VECTRA
SECURITY THAT THINKS.®

DATA SHEET

Cognito Stream: Network metadata with an opinion

Cognito Stream™ from Vectra® delivers scalable, security-enriched metadata from native cloud, hybrid cloud and enterprise traffic that empowers skilled security analysts and threat hunters to perform conclusive incident investigations.

Security data today is broken. NetFlow is incomplete while PCAPs are storage and performance intensive. Organizations that choose to deploy and maintain open-source Zeek must face the resource- and time-intensive effort of hardware assembly and configurations, software configurations, and building integration into existing tooling. This leaves security practitioners in an untenable state.

With Cognito Stream, security teams are empowered with the rich network context necessary to build custom tooling as well as feed models to detect, investigate and hunt. Delivered in open-source Zeek format, it seamlessly integrates security insights into data lakes and SIEMs without the overhead and scale limitations that accompany open-source Zeek.

The metadata from Cognito Stream is enriched with host identity, enabling investigations based on device names rather than just IP addresses. This eliminates the need to search DHCP logs in parallel to find the device using an IP address at specific times, and to track the changes in the device's IP address for the period of time relevant to an investigation. Searching by device name saves time when speed is crucial. Security insights embedded in the metadata provide threat hunters with intelligence for investigations and threat hunting.

Security-enriched cloud and network metadata streamed to SIEMs and data lakes ready for your own custom models

HIGHLIGHTS

- Forward searchable metadata in Zeek format to the data store of your choice with Kafka, syslog and Elastic support
- Metadata enriched with security insights to simplify investigations
- Build custom tools and models to detect, investigate and hunt
- Leverage all existing Zeek tooling
- Correlate cloud and network metadata with data from hosts and devices in your data lake (e.g.,application logs, processes, memory)
- Deployment simplicity – no performance tuning or ongoing maintenance needed
- More than five-times the single- sensor performance of Zeek

Empower threat hunting and incident investigation

- **Actionable network data in Zeek format.** Cognito Stream extracts hundreds of metadata attributes collected from the cloud to enterprise and presents them in a compact, easy-to-understand Zeek format that leverages all existing tooling. Stream provides the details analysts need, compared to NetFlow, without the storage complexity of full packet capture.
- **Embedded security insights.** Security insights generated by machine learning are embedded in the metadata (e.g. beaconing activity, domain rarity) to provide powerful building blocks threat hunters can combine with their own unique expertise to quickly reach conclusions.
- **Cognito Stream also leverages Privileged Access Analytics** to automatically analyze behaviors and uses artificial intelligence to identify entities that have privilege and differentiate between approved and malicious uses. It is available across the Vectra Cognito platform as searchable security enrichments in Cognito Stream and Cognito Recall and as detections in Cognito Detect. Custom use-cases are also supported by accessing its attributes through the Cognito REST API.
- **Investigations based on hosts, not IP addresses.** Cognito Stream 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 among groups of hosts.
- **Set-and-forget ease of use.** Cognito Stream sets up in less than 30 minutes, requires no performance tuning or ongoing maintenance,and delivers more than five times the single-sensor performance of Zeek. As a result, security teams can focus on investigations and avoid the management overhead of open-source Zeek.

The Cognito platform

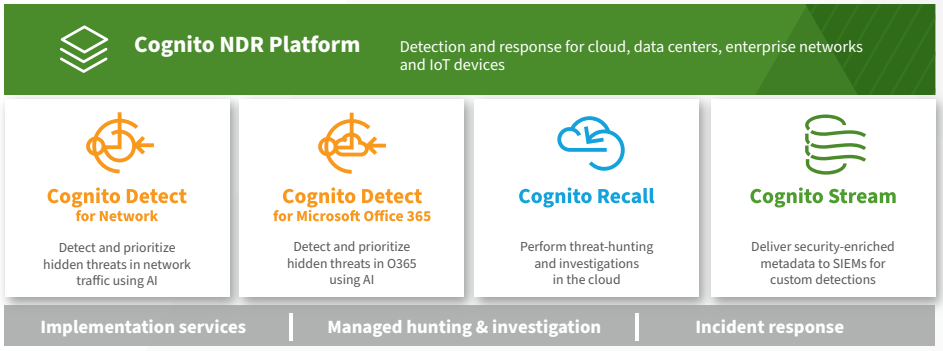
The right data with the right context

Vectra is the leader in network detection and response. Vectra is revolutionizing network security with the Cognito® platform that replaces legacy technology which fails to solve today's detection and response challenges – from cloud and data center workloads to user and IoT devices.

The Cognito platform accelerates customer threat detection and investigation using sophisticated artificial intelligence to collect, store and enrich network metadata with the right 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 physical, virtual and cloud sensors to provide 360-degree visibility across cloud, data center, user and IoT networks.

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 and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed.



How Cognito Stream works

Forward enriched metadata to data lakes

Cognito Stream provides visibility into network traffic by extracting metadata from all packets and storing it in your data lake or SIEM for correlation, search and analysis. Every IP-enabled device on the network is identified and tracked.

This visibility extends to servers, laptops, printers, BYOD and IoT devices as well as all operating systems and applications, including traffic between virtual workloads in data centers and the cloud. The metadata includes connectivity and details across the protocols critical for threat hunting and investigating incidents.

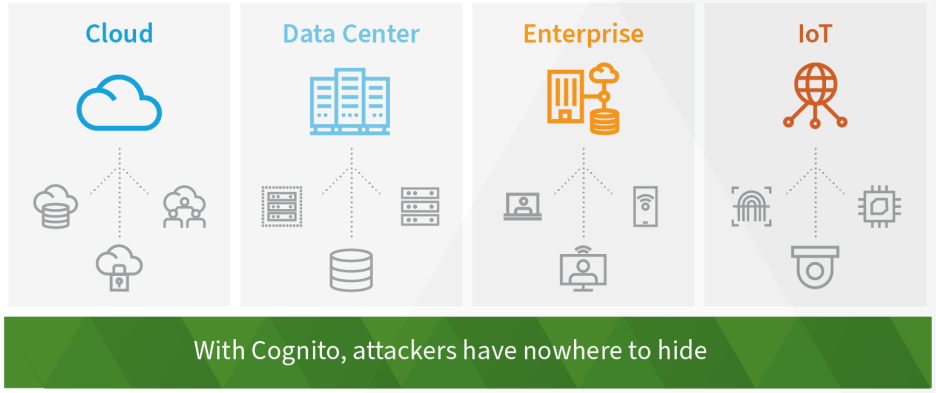
Metadata is captured from all internal (east-west) traffic, internet- bound (north-south) traffic, virtual infrastructure traffic and traffic in cloud computing environments. Cognito Stream forwards searchable metadata to data lakes with Kafka, syslog, and Elastic support.

Simplified deployment using the Cognito platform

Organizations can deploy the Cognito platform in 30 minutes or less and start hunting for threats or investigating incidents without the operational overhead of managing the sensor infrastructure:

- Physical and virtual sensors collect metadata from different parts of the network, such as the campus, data center and cloud.

The sensors connect to a central entity ("Brain") that de-duplicates the flows and runs the host identification and enrichment algorithms. Cognito Stream is deployed as an on-premises virtual machine (VM). The VM normalizes the metadata into Zeek-format and delivers it to a data lake or SIEM that can be running on-premises or in the cloud.



Threat hunting

Indicators of compromise (IoCs) are found in the course of an analyst's daily workflow or learned from open source intelligence being shared or internal research. Searching enriched network metadata for IoCs enables an analyst to search retrospectively for IP addresses, domains, URLs, hashes and SSL certificates used in the course of a cyberattack. With long-term metadata retention, searching for high-value IoCs is very powerful.

Correlate network and host data

Effective threat hunting is achieved with total visibility over the IT assets, risks, and flows within an organization's network. The data needed for this type of visibility break down into three categories:

- Network metadata has visibility into all communications between hosts, describing the interactions of entities, such as users, devices, workloads, IP addresses and domains across a network. Using these interactions, threat hunters can identify an adversary's activities within the network.
- Host data provides visibility to events that occur on the hosts within its environment, including user account activity and system processes.
- Application datasets are events logged by the programs running in the environment.

Network metadata provides an analyst with a high-level view of patterns and events as they occur across an entire network.

Host and application data (combined into device data) provides an analyst with granular, low-level details to behaviors at the host level including system processes and memory access.

Combined, these datasets provide a comprehensive map of the enterprise, giving a multilevel view of what might be going on. These datasets are most effectively used in tandem by hunters to detect advanced threats.

Build custom tools and models to detect, investigate and hunt

With custom detections, an analyst can monitor events for any kind of behavior such as suspicious or emerging threats, compliance violations, internal misuse or industry-specific attack vectors. Security insights in Cognito Stream provide machine-learning building blocks embedded in the metadata that can be combined with other attributes to create powerful custom models correlated to a specific host, or user account.

Conclusive incident investigations

Cognito Stream enables security analysts to conduct deeper, more conclusive incident investigations in an existing data lake or SIEM with remarkable efficiency.

By leveraging enriched network metadata, security analysts can easily follow the chain of related events from attack detections found by Cognito Detect, third-party security products, and searchable, high-quality threat intelligence in historical network metadata.

When incidents are reported by the Cognito Detect application or third-party security products, Cognito Stream ensures that security analysts have a complete 360-degree view of all workload and device activity.

With Cognito Stream, security analysts can investigate incidents with unprecedented efficiency using complete context about the transactions across the network, along with relevant details about associated devices, accounts and network communications.

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

Email info@vectra.ai vectra.ai