VECTRA®

Cognito Recall is the most efficient way to hunt for threats

HIGHLIGHTS

- Provides high-fidelity visibility from cloud to enterprise by collecting and storing security-enriched network metadata, relevant logs and cloud events in real-time.
- Perform retrospective threat hunting using security-enriched network metadata.
- Dive deep into incidents triggered by security tools to identify other host devices, accounts and external actors involved in an incident.
- Store and search metadata for as long as it is needed with cloud-powered limitless scale.

A cornerstone of the Cognito® cyberattack-detection and threat-hunting platform, Cognito Recall™ from Vectra® provides the most efficient way to perform AI-assisted threat hunting in cloud and data center workloads and user and IoT devices.

A comprehensive source of security-enriched network metadata, Cognito Recall also empowers skilled security analysts and professional threat hunters to conduct conclusive incident investigations.

The metadata in Cognito Recall is organized by host name, not just IP address. This eliminates the need to search through DHCP logs to find the host device that was using an IP address at the time and to piece together IP address changes during an investigation. Searching by device saves time when speed is essential.

Cognito Recall 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.

Cognito Recall enables incident responders to follow the chain of events from an initial threat signal – whether from Cognito Detect™, another security event or threat intelligence – using security-enriched network metadata that is searchable by host name.

Cognito Recall is like a transactional record of every conversation from the cloud to the enterprise. But the collection and storage of historical metadata, instead of packet payloads, ensures data privacy and supports compliance mandates like GDPR.

And since Cognito Recall is delivered as a service in the cloud, there's no big data infrastructure to purchase, install and manage. Just a single click to forward metadata to the Vectra cloud.

Summary of capabilities

- **Empowers threat hunters** with real-time collection and storage of security-enriched network metadata, relevant logs and cloud events, enabling them to leverage their deep knowledge of advanced cyberattacks.
- **Enables intelligent investigation of device activity** by associating devices, workloads and host names, regardless of IP address changes.
- **Provides infrastructure-wide visibility** into the actions of all cloud and data center workloads and user and IoT devices.
- **Delivers cloud-powered limitless scale** to store and search metadata for as long it is needed while Vectra manages the infrastructure.

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

The power to Detect and Recall

Cognito Recall allows security analysts to perform in-depth investigations based on the high-fidelity, actionable incidents identified by Cognito Detect, which automates AI-driven cyberattack detection and response.

With Cognito Recall, senior security analysts can also perform threat hunting based on alerts from third-party security solutions and use new, high-quality threat intelligence to hunt retrospectively.

	CYBERATTACK DETECTION	INVESTIGATION AND AI-ASSISTED HUNTING
Product	Cognito Detect	Cognito Recall
Goal	Identify compromised hosts as an investigation starting point	Manually investigate; Find threats that detection has missed
Scope	Initial detection → Validate detection	Complete investigation
Needs	Real time; High-fidelity signal; and Automation	360-degree view of historical metadata; Efficient search

How Cognito Recall works

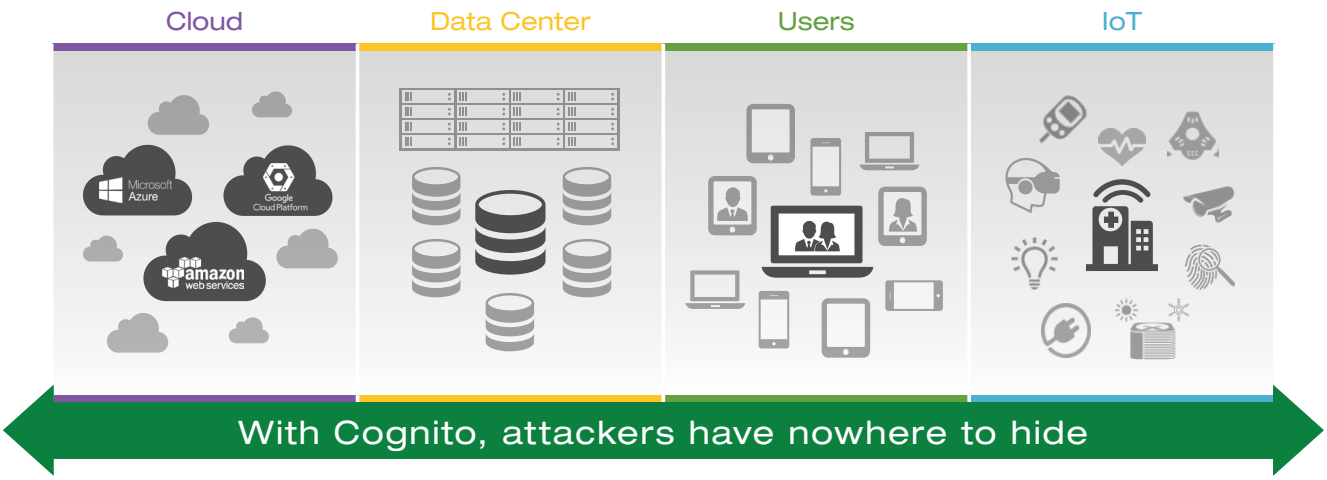
High-fidelity visibility across the enterprise

Cognito Recall provides visibility into network traffic by extracting metadata from all packets and storing it in the cloud for search and analysis. Every IP-enabled device on the network is identified and tracked and data can be stored for any amount of time.

Captured metadata includes all internal (east-west) traffic, internet-bound (north-south) traffic, virtual infrastructure traffic, and traffic in cloud computing environments.

This visibility extends to laptops, servers, printers, BYOD and IoT devices as well as all operating systems and applications, including traffic between virtual workloads in data centers and the cloud, even SaaS applications.

System, authentication and SaaS logs provide context enrichment to network metadata analysis for accurate identification of systems and users.



Cognito Recall collects security-enriched network metadata from the cloud to user and IoT devices

Threat hunting

AI-assisted threat hunting with Cognito Recall can be triggered by attacker detections from Cognito Detect, existing indicators of compromise and anomalies in data identified by security analysts.

Hunt using indicators of compromise

With full metadata search capabilities and limitless data storage, Cognito Recall enables security analysts to determine whether indicators of compromise exist in metadata, including user agents, IP addresses and domains.

Cognito Recall also delivers in-depth information for more efficient threat hunting, such as PowerShell commands from a remote machine to a server or a specific type of connection from a remote site.

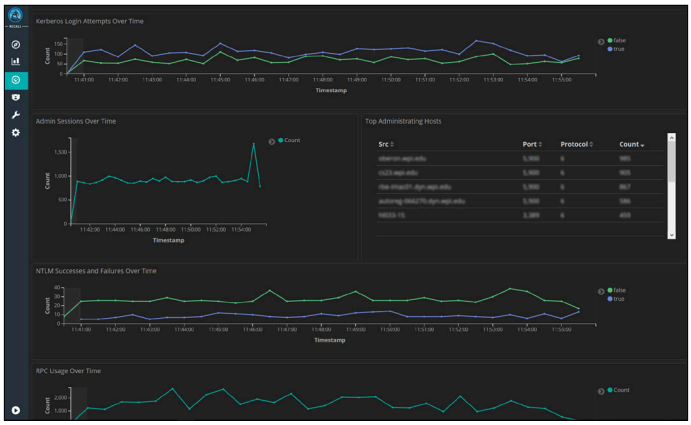
Cognito Recall provides full metadata search capabilities and limitless data storage

Hunt for anomalous behaviors

Cognito Recall enables professional threat hunters to identify anomalous behaviors that are displayed through visual graphs. Anomalous behaviors that can be exposed using Cognito Recall include:

- Atypical use of TCP and UDP ports and applications
- Unusually high connection rates
- Heuristic indicators
- New beaconing activity
- Volumetric thresholds for connection counts, login failures and excessive internal and external data transfers

In some instances, anomalies could consist of any combination of these behaviors, such as unusual amounts of data sent to an uncommon IP address.



Cognito Recall enables threat hunters to identify anomalous behaviors

Conclusive incident investigations

Cognito Recall enables security analysts to conduct deeper, more conclusive incident investigations with remarkable efficiency.

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 events or alerts are received from Cognito Detect or third-party security products, Cognito Recall ensures that security analysts have a full 360-degree view of all workload and device activity.

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

Host-based investigations

Cognito Recall allows security analysts to identify the activity of host devices surrounding the time of a threat detection and reveal significant changes in the overall behavior of host devices.

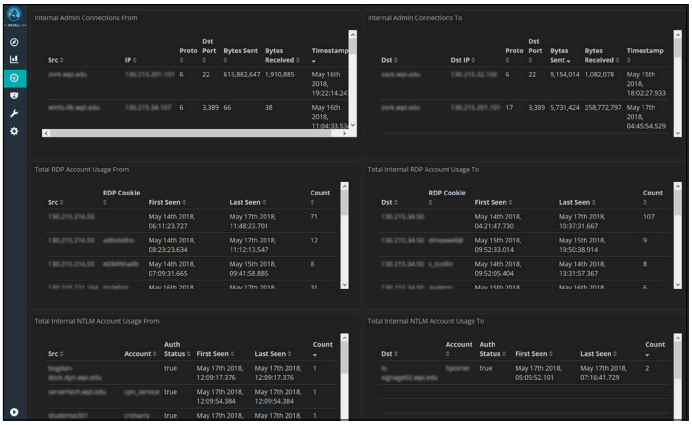
Through visual graphs and search capabilities, Cognito Recall exposes other host devices, accounts, and external domains and IP addresses, which enables security analysts to identify the full scope of the incident.

Security analysts can easily sequence through a wide range of suspicious behaviors to identify the trail of evidence that leads to other host devices and efficiently search for indicators of compromise along the way.

Account-based investigations

Cognito Recall enhances account-based investigations by providing the details that security analysts require to identify all uses and actions of potentially-compromised accounts in specific timeframes as well as actions against targets.

By leveraging Cognito Recall, security analysts are also presented with a broader picture of an overall cyberattack, which can be instrumental during investigations into other host devices that might have compromised accounts.

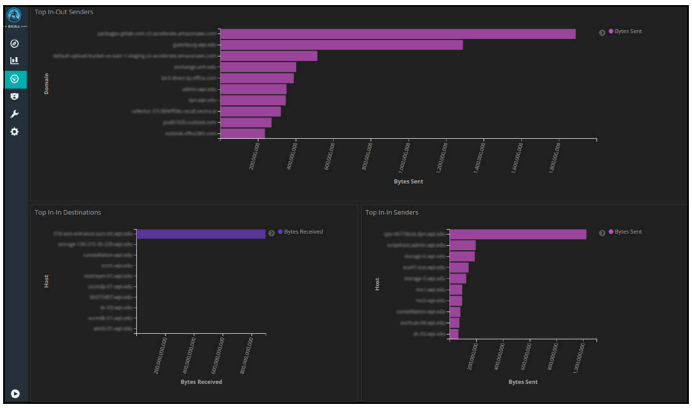


Cognito Recall shows details that enhance account-based investigations

Target domain and IP address investigations

Once the compromised host device at the center of an attack is identified, it is important for security analysts to understand what other host devices are communicating with a malicious domain or IP address used in an attack.

Cognito Recall tracks all outbound and inbound communication so security analysts can determine the host devices that have communicated with the same domain or IP address over a specific timeframe, including what occurred during the communication.



Cognito Recall tracks all outbound and inbound communication from host devices

Greater context about attacker behaviors

When investigating cyberattack behaviors identified by Cognito Detect, it can be useful to have greater understanding about the details of all network activity that occurred during the incident.

By pivoting with one click between Cognito Detect and Cognito Recall, security analysts gain deeper, more meaningful context about malicious network communications.

Cognito Detect provides information about specific attack behaviors and compromised host devices involved in an attack while Cognito Recall enables security analysts to search stored data about network communications that occurred in the same timeframe as the attack.

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