VECTRA®

The dark side of Darktrace

Why Vectra beats the competition

Network detection and response (NDR) solutions are not created equal. At Vectra®, we often see Darktrace show up for proof-of-concept (POC) evaluations alongside our Cognito® platform, and we love it.

For one, friendly competition is what keeps us honest and on our toes. But the real reason is because we win. Especially if the customer is using a red team to simulate real-world attacks. That's because our AI models have been developed by security researchers and data scientists working together to create supervised and unsupervised machine learning algorithms.

Darktrace has a tough time learning

The Cognito AI platform also starts detecting threats from day one, whereas Darktrace requires two weeks of baselining before customers are allowed to even view the solution. Considering that it only takes a few minutes for attackers to execute an initial compromise, the Vectra advantage in time-to-value is strikingly clear.

Manipulating results through a VPN

And what about the VPN connection Darktrace uses for its POC trials? Darktrace insists on a persistent VPN Call-Home function during a POC. If a customer refuses this connection, the quality of Darktrace connections dramatically drops.

And at the other end of that VPN connection is a person working behind the scenes to optimize your POC results. Unfortunately, that person is not included with the purchase of your Darktrace solution, so once you buy it, you're on your own.

Prepare for an onslaught of anomaly alerts

When pitted against real humans rather than canned attacks, Cognito algorithmic models outshine Darktrace's simple signature-based detections. In fact, the Cognito platform supports over 85% of the MITRE ATT&CK framework. This comprehensive detection capability quickly becomes apparent for our customers during the POC.

As an anomaly-based detection system, Darktrace can't identify the highest-risk threats and will overwhelm your security team with a deluge of alerts that you have to manually investigate.

In stark contrast, Cognito reduces security operations workload by 34X. It automatically triages alerts into incidents, prioritizes host devices that pose the highest risk, and extracts security-enriched metadata from network traffic for investigations and forensics.

Conversely, Darktrace alerts must be manually and individually triaged, which increases your security operations workload. This creates an unwanted burden on already-overtasked security teams in search of an NDR solution.

Darktrace doesn't play well with others

Lastly, most security leaders know better than to add siloed technology that doesn't fully integrate with other solutions in your security stack. Darktrace thinks it solved integration problems by sending syslogs to SIEMs and believes it can fully address the needs of incident response.

However, it relies mainly on sending TCP resets and applies active lists to firewalls – adding to your management headache. Besides being useless if an attacker uses UDP, this adds extra traffic to your network and fails to terminate an attacker's very short connection.

Cognito: NDR that works

The Cognito platform, on the other hand, easily integrates with your enterprise security stack via APIs to block new classes of threats. Our ecosystem of technology partners are among the leaders in endpoint detection and response, next-generation firewalls, SIEMs, security orchestration, and network access control.

Cognito also provides an excellent starting point for incident investigations and retrospective threat-hunting by feeding security-enriched network metadata – containing unique security insights and context – to your own data lake or SIEM.

The Cognito platform gives you the following advantages over Darktrace:

- Detects real-world attacks based on the supervised and unsupervised machine learning algorithms, from cloud workloads to user and IoT devices.
- Identifies threats from day one without requiring a baseline learning period.
- Reduces your SOC workload by 34X. Cognito triages security alerts into prioritized incidents for the fastest, conclusive response.
- True platform performance integrates with other solutions in your security stack.

Network Traffic Analysis Capability	Vectra	Darktrace	Assessment
Data source	Security-enriched network metadata	Network metadata	Cognito delivers high-fidelity network metadata – knowledge of what's happening in every conversation – enriched with context specific to security applications, e.g. the names of hosts, existence of beacons, and the privilege level of accounts.
Metadata streaming to data lake/SIEM	✓	✗	Vetra Cognito streams searchable metadata in Zeek format to the data store of your choice with Kafka, syslog and Elastic support. Darktrace does not.
AI-derived metadata enrichments	✓	✗	Inherent and embedded into the platform, ML-enrichments derived by an award-winning team of Ph.D. data scientists and security researchers provide security teams with the insights for effective threat hunt. Example use cases and enrichments can be found in the following blog.
Deep learning	✓	✗	The Cognito platform from Vectra applies optimized AI techniques – supervised, unsupervised machine learning and deep learning – to precisely identify attacker behaviors with greater efficacy and fewer false positives. Vectra delivers a higher fidelity signal and much lower noise than Darktrace, which is limited to using unsupervised machine learning that only detects anomalies. Anomaly detection generates a significant number of false positives; many anomalies are not threats.
Supervised machine learning	✓	✗	
Unsupervised machine learning	✓	✓	
Imports IoCs for detection	✓	✗	Only Vectra combines the detection of hidden threats using AI with the detection of known threats using high-quality IoCs. Darktrace is limited to detecting anomalies and can't correlate them with detections based on high-quality IoCs.
Aggregates individual alerts into incidents with full PCAP on-demand for forensic investigation	✓	✗	Vectra delivers a greater reduction in the security operations workload by triaging and correlating security alerts into incidents, prioritizing hosts with incidents, and providing PCAPs for incident investigations and forensics. Darktrace alerts must be individually triaged, which increases the security operations workload.
Tracks cyberattacks across the enterprise and shows all compromised workloads and devices	✓	✗	Vectra empowers security operations teams to address all workloads and devices that may be impacted by a cyberattack, which speeds-up response time and reduces the overall security operations workload. With Darktrace, security analysts must manually correlate hosts with similar alerts to understand the scope of an attack, which delays response and increases risk to an organization.
Includes detection models specific to data center and cloud use-cases	✓	✗	Vectra delivers complete enterprise coverage from cloud and data center workloads to user and IoT devices using the broadest set of machine learning algorithms, leaving attackers with nowhere to hide. Vectra empowers organizations to embrace hybrid cloud architectures with purpose-built detection models for securing workloads on-premises and in the cloud. Darktrace simply applies the same generic anomaly detection models it uses for IoT and user devices to data center and cloud workloads.
Integrates with firewall, NAC, endpoint, SIEM and SOAR products to streamline incident response	✓	!	Vectra has the agility to respond appropriately based on the detected threat. Vectra immediately integrates into an enterprise's security architecture, enabling existing endpoint, NAC and firewall security to block new classes of threats and provide the best starting point for an investigation in a SIEM or data lake. Aside from sending syslog to SIEMs, Darktrace believes it can fully address the needs of incident response with Antigena, which uses TCP resets and applies active lists to firewalls.
Delivers a complete solution for network detection and response	✓	✗	Vectra delivers a platform for network detection and response (NDR) with Cognito Detect, Cognito Recall and Cognito Stream. Vectra has the longest tenure and greatest investment in the development of AI for detecting attacker behaviors as well as collecting and enriching metadata for threat hunting and incident investigations. Darktrace only saves a limited amount of metadata (less than two weeks based on packet volume) and cannot send metadata to data lakes, use existing Zeek (Bro) tooling or build custom queries with tools like Elasticsearch.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai