VECTRA®

Threatscape

Cognito Detect is the most powerful way to find and stop cyberattackers in real time

HIGHLIGHTS

- Always-learning behavioral models use AI to find hidden and unknown attackers, enable quick, decisive action, and provide a clear starting point for AI-assisted threat hunting.
- Detects known threats by using AI and integrating other critical sources of threat intelligence.
- Analyzes enriched network metadata, relevant logs and cloud events to gain high-fidelity visibility into cyberattacker behaviors in all cloud and data center workloads and user and IoT devices.
- Unique context eliminates the endless hunt-and-search for threats and enables immediate action by proactively putting the most relevant information at your fingertips.
- Works with EDR, NAC firewalls and other enforcement points to block new classes of threats.
- Provides a clear starting point for more extensive investigations with Cognito Recall, SIEMs and forensic tools.

A critical part of the Cognito™ cyberattack-detection and threat-hunting platform, Cognito Detect™ from Vectra® is the fastest, most efficient way to find and stop cyberattackers in public clouds, private data centers and enterprise environments. It uses artificial intelligence to deliver real-time attack visibility and put attack details at your fingertips.

In addition to empowering quick, decisive action in response to in-progress attacks, Cognito Detect provides a vital starting point for professional threat hunters that use Cognito Recall™ for deeper investigations.

By combining advanced machine learning techniques – including deep learning and neural networks – with always-learning behavioral models, Cognito Detect quickly and efficiently finds hidden and unknown attackers before they do damage.

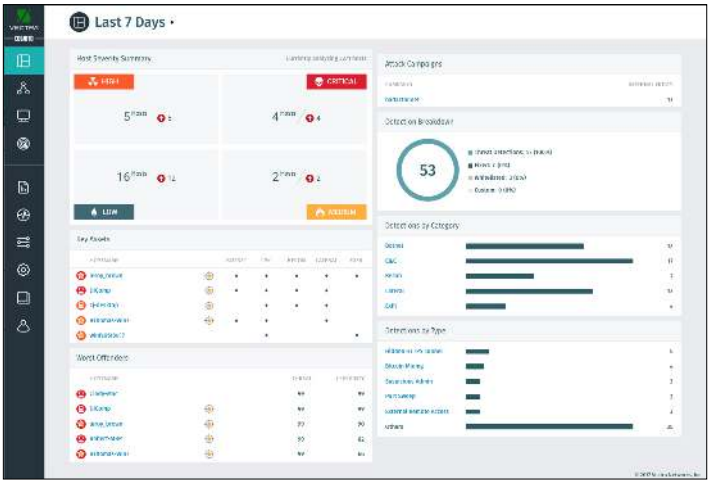
Cognito Detect provides enterprise-wide visibility into hidden cyberattackers by analyzing all network traffic and logs from security systems, authentication systems and SaaS applications. This leaves attackers with nowhere to hide – from cloud and data center workloads to user and IoT devices.

As part of the Cognito Detect subscription, software updates with new threat detection algorithms are delivered to customers on a regular basis to ensure they are continuously protected from the latest advanced threats.

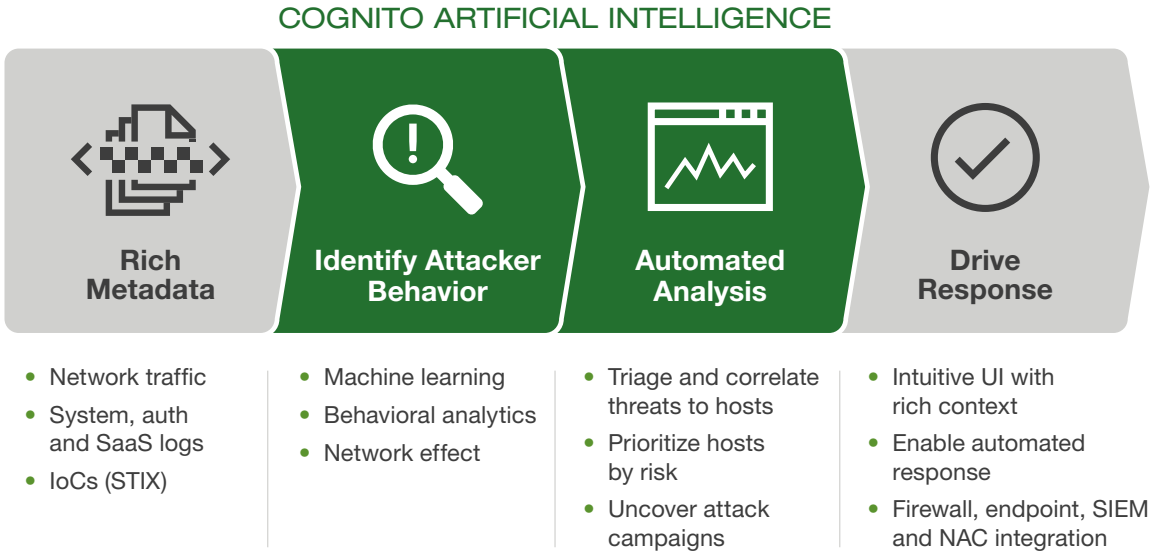
Security analyst in software

Cognito Detect automates the hunt for cyberattackers, shows where they're hiding and tells you what they're doing. The highest-risk threats are instantly triaged, correlated to hosts and prioritized so security teams can respond faster to stop in-progress attacks and avert data loss.

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



Attacker detections are instantly prioritized, scored and correlated to compromised host devices



By automating the manual, time-consuming analysis of security events, Cognito Detect condenses weeks or months of work into minutes and reduces the security-analyst workload on threat investigations by 32X.

This enables security operations teams that are understaffed and under siege to stay ahead of cyberattackers and respond faster to hidden threats.

How Cognito Detect works

Rich metadata

Cognito Detect gives you real-time visibility into network traffic by extracting metadata from packets rather than performing deep packet inspection, enabling protection without prying.

Metadata analysis is applied to all internal (east-west) traffic, Internet-bound (north-south) traffic, virtual infrastructure, and cloud computing environment. Cognito Detect identifies, tracks, and scores every IP-enabled device inside the network.

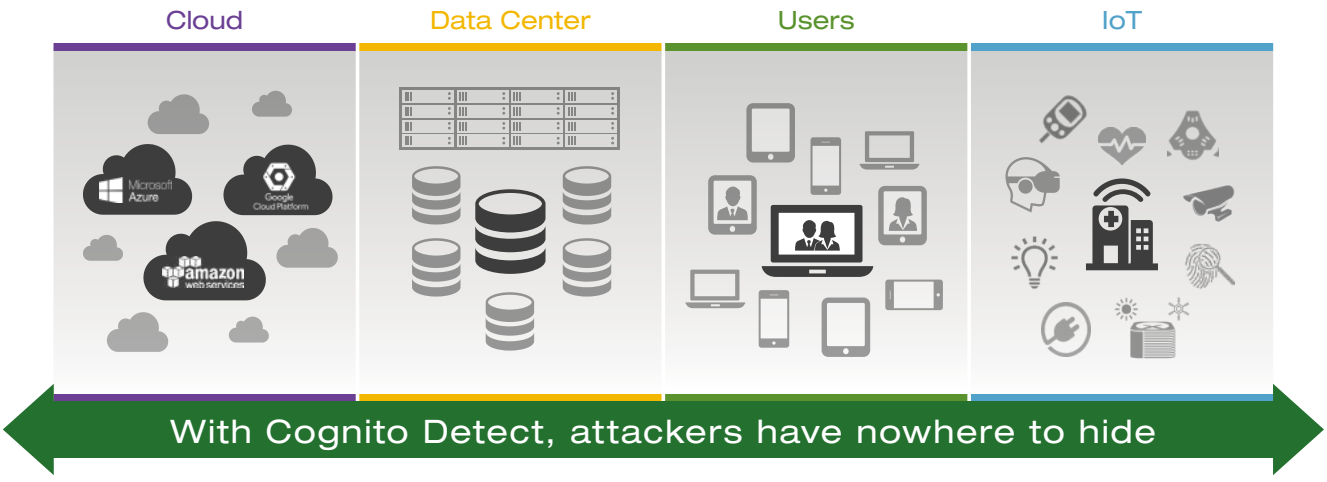
This visibility extends to laptops, servers, printers, BYOD and IoT devices as well as all operating systems and applications, including traffic between virtual workloads in data centers and the cloud, even SaaS applications.

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

Cognito Detect uses STIX threat intelligence to detect threats based on known indicators of compromise derived from threat intelligence. These are correlated with other attacker behaviors to ensure pinpoint accuracy of host threat and certainty scores to prioritize risk.

Identify attacker behaviors

The collected metadata is analyzed with behavioral detection algorithms that spot hidden and unknown attackers. This exposes fundamental attacker behaviors in network traffic, such as remote access tools, hidden tunnels, backdoors, credential abuse, and internal reconnaissance and lateral movement.



Cognito Detect provides threat detection coverage across the entire enterprise

Cognito Detect continuously learns your local environment and tracks all physical and virtual hosts to reveal signs of compromised devices and insider threats. A wide range of cyberthreats are automatically detected in all phases of the attack lifecycle, including:

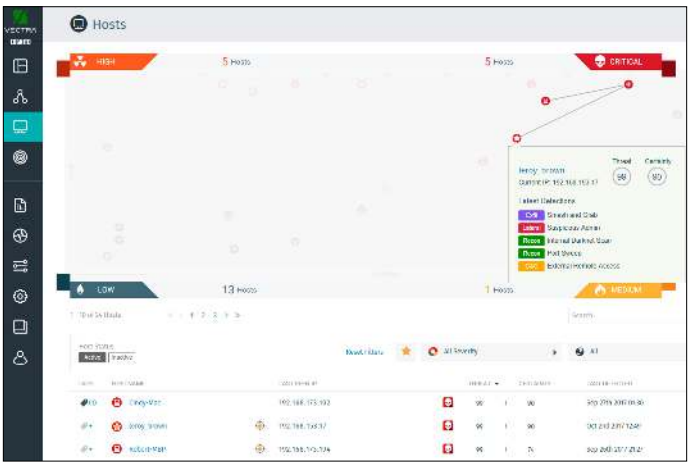
- Command-and-control and other hidden communications
- Internal reconnaissance
- Lateral movement
- Abuse of account credentials
- Data exfiltration
- Early indicators of ransomware activity
- Botnet monetization
- Attack campaigns, including the mapping of all hosts and their associated attack indicators

Cognito Detect also monitors and detects suspicious access to critical assets by authorized employees, as well as policy violations related to the use of cloud storage, USB storage and other means of moving data out of the network.

Automated analysis

The Threat Certainty Index™ in Cognito Detect consolidates thousands of events and historical context to pinpoint hosts that pose the biggest threat.

Instead of generating more events to analyze, Cognito Detect boils down mountains of data to show what matters most. Threat and certainty scores trigger notifications to your staff or a response from other enforcement points, SIEMs and forensic tools.



The Threat Certainty Index in Cognito Detect

The Attack Campaigns feature further automates security detections by connecting the dots of related attacker behaviors and exposing the relationship between hosts across internal detections, external advanced command-and-control detections, and connectivity to common command-and-control infrastructures.

As attackers perform reconnaissance and move laterally from host to host in a network, Cognito Detect correlates their behaviors across all involved hosts and detections and presents a synthesized view of the entire attack campaign.

Cognito Detect presents a synthesized view of an entire attack campaign

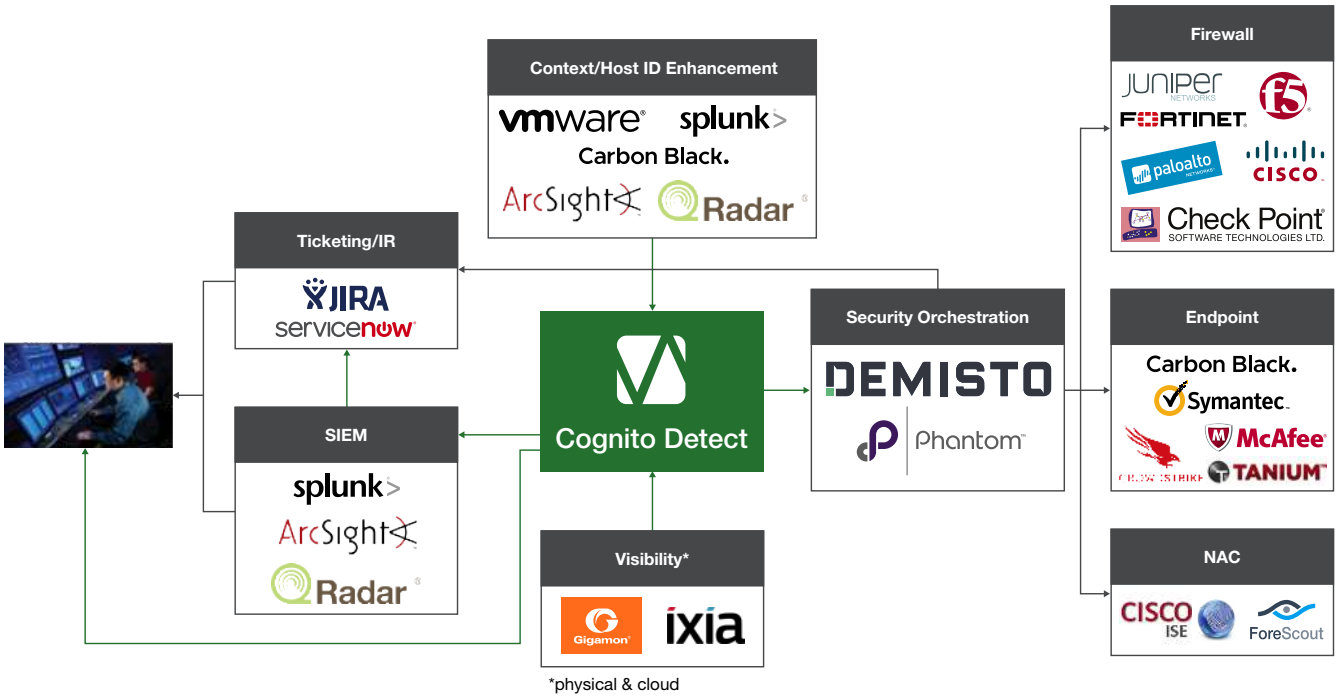
Cognito Detect pivots to show views of hosts or related campaign detections, and analyzes event history spanning its entire lifetime to better understand the activity and full scope of attack.

Drive response

Respond quickly and decisively to threats by putting the most relevant information and context at your fingertips. Unlike security analytics products, Cognito Detect eliminates manual investigations by automatically prioritizing and correlating threats with compromised hosts and key assets that are the target of an attack.

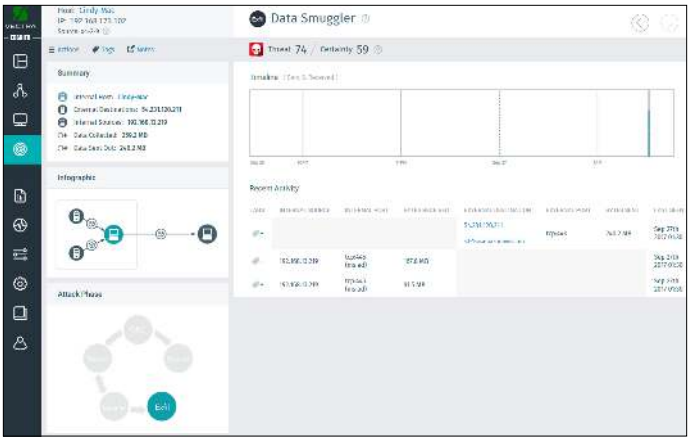
Cognito Detect puts threat detection details – including host context, packet captures, and threat and certainty scores – within immediate reach.

In addition, Cognito Detect works with your next-generation firewalls, endpoint security, NAC, and other enforcement points to automatically block unknown and customized cyberattacks. Cognito Detect also provides a clear starting point for threat investigations, which boosts the efficiency of SIEMs and forensic analysis tools.



Cognito Detect works with widely used security enforcement points, SIEMs and forensic analysis tools

Security that thinks®



Real-time detection of data exfiltration in progress

Security context that saves time

Cognito Detect unburdens and empowers security operations teams that are understaffed. This is achieved by automating the time-consuming analysis of security events and eliminating the need to endlessly hunt for hidden threats.

Each detection is explained in detail, along with the underlying event and historical context that led to the detection. Security analysts can instantly view a connection map of any host to see other hosts the device is communicating with and how.

Cognito Detect also provides on-demand access to enriched metadata from captured packets for further forensic analysis. This gives security teams the proof and accuracy they need to take immediate, decisive action.

Strengthen your existing security infrastructure

Whether providing the intelligence to block a new class of threat with firewalls, endpoint security, NAC and other enforcement points, or providing a clear starting point for a more extensive search with SIEMs and forensic tools, Cognito Detect gives you more value from existing security technologies.

Cognito Detect integrates with leading endpoint security solutions to automatically add enriched context to investigations and enables security operations teams to isolate compromised host devices.

A robust API enables automated response and enforcement with virtually any security solution. Cognito Detect also generates syslog messages and CEF logs for all detections as well as prioritized host scores. This makes Cognito Detect much more than just another source of logs and provides an ideal trigger for investigations and workflows within your SIEM.

Full lifecycle detection of ransomware

Cognito Detect identifies ransomware campaigns against enterprises and other organizations across all phases of an attack. By monitoring all internal network traffic, Cognito Detect identifies in seconds the fundamental behaviors of a ransomware attack as it attempts to take critical assets hostage.

In addition to detecting ransomware directly, Cognito Detect exposes ransomware precursors, including command-and-control traffic, network scans and spreading behavior that ransomware relies on to find and encrypt critical assets.

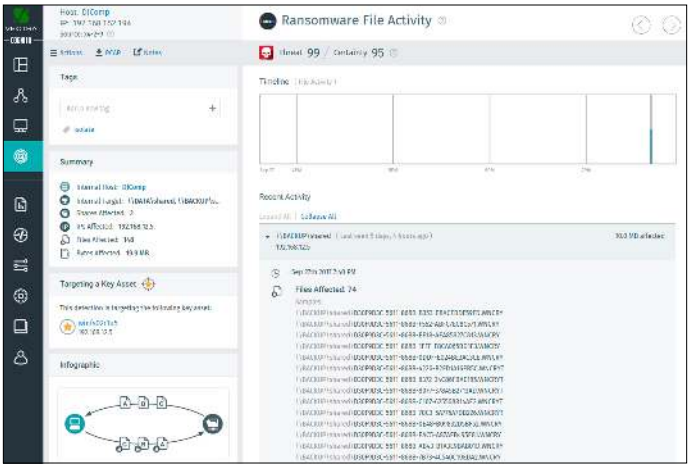
Watching the watchers

While attackers may initially compromise an end-user device, the real prize involves commandeering administrator or system credentials. Cognito Detect goes beyond simple user-behavior monitoring to detect signs of compromised administrators.

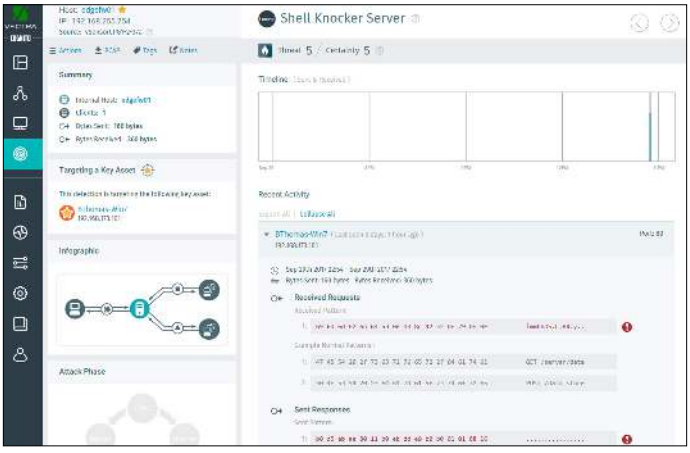
Cognito Detect tracks administrative protocols and learns the specific machines or jump systems that are used to manage specific hosts, servers and workloads. This vigilance quickly reveals when a cybercriminal attempts to use administrative credentials and protocols to escalate an attack on the network.

Native security for your private cloud

The private-cloud data center has become the heart and soul of many organizations, yet often remains a blind spot for security teams. Cognito Detect persistently monitors critical data center applications, data, and infrastructure with the ability to detect even the most sophisticated attacks.



The Cognito Detect ransomware detection



The Cognito Detect Shell-Knocker detection

Some 80% of data center traffic never leaves the data center and is not monitored by traditional perimeter-based security. Cognito Detect virtual sensors (vSensors) connect to any VMware vSwitch to ensure visibility into all traffic and detect threats passing between workloads in the virtual environment.

Cognito Detect also integrates with VMware vCenter to provide an authoritative, always up-to-date view of your virtual environment. In fact, Cognito Detect was the first to bring together the required visibility, context and intelligence to find advanced attacks inside the data center.

Security from hardware to workload

Data center security goes beyond virtualization and includes the physical server hardware and low-level tools used to manage the data center. Cognito Detect provides unprecedented threat detection that extends from the application layer down to the underlying hardware.

For example, the Cognito Detect Port Knocking detection reveals servers that are compromised by a rootkit, which could reside below the physical operating system itself. In addition, Cognito Detect monitors and detects the improper use of low-level management protocols such as IPMI and iDRAC.

Normally used by administrators for infrastructure-lights-out management of server hardware, these protocols are increasingly targeted by attackers because they give an always-on backdoor into the virtual environment yet are not logged and are rarely monitored by security.

Unifying data center operations

Modern data centers require constant coordination between networking, application development, virtualization teams, and of course, the security team. Cognito Detect makes it easy for all groups to remain in sync and retain full visibility into the virtual environment, even when workloads are constantly on the move.

Cognito Detect visually displays the connections between all workloads and the type of traffic flowing between them. With full VMware vCenter integration, Cognito Detect provides an always up-to-date view of the environment and alerts about any assets that are not monitored for threats.

VECTRA®
Security that thinks®

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

Threatscape

Email info@threatscape.com **Phone** 0203-653-0000 (UK) & 01-901-7000 (Ireland)
www.threatscape.com