VECTRA
SECURITY THAT THINKS.®

DATA SHEET

The Cognito NDR Platform

The Cognito® Network Detection and Response (NDR) platform from Vectra® applies AI-derived machine learning algorithms to automatically detect, prioritize and respond to in-progress cyberattack behaviors.

From hybrid and cloud-native AWS and Azure environments to software-as-a-service (SaaS), data center workloads, IoT, and enterprise networks, the Cognito NDR platform prioritizes threat behaviors that pose the highest-risk to your organization so you're always certain where to start hunting and investigating.

- Detects, prioritizes and responds automatically to hidden cyberthreats inside cloud, data center, IoT, and enterprise networks.
- Speeds-up threat detections and incident response by capturing metadata at scale from all traffic across the data infrastructure.
- Enriches metadata with deep security insights and context 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 practitioners more time to proactively hunt for threats and investigate incidents with greater success.
- Accelerates response time by integrating and sharing security insights with EDR, SIEMs and SOAR tools for end-to-end threat management and visibility.

The Cognito NDR platform is the fastest and most efficient way to find and stop cyberattacks – across cloud, data center, IoT, and enterprise networks.

With Cognito, attackers have nowhere to hide

Automates threat detections

Detect threats in real-time using always-learning behavioral models derived from machine learning. With a clear starting point for AI-driven threat hunting, you'll find attackers quickly and decisively.

Empowers threat hunters

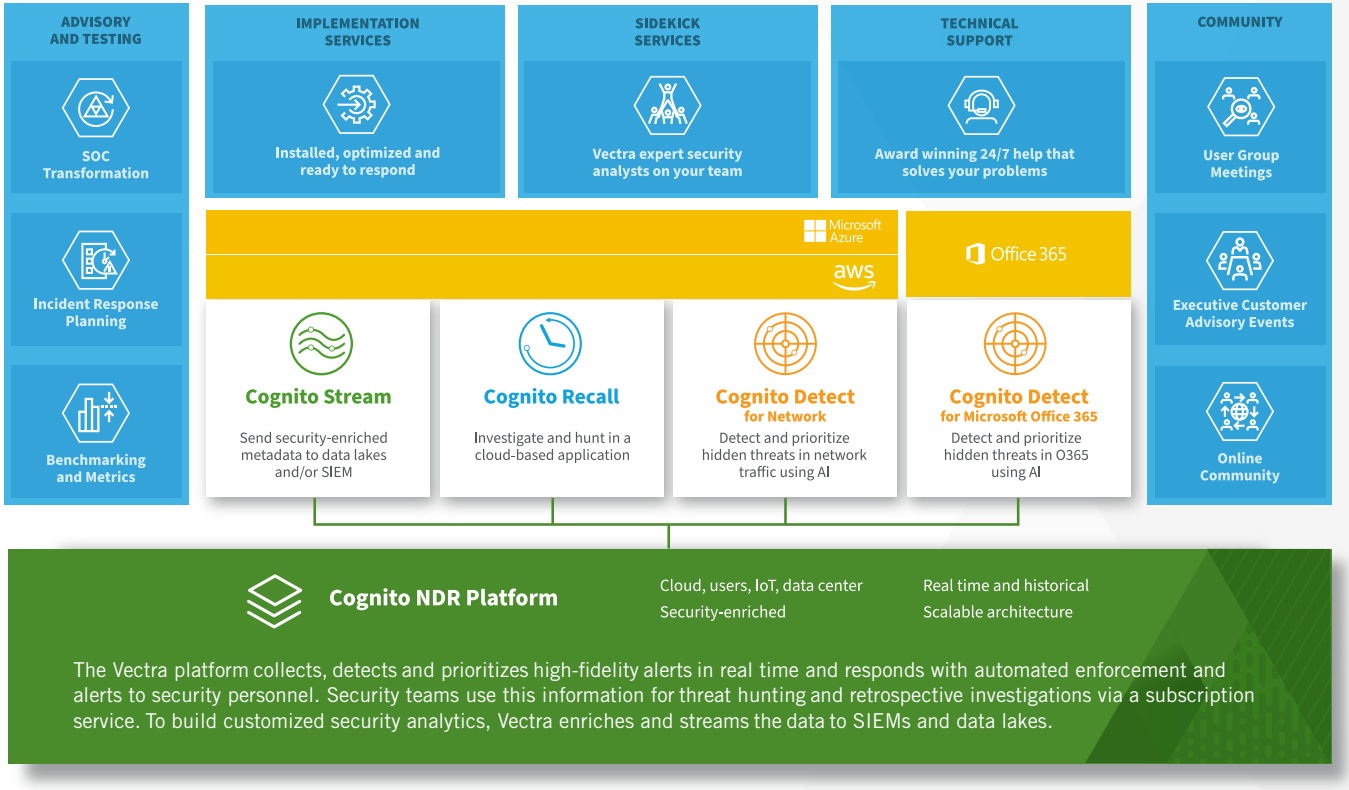
Launch deeper and broader investigations into incidents that are detected by the Cognito platform or third-party security solutions and successfully perform retrospective threat hunting with greater efficiency.

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, servers, host devices, accounts, and users.

Captures once and does many things

Access security-enriched network 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 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.

Cognito is the ultimate AI-driven NDR platform

Cognito Detect®: High-fidelity cloud, SaaS and NDR

Detect more – Eliminate alert fatigue and focus on what matters most with real-time attacker behavior detections

- **See** threat behaviors for unknown and known attacks by tracking internal reconnaissance and lateral movement.
- **Identify** host devices, workloads and accounts that are at the center of an attack.
- **Expose** stealthy low-and-slow attacks. The Cognito platform never rests and enables security teams to use their time to wisely.

Empower teams – Expand human expertise and increase speed by having AI do the thinking. Our security domain-based AI adds value to your security team.

- **Automate** a related chain of events into a single attack campaign to understand the scope and meaning, and prioritize threats based on risk and privilege.
- **Triage** the highest-risk threat detections automatically and mitigate attacks that pose the greatest risk to your organization – all in real time.
- **Investigate** behavior-based threat signals, not volumes of anomalies. Security context is instantly available for conclusive answers about threat behaviors.

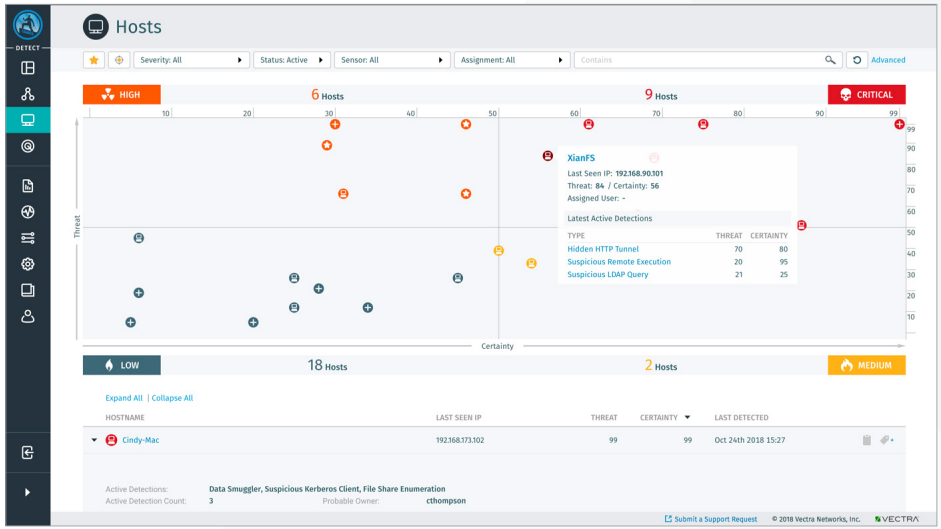
Address threats – Respond to in-progress threats with renewed confidence and precision while minimizing the impact on security workflows and business operations.

- **Respond** with accurate and high-confidence signals and eliminate the noise that causes false positives.
- **Enforce** signals from threat behaviors based on user identity and host device – intelligently at the source.
- **Add value** to existing investments by sharing enforcement data from Cognito with your third-party security solutions.

Cognito Detect® for Office 365: Detect and stop data breaches

Widespread threat coverage – Stop data breaches by detecting threats in Office 365 attack vectors and leveraging AI to identify malicious behaviors and hijacked privileges.

- **Deploy** in minutes with a cloud-native approach that quickly starts to monitor, detect and stop attacks.
- **Regain** comprehensive security coverage between Office 365 and your local enterprise infrastructure.
- **Stop** unknown and known attacks and account takeovers in real time before they lead to data breaches.



Cognito Recall®: The SaaS threat-hunting and investigative workbench

Hunt – Perform AI-driven threat hunting and retrospective threat hunting using behavioral detection algorithms derived from security domain-tailored machine learning.

- **High-fidelity** data from machine learning-derived, security-enriched metadata – no packet captures or NetFlow.
- **Visibility** using cloud logs and API calls. Integrate and share data with other security solutions – not just connectivity attributes.
- **Data-driven hunting** with insights based on devices, privilege, identity, host names, and workloads – not solely IP addresses.

Investigate – Speed-up investigations by correlating threat-behavior data with host devices and workloads. The right information is always at your fingertips.

- **Instant security insights** give organizations complete visibility into relevant host activities and behaviors.
- **Observe and understand** common threads between compromised host devices, accounts and assets.
- **Complete views** of attack progression and campaigns help identify other issues related to the attack.

Expose – Gain complete visibility into unseen security vulnerabilities and gaps in regulatory and compliance mandates.

- **Identify** and categorize gaps in compliance to meet government and corporate regulatory directives.
- **Visualize** and report on security-policy posture with unique Vectra data that is not available in other products.
- **Extend and enhance** security and compliance through recurring assessments, detailed reports, and other Vectra services.

Cognito Stream®: Security-enriched network metadata streamed to SIEMs and data lakes

Actionable data – Our network metadata is enriched with security insights and context so you can build custom tools and feed models to improve detections, investigations and hunting.

- **Hundreds of relevant metadata attributes** are collected from all traffic in cloud, data center, IoT, and enterprise networks.
- **Security insights and context** from machine learning-derived models are embedded to make the data very useful.
- **Conclusive investigations** can be based on host devices and identities – you're not limited to only IP addresses.

Limitless scale, no overhead – Delivered in an open-source Zeek format, it streams security insights into data lakes and SIEMs – without the overhead and scaling limits of Zeek.

- **Compatible** data is presented in a compact, easy-to-understand Zeek format.
- **Maintenance-free** operation require zero performance tuning.
- **High-performance** with over five-times the horsepower of self-managed deployments.

Extensive correlation – All detected threats are correlated across the entire data infrastructure, including cloud and data center workloads as well as IoT and enterprise networks.

- Support multiple deployment scenarios – hybrid, cloud-native and SaaS.
- Integrate with infrastructure-as-a-service (IaaS) providers without using agents.
- Improve threat detections and hunting in cloud, data center, IoT, and enterprise networks.

Vectra services and support

Vectra Advisory Services – Get strategic advice from security experts to strengthen SOC capabilities, improve security posture and enhance incident response.

- **Transform** your SOC with Vectra consultants, who will improve the agility and performance of your security analysts.
- **Measure and compare** your detection and response performance with relevant metrics from other Cognito NDR deployments.
- **Experience** real-world attack scenarios and learn how to detect and respond quickly to avoid a catastrophic data breach.

Vectra Implementation Services – Access our dedicated team of security and network experts, who will guide you through the rollout process of the Cognito NDR platform.

- **Design and architect** the Cognito NDR platform deployment based on your network topology and traffic flows.
- **Install** Cognito and **train** your security team about the fundamentals skills that are required to fully leverage the platform.
- **Analyze** traffic flows to all Vectra sensors to optimize the health of flows and improve Cognito platform performance.

Vectra Sidekick Services – Extend the value of your Cognito investment. Work with experts who meticulously analyze your deployment results to strengthen security posture.

- **Investigate and report** on threat events detected by your Cognito platform and identify relevant events in your organization.
- **Proactively notify** your team about critical detections, hosts and Priority 1 events that require immediate attention and response.
- **Fine-tune** your Cognito platform by creating filters for authorized behaviors and making your triage process more effective.

Vectra Technical Support – Our technical support team has in-depth knowledge and expertise about the Cognito platform and its operational use in customer environments.

- **Access** weekday support with a four-hour response. Support for critical issues is available 24 hours a day, every day.
- **Receive** timely software updates. Due to unmatched reliability, most hardware issues are quickly resolved without replacement.
- **Proactively monitor** cloud-connected instances to avoid health issues. Alerts that exceed thresholds trigger an investigation.

For more information please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai