Market Guide for Network Detection and Response

Published 11 June 2020 - ID G00718877 - 23 min read

By Analysts Lawrence Orans, Jeremy D'Hoinne, Josh Chessman

Network detection and response (formerly known as network traffic analysis) vendors are adding more automated and manual response features to their solutions. Here, we provide an overview of the market and highlight some of the key vendors to be considered by security and risk management leaders.

Overview

Key Findings

- Applying machine learning and other analytical techniques to network traffic is helping enterprises detect suspicious traffic that other security tools are missing.
- Network detection and response (NDR) remains a crowded market with a low barrier to entry, as many vendors can apply common analytical techniques to traffic monitored from a SPAN port. Customer references, from a broad set of vendors, are generally satisfied with their tools.
- Response capabilities fall into two categories: manual and automatic. Vendors have been actively enhancing their manual (threat hunting and incident response) features, and have been adding partners to broaden their automatic response functionality.

Recommendations

To improve infrastructure security and the detection of suspicious network traffic, security and risk management leaders should:

- Implement behavioral-based NDR tools to complement signature-based detection solutions.
- Include NDR-as-a-feature solutions in their evaluations, if they are available from their current security information and event management (SIEM), firewall or other security vendors.
- Decide early on in the evaluation process if they desire automated response versus manual response capabilities. A clearly defined response strategy is valuable in selecting a shortlist of NDR vendors.

Market Definition

NDR solutions primarily use non-signature-based techniques (for example, machine learning or other analytical techniques) to detect suspicious traffic on enterprise networks. NDR tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect suspicious traffic patterns, they raise alerts. In addition to monitoring north/south traffic that crosses the enterprise perimeter, NDR solutions can also monitor east/west communications by analyzing traffic from strategically placed network sensors.

Response is also an important function of NDR solutions. Automatic responses (for example, sending commands to a firewall so that it drops suspicious traffic) or manual responses (for example, providing threat hunting and incident response tools) are common elements of NDR tools. In 2019, Gartner named this market "network traffic analysis." This year, we renamed it "network detection and response," because this term more accurately reflects the functionality of these solutions.

Market Description

Dozens of vendors claim to analyze network traffic (or flow records) and to detect suspicious activity on the network. We have applied the following criteria to identify the most relevant vendors.

Inclusion Criteria

Vendors must:

- Analyze raw network packet traffic or traffic flows (for example, NetFlow records) in real time or near real time.
- Monitor and analyze north/south traffic (as it crosses the perimeter), as well as east/west traffic (as it moves laterally throughout the network).
- Be able to model normal network traffic and highlight suspicious traffic that falls outside the normal range.
- Offer behavioral techniques (non-signature-based detection), such as machine learning or advanced analytics that detect network anomalies.
- Provide automatic or manual response capabilities to react to the detection of suspicious network traffic.

Exclusion Criteria

We exclude solutions that:

- Require a prerequisite component — for example, those that require a SIEM or firewall

platform.

- Emphasize network forensics over detection functionality, primarily through the storage and analysis of full PCAP data.
- Work primarily on log analysis.
- Are based primarily on analytics of user session activity — for example, user and entity behavior analytics (UEBA) technology.
- Focus primarily on analyzing traffic in Internet of Things (IoT) or operational technology (OT) environments, because specialized solutions are optimized to address this use case.

Market Direction

Vendors are focused on enhancing their detection and response capabilities. For detection, we expect vendors to continue enhancing their ability to detect suspicious patterns in encrypted traffic. Some vendors will add the ability to terminate, decrypt and analyze TLS traffic natively in their sensors. However, most vendors, particularly the ones with out-of-band sensors, will enhance their ability to detect suspicious traffic without decrypting the TLS traffic and inspecting the payload. Some vendors detect suspicious SSL/TLS Server Certificates for this purpose. Also, some vendors use techniques such as analyzing the length of individual packets, the timing between packets, the duration of connections and other methods to detect suspicious TLS traffic. We expect that more vendors will enhance their solutions with similar functionality.

Vendors will also be enhancing their response capabilities. For automated responses, they will broaden partnerships with firewall vendors (send commands to firewalls to drop suspicious traffic), network access control vendors (send commands to the network access control [NAC] solution to isolate an endpoint), security operations automation response (SOAR) vendors (respond to events with playbooks), endpoint detection and response (EDR) vendors (to contain compromised endpoints) and other security vendors. For manual response, vendors will improve their threat hunting and incident response functions by improving workflow features (for example, helping incident responders prioritize which security events they need to respond to first).

Market Analysis

Here, we analyze the segments of the NDR market:

- **Pure-play NDR companies.** The vendors in this category are mostly smaller specialty companies whose only product is an NDR solution.
- **Network-centric companies:** Several companies that have historically targeted network use cases, such as network performance monitoring and diagnostics (NPMD; see "Market Guide for Network Performance Monitoring and Diagnostics"), have developed solutions to

address security use cases. These network-centric solutions were already monitoring network traffic, and these vendors have applied analytical techniques, such as machine learning, to detect anomalous traffic.

- **Others.** A few vendors do not fit cleanly in the two categories defined above. For example, large, diversified network security providers, such as Cisco and Hillstone Networks, also offer NDR solutions. Cisco has Stealthwatch, and Hillstone has the Server Breach Detection System.

Representative Vendors

Market Introduction

Table 1 highlights the NDR vendors that meet our inclusion criteria and were not eliminated by our exclusion criteria.

Table 1: Representative Vendors in Network Detection and Response

Vendor	*Product, Service or Solution Name*
Awake Security	Awake Security Platform
Blue Hexagon	Blue Hexagon
Bricata	Bricata
Cisco	Stealthwatch
Corelight	Corelight Sensors
Darktrace	Enterprise Immune System
ExtraHop	Reveal(x)
Fidelis Cybersecurity	Fidelis Elevate
FireEye	SmartVision
Flowmon	Flowmon Anomaly Detection System (ADS)
Gigamon	ThreatINSIGHT

Vendor	*Product, Service or Solution Name*
GREYCORTEX	MENDEL
Hillstone Networks	Server Breach Detection System (sBDS)
IronNet	IronDefense
Lastline	Lastline Defender
Plixer	Scrutinizer
Vectra	Cognito Detect

Source: Gartner (June 2020)

Please refer to Note 2 for a list of other vendors that we are tracking.

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

Vendor Profiles

Awake Security

Based in Santa Clara, California, Awake Security uses supervised machine learning, unsupervised machine learning and some deep learning techniques to detect suspicious traffic. Awake does not decrypt TLS traffic. It also does not use JA3 signatures, but Awake has developed its own application/TLS fingerprinting algorithms. It also uses encrypted traffic analysis techniques. For example, it can identify attempts to tunnel malicious traffic over DNS and other protocols.

Awake's solution includes manual and automatic response capabilities. Its Ava tool performs automated threat hunting, incident triage and response. Awake partners with multiple firewall vendors, orchestration tools and other solutions to enforce automated responses. Awake sells the solution as an annual subscription, based on aggregate throughput. Virtual appliances are available at no charge, and physical devices are available for a fee. Customers can deploy Awake in two modes. With the first option, no customer sensitive data ever leaves the customer's environment. With the second option, customers deploy the central analytics and management in an Awake hosted cloud. In this scenario, each customer's data is isolated and can only be accessed by the customer that owns the data. Awake also offers a managed

network detection and response service built on the technology platform.

Blue Hexagon

Blue Hexagon is based in Sunnyvale, California. It launched its network and IaaS (Amazon Web Services [AWS] and Microsoft Azure) network detection solution in 2019, with a cloud management console. The vendor serves the U.S. market and plans expansion internationally in 2020. Blue Hexagon's detection engine inspects network traffic and files, and is based on deep learning to detect threats. The solution cannot decrypt TLS. It relies on TLS handshake and tunnel characteristics to detect anomalies on encrypted traffic, using its deep learning models. The vendor uses threat intelligence feeds, but also uses deep learning to classify sources as malicious.

Blue Hexagon can be deployed in-line and out-of-band. When deployed out-of-band, it integrates with endpoint security and firewall solutions, as well as SIEM, SOAR and AWS/Azure to provide automated response. When deployed in-line ("bump in the wire" or through ICAP), it can directly block traffic. Licensing for Blue Hexagon follows a traditional network security approach, with hardware purchase (virtual appliance is free of charge) and licensing based on required bandwidth, which includes vendor support. IaaS pricing can be bandwidth-based or per hour.

Bricata

Headquartered in Columbia, Maryland, Bricata is a network security vendor primarily targeting the U.S. and European markets. The vendor's solution leverages the Suricata IDPS module for signature-based controls and the Zeek (formerly Bro) engine for protocol and behavioral analysis, while capturing full-packet traffic data for retrospective analysis. Bricata is a highly customizable solution, where users can tune detections and create specialized detections. Bricata also includes the Cylance Infinity engine for file analysis. The network sensors and centralized management are available in physical and virtual appliances. They can also be deployed on the main IaaS platforms. The sensors do not decrypt TLS traffic, and rely on JA3 fingerprinting to provide encrypted session analysis. The vendor recently released the ability to tag alerts based on the MITRE ATT&CK framework, to aggregate similar events in the dashboard, and to run files in the Cuckoo Sandbox.

The vendor's response capabilities rely on SIEM and SOAR integration, and API documentation is available to create custom response scenarios with firewall, NAC and other products. Bricata's software pricing is based on aggregated bandwidth of inspected traffic. Customers can also purchase hardware appliances through Bricata's channel partners.

Cisco

Cisco, based in San Jose, California, offers two deployment options for its Stealthwatch solution. Stealthwatch Enterprise collects, stores and analyzes information in the customer's environment. Stealthwatch Cloud is a SaaS offering. It can monitor a customer's private network or a public cloud environment (through integrations with AWS, Azure or Google Cloud

Platform). Stealthwatch detects suspicious traffic primarily by analyzing NetFlow, IPFIX or sFlow records. Stealthwatch uses multiple analytical techniques to detect suspicious traffic, including supervised machine learning, unsupervised machine learning and some deep learning algorithms. The solution does not decrypt TLS traffic. Stealthwatch uses Cisco's Encrypted Traffic Analysis (ETA) functionality to analyze TLS traffic without decrypting it.

Stealthwatch provides historical information to enable a security analyst to manually respond to incidents. It also enables automated responses through integration with Cisco's Identity Services Engine (ISE). Stealthwatch alarms and events can be shared with Cisco's SecureX platform, where responses can be automated via SecureX playbooks. Stealthwatch is sold as a subscription based on the necessary flows per second, network device count or total monthly flows.

Corelight

Corelight is headquartered in San Francisco, California, serving customers essentially in North America and Europe. The vendor's founders created the Zeek (formerly Bro) network monitoring framework and the solution's sensors are available in the form of appliances (physical and virtual) on AWS and, more recently, on Azure. Corelight uses Zeek as its main engine and as a support for its own detections and integrating third-party threat intelligence feeds. Corelight mainly relies on its own analysis of the traffic metadata, and can also extract files to forward them to third-party file inspection devices. Corelight Sensors do not decrypt TLS, but the vendor just added additional encrypted traffic analysis for SSH — to detect brute force attempts and interactive connections — and TLS, including JA3 fingerprinting and certificate analysis.

As Corelight Sensors are more frequently deployed out of band, the vendor focused its response capabilities on integrating with a broad portfolio of SIEM and SOAR tools. Customers interested in Corelight will purchase hardware appliances and attached subscriptions based on sensors' expected bandwidth capacity.

Darktrace

Darktrace is based in Cambridge, U.K., and San Francisco, California. It's detection capability is primarily based on unsupervised machine learning, and it also utilizes supervised machine learning and deep learning algorithms. To analyze encrypted traffic, Darktrace relies primarily on unsupervised machine learning to detect unusual and anomalous JA3s. Darktrace offers a SaaS module to monitor traffic between users and Microsoft Office 365. In 2019, Darktrace introduced the Cyber AI Analyst capability. It uses analytical techniques to automatically investigate threats detected by Darktrace's flagship Enterprise Immune System (EIS). Cyber AI Analyst investigates the most important incidents on a dashboard, and it provides written reports on these incidents.

Darktrace's optional Antigena tool automates the response to incidents detected by EIS. It sends commands to leading firewall vendors to drop suspicious traffic. It also integrates with

some SOAR tools, some EDR tools and NAC tools. Cyber AI Analyst is Darktrace's primary tool for automatically investigating and responding to threats. Pricing for EIS is based on an annual subscription. The price for Antigena for Network is 50% of the cost of the EIS license. The price for Antigena for Email is based on the number of users in the organization.

ExtraHop

ExtraHop is a large network monitoring and security vendor, based in Seattle, Washington. It launched its NDR product, named Reveal(x), in January 2018. The vendor quickly gained visibility on shortlists among its existing customers and across multiple regions in pure NDR evaluations. ExtraHop delivers Reveal(x) as a self-service on-premises or IaaS appliance solution, or as cloud-hosted SaaS. Reveal(x) sensors extract enriched metadata to feed multiple analysis engines and build correlated security events. ExtraHop also offers full-packet capture or event-triggered packet capture. Users can drill down from summary metadata into the raw packets as Reveal(x) allows filtering and downloading of only the range of packets required. Reveal(x) can decrypt TLS traffic, if given access to the server secret keys or the symmetric session key, and relies on JA3 fingerprinting and other traffic analysis techniques when decryption is not an option. ExtraHop detection capabilities leverage a combination of techniques, including rule- and reputation-based controls, but also combine supervised and unsupervised machine learning to detect anomalies and deviation from normal network behaviors.

ExtraHop chose to integrate with ticketing, SIEM and SOAR for automated orchestration, and with firewalls or endpoint protection solutions for automated response. Reveal(x) is priced as a set of subscriptions, which depends on the number of endpoints, and so-called "critical assets" combined with bandwidth tiers. Additional features, such as full-packet capture and physical appliances, are priced separately.

Fidelis

Fidelis is based in Bethesda, Maryland. In addition to its NDR solution, the vendor also sells its own EDR and deception products. Fidelis combines multiple techniques to detect malicious traffic, including supervised and unsupervised machine learning, signatures, and statistical analysis. In April 2020, Fidelis launched a stand-alone TLS decryption appliance. It plans to add TLS decryption as an option on its sensors in 3Q20. It also uses JA3 signatures and machine learning techniques to analyze encrypted TLS traffic.

Fidelis Network does not directly integrate with any firewall solutions. It provides automated responses, such as packet drops, TCP resets and email quarantine, as well as quarantining files and custom playbooks, through its integration with its own EDR tool, Fidelis Endpoint. Fidelis also integrates with Carbon Black Cloud and other EDR tools. Fidelis can export data to SIEM and SOAR products. Manual response capabilities include the ability to search metadata, which can be stored for as long as the customer decides to keep it. Fidelis Network is licensed on an aggregate bandwidth and metadata storage model. An on-premises license can be purchased as a subscription or a perpetual model. A cloud license (managed from the cloud

with data stored in the cloud) can only be licensed as a subscription.

FireEye

FireEye is a global security company, based in Milpitas, California. FireEye SmartVision is its NDR solution, specialized on server-side traffic. SmartVision physical or virtual sensors are deployed typically to intercept client-to-server traffic. SmartVision detection engines heavily leverage IDS and threat intelligence rule-based controls. FireEye products are powered by a proprietary Multi-Vector Execution (MVX) engine, which can be hosted on-premises or in the cloud. FireEye Network Forensics provides full-packet capture and analysis of traffic. Machine learning techniques also apply to traffic and file analysis.

FireEye SmartVision response capabilities are available through the vendor's orchestration and endpoint solutions, or via numerous integrations. Additional investigation tools are part of the FireEye Helix threat hunting and managed security service offering. The SmartVision solution can be purchased with a perpetual license (customers buy appliances), or as an annual subscription (based on Mbps of throughput or on a per-user basis).

Flowmon

Flowmon is based in Brno, Czechia. Its detection algorithms are based on a combination of multiple techniques, including machine learning, heuristics, statistical and signature-based methods. Flowmon does not decrypt TLS traffic. It uses encrypted traffic analysis techniques to look for indicators of compromise and compliance-related risks. It also uses JA3 fingerprints, but it does not rely heavily on this technique. Flowmon can ingest flow data (for example, NetFlow, IPFIX and others) from the network infrastructure, but it achieves the best results when customers implement its probes. These probes generate metadata that provides visibility into Layer 7 traffic across multiple protocols. The probes also include a memory buffer to support event-triggered packet captures.

Flowmon supports some automated response capabilities through formal partnerships and integration with Cisco's NAC tool, Fortinet and Hillstone firewalls, and some other products. The tool also enables manual response by providing the ability to query and analyze origin data for threat hunting and incident analysis. Flowmon's detection engine is licensed per volume of processed flows per second (fps). Customers can purchase yearly subscriptions or perpetual licenses. Flowmon collectors are licensed based on performance (fps) and storage capacity. Stand-alone probes are licensed per number of interfaces and speeds.

Gigamon

Based in Santa Clara, California, Gigamon's ThreatINSIGHT solution is based on technology from its acquisition of ICEBRG in 2018. ThreatINSIGHT uses a combination of techniques to detect suspicious traffic, including supervised and unsupervised machine learning, deep learning, and signatures. ThreatINSIGHT can analyze decrypted TLS traffic when it is coupled with Gigamon's SSL decryption feature (an optional component of Gigamon's flagship GigaVUE network packet broker). To analyze unencrypted TLS traffic, ThreatINSIGHT uses JA3

signatures and it applies machine learning techniques to detect anomalous patterns of communication within the encrypted traffic stream.

When compared to many of its competitors, ThreatINSIGHT has limited integrations with technology partners to automatically respond to detections. It integrates with Demisto, Splunk and Mimecast, but it does not have any partnerships with firewall vendors (to drop suspicious traffic) or NAC vendors (to isolate a compromised endpoint). The Insight Query Language (IQL) feature allows incident responders to perform threat hunting and incident response by searching through a store of metadata. ThreatINSIGHT is available as a subscription service, priced according to bandwidth. As part of the subscription, every ThreatINSIGHT customer receives a dedicated Technical Account Manager, regardless of their size.

GREYCORTEX

With headquarters in Brno, Czechia, GREYCORTEX is a pure-play NDR vendor offering a solution called MENDEL. GREYCORTEX offers its solution mainly in Europe and the Asia/Pacific region. MENDEL consists of virtual and physical appliances. It can work with a single device, combining traffic gathering (sensors) and analysis (collectors), and expand to a three-tier architecture by adding a centralized management to handle multiple collectors. GREYCORTEX combines numerous supervised and unsupervised machine learning models, then correlates it with rule-based controls. It also provides solutions for ICS/SCADA networks. GREYCORTEX NDR supports configurable packet capture, and uses JA3 fingerprinting for TLS analysis and supports TLS decryption.

MENDEL can automatically block by instrumenting third-party network and security devices, leveraging their management API. Default configuration includes one month of searchable metadata. Two pricing models are available. Customers can purchase perpetual licenses based on sensor throughput and flows per second. Alternatively, customers can purchase a subscription license, also based on sensor throughput and flows per second (the subscription price includes support).

Hillstone Networks

Hillstone Networks is a large network security vendor, based in Suzhou, China, with regional headquarters in Santa Clara, California. Its Server Breach Detection System (sBDS) can be deployed as a stand-alone product, and its threat detection sensors can also be bundled in the vendor's centralized analytics solution (i-Source). Hillstone's solution combines the various engines from its security portfolio, including IDS and malware inspection, but does not decrypt or analyze TLS sessions. Its use of unsupervised machine learning is focused on baselining client-to-server traffic patterns and spotting deviations.

Hillstone's NDR solution integrates with other products from the vendor for incident response. Pricing is based on appliance purchase and attached subscriptions.

IronNet

Based in Fulton, Maryland, IronNet targets large enterprises that are concerned about attacks from nation states. Its solution uses a combination of behavioral detection techniques, including supervised and unsupervised machine learning and some deep learning. It also uses statistical analysis and some heuristic techniques to detect suspicious traffic. IronNet does not decrypt TLS traffic, and it does not support JA3 fingerprints. However, it uses a range of artificial intelligence and machine learning techniques to detect suspicious TLS traffic.

Unlike many vendors in this market, IronNet does not automatically respond to threats by integrating with firewalls to drop suspicious network traffic. However, it does integrate with leading SOAR and SIEM products. IronNet has strong manual hunt capabilities, enabling threat hunters to investigate across network flow data and pull packet capture (PCAP) on any flow (not just what IronDefense deems as high risk). The Expert System feature in the IronDefense product prioritizes threats and provides contextual information for incident responders. The solution also provides a crowdsourcing feature that enables communities of peer enterprises to collaborate against targeted threats. Pricing for IronDefense is based on a flat monthly fee based on analytical throughput (not ingest throughput) or by number of users. Customers must purchase IronDefense physical or virtual sensors.

Lastline

On 4 June 2020, VMware announced the intent to acquire Lastline. Gartner expects the deal to close by the end of June. After the deal has closed, Gartner expects that VMware will integrate Lastline technology into its NSX product.

Lastline is based in San Mateo, California. Its Defender product uses a combination of techniques to detect suspicious traffic, including supervised and unsupervised machine learning, and some deep learning functions. It also uses signatures, statistical analysis and heuristics, as well as a sandbox to detect malicious files. Defender does not natively decrypt TLS traffic. Instead, it applies anomaly detection to JA3 hashes. It also applies encrypted traffic analysis techniques to detect suspicious traffic without inspecting the payload.

Lastline's automated response with firewall vendors (to send a command to the firewall, so it drops suspicious traffic) is limited to only Check Point Software Technologies. However, Lastline integrates with many other security products, including VMware Carbon Black Cloud, Symantec (Blue Coat), Splunk (Phantom), Trend Micro (Tipping Point), Palo Alto Networks and several others. When the Lastline sensors are deployed in-line, they can block suspicious traffic. For manual response, Lastline provides good threat hunting and incident response capabilities. The solution includes the open-source Kibana search and visualization product. Lastline has also built a query language to do more complex searches. The solution includes a triage functionality that correlates multiple alerts into a single high-fidelity alert. Defender is sold as a subscription. Organizations can purchase based on either the number of protected hosts or the number of protected users.

Plixer

Based in Kennebunk, Maine, Plixer is a network performance monitoring and security vendor, offering an NDR solution based around Scrutinizer. Its customer base is mainly in the U.S. and Europe. Scrutinizer is deployed as physical/virtual sensors or as a SaaS. Scrutinizer collects metadata from the existing network infrastructure (switches, routers, firewalls, packet brokers, etc.), as well as from Plixer FlowPro, which is an optional sensor. The vendor recently acquired endpoint monitoring software, which promises to add more endpoint-related monitoring. Plixer offers integration with Endace for full-packet capture. Scrutinizer includes multiple rule-based and heuristic detections, detecting network anomalies, and security incidents. It complements these techniques with traffic baselining for anomaly detection and JA3 fingerprinting for TLS session analysis.

Scrutinizer's response capabilities include incident-based and threshold-based triggers to update firewall or other network equipment through API calls. Plixer's subscription licensing is based on flow rate and the number of metadata-exporting network devices. Threat hunting capabilities are integral to Scrutinizer.

Vectra

Vectra is a global NDR vendor, with headquarters in San Jose, California. Vectra Cognito is the company's main product offering. The vendor was early on the NDR market with its Cognito platform. Vectra is highly visible in Gartner client inquiries across the Americas and EMEA regions, and growing in the Asia/Pacific region. Cognito Detect, the NDR product, leverages physical appliance sensors and virtual machines deployable on hypervisors and on IaaS platforms, and can interact with some SaaS through APIs to gather SaaS events. The analysis engine (Vectra Brain) can be deployed on-premises or on public cloud. Vectra uses supervised machine learning to detect global threats, and combines it with threat intelligence for more accurate detection of known bad actors. It uses unsupervised learning models for more contextualized anomaly detection. The vendor uses JA3 fingerprinting and other techniques to provide detection coverage for encrypted traffic, but does not decrypt TLS. Vectra provides easy-to-understand dashboards, and a "campaign view," which puts multiple events in context and eases the investigation. Vectra recently launched a beta program for an Office 365 monitoring offering, and released Lockdown, an event aggregation and automated response (via partner integrations) feature that is part of Cognito Detect.

Vectra's Lockdown solution integrates with endpoint controls, firewalls, SOAR and SIEM to provide response capabilities. It can also directly integrate with the infrastructure, taking down workload or temporarily disabling compromised user accounts. Vectra's pricing, in addition to the hardware costs, is based on the number of active monitored IP addresses. Additional subscriptions are available to forward enriched, Zeek-formatted data in real time to a third-party data lake (Cognito Stream), or to a SaaS that is integrated with Cognito Detect (Cognito Recall) for threat hunting purposes.

Market Recommendations

Enterprises should strongly consider NDR solutions to complement signature-based tools and

network sandboxes. Many Gartner clients have reported that NDR tools have detected suspicious network traffic that other perimeter security tools had missed.

When evaluating NDR vendors, assess these factors:

- Response — Some vendors focus more on automated responses (for example, sending a command to a firewall to drop suspicious traffic), whereas other vendors focus more on manual responses (for example, providing strong threat hunting tools). Enterprises should decide which approach is a better fit for them and should analyze the vendors with response features that best meet their requirements.
- Pure-play versus NDR as a feature — Is it more sensible to implement NDR as a feature from another technology vendor (for example, SIEM), or do you require a more full-featured, pure-play NDR solution from one of the vendors analyzed in this Market Guide?

Note 1
Representative Vendor Selection

These vendors were selected because they met Gartner's inclusion criteria, and were not eliminated by our exclusion criteria.

Note 2
Other Vendors That We Are Tracking

IoT and OT Specialization Vendors

- Armis
- Cyberbit

NDR as a Feature Vendors

- IBM (QRadar Network Insights)
- LogRhythm (NetMon)
- Palo Alto Networks (Cortex XDR)

Other Vendors

- Accedian
- aizoOn
- Braintrace

- cPacket
- Kaspersky (see Note 3)
- Lumu
- MistNet
- MixMode
- Noble
- Nominet
- Quadminers
- Qianxin Technology Co., Ltd. (SkyEye)
- Qihoo 360
- RSA
- Stellar Cyber
- Tencent (T-Sec NTA)
- ThreatBook
- Vehere
- VIAVI

Note 3: Kaspersky

In September 2017, the U.S. government ordered all federal agencies to remove Kaspersky's software from their systems. Several media reports, citing unnamed intelligence sources, made additional claims. Gartner is unaware of any evidence brought forward in this matter. At the same time, Kaspersky's initial complaints have been dismissed by a U.S. District of Columbia Court.

Kaspersky has launched a transparency center in Zurich where trusted stakeholders can inspect and evaluate product internals. Kaspersky has also committed to store and process

adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."