VECTRA
SECURITY THAT THINKS.®

DATA SHEET

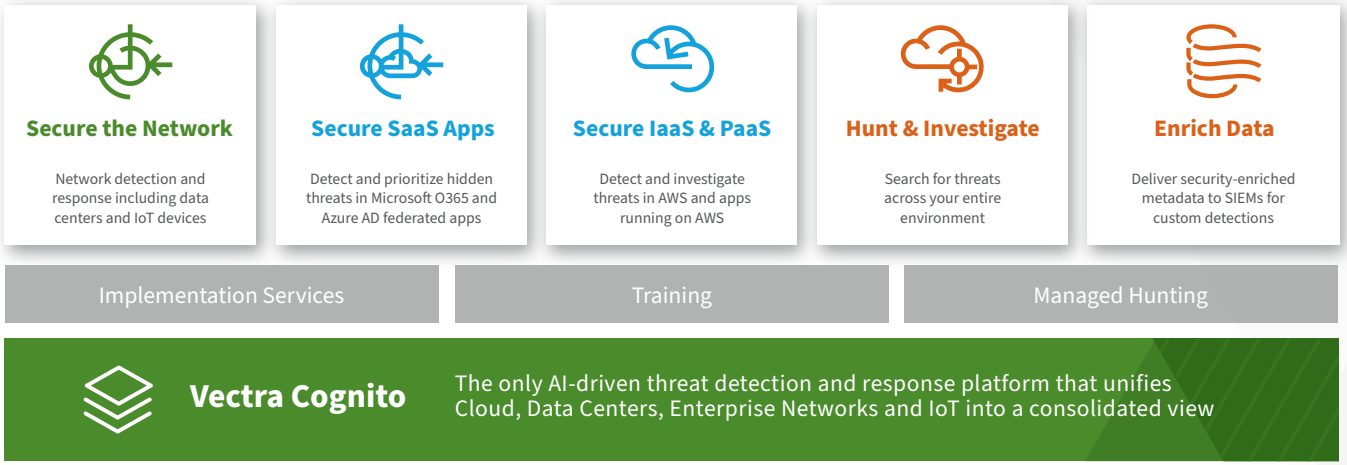
The Cognito Threat Detection and Response Platform

The Vectra Cognito® Threat Detection and Response platform is driven by AI, providing the fastest and most efficient way to see and stop attacks. From hybrid and cloud-native apps, as well as AWS and Azure environments, including software-as-a-service (SaaS) applications such as Microsoft Office 365 using Identity on Azure AD to data center workloads, IoT, and enterprise networks. The Cognito platform prioritizes the threat behaviors that pose the highest-risk to your organization and provides actionable data and automated response so you're always certain where to start hunting and investigating.

- Automatically detects, prioritizes, and responds to hidden cyberthreats inside cloud, data center, IoT, and enterprise networks.
- Speeds-up threat detections and reduces investigation time by capturing metadata at scale across the cloud and enterprise infrastructure.
- Collects and enriches security metadata with deep insights and context to allow analysts to stop a wide range of attack scenarios early and consistently.
- Automates the manual tasks associated with Tier-1 and Tier-2 analysis to reduce the overall security operations workload.
- Gives security analysts more time to proactively hunt for threats and investigate incidents with greater success by stopping ongoing attacks.
- Accelerates response time by integrating and sharing security insights with EDR, SIEMs and SOAR tools for endpoint to cloud threat management and visibility.

With Cognito, attackers have nowhere to hide

The Cognito platform is driven by AI, providing the fastest and most efficient way to see and stop attacks across public and hybrid cloud, as well as enterprise networks including data centers and IoT devices.



Automates threat detections

Detect threats in real-time using always learning behavioral models derived from machine learning. Vectra's patented AI correlates detections with specific hosts and account so you'll find attacks faster and remediate quickly.

Empowers threat hunters

Launch deeper and broader investigations into incidents that are detected by the Cognito platform or third-party security solutions and successfully perform proactive threat hunting with greater efficiency.

Provides increased visibility

Collect analyze and store security-enriched network metadata, relevant logs and cloud events for unprecedented visibility into the actions of all workloads, services, servers, host devices, accounts, roles, and users.

Captures once and does many things

Access security-enriched metadata from a single platform to automate threat detections and incident response, as well as accelerate investigations and AI-driven threat hunting.

The Cognito platform allows all detections, host and account scores and metadata to be accessed via APIs and strives to be partner- and vendor-neutral. This enables security practitioners to leverage best-in-class solutions to build world-class security infrastructures at true enterprise scale.

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

Email info@vectra.ai vectra.ai