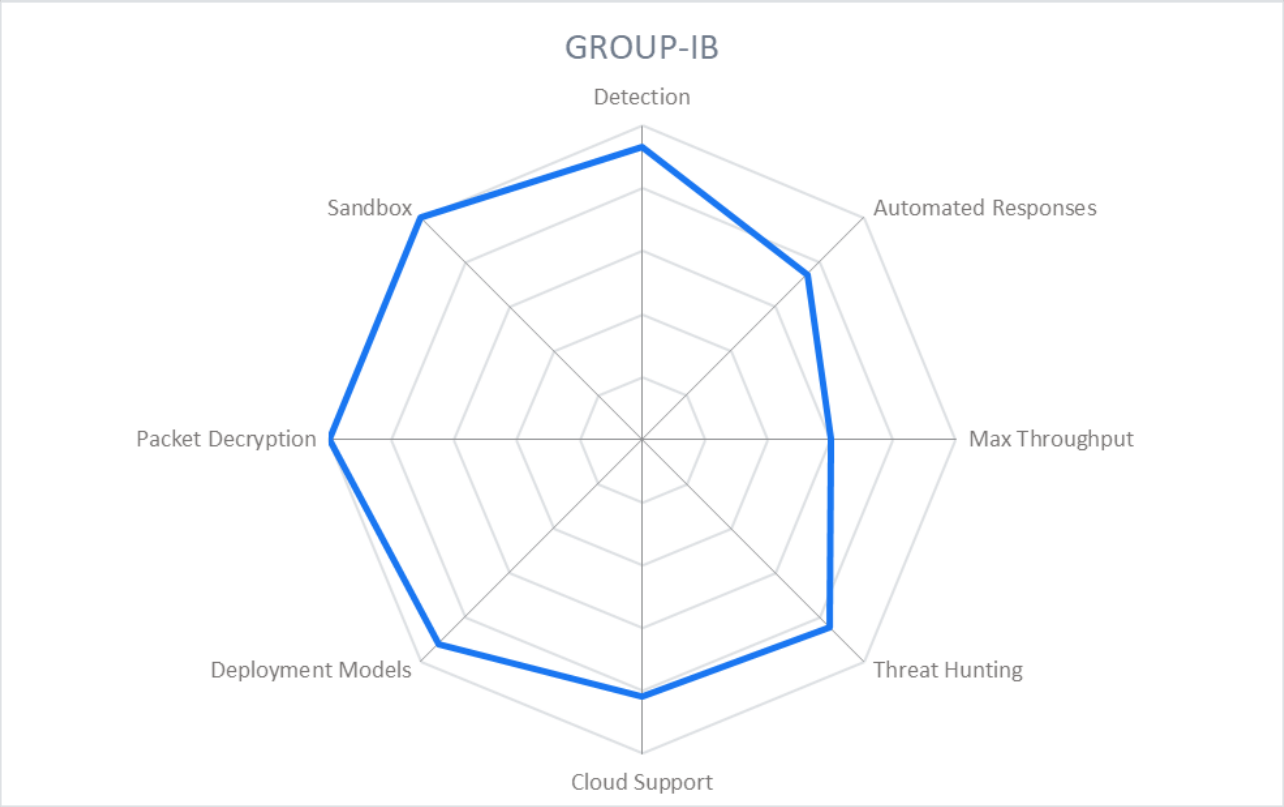
- Most flexible deployment options, including full decryption and sandbox
- 10-20 Gbps throughput
- Long default data retention period
- Industrial Control Systems support
- Wide array of detection techniques
- Continuous authentication based on device intel and UBA for admins

Challenges

- Complex licensing models
- No North America or LatAm presence yet, with their strongest presence in Russia/CIS and Eastern Europe

Leader in




GROUP-IB
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.6 Gurucul Network Traffic Analysis (NTA)

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. The solution can be installed on-premises 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, and AMI and ISO images are available. Gurucul supports private cloud and hybrid deployment models also. It acts as a log aggregation service, so it is not deployed in-line or off span ports, and throughput isn't measured. If traffic capture is enabled and it is configured with server keys, it can decrypt traffic. 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.

NTA collects logs from other devices and relies on other agents to capture packets and forward them. Packet decryption is possible, and the solution has sandbox options, including on-site deployment or using their cloud instance. NTA applies Gurucul's excellent unsupervised and supervised ML models to detect a wide range of anomalous and malicious behaviors. They have dedicated detection models for finance, retail, healthcare, and IoT. Recommended baseline period is one week. Customers can activate/deactivate ML models as needed, and Gurucul UI Studio allows customers to build their own as needed. Models are updated quarterly.

Customers can be alerted by email, syslog, and tickets. Pre-defined reports are available, and customers can build their own. Gurucul provides playbooks for recommended responses. Given that NTA is deployed out-of-band, all responses, such as host isolation, session termination, port blocking, etc. require API integration with 3rd-party security tools. Gurucul has connectors for many of the common security tools that enterprises have. The solution generates risk and confidence levels for analysts. Threat hunters can use the GUI or CLI. Basic reports are available OOTB and customization is possible. Recording/playback functions are not available but NTA has timeline-based anomaly reports.

Gurucul curates its own threat intel, which can be supplemented by external sources via support for CyBox, STIX, and TAXII. Interoperability with DLP, EDR, SIEM, SOAR, ticketing, and other security tools is made possible by APIs.

Their platform has been mapped to MITRE ATT&CK. Gurucul accepts SAML for authentication and authorization, enabling it to interoperate with major MFA providers. Role-based and delegated access control are supported.

Gurucul is well-known for their UBA product and leverages sophisticated ML models to detect malicious behavior at the network level. Support for industry specific use cases, such as finance, retail, healthcare, and IoT is especially useful for those customers. In-line, off-span port, or off-network packet broker deployment models would reduce dependencies on other devices and

agents, thereby increasing flexibility.

Security	●●●●●
Functionality	●●●●○
Integration	●●●●○
Interoperability	●●●●●
Usability	●●●●●

GURUCUL

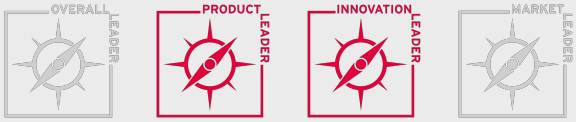
Strengths

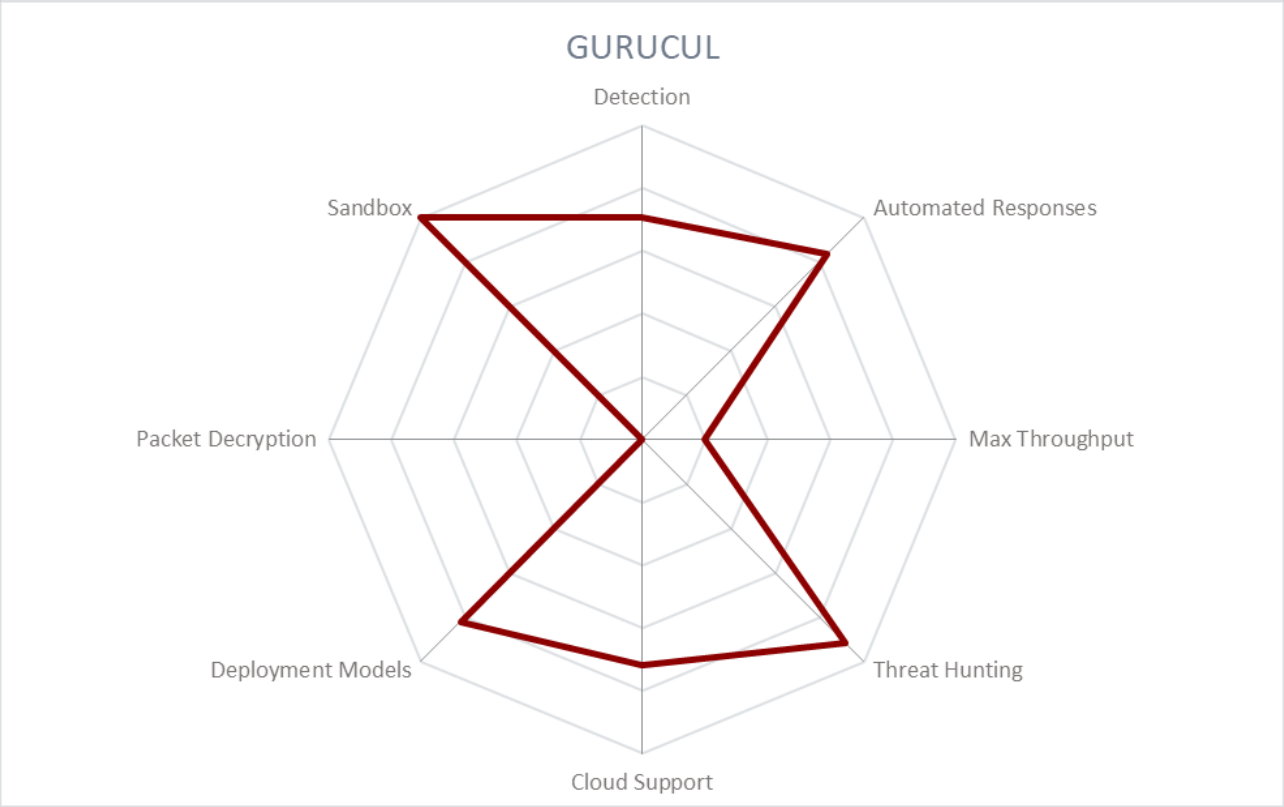
- Excellent ML implementation, with use case specific models
- Customers can create their own detection models
- Support for admin MFA and federation

Challenges

- Short default data storage period in SaaS, but can be extended for a fee
- Recording/playback not supported
- Passive-mode log aggregation deployment model

Leader in




GURUCUL
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.7 HelpSystems Core Network Insight

Minnesota-based HelpSystems acquired CoreSecurity and their Core Network Insight product in 2019. HelpSystems has other security, IAM, and general IT solutions in their portfolio. The solution is delivered as an appliance or virtual appliance. It is deployed off span ports at egress points. It doesn't decrypt traffic. It also works in AWS and Azure. Throughput can scale up to 10 Gbps for appliances. Management console comes on a Debian appliance, which must be maintained by the customer. Data storage is on customer premises. Licensing is per node or appliance. Managed services are not offered.

Network Insight scans all basic network protocols and can turn on full packet capture when malicious activity is suspected. Network Insight doesn't decrypt, but HelpSystems hosts a malware detonation sandbox. It uses unsupervised ML for DGA analysis and supervised ML (including some atypical algorithms and methods) for malware analysis and metadata analysis. They have dedicated detection models for IoT. The solution does not baseline, but rather assumes malicious activity may be present already. Customers cannot tweak, write, or deactivate models. However, models are updated daily by HelpSystems.

Customers can be alerted by email, syslog, and tickets. Basic reports are built-in, but customers cannot create their own. Playbooks are not provided or supported. Response actions must be created and executed in external SOAR systems. Network insight generates risk and confidence levels for analysts. No natural language query interface is in place for threat hunting. Recording/playback can be configured.

HelpSystems generates its own threat intel, which is augmented by external sources such as Cyber Threat Alliance and Virus Total. CyBox, STIX, and TAXII are not supported. Network Insight supports CEF, syslog, and various NAC APIs for security tool interoperability.

Their platform has not been evaluated against MITRE ATT&CK. LDAP and RADIUS can be used for admin authentication, and thus MFA could be configured, but there is no built-in MFA or SAML support. Role-based access control is supported.

HelpSystems Network Insight provides some essential NDR functions but is missing some key features as outlined above. Explicit support for IoT, ICS and SCADA environments will be of interest to some organizations with those types of environments.

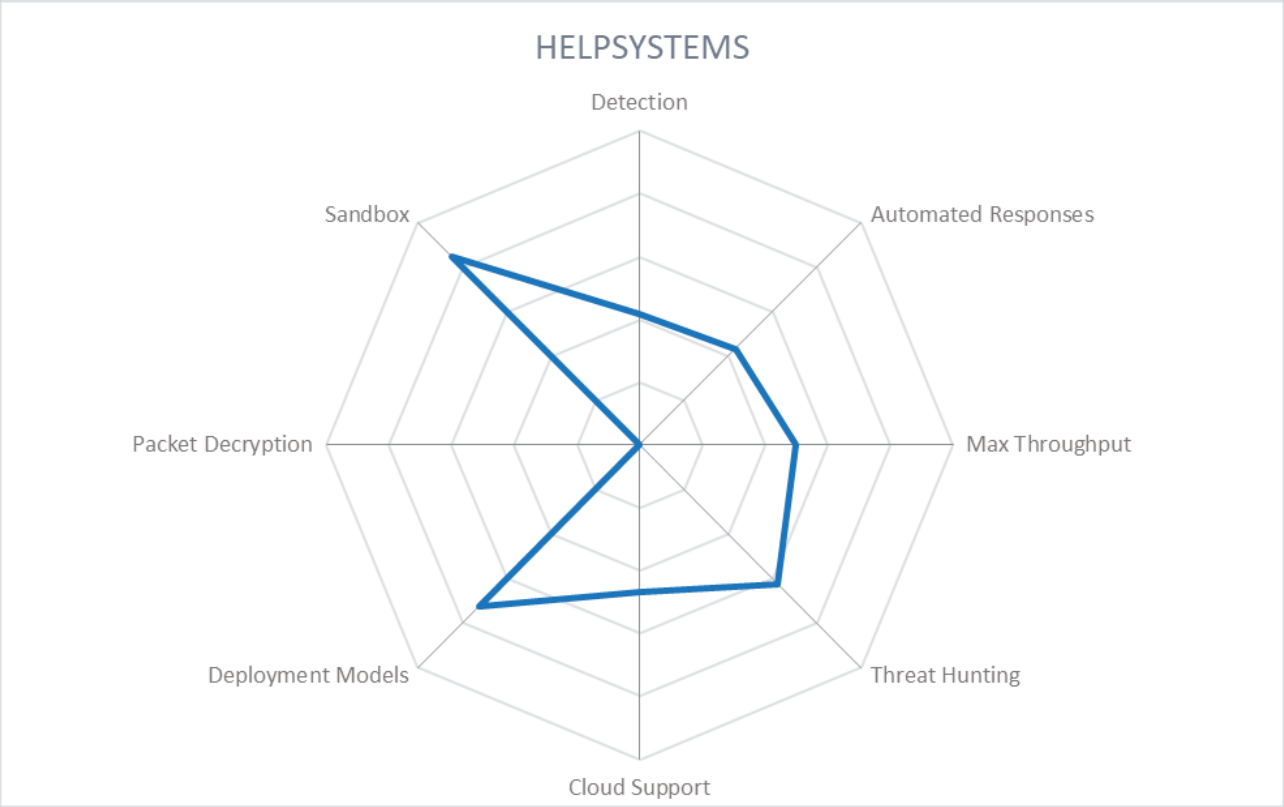
Security	● ● ● ○ ○
Functionality	● ● ● ○ ○
Integration	● ● ● ● ○
Interoperability	● ● ● ○ ○
Usability	● ● ○ ○ ○

Strengths

- IoT, ICS, and SCADA support
- Innovative use of unconventional ML models

Challenges

- No SaaS console or managed services
- North-south focus may miss lateral movement and reconnaissance
- Detection and alerting only; responses must be coordinated in external SOARs
- Needs native MFA for admins


HELPSYSTEMS
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.8 Kaspersky Network Threat Detection

Kaspersky has been providing cybersecurity solutions for more than two decades. Though headquartered in Russia, Kaspersky has a global presence with transparency centers in Switzerland and Spain. Their solution consists of components listed above. It is delivered as a Linux package or virtual appliance. KATA is deployed off span ports or in parallel. KATA includes Kaspersky Endpoint Detection & Response. KSMG and KWTS are deployed in-line. KWTS can decrypt traffic. KSMG, KWTS, and core node can work in AWS and Azure. KWTS can handle 300 Mbps, and KATA can process 4 Gbps; processing nodes can be clustered to achieve higher throughput. Management console comes on a CentOS package, which must be maintained by the customer. Data storage is on customer premises; no SaaS options currently available. Licensing is per processing node or by bandwidth for KATA; KWTS is licensed per protected endpoint or traffic; KSMG is licensed by number of protected mailboxes. Kaspersky offers full managed NDR services.

Kaspersky examines the basic network protocols. It can do full packet capture and decryption. The solution contains a sandbox. Kaspersky's NDR suite looks for all known attacker TTPs. Kaspersky extensively uses ML and DL for malware detection in their EPP, EDR, and sandbox products, and different ML detection models in KATA, KSMG, and KWTS that are focused on network connection metadata anlaysis. It does not use JA3/S fingerprinting. The solution does not baseline customer networks. Customers can choose to omit certain IoCs by means of adding whitelists, but they cannot directly configure detection models. Kaspersky creates model updates as needed, generally between weekly and monthly.

Customers can be alerted by email, syslog, and through the dashboard. Basic reports are built-in, and customers can create their own. Playbooks and limited response actions such as process termination and node isolation are provided via the included KEDR product. KATA generates RCA reports with confidence levels for analysts. Threat hunters can use the console and write YARA rules. Recording but not playback can be configured.

Kaspersky curates its own high-quality threat intel, and has sharing arrangements with Interpol, Europol, and law enforcement agencies around the world. They host a SaaS research sandbox for outside security experts. Kaspersky consumes 3rd-party threat intel, but customers cannot configure additional feeds. CyBox, STIX, and TAXII are not supported. Kaspersky supports CEF, syslog, and various APIs for security tool interoperability. This NDR solution integrates with Autotask, ConnectWise Automate and Manage, N-Central, SolarWinds RMM, and TigerPaw.

Their solution has been evaluated against MITRE ATT&CK, and they often contribute to it. Moreover, analytics and reports are mapped to the elements of MITRE ATT&CK. Role-based access control is supported. But there are no strong MFA options yet, though it is on the roadmap for end of 2Q2020.

Kaspersky is well-known for cybersecurity solutions, particularly their endpoint products and

threat research. Their entry in the NDR space requires multiple components and can be complex to deploy.

Security	●●●○○
Functionality	●●●●●
Integration	●●●●○
Interoperability	●●●●●
Usability	●●●●○

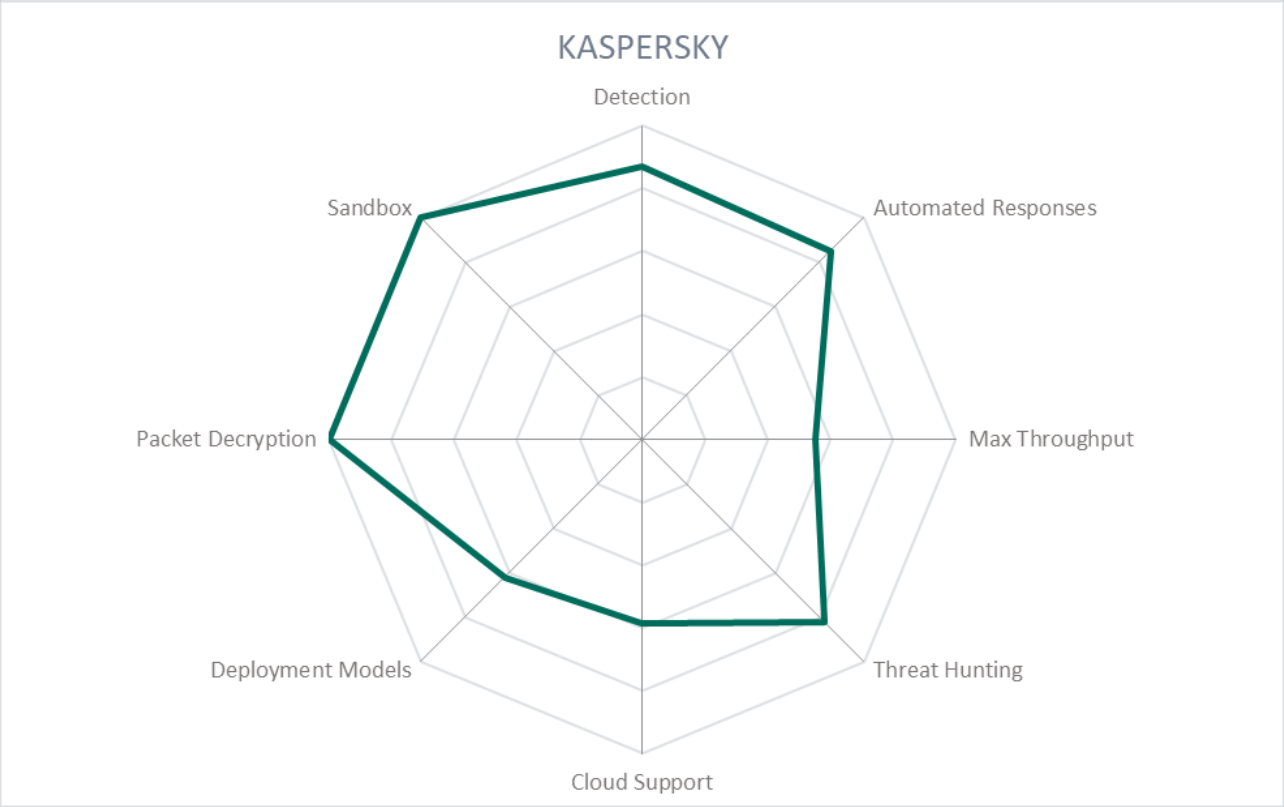
kaspersky

Strengths

- Integrated with Kaspersky's Threat Intelligence Portal and APT research data
- KWTS can decrypt packets
- Sophisticated sandbox detection capabilities
- KATA includes KEDR
- Excellent detection rate in real-world tests
- Global Transparency Centers

Challenges

- Multiple products with differing requirements needed for NDR functionality results in complex deployments
- SaaS offering slated for near-term improvement
- 4 Gbps max throughput without clustering
- MFA for admins and analysts on the roadmap


KASPERSKY
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.9 Lastline Defender

Lastline was founded in the Bay Area in 2011. It is a purpose-built NDR solution. It ships as an appliance or virtual appliance (VMWare ESX). AMIs for AWS and VHDs for Azure are available for cloud workloads. Enterprise console can be run on-prem, in AWS or Azure, and Lastline hosts a SaaS version. It can be deployed in-line, or off span/tap ports or network packet brokers. Max throughput for one appliance is 10 Gbps, although they can be load-balanced for higher throughput if needed. It does not decrypt packets. The licensing model is based on the number of users on the on-premise networks and number of instances for IaaS agents. Lastline OEMs some of their NDR components to other security vendors. Lastline doesn't provide managed services, but MSSPs use their product.

Lastline analyzes the expected set of network metadata and protocols, but also can perform application layer content level inspection of data objects if decrypted. Lastline doesn't decrypt packets, but rather uses a proprietary method based on packet sizes and timing to extract traces and features that can indicate malicious traffic. It also performs JA3/S SSL/TLS analysis. Lastline has a malware detonation sandbox which can be run on-prem, or customers can point to their cloud instance. Lastline employs multiple ML algorithms for anomaly detection and clustering. Supervised ML models classify results. Models are updated every few days as needed. Customers can suppress detection models which they believe do not apply in their environments and can customize IDS/NTA type rules. Initial baselining takes on average 1-14 days depending on environment.

Lastline can send alerts via syslog or APIs. Basic reports are provided, and customers can extend with ELK stack. Lastline gives analysts guidance for playbook development. Communication restrictions based on address, port, and protocol can be enforced by Lastline in in-line mode. Session termination and node isolation are possible by working in conjunction with 3rd-party security tools if in passive mode. Lastline can DNS sinkhole domains, which is not a common feature in NDR products. Lastline does not have recording/playback but does have Lucerne and Kibana for directed IoC searches across the enterprise and a GUI-driven threat hunter interface.

Lastline uses in-house sources for IoCs primarily. Customers can configure more external feeds thanks to their support of CyBox, STIX, and TAXII. They contribute to Cyber Threat Alliance. Lastline utilizes APIs to interact with SIEM, SOAR, and NAC type tools.

LDAP authentication and SAML federation is supported for on-premise deployments, but not for their SaaS instance. MFA is not supported at this time. Basic administrator roles are defined, but not segregation of duties. Appliances require admin privileges, and Lastline can work with PAM solutions.

Lastline specializes in NDR. Their solution uses a good mix of ML models to cover common NDR use cases. The ability to use DNS sinkholing is beneficial and not common in the space. The

product needs native MFA options and to support SAML for SaaS. Organizations that are looking for strong standalone NDR solutions should consider Lastline.

Security	●●●●○
Functionality	●●●●●
Integration	●●●●○
Interoperability	●●●●●
Usability	●●●●●

lastline®

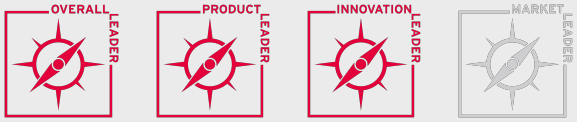
Strengths

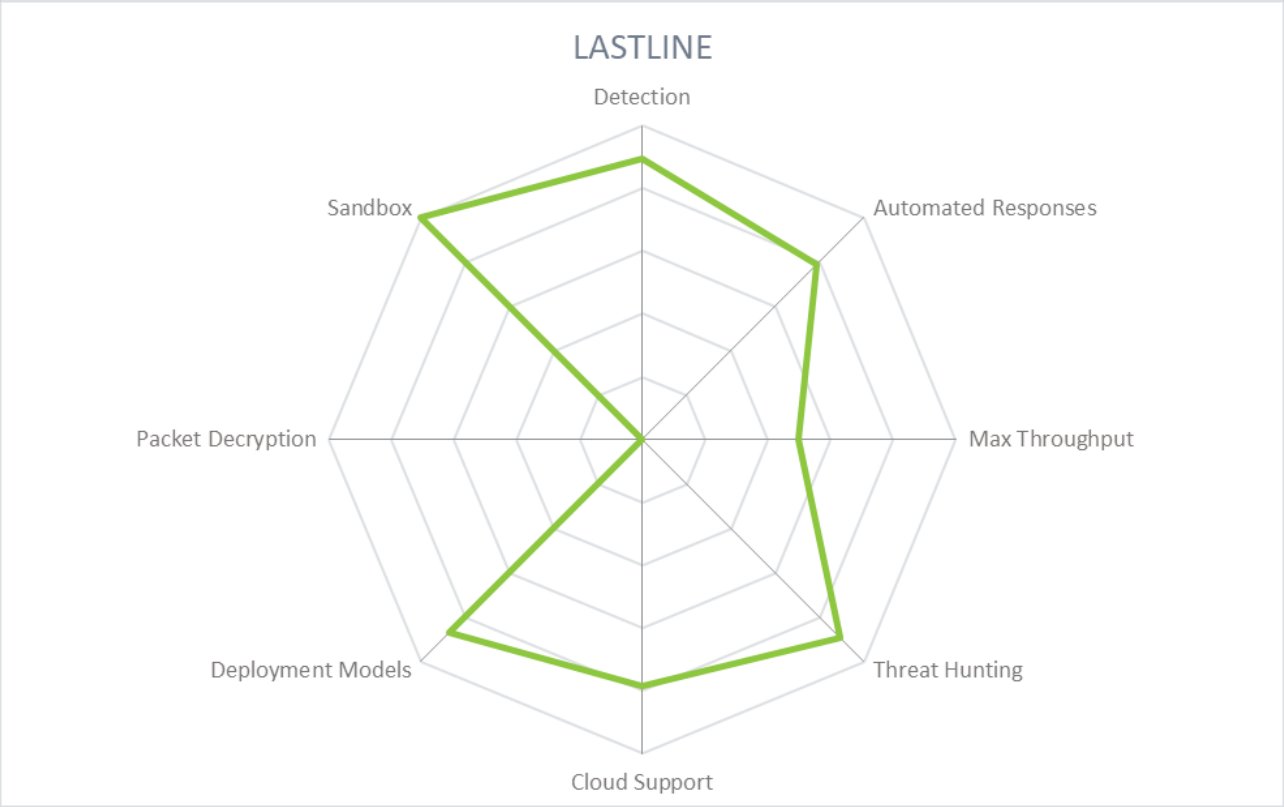
- Sandbox for malware detonation
- Non-invasive proprietary method of detecting malicious traffic
- Excellent ML detection model design
- Can send DNS redirects and sinkhole malicious traffic

Challenges

- Short default data storage period for SaaS version, but extensible
- No built-in MFA for admins; customers can't federate to SaaS

Leader in




LASTLINE
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.10 RSA NetWitness Platform

RSA Security is a longstanding cybersecurity vendor and are in the process of being acquired by Symphony Technology Group. Their headquarters is in Boston and 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. Physical appliances can capture at 10 Gbps, and virtual appliances and cloud agents can capture at 2 Gbps. Packet decryption is supported. They have packages for AWS and Azure, and GCP will be supported soon. Management console can run on-prem or in AWS or Azure, but RSA does not host it as SaaS. Their licensing model is based on throughput per day in Gbps/Mbps. UBA options are licensed separately. RSA does not offer MDR services but have approved partners.

NetWitness examines a comprehensive list of network connection metadata attributes and protocols for IoCs. It can be configured to decrypt traffic; NetWitness has a sandbox and customers can choose to use 3rd-party sandboxes. For customers who choose not to do decryption, NetWitness also performs JA3/S analysis. NetWitness can work in conjunction with their UEBA and Event Streaming Analytics (ESA) modules (sold separately) for full coverage of attacker TTPs. RSA uses unsupervised ML and Event Streaming Analytics (ESA) module for anomaly detection as well as complex static and correlative rules for threat classification. These rules can be customized as needed. Thirty days are needed for initial baselining. Customers can write and edit rules but cannot configure the ML models.

NetWitness shows alerts on the dashboard and can be configured to send others using other applications. Dozens of pre-defined reports are available, and customers can create more. NetWitness Orchestrator is the automation platform where playbooks are configured and responses involving 3rd party solutions are coordinated. Node isolation response can be triggered with NetWitness Endpoint, but other responses require integration of other security tools through Orchestrator. The console, which includes a query builder, is an excellent resource for threat hunters. Full recording/playback functions are supported.

NetWitness Platform provides its own comprehensive IoC sources, and customers can augment that by configuring external feeds. RSA supports CyBox, STIX, and TAXII. NetWitness Orchestrator can work with over 500 different security tools.

NetWitness is hardened according to STIG and Common Criteria. RSA SecurID is used for MFA, and PKI and SAML federation are supported via Microsoft ADFS. It can integrate with 3rd-party PAMs to lockdown admin accounts. Role-based and delegated administration are supported.

NetWitness has excellent anomaly detection capabilities built into the product. Strong MFA options are available. The native response options are quite limited but can be extended through Orchestrator. 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. 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	●●●●○
Integration	●●●○○
Interoperability	●●●●○
Usability	●●●●○

RSA

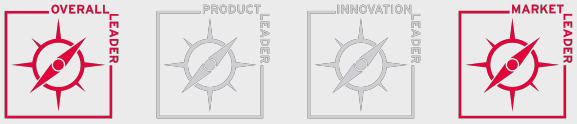
Strengths

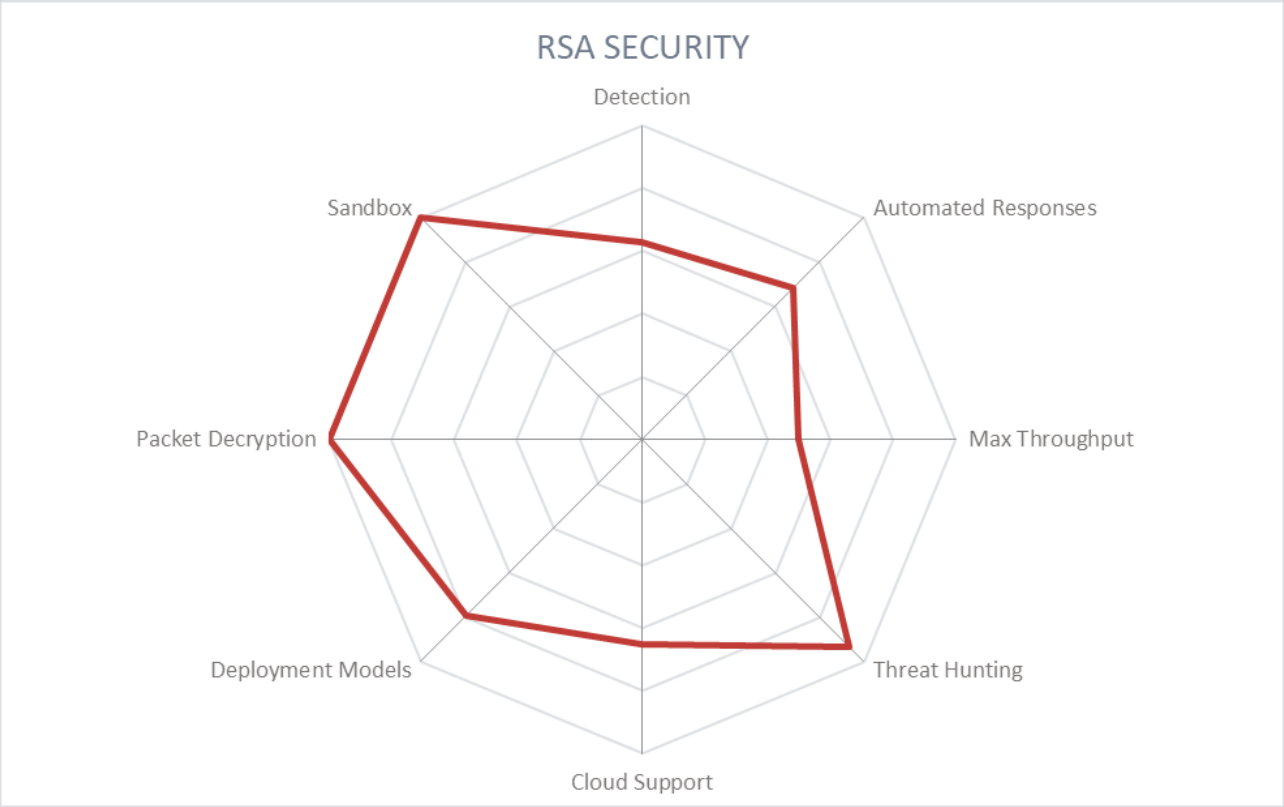
- Extensive list of IoC and attribute types analyzed
- Packet decryption and sandboxing
- Customers can add threat intel sources easily
- Strong MFA options are present; federation is supported

Challenges

- Optimal NDR capabilities require UEBA and Orchestrator modules
- Unsupervised ML only
- Infrequent model updates
- Limited built-in response functions unless Orchestrator module is purchased

Leader in




RSA SECURITY
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.11 Symantec Network Threat Detection

Broadcom is a large IT vendor with a diverse portfolio of security products, including the recently acquired Symantec Enterprise Security Business, which is maintaining separate branding. Their NDR solution is primarily 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 Appliance customers can take advantage of decrypted packet analysis. Symantec's solution also works inside AWS, Azure, and Oracle IaaS. Manager console can be run either on-prem or in the cloud; Symantec also offers hosted Secure Web Gateway for customers as a SaaS. Annual licensing for Security Analytics is per appliance with charges for additional storage. Symantec partners also provide managed NDR services.

Symantec's suite examines over 3,000 network applications, thousands of network metadata attributes, and is protocol aware. Symantec Security Analytics extracts potentially malicious files from traffic flows and checks against Symantec Content Analysis (sandbox), which has anti-evasion capabilities and supports detailed customization of emulation types. It can also point to 3rd-party sandboxes if configured. Symantec uses both unsupervised and supervised ML algorithms for continuous baselining, anomaly detection, and threat analysis, which can be supplemented with UBA from add-on Information Centric Analytics product. Symantec claims baselining can take as little as 6 hours. Customers can select specific threat models to activate and customize.

Symantec can send alerts and share metadata via its Integrated Cyber Defense (ICDx – the backend communication framework), SNMP, syslog, and Splunk Phantom triggers. All functions are addressable over APIs. Many pre-defined reports are available, and customers can build their own. Playbooks are pre-programmed for alert enrichment, malware detonation, IoC verification, and threat sharing. Through API integration with Symantec EDR, it can automatically isolate nodes and/or block traffic by port or protocol. The solution generates risk and confidence levels for analysts; threat hunters can use their natural language query functions.

Symantec has its own threat intelligence and IoC sources (Symantec Global Intelligence Network), and their solution is enriched with multiple external sources as well. CyBox, STIX, and TAXII are supported through ICDx. APIs permit interoperation with other security applications such as Demisto and Splunk.

Their platform has been evaluated against MITRE ATT&CK. CAC cards, Kerberos, LDAP, and RADIUS are available for strong authentication. It can use 3rd-party PAMs to lockdown admin or service accounts. Role-based and delegated administration are supported. Symantec has a unique Data Access Control feature which a master admin to define which categories of data within the solution are visible to lower-level admins.

Symantec's NDR solution is top-notch, covering all the basic plus providing support for advanced use cases requiring full packet decryption and analysis and sandboxing. Symantec Content Analysis also supports limited deception functionality: deploying customizable tripwires to find attackers targeting unique assets. 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	●●●●●
Integration	●●●●○
Interoperability	●●●●○
Usability	●●●●●

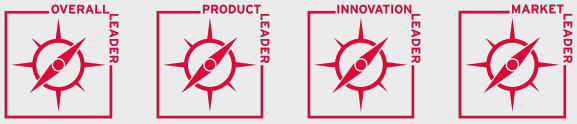
Strengths

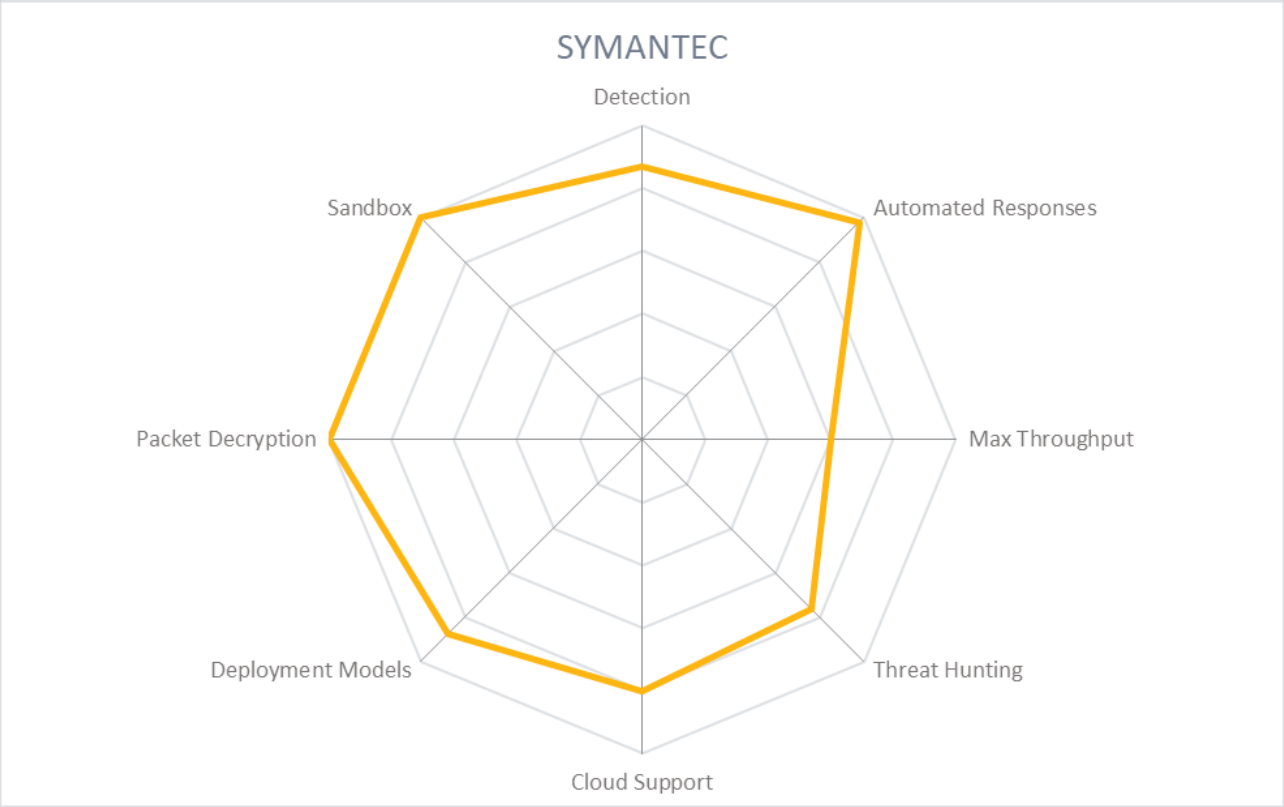
- Extreme scalability, processing billions of lookups per day
- Packet decryption and sandboxing available
- Deception/tripwire capabilities
- Customizable ML models
- Tight integration with Symantec security products

Challenges

- More MFA or SAML support for administrators is needed
- Threat Hunting Center is an add-on
- Multiple products needed to achieve complete NDR functionality

Leader in




SYMANTEC
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

5.12 Vectra Cognito

Vectra was established in 2010 in San Jose, CA. Their NDR suite is composed of Detect, Recall, Sidekick, and Stream products. The solution comes as an appliance or VMWare ESX virtual appliance, which is deployed off span/tap ports. It does not decrypt packets. It has a high throughput rate of 40 Gbps. It can also be installed in AWS and Azure, and it can take in logs from SaaS. Management console can be run on-premises or hosted in AWS, Azure, or their SaaS. Contracts are fixed price based on deployed hardware, GB/day of metadata, and charges for storage if Recall module is used. Sidekick is their managed service, and they partner with MSSPs as well.

Vectra analyzes an exhaustive list of connection attributes and protocols. Vectra does not decrypt packets thus it has no sandbox. Rather, Vectra focuses on advanced ML techniques to find even low level/volume traffic that may be malicious. Their use of ML is well thought out: each of the 100+ detection models employs an array of unsupervised and supervised ML and DL algorithms targeting specific behavioral sets. Models are configurable by customers, and customers can even create their own. Initial baselining takes about 5 days.

Alerting happens in the console and can be piped through SIEMs to other systems. Vectra provides recommended remediation steps, which require 3rd-party security tools to execute. Through API integration with network enforcement tools, Vectra can automatically terminate connections, isolate nodes and/or block traffic by port or protocol. The solution generates risk and confidence levels for analysts; threat hunters can use their natural language query tool. Vectra supports real-time analysis as well as recording/playback.

Vectra uses its in-network threat intel and it draws data from Virus Total. Customers can configure STIX/TAXII formatted external feeds. Vectra has API-level integration with ArcSight, AWS, Carbon Black, Cisco, CrowdStrike, Demisto, Forescout, IBM, Ixia, LogRhythm, Microsoft Azure, Palo Alto Networks, Service Now, Splunk, Swimlane, and VMWare.

Vectra is aligned to MITRE ATT&CK. They contribute to Cyber Threat Alliance. Appliances don't need admin credentials, so no interoperability with PAM solutions is present. MFA for admins is possible using RADIUS and IDaaS providers such as Duo and Okta, although significant customization is required. Vectra does not support SAML federation. Admin roles can be customized.

Vectra's strategy focuses on highly tuned ML models that provide a good signal-to-noise ratio thereby making the analysts' jobs easier. As a passive mode solution, it relies on 3rd parties for the critical response functions. MFA should be built-in to the console. Organizations that are looking for advanced NDR capabilities that have the potential to be somewhat less labor intensive should consider Vectra for RFPs.

Security	●●●●○
Functionality	●●●●●
Integration	●●●●○
Interoperability	●●●●●
Usability	●●●●●

VECTRA®
Security that thinks®

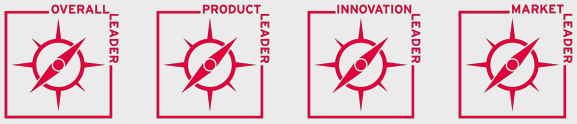
Strengths

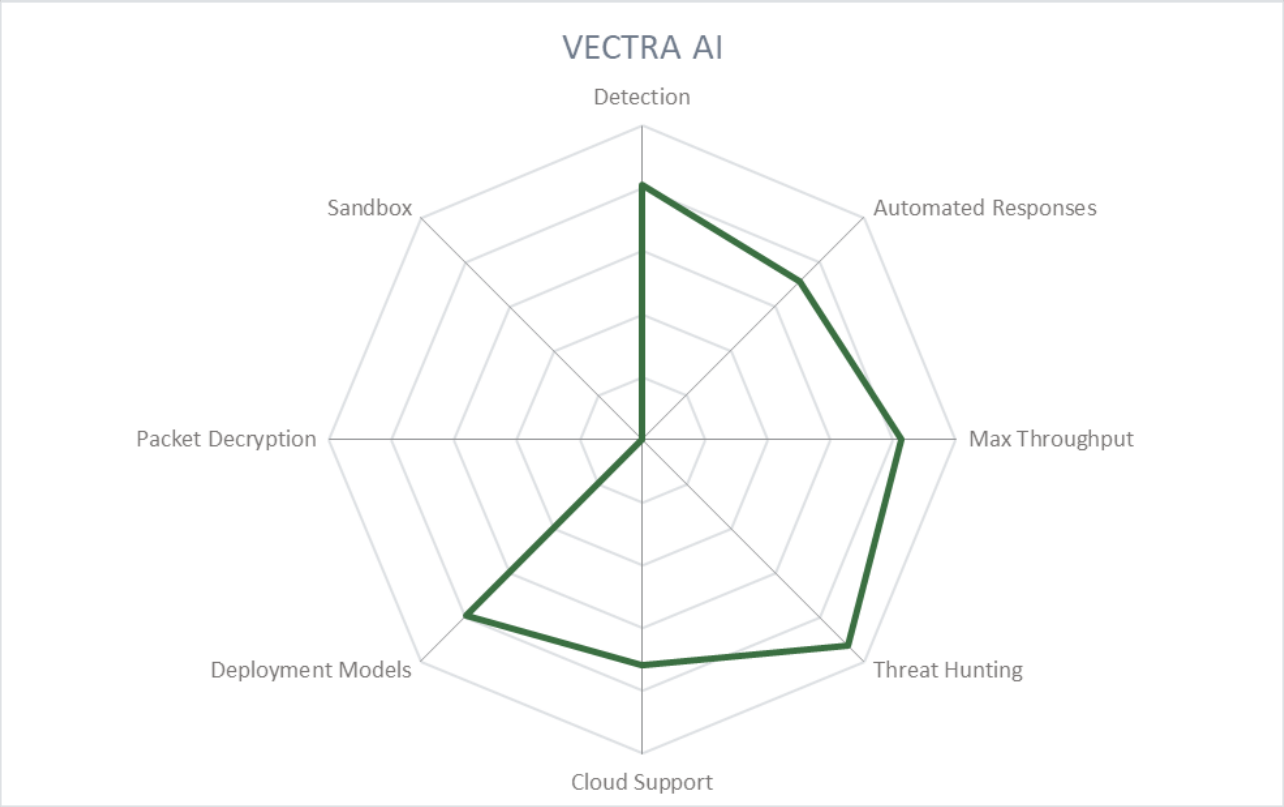
- 40 Gbps throughput
- Expertly architected ML/DL usage
- Natural language query interface for threat hunting
- API integration to many common security tools

Challenges

- Some remediation responses require integration with 3rd-party security tools
- No support for SAML federation for admins
- MFA for admins requires customization

Leader in




VECTRA AI
Detection
Automated Responses
Max Throughput
Threat Hunting
Cloud Support
Deployment Models
Packet Decryption
Sandbox

6 Vendors and Market Segments to Watch

Aside from the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors but do not fully fit into the market segment of Network Detection and Response or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

6.1 Awake Security

Awake Security was founded in 2014 in Santa Clara, California. The sensors are delivered as VMWare OVA virtual appliances and are deployed off span/tap network ports or off network packet brokers. Awake also works inside AWS, Azure, and GCP IaaS. Manager console can be run either on-prem or in the cloud; Awake also hosts customer consoles as SaaS. Awake launched a managed service for their Security Platform in February 2020.

6.2 BitDefender Network Traffic Security Analytics

BitDefender, a well-known anti-malware vendor headquartered in Bucharest, also has an NDR product. It is a passive mode solution which forwards network metadata to deployed appliances for analysis against ML detection models. NTSA allows for a variety of automated investigation techniques and remediation responses. It integrates with BitDefender Gravity Zone.

6.3 ExtraHop

Seattle-based ExtraHop provides security and analytics services for on-premise networks and cloud. Their Reveal(x) and Reveal(X) Cloud products are their NDR offerings. ExtraHop did not respond to our request for information, and thus it was not possible to evaluate their product on technical details for this report.

6.4 Gigamon ThreatINSIGHT

Gigamon was founded in 2001 in the Bay Area. They started as a network packet broker vendor, and thanks to the acquisition of ICBERG, picked up NDR functionality. ThreatINSIGHT can analyze hundreds of network connection metadata attributes and understands common protocols. ThreatINSIGHT employs a smartly designed array of unsupervised and supervised ML algorithms and models. Playbook actions and automated responses must be carried out via API integration with 3rd party tools. Threat hunters can use their Insight Query Language, which is based on STIX. ThreatINSIGHT is a newer service offering from Gigamon, and with enhancements on the roadmap, the feature set is likely to grow in the months ahead.

7 Related Research

Leadership Brief: Introduction to the IPLC Lifecyle and Framework – 80370
Leadership Brief: Do I Need Network Threat Detection and Response – 80296

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 in that market segment. It is the compass which assists you in identifying the vendors and products/services in a market segment 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

As part of our evaluation of products in this Leadership Compass, we look at four leadership types:

- **Product Leaders**: Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what 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 become an Overall Leader by being above average in all areas.

For every leadership type, we distinguish between three levels of products:

- **Leaders**: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular 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 products which lag behind 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 the 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 a given 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, as well as other sources.

Product rating

KuppingerCole as an analyst company regularly conducts evaluations of 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 of 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**
- **Integration**
- **Interoperability**
- **Usability**

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole Analysts IT Model. Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such

issues and the way a vendor deals with them.

Functionality – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

Integration – integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability – interoperability also can have many meanings. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs.

Usability – accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well-integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user

interface design.

We focus on security, functionality, integration, 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 potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product security, functionality, integration, interoperability, and usability which the vendor has provided are of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

Vendor rating

For vendors, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are:

- **Innovativeness**
- **Market position**
- **Financial strength**
- **Ecosystem**

Innovativeness – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. 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. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. 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 overall markets in which a vendor is active, e.g. 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 become an acquisition target, with massive risks for the execution of the vendor's roadmap.

Ecosystem – this dimension looks at the ecosystem of the vendor. 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 – beyond the Leadership rating in the various categories – a separate rating with five different levels. These levels are

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

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. 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. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., 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.
- **Denial of participation:** Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular 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 of 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 ompany, 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 back 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.