VECTRA
SECURITY THAT THINKS.®

COMPETITIVE BRIEF

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. Unlike Darktrace that uses discrete anomalies, Vectra uses multiple AI behavioral models, choosing the best for the potential threat. It is when Vectra provides the enriched and prioritized analysis that customers can achieve the benefit in reduced workload and wasted investigations

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.

The Cognito AI platform starts detecting threats from day one, whereas Darktrace requires two weeks of baselining before customers are allowed to even view the solution.

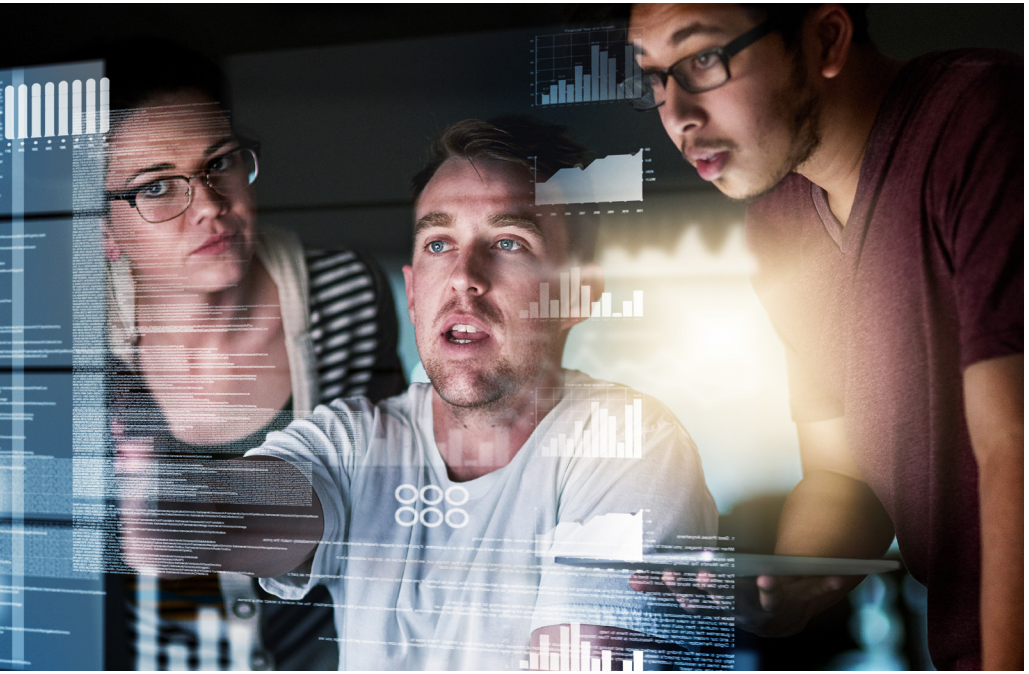
85%

The Cognito NDR platform supports over 85% of the MITRE ATT&CK framework

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. Darktrace runs a significant risk of learning an existing actual malicious behavior as a benign event. Organizations suffer from false positives and negatives with Darktrace.

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 detections 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 have to constantly and manually investigate. A costly and time consuming process.

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 network resets or integration with their own products (read as – replace the investment in EDR, NAC, etc.) and applies active lists to firewalls – adding to your management headache.

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 has tight integrations with AWS and Azure for customers who are moving to the cloud.

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 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, automatically overlays the attacker's objectives to the Mitre framework and correlates user, host, service and cloud identities for the fastest, most conclusive response.
- True platform performance integrates with other solutions in your security stack.

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

Email info@vectra.ai vectra.ai