VECTRA®
SECURITY THAT THINKS

EDUCATION GUIDE

Network Detection and Response

VECTRA
SECURITY THAT THINKS

What is Network Detection and Response?

The network security market has seen a resurgence in activity by vendors looking at the challenges of detection and response inside the network, but these vendors have been addressing the use-cases from different angles.

Detection and response are security operations capabilities and practices that enable the timely discovery of security events and support the ability to contain the impact of a potential cyberattack.

– NIST

Some of the vendors are decades old while others are new. Some provide security analytics as their core business while others are pivoting from the network performance monitoring space into network detection and response (NDR).

NDR goal: Empower security analysts to receive alerts quickly and be able to discern what is critical versus what is benign. It also focuses on lowering the time from compromise to incident detection and containment.

"With Vectra's early-detection capabilities, we have more confidence in stopping cyberattackers before critical infrastructure is damaged or valuable data is stolen."

Jojo Maalouf
IT Security Manager
Hydro Ottawa

Read the case study

VECTRA
SECURITY THAT THINKS

The network

The network will continue to connect everything even as the definition of computing evolves and changes with ever more advanced technology.

SIEM requires several log types to be enabled, collected and correlated to form a coherent picture. EDR needs agents nearly everywhere for decent visibility. Traditional IDS can provide broad visibility if it is widely deployed at the gateway and internally, but its reliance on signatures and reputations lists limit it to exposing only known attacks.

– NIST

The basic concept of networking will change as it manifests in different formats – from intercommunication using APIs within a specific cloud architecture to the expanding network of devices on the connected smart grid using 5G technology. But what will remain the same is the communication between devices and the behaviors this communication represents. This will drive future innovation in cloud, data center, IoT and enterprise networks.

NDR provides the broadest visibility into activities on the internal network by monitoring users, devices and their traffic.

For this reason, the network will continue to be a critical part of any detection and response capability. It provides the richest and most useful point for organization-wide visibility to any kind of device that communicates with any other device, from cloud workloads to IoT devices.

"Vectra is important to our journey. We're moving to cognitive security, where we can predict, prevent, detect and respond to cyberthreats faster – and continually improve our practices."

Liam Fu
Head of Information Security
The Very Group

Read the case study

VECTRA
SECURITY THAT THINKS

Detection

The detect function enables the timely discovery of cybersecurity events. Examples of the NIST outcome categories within this function include anomalies and events, continuous security monitoring, and detection processes.

The function of a security operation's detection capability is to develop and implement appropriate activities to identify the occurrence of cybersecurity events and to prioritize threat incidents that represent a high risk.

– NIST

Incidents should not be handled on a first-come, first-served basis because of resource limitations. Instead, handling should be prioritized based on relevant factors.

A security alert raises dozens of questions that an analyst must answer to verify if the alert is legitimate and determine its priority.

Prioritizing the handling of the incident is the most critical decision point in the process.

This process impacts the total time to detect and contain. Network detection should consider the process of detection, triage and prioritization in the core of its design.

"Cognito filled a gap. We needed to know what we didn't know, and Cognito showed us what was hidden."

Brett Walmsley
CTO
NHS Bolton

Read the case study

VECTRA
SECURITY THAT THINKS

5 key principles of network detection and prioritization capabilites

Use the checklist below as a benchmark

1. **Does it include post-compromise detection?**
   Post-compromise detection capabilities are necessary when a threat bypasses established defenses or uses new means to enter a network. ☐

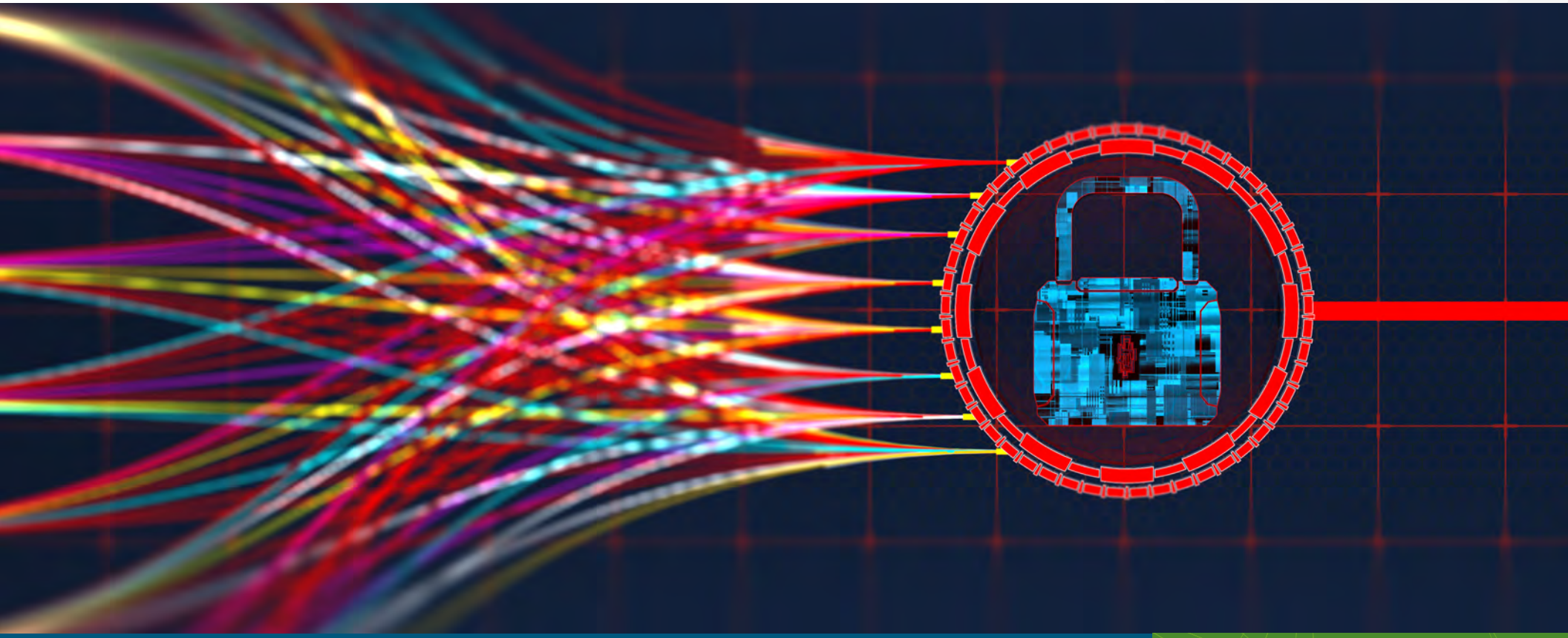
2. **Does it focus on attacker behaviors?**
   Attacker behaviors provide context about what has occurred and leads to the ability to define an actionable response. Detection techniques should also incorporate detecting and learning from post-compromise adversary behaviors. ☐

3. **Does it use a threat-based model?**
   An accurate and well-scoped threat model is necessary to ensure that detection activities are effective against realistic and relevant adversary behaviors. ☐

4. **Can it support a combination of behavior models with custom models?**
   Overlay a broader set of information on top of network traffic patterns. This enables correlation of suspicious internal traffic to specific known threats in the wild. ☐

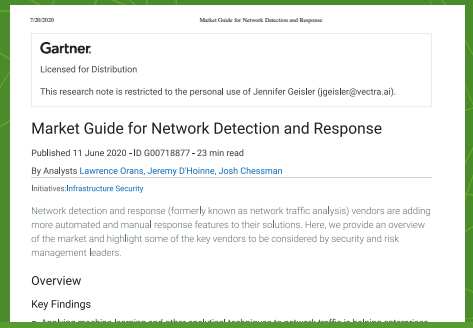
5. **Can it track attacks in real-time?**
   Show compromised workloads and devices. Inside the network, attackers perform internal reconnaissance and move laterally from host device to host device. ☐

VECTRA
SECURITY THAT THINKS



"The escalating sophistication of threats requires organizations to use multiple sources of data for threat detection and response. Network-based technologies enable technical professionals to obtain quick threat visibility across an entire environment without using agents."

Gartner research report "*Applying Network-Centric Approaches for Threat Detection and Response*" published March 18, 2019 (ID: G00373460), Augusto Barros, Anton Chuvakin, and Anna Belak


7/20/2020 Market Guide for Network Detection and Response

Gartner.

Licensed for Distribution

This research note is restricted to the personal use of Jennifer Geisler (jgeisler@vectra.ai).

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

Initiatives:Infrastructure Security

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

Download the report

Response

When looking at response capabilities, there are two broad categories of action that can occur for an incident:

The function of a security operation's detection capability is to develop and implement appropriate activities to identify the occurrence of cybersecurity events and to prioritize threat incidents that represent a high risk.

– NIST

1. Automated response
2. Manual response

Response APIs can be used for automated responses or to integrate with security automation and orchestration and SIEMs for customized actions.

Some types of alerts are good candidates for automated response. If the detection tool has a high degree of confidence that an endpoint has been compromised, that endpoint can be automatically isolated from the network.

Automating response actions is not a one-size-fits-all proposition.

Responding to more complex and targeted attacks involves investigations and threat hunting. These activities require network data that is searchable with the right context, enabling incident responders to quickly mitigate attacks and investigate threats.

Every security platform should enable analysts to choose and trigger the correct response based on policy and human analysis.

"Vectra detected red team activity during the proof-of-concept," says the information security architect. "That was the first time we ever detected a threat."

Information security architect
Beauty industry retailer

Read the case study

VECTRA
SECURITY THAT THINKS

5 key principles of network response capabilities

Use the checklist below as a benchmark

1 **Is the data searchable by humans?**

Speed of response depends on the analyst's ability to quickly search and interpret data to gain context about an incident. Network packets were not designed for human interpretation and are difficult to search, especially when storing costly terabytes of network traffic.

☐

2 **Does it have sufficient data with context about environmental variables?**

Analysis works best when data is enriched with helpful contextual information and supports data visualization to identify links between data sets.

Analysts are more effective when they can look past individual alerts to identify patterns and abnormalities. Security analytics and machine learning make this possible.

The ability to correlate events to a single incident enables threat hunters to identify an adversary's larger effort inside the organization against a backdrop of network noise.

☐

3 **Does it know for certain where to investigate?**

Analysts should always be creating hypotheses about attacks and it is advantageous to know where to begin hunting and investigating with some degree of certainty.

Guidance from intelligence feeds that are channeled into a primary source of threat data can revolutionize the way analysts hunt and investigate. Advanced machine learning can also improve the fidelity of findings. Collectively, they help analysts confirm with greater certainty where they should start looking and whether they have found something.

☐

4 **Does the investigation and hunting correlate?**

Another critically important action is the ability to pivot through data. Analysts must draw fast investigative conclusions, which requires them to have immediate access to data from multiple, disparate sources.

☐

5 **Can it integrate with other incident response tools for attack containment?**

Not every attack is the same and not every response should be the same. The ability to share intelligence across the existing security infrastructure will reduce the time to respond.

The integration of response capabilities should be simple and straightforward. It can occur through APIs, outbound events or automation platforms that provide standardization between different products.

☐

VECTRA
SECURITY THAT THINKS

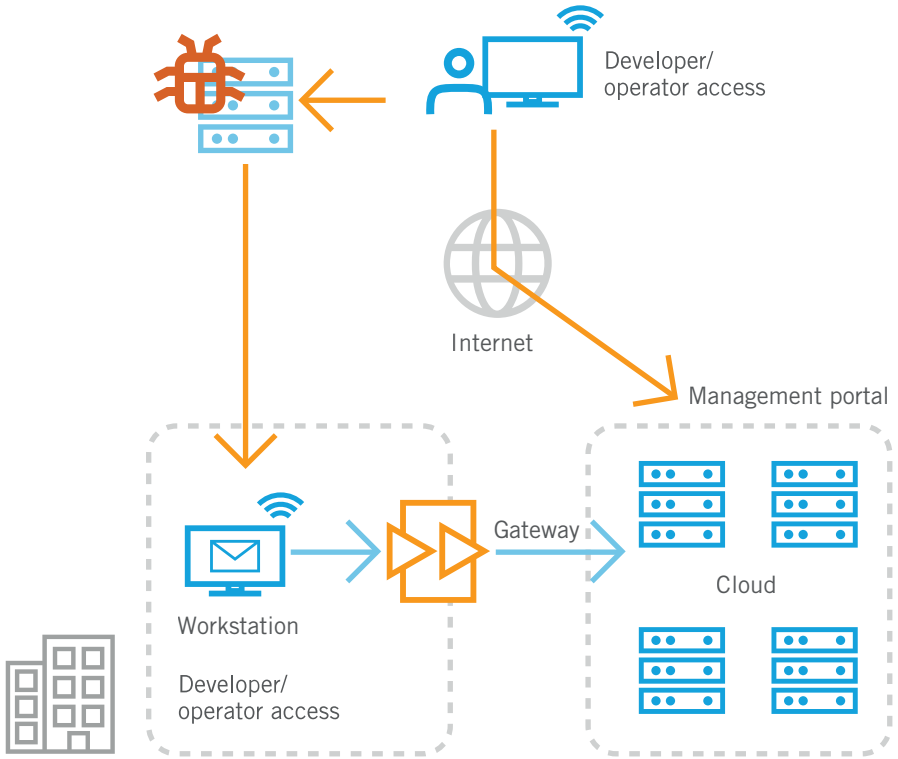
Why NDR?

- Collect, detect and prioritize high-fidelity threat behaviors in real-time
- Respond with automated enforcement and share threat data with IR tools
- Hunt efficiently for threats and conduct conclusive incident investigations
- Feed security-enriched network metadata to SIEMs and data lakes

Why NDR now?

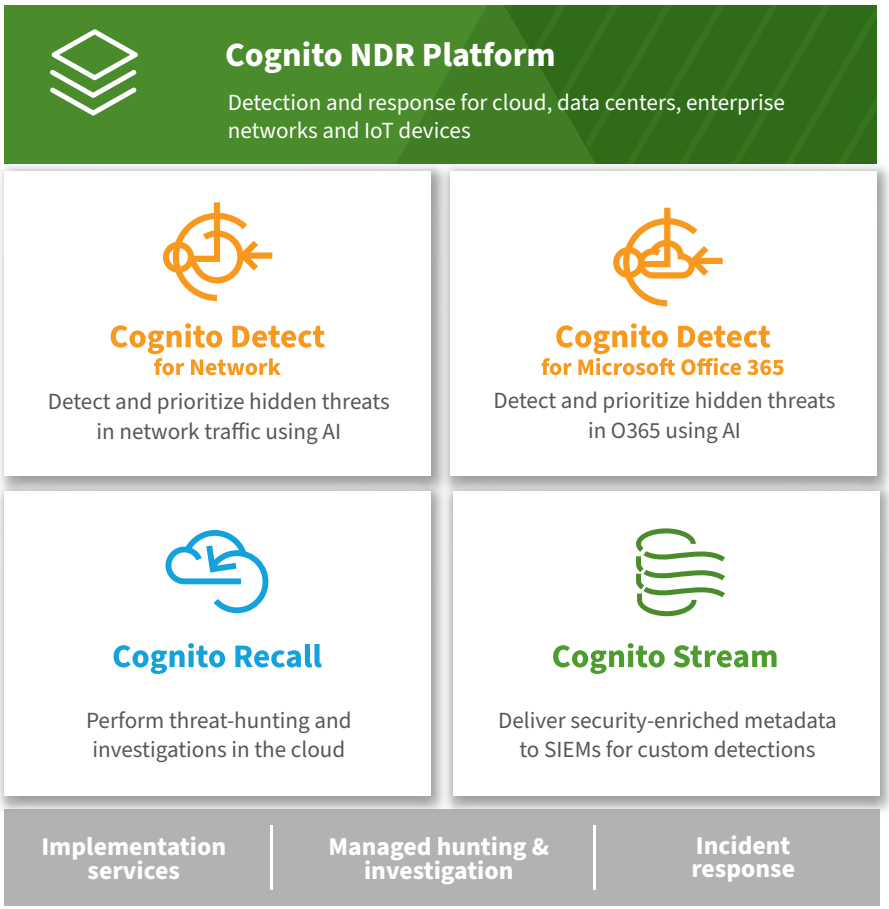
Sophisticated cyberattackers constantly invent and reinvent more effective ways to mount their assaults. Their evasive behaviors and the invisible footprints they leave behind change with dizzying frequency. Traditional legacy security designed to keep out attackers are blind to these ever-changing threat behaviors, giving cybercriminals free rein to spy, spread and steal.

What's needed is a reliable way to detect hidden attackers who get inside and respond instantly to stop in-progress threats from becoming a data breach. One that proactively hunts for evasive threats, augments your existing security investments, keeps up with the changing threat landscape, and offers exceptional scale across cloud, data center, IT and IoT networks.



Sophisticated cyberattackers constantly invent and reinvent more effective ways to mount their assaults.

VECTRA
SECURITY THAT THINKS



Why Vectra?

The Vectra NDR platform is in 100% service of detecting and responding to attacks inside cloud, data center, IoT, and enterprise networks. Our job is to find those attacks early and with certainty.

It starts with having the data to make this happen. This is not about the volume of data. It is about the thoughtful collection of data from a variety of relevant sources and enriching it with security insights and context to solve customer use-cases.

Attack behaviors vary, so we continuously create unique algorithmic models for the widest range of new and current threat scenarios. Performing well beyond the abilities of humans, Vectra gives you a distinct advantage over adversaries by detecting, clustering, prioritizing and anticipating attacks.

By doing the thinking and reducing the security operations workload, you will spend more time on threat hunting and incident investigations. Now you know why Vectra is known as Security that thinks®.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai