VECTRA SECURITY THAT THINKS® | FIREEYE™

SOLUTION BRIEF

Detect and stop cyberattacks with Vectra and FireEye

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.

A new model of threat detection

A new model of threat detection Cognito Detect from Vectra automates the detection of hidden cyberthreats by continuously analyzing all network traffic and cloud logs– 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.

When a threat is detected, Cognito Detect and FireEye provide security teams with instant access to additional information for verification and investigation.

CHALLENGE

Today's cyberattacks frequently evade preventative security defenses along the network perimeter and move laterally between cloud and hybrid environments with ease. Legacy security solutions are often ill equipped to handle this expanded perimeter and the modern attacks on it and cause an overload of inconclusive alerts and hamper investigations.

Once attackers gain access, they often go undetected for many months – which is plenty of time to steal key assets and cause irreparable damage and public embarrassment.

SOLUTION

Cognito Detect from Vectra and FireEye Endpoint Security integrate two authoritative views of a cyberattack – the network and the endpoint. Giving full visibility into modern hybrid cloud enviroments and the devices and accounts involved. Cognito Detect analyzes all network traffic and cloud logs to automatically detect attack behaviors and prioritizes each one based on the risk they pose to your organization. FireEye Endpoint Security protects both client and server endpoints with multi-engine defense and detects and enables response to affected endpoints.

In addition to putting network and cloud-based threat context at your fingertips, Cognito Detect conveniently allows security teams enrich detection with the deep endpoint context of FireEye provides to perform additional investigation and isolate the compromised host to stop an attack.

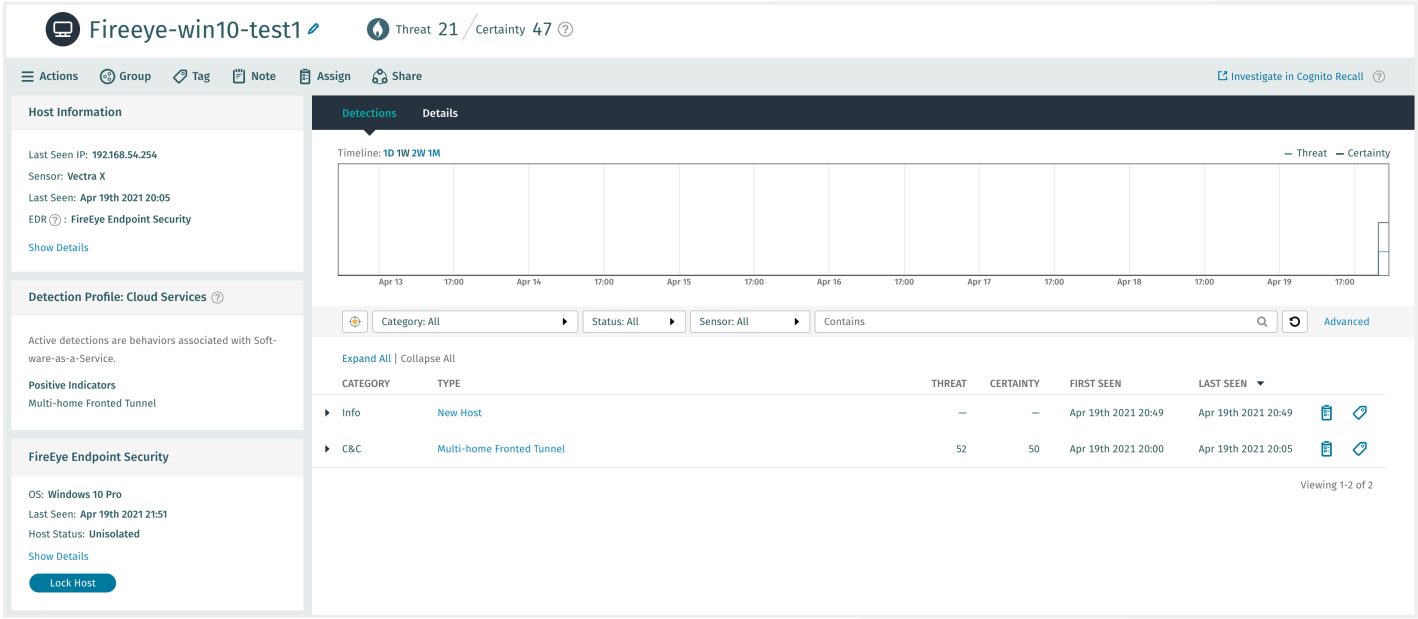
BENEFITS

The integration of Cognito Detect and FireEye Endpoint Security reduces valuable time between detection and response, reducing the time on investigating an alert. This combined solution also enables security teams to take manual or automated action before cyberattacks lead to data loss. Together, Cognito Detect and FireEye Endpoint Security create an efficient security operations workflow that reduces response and investigation time, enabling security teams to quickly mitigate high-risk threats.

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.



Using artificial intelligence, Cognito Detect combines data science, machine learning and behavioral analytics to reveal the attack behaviors without signatures or reputation lists.

Multi-Engine protection with detection and response

To protect against cyber threats and reduce risk, security teams need comprehensive endpoint defense for both common and advanced cyber-attacks.

While protection does not stop everything, a multi-engine, targeted defense does stop the majority of common and advanced attacks. In Endpoint Security, protection begins with filtering out the noise of common attacks with our signature-based protection engine. For uncommon and advanced attacks, FireEye created a machine learning engine, call MalwareGuard, the uses the vast library of threats that FireEye Mandiant has responded to train the engine. Even with the best protection a user may inadvertently click on a link or download an infected document. To stop exploits in browsers and common business software, FireEye uses a heuristic behavior analysis engine, called ExploitGuard to stop an attacker from using exploits.

For attacks that bypass all the various protections, Endpoint Security detects advanced attacks and enables response with tools and techniques developed by the world's leading frontline responders. The indicator of compromise engine in FireEye Endpoint Security detects the human attacker using built in windows tools, stolen credentials or legit applications to move around laterally providing early detection and remediation of an attack in near real time. These indicators can be passed to tools, such as Cognito Detect to analyze and pinpoint the threat.

In addition to reducing the time to investigate threats, Cognito Detect and FireEye let security teams take swift, decisive action.

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

Easily integrate network and endpoint context

When a threat is detected, Cognito Detect and FireEye provide security teams with instant access to additional information for verification and investigation. Host identifiers and other host device data from FireEye are shown automatically in the Cognito Detect UI.

FireEye easily reveals traits and behaviors of a threat that are only visible inside the host device. This enables security teams to quickly and conclusively verify a cyberthreat while also learning more about how the threat behaves on the host device itself.

Cognito Detect from Vectra and FireEye seamlessly integrate two authoritative views of a cyberattack – the network and the endpoint.

Take action

In addition to reducing the time to investigate threats, Cognito Detect and FireEye 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.

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

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 FireEye

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

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

Email info@vectra.ai vectra.ai