VECTRA SECURITY THAT THINKS® | vmware® Carbon Black

SOLUTION BRIEF

Detect and mitigate cyberattacks with Vectra and VMware Carbon Black

The integration of Cognito® Detect from Vectra® with VMware Carbon Black Cloud™ Endpoint enables security teams to automate the detection of hidden cyberattackers in real time, while unifying network and endpoint context to quickly verify and isolate advanced threats in the enterprise.

Together, Cognito Detect and Carbon Black Cloud Endpoint solve the most persistent security problems facing enterprise organizations today: Finding and stopping active cyber attacks while getting the most out of limited time and manpower of IT security teams.

The need for a new approach to security

Modern cyberattackers can easily evade prevention security defenses at the network perimeter. Unable to rely solely on prevention defenses, security teams must manually investigate threats and sift through the noise in search of a weak signal.

In practice, this often means that cyberattacks are first detected and reported by an external third party, turning their discovery into a post-breach forensic drill rather than a proactive attack mitigation exercise.

The integration of Cognito Detect and CB Cloud Endpoint saves time and effort and allows security teams to take action before cyberattacks lead to data loss.

CHALLENGE

Today's cyberattackers are adept at evading prevention security defenses along the network perimeter, and security teams are often overloaded with inconclusive alerts and slow investigations.

Once attackers get inside the network, they often go undetected for many months – giving them plenty of time to steal key assets and cause irreparable damage and public embarrassment.

SOLUTION

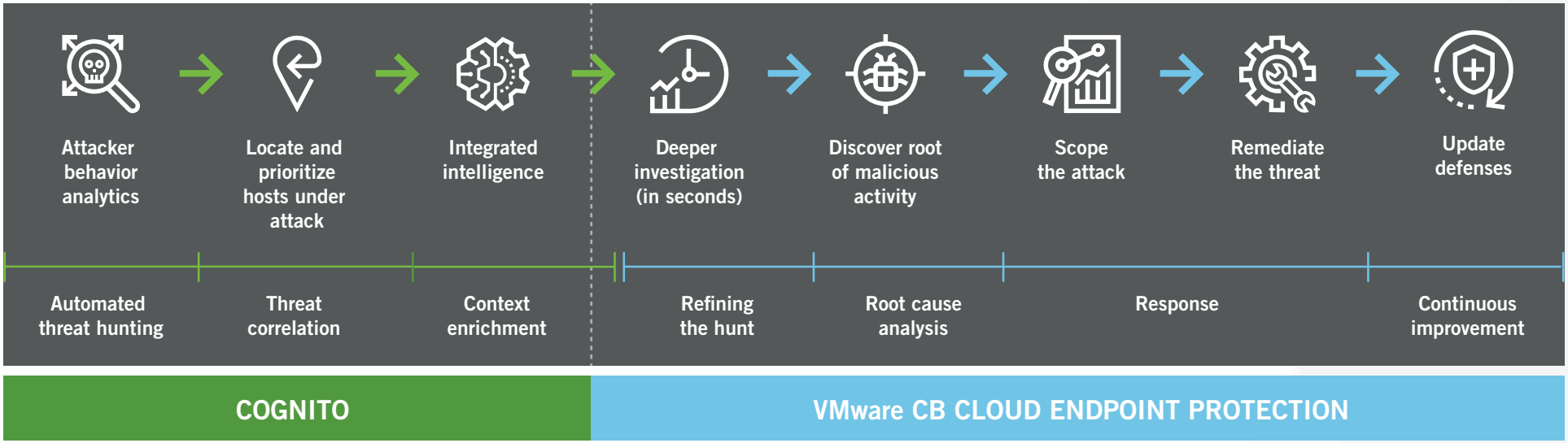
Cognito Detect from Vectra and CB Cloud Endpoint from VMware Carbon Black integrate two authoritative views of a cyberattack – the network and the endpoint. Cognito Detect analyzes all network traffic to automatically detect attack behaviors and prioritizes each one based on the risk they pose to your organization.

In addition to putting network-based threat context at your fingertips, Cognito Detect conveniently allows security teams to pivot into the endpoint context of CB Cloud Endpoint to perform additional investigation and isolate the compromised host device from the network.

This integration allows security teams to cover the network, endpoints, and the cloud for full visibility and coverage across workloads.

BENEFITS

The integration of Cognito Detect and CB Cloud Endpoint saves time and effort and allows security teams to take action before cyberattacks lead to data loss. Together, Vectra and VMware Carbon Black create an efficient security operations workflow that reduces response and investigation time, enabling security teams to quickly mitigate high-risk threats.



Automated, real-time threat hunting and remediation across the enterprise

A new model of threat detection

Cognito Detect from Vectra automates the detection of hidden cyberthreats by continuously analyzing all network traffic – from cloud and data center workloads to user and IoT devices – to detect the earliest signs of attacker behaviors.

In addition to automatically correlating detected threats with host devices that are under attack, Cognito Detect provides unique context about what attackers are doing and prioritizes threats that pose the biggest risk. This enables security teams to quickly focus their time and resources on preventing or mitigating loss.

Using artificial intelligence, Cognito Detect combines data science, machine learning and behavioral analytics to reveal the attack behaviors without signatures or reputation lists. Cognito Detect even exposes threats in encrypted traffic without using decryption.

Cognito Detect applies this intelligence to all phases of the cyberattack lifecycle, from command-and-control, internal reconnaissance, lateral movement, and data exfiltration behaviors.

This enables security teams to detect unknown, customized and known cyberattacks as well as threats that do not rely on malware, such as those carried out by malicious insiders and compromised users.

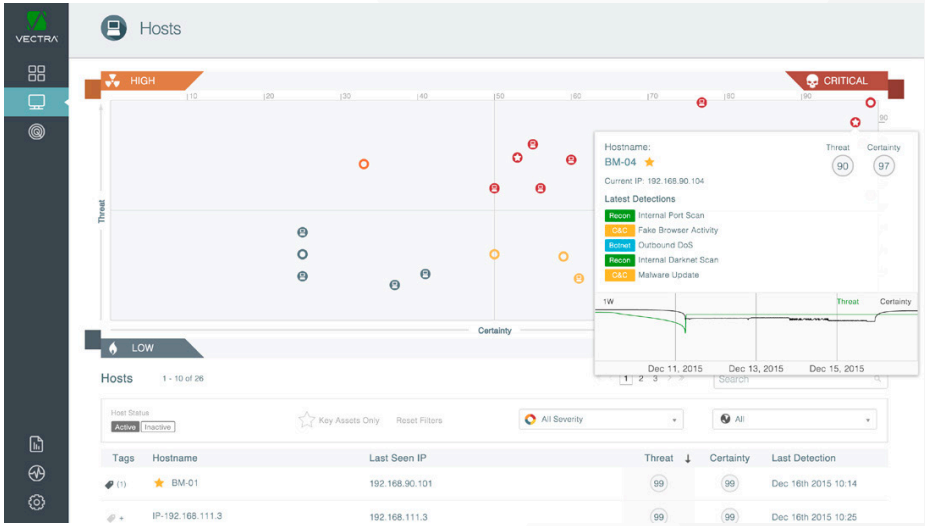
Easily integrate network and endpoint context

When a threat is detected, Cognito Detect and CB Cloud Endpoint provide security teams with instant access to additional information for verification and investigation. Host identifiers and other hose device data from VMware Carbon Black are automatically shown in the Cognito Detect UI.

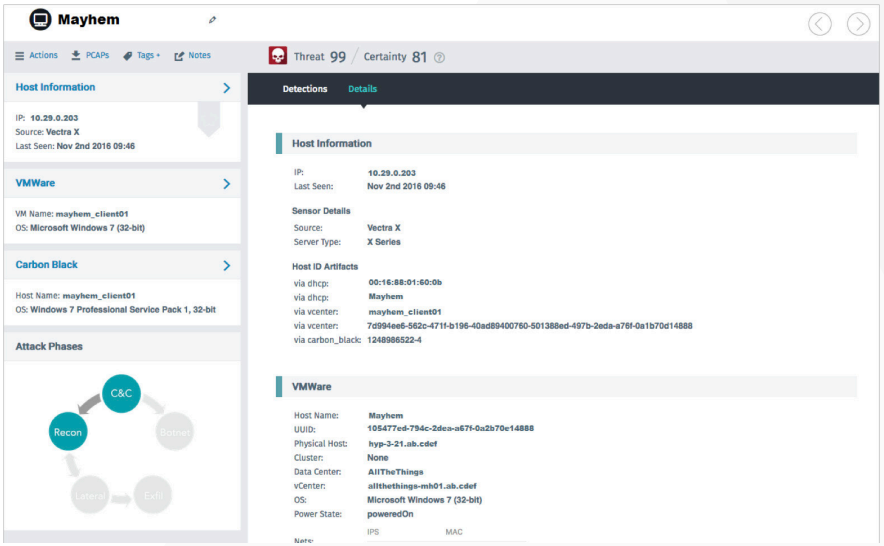
Next, a single click allows security teams to easily pivot between the Cognito Detect UI and the CB Cloud Endpoint UI for the same host device or to securely connect directly to the host device using the CB Cloud Endpoint Live Response capability.

CB Cloud Endpoint easily reveals traits and behaviors of a threat that are only visible inside the host device, while CB Cloud does the same for cloud workloads. This enables security teams to quickly and conclusively verify a cyberthreat while also learning more about how the threat behaves on the host device – or in the cloud – itself.

Cognito Detect from Vectra and CB Cloud Endpoint from VMware Carbon Black integrate two authoritative views of a cyberattack – the network and the endpoint.



Vectra shows threat-detection details of a specific host device and the progression of threat and certainty scores over time



Host identifiers and other host device data are shown in the Cognito Detect UI

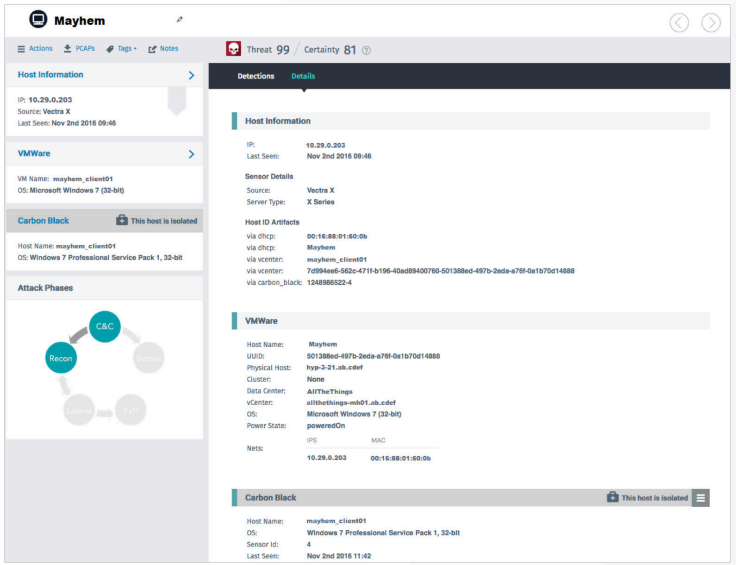
Take action with Lockdown

In addition to reducing the time to investigate threats, Cognito Detect and CB Cloud Endpoint let security teams take swift, decisive action. Armed with network and endpoint context, security teams can quickly isolate compromised host devices from the network to halt cyberattacks and avoid data loss.

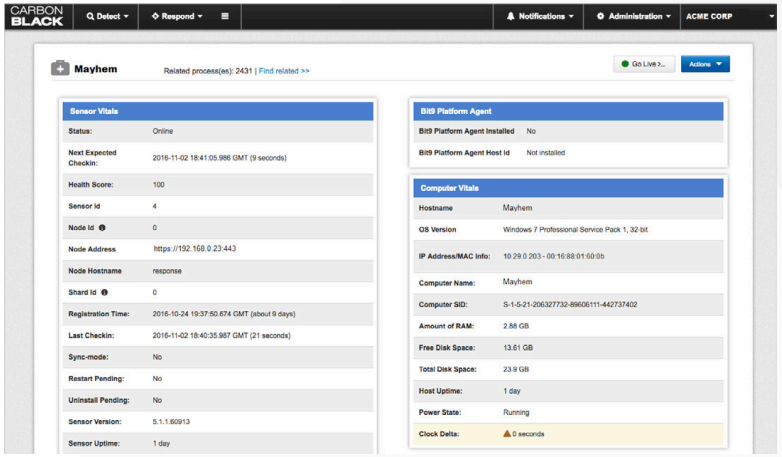
The Host Lockdown feature enables the Vectra Cognito platform to automatically disable hosts that demonstrate suspicious activity at the endpoint or through cloud apps. If analysts need to take matters into their own hands, they have the option to manually disable hosts during a security investigation. Disabling a host will significantly slow down an active attack by limiting an attacker's access to additional resources. This drastically curtails the attack's reach and gives the Security Operations Center (SOC) more time to investigate and remediate attacks.

Host Lockdown ensures that automation causes as little disruption as possible while giving you greater confidence that attackers are stopped in their tracks.

Together, Cognito Detect and VMware Carbon Black create an efficient security operations workflow that reduces response and investigation time, enabling security teams to quickly mitigate high-risk threats.



The Cognito Detect UI shows that VMware Carbon Black isolated a compromised host device that was initially detected and assigned threat and certainty scores by Cognito Detect



The VMware CB Cloud Endpoint Platform reveals traits and behaviors of a threat that are only visible inside the host device

About Vectra

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is Security that thinks®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

About VMware Carbon Black

VMware Carbon Black has designed the most complete next-gen endpoint-security platform, enabling organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The VMware Carbon Black Cloud™ Endpoint Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats.

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

Email info@vectra.ai vectra.ai