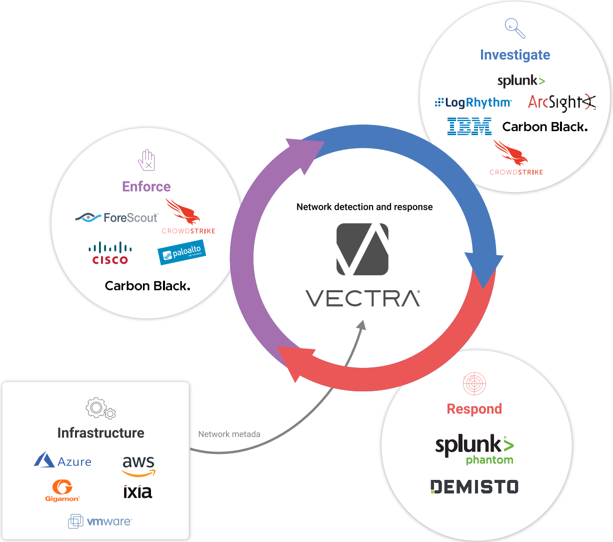
VECTRA®

Security that thinks.®

Vectra is the world leader

in applying artificial intelligence to detect and respond to advanced cyberattacks in real time.

Vectra® is revolutionizing network detection and response with the Cognito® platform, which replaces legacy technology that fails to solve today's security challenges – from hybrid and cloud-native AWS and Azure environments to data center workloads, and user and IoT devices.



The Cognito platform

The Cognito platform accelerates customer threat detection and investigation using sophisticated artificial intelligence to collect, store and enrich network metadata with insightful context to detect, hunt and investigate known and unknown threats in real time.

The Cognito platform scales efficiently to even the largest enterprise networks with a distributed architecture that supports a mix of sensors to provide 360-degree visibility across cloud, data center, user and IoT infrastructures.

Vectra offers three applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store enriched metadata and investigate threats. Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed.

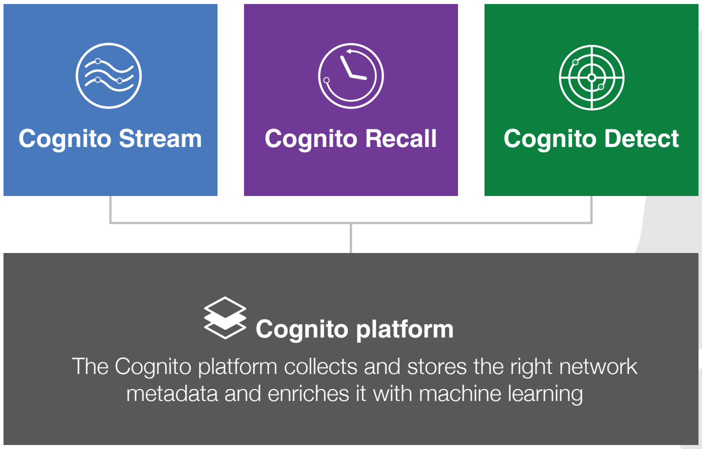
I am artificial intelligence.
The driving force behind the hunt for cyberattackers.
I am Cognito.

The right data for detection and response

Cognito relies on the only source of truth during a cyberattack – network traffic. Only traffic on the wire – whether in public clouds, private data centers or enterprise environments – reveals the truth with complete fidelity and independence. Attackers can delete logs, but they can never erase their footprints in the network.

Cognito is the ultimate network threat detection and response platform

I provide a 360-degree view within your cloud, IoT and enterprise networks, leaving attackers nowhere to hide.



Cognito Stream

Cognito Recall

Cognito Detect

Cognito platform

The Cognito platform collects and stores the right network metadata and enriches it with machine learning

Cognito Stream: Network metadata with an opinion

Sends security-enriched metadata to a data lake or SIEM

Actionable network data
Extract hundreds of metadata attributes from raw network traffic and presents them in a compact, easy-to-understand Zeek format that leverages existing software tooling.

Embedded security insights
Security insights generated by machine learning are embedded in the metadata to provide powerful building blocks threat hunters can combine with their own unique expertise to quickly reach conclusions.

Investigations based on hosts, not IP addresses
Automatically associates network metadata with other attributes to create a unique host identity. This enables security analysts to efficiently investigate hosts regardless of IP address changes as well as explore relationships between groups of hosts.

Cognito Recall: Built for investigation and hunting

Cloud-based application to store and investigate security-enriched metadata

Empower threat hunters
Real-time collection and storage of enriched network metadata, relevant logs and cloud events enables threat hunters to leverage the deep knowledge and insight of advanced attackers.

Intelligent investigation of device activity
Associates network metadata with devices, not just IP addresses, and provides an instant view of device activity over time, regardless of IP address changes.

Cloud-powered limitless scale
Threat hunters can rely on enriched network metadata that is stored and searched for as long as they need it, while Vectra manages the infrastructure.

Cognito Detect: The power of AI to detect and prioritize

AI to reveal hidden and unknown attackers at speed

AI-powered threat detection
Always-learning behavioral models use AI to efficiently find hidden and unknown attackers to enable quick, decisive action and provide a clear starting point for an incident investigation.

The right context, right now
Eliminates the endless hunt and search for advanced cyberattacks and enables immediate action by proactively putting the most relevant context at the security analyst's fingertips.

Force-multiplier for existing security investments
Integrates with endpoint detection and response, network access control, firewalls and other enforcement points to block new classes of threats and provide a starting point for incident investigations within Cognito Recall, data lakes and SIEMs.

To request a demo, please go to vectra.ai/demo

VECTRA®
Security that thinks.®

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