VECTRA®

How Cognito enables the implementation of an adaptive security architecture

Historically, enterprises have relied on prevention and policy-based controls for security, deploying products such as antivirus software and firewalls.

But as security experts know, and industry research firms have stated, these mechanisms alone are insufficient in addressing today's threat environment, which is characterized by a wide range of advanced and targeted attacks.

Gartner recommends the following to information security architects:

- Shift your security mindset from "incident response" to "continuous response," wherein systems are assumed to be compromised and require continuous monitoring and remediation; and
- Adopt an adaptive security architecture for protection from advanced threats using Gartner's 12 critical capabilities as the framework.[1]

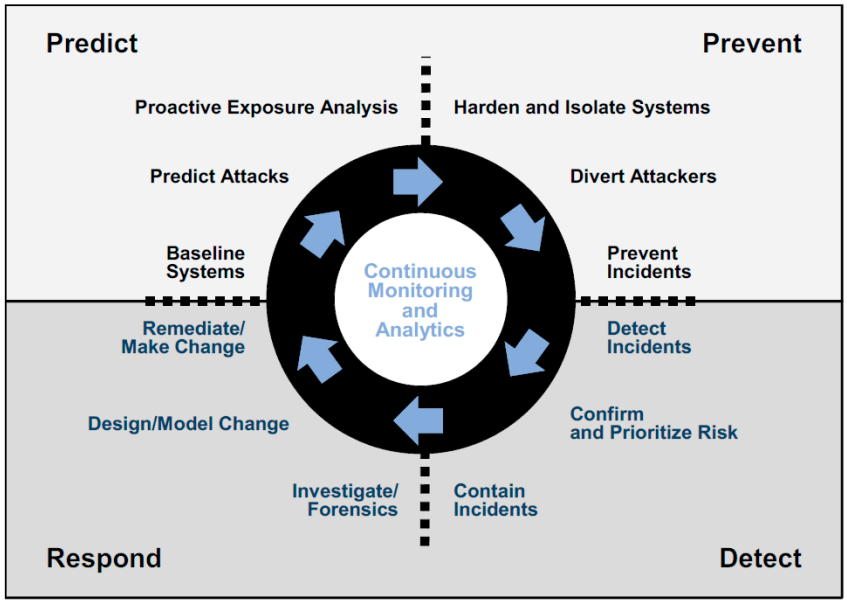
Components of an adaptive security architecture

At its core, an adaptive security architecture has continuous, pervasive monitoring and visibility, with the collected data analyzed constantly for indications of compromise.

Monitoring should encompass as many layers of the IT stack as possible, including network activity, endpoints, system interactions, application transactions, and user activity.

An adaptive security architecture encompasses four vitally important capabilities – prevention, detection, response and prediction – all of which must work in concert.

Recognizing that no one vendor is likely to deliver a complete security solution, vendors should partner with each other to provide customers with a comprehensive, interoperable solution.



Source: Gartner (February 2014)

[1] Gartner, "Designing an Adaptive Security Architecture for Protection from Advanced Attacks," by Neil MacDonald and Peter Firstbrook, 12 February 2014, refreshed 28 January 2016, ID G00259490, https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection

Prevention

These products and processes reduce the surface area for attack by blocking known threats before they impact the enterprise.

Detection

Designed to find attacks that have evaded prevention security, this category of products reduces the dwell time of threats and any potential damage from them.

Look for solutions that analyze data – collected via continuous monitoring – for attacker behaviors that blend into normal patterns of network or endpoint behavior as attackers attempt to remain hidden.

Also examine security solutions that provide threat detections based on how cybercriminals and malware behave and automatically correlate behaviors that are related to the same attack.

Network traffic can be analyzed using techniques such as heuristics, machine learning, statistical analysis, inference modeling, clustering analysis, and Bayesian modeling. All detected threats should be triaged and prioritized according to their risk levels so security teams can address the most critical issues first.

Look for security platforms that provide risk-prioritized, actionable insight derived from embedded domain-specific analytics capabilities within the platform.

Response

Robust response capabilities are required to investigate and remediate all issues that are discovered. They often provide forensic analysis, root cause analysis and recommend preventive measures to avoid future incidents. Network flow data alone may be insufficient for a complete investigation, so consider solutions that use full packet capture.

The most optimal solutions can automatically change policies or controls to prevent reinfection of systems or new attacks. For example, some security platforms automatically generate new signatures, rules or patterns to catch newly discovered attacks.

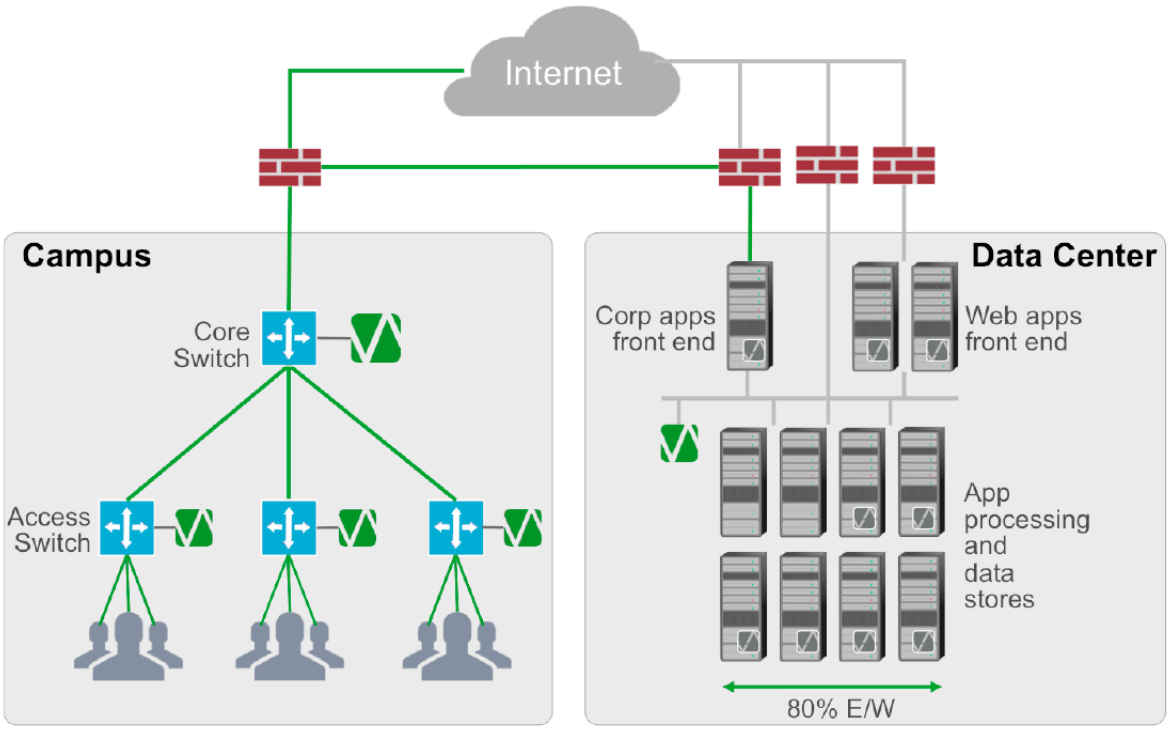
Prediction

Security solutions should incorporate information gleaned by the security community in response to real world events as well as anticipated threats.

For example, security organizations can monitor the hacker underground to cull information about potential new attack types and use that information to shore up prevention and detection capabilities.

Cognito enables the implementation of an adaptive security architecture

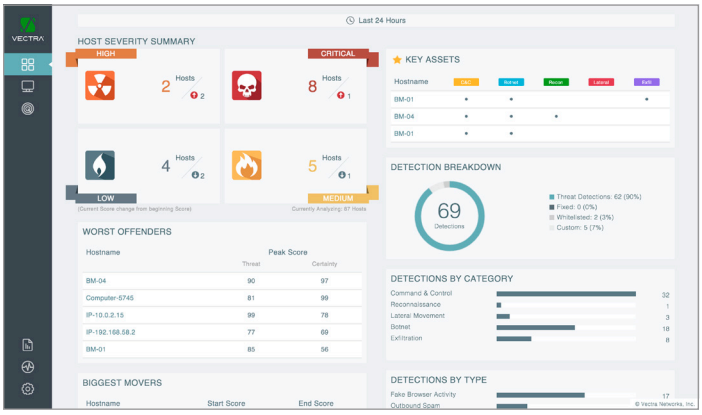
The Cognito™ AI-based threat detection and response platform from Vectra® addresses the need for an adaptive security architecture. Cognito provides continuous, automated threat hunting across the entire enterprise network, from cloud and data center workloads to user and IoT devices.



Cognito detects active cyber attacks that can spread inside networks – from cloud and data center workloads to user and IoT devices

The Cognito cybersecurity platform gives security teams the following critical capabilities:

- Real-time visibility into network traffic by extracting metadata from packets rather than performing deep packet inspection, enabling protection without prying.
- Analyzes the metadata with behavioral detection algorithms that spot hidden and unknown attackers.
- Puts threat detection details – including host context, packet captures, the seriousness of the threat, and certainty scores – within immediate reach.



Metadata collected by Cognito is presented in a dashboard that enables security teams to respond quickly and accurately to detected threats

Cognito combines continuous monitoring and automated threat detection to deliver the requirements of an adaptive security architecture. Whether alone or working with a wide range of technology partners, Cognito provides customers with a variety of capabilities that address prevention, detection, response and prediction.

Prevention

Perimeter and endpoint security remain key to prevention. Cognito complements prevention efforts by providing intelligence about what to block and when.

For example, Cognito has integrated its technology with endpoint, network access control (NAC) and firewall solutions from companies like Carbon Black, CrowdStrike, Tanium, Cisco, Juniper Networks, and Palo Alto Networks.

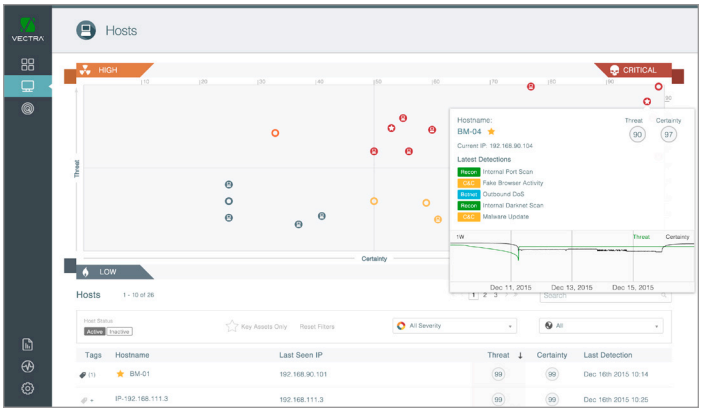
Through these integrations, Cognito behavior-based threat detection models coordinate in real time with firewalls, endpoint protection, and other security products to block the traffic associated with a cyber attack.

By integrating with firewalls and other prevention systems, Cognito ensures that security teams can quickly expose a variety of hidden attacker behaviors, pinpoint the specific hosts at the center of an attack, and mitigate the threat before data is lost.

Detection

Cognito brings significant detection capabilities to an adaptive security architecture. Designed to find attacks that evade prevention security, Cognito provides an exceptional range of detection capabilities:

- Continuously monitors and analyzes all network traffic, from cloud and data center workloads to user and IoT devices, including internal traffic between physical and virtual hosts with an IP address as well as Internet traffic. Cognito monitors traffic from laptops, servers, printers, personal smart-devices, IoT and BYOD devices – regardless of the operating system or application.
- Provides high-fidelity visibility into the actions of all devices.
- Uses artificial intelligence based on a combination of data science, machine learning and behavioral analytics to reveal attack behaviors without signatures or reputation lists. Cognito reveals customized and unknown threats as well as attacks that do not rely on malware, such as malicious insiders and compromised users.
- Behavioral detection algorithms constantly learn from the local environment and from global trends to reveal the fundamental behaviors at the root of an attack.
- Deterministically identifies attack behaviors, including the use of remote access Trojans, encrypted tunnels, botnet behaviors, and reconnaissance tools. Cognito persistently tracks threats over time and across all phases of an attack, ranging from command-and-control (C&C), internal reconnaissance, lateral movement, and data exfiltration behaviors.
- Leverages behavioral detection models – instead of payload-based analysis – to detect threats within SSL/TLS encrypted traffic without requiring decryption.
- Automatically correlates threats with host devices under attack, provides unique context about what attackers are doing, scores all threats using the Vectra Threat Certainty Index™, and prioritizes threats that pose the biggest risk.
- Delivers conclusive detections, with each one explained in detail, along with the underlying event and historical context that led to the detection.
- Automates manual, time-consuming Tier 1 analysis of security events, reducing the time spent on threat investigations by 75% to 90%. This enables security teams to focus their time and resources on loss prevention and mitigation.
- Provides on-demand access to metadata from captured packets for further forensic analysis.



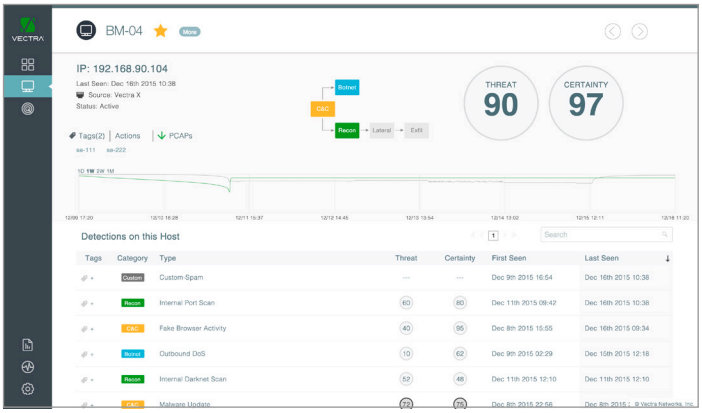
Cognito automatically consolidates events and historical context to identify compromised hosts that pose the biggest risk

Response

The Cognito cybersecurity platform provides the fastest, most efficient way to find and stop attackers inside the network.

The Vectra Threat Certainty Index displays alerts so security teams instantly know which network hosts with attack indicators pose the biggest risk with the highest degree of certainty. In addition, threat and certainty scores are capable of:

- Triggering real-time notifications to security teams.
- Driving dynamic response rules or triggering a response from existing security enforcement solutions.
- Providing a precorrelated starting point for security investigations within security information and event management (SIEM) systems and forensic tools.



The Vectra Threat Certainty Index shows threat and certainty scores for all detections and in every phase of the attack kill chain

Cognito supports a robust API that enables automated response and enforcement with virtually any security solution. Vectra has partnered with a range of best-in-class security vendors to provide an integrated, automated response to threats, ensuring that action is taken quickly and without manual analysis.

It is important to understand that automating analysis and response can condense weeks of work into a few minutes and even seconds, allowing actions to be taken before damage is done.

Whether providing the intelligence to block a new class of threat with existing enforcement points such as a firewalls, endpoint security and NAC, or providing a clear starting point for a more extensive search with SIEMs, Cognito unlocks more value from existing security technologies and teams.

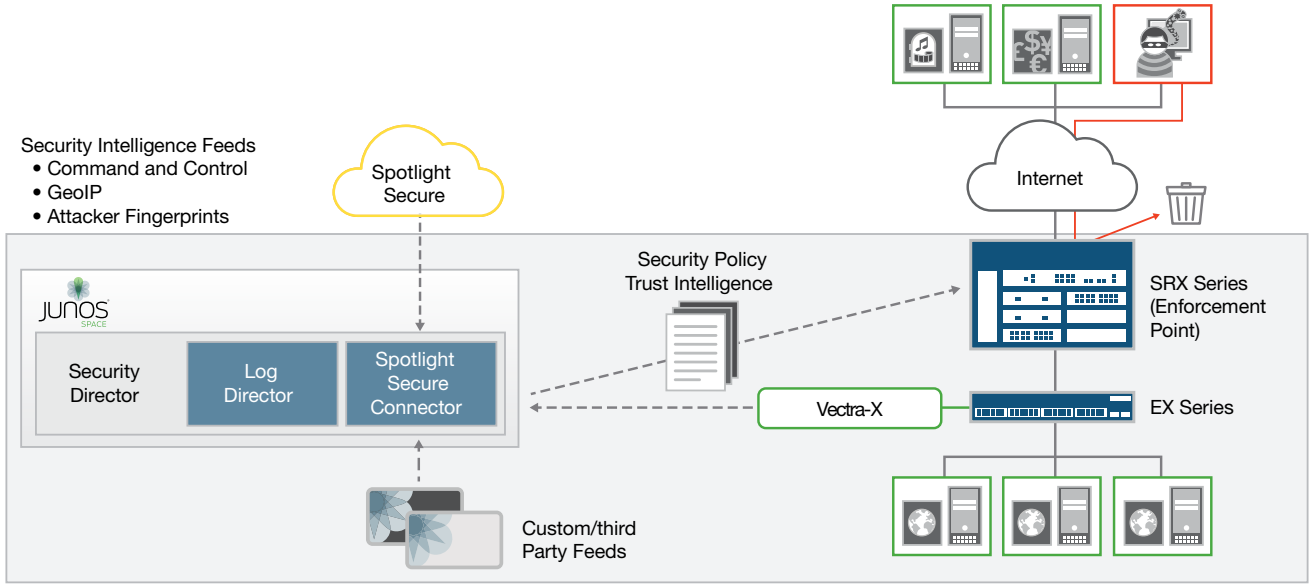
Next-generation firewalls

Cognito integration with next-generation firewalls from Palo Alto Network, Cisco Systems (ASA platforms), and Juniper Networks (SRX Series Services Gateways, Spotlight Secure Connector and Juniper Security Intelligence framework) makes it easy to block a compromised host device that poses a threat.

For example, the Vectra Active Enforcement™ (VAE) application ties into Palo Alto Networks dynamic block lists, triggering actions to stop malicious traffic or quarantine a compromised host. Actions can occur manually or automatically to support any operational workflow.

Security analysts can trigger blocking from the Cognito UI by using predefined event tags. Alternatively, blocking can be fully automated based on the type of threat, as well as threat and certainty scores of specific hosts, such as hosts with protected health information or payment card data.

Similarly, in Juniper environments, once Cognito identifies an infected host, its IP address and threat certainty are pushed to the Juniper Security Intelligence framework, enabling SRX Series Services Gateways to quarantine the infected device, stop communication with a C&C server, and prevent data exfiltration.



Working with Cognito, the Juniper Security Intelligent framework makes it easy to block a compromised host device that poses a threat

Network access control

Cognito integrates with the Cisco Identity Services Engine to immediately isolate or quarantine a host.

For instance, host devices can be placed in remediation VLANs based on detection types or host threat scores. This enables further investigation of a compromised host as it is actively running while limiting its ability to pivot further into an organization.

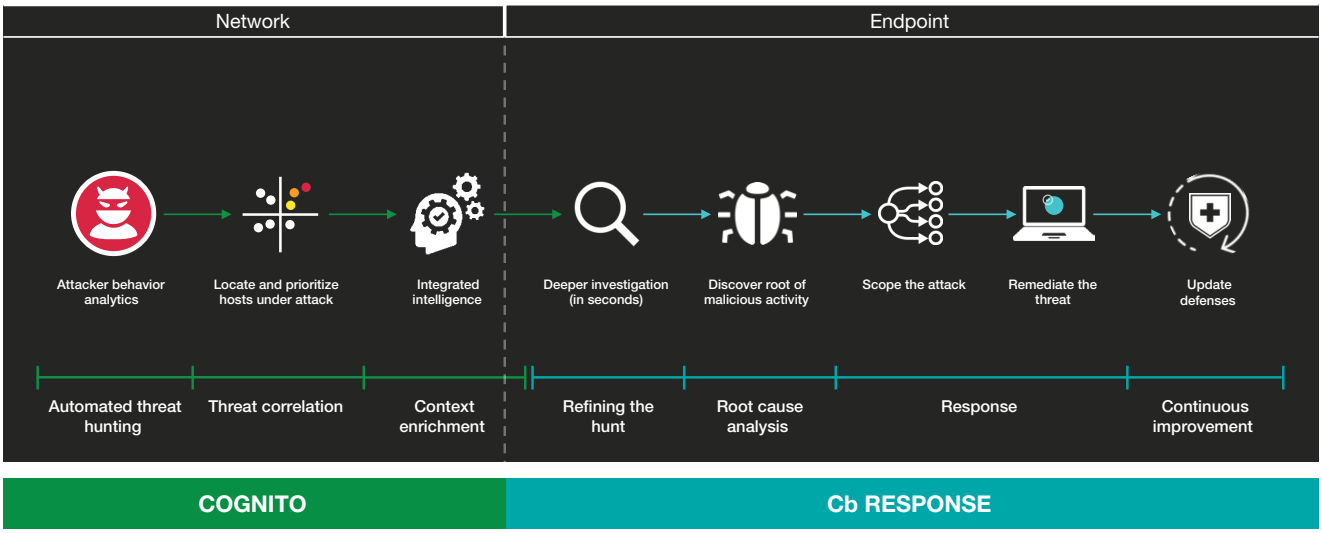
Advanced endpoint solutions

When a threat is detected, Cognito works with Carbon Black to rapidly isolate or quarantine a host device and kill a malicious process. Together, Cognito and Carbon Black unify network and endpoint context so that cyber attacks can be quickly detected, verified and isolated.

When Cognito detects an active threat inside the network, host identifiers and other host data from the Carbon Black Cb Response incident response tool are shown automatically in the Cognito UI.

A single click then allows security teams to pivot between the Cognito UI and the Cb Response UI for the same host or to securely connect to the host using the Cb Response Live Response capability.

Cb Response reveals traits and behaviors of a threat that are only visible inside the host, enabling security teams to quickly verify a cyber attack and learn how the threat behaves on the host. The integration of Cognito with Cb Response creates an efficient security operations workflow that reduces response and investigation time.



Cognito integrates with Carbon Black to provide real-time, automated threat hunting and remediation across the enterprise

SIEMs

Vectra has partnered with Micro Focus and IBM to integrate automated threat hunting with their SIEM platforms. These integrations save time and manpower, reduce attacker dwell time, and speed incident response before data is stolen or damaged.

Integrating Cognito with SIEMs also enables real-time investigations by showing the infected hosts that pose the highest risk based on Cognito analysis, and automatically correlating these investigations with logs generated by other devices.

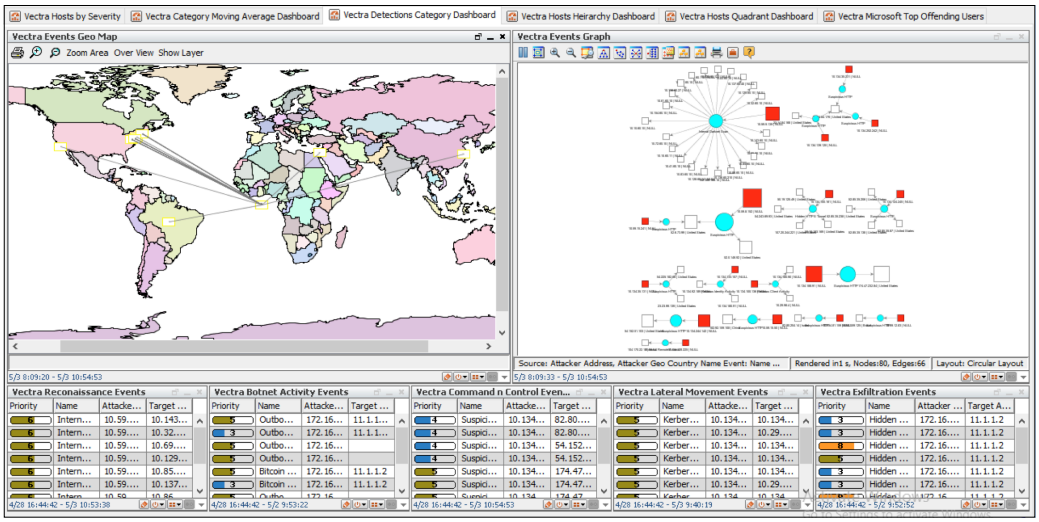
For example, the Micro Focus ArcSight Resource Package from Vectra provides bidirectional integration that brings all Cognito detections and host scores directly into the ArcSight dashboard.

As a result, ArcSight administrators receive precorrelated threat detections that enable further correlation with information and events within ArcSight, such as user names from Microsoft domain controllers. This allows security teams to quickly pinpoint and mitigate active intrusions.

Security teams can also feed Cognito real-time threat detection information into ArcSight dashboards, build custom rules and integrations, and update active lists and filters.

Similarly, Vectra and IBM QRadar Device Support Modules (DSMs) bring real-time, precorrelated threat detections and host scores from Cognito into the QRadar platform. All Cognito threat detections are automatically mapped to the appropriate QRadar categories.

This mapping allows QRadar to use Cognito advanced attack detections and behavioral traffic analysis to easily build customized rules within QRadar to enrich the context of real-time threat investigations.



A geographical map from within Micro Focus ArcSight automatically shows real-time detection events from Cognito

Security orchestration automation

Cognito integration with leading security automation and orchestration platforms automates network defenses by combining behavior-based threat detections with real-time enforcement.

Powered by security automation and orchestration platforms, Vectra Active Enforcement automates the response phase of attack mitigation by enabling quick and effective enforcement action by perimeter, endpoint, NAC, and other security solutions.

Response actions by security orchestration and automation platforms can be triggered based on the type of threat, risk and certainty, and include blocking attacker behaviors and quarantining compromised hosts.

For instance, simple event tags can be used to trigger response actions. A response can be fully automated based on the type of threat, as well as threat and certainty scores of specific hosts, including hosts with personally identifiable or protected health information.

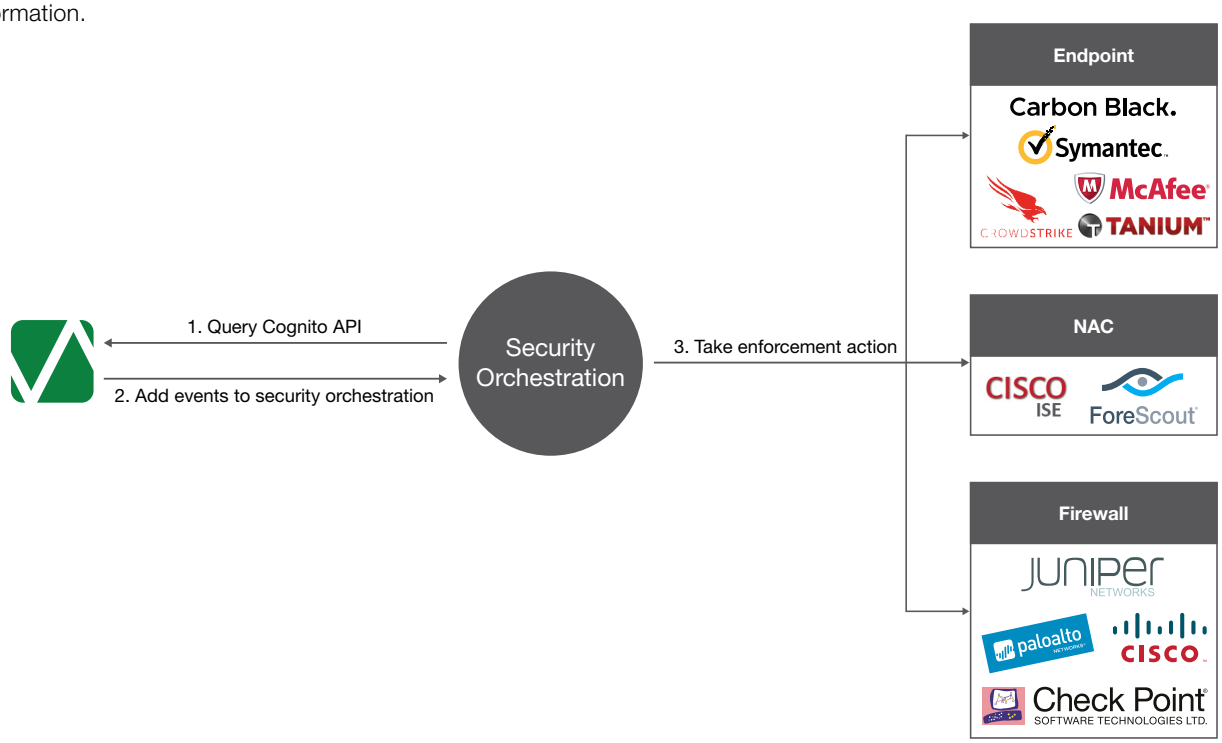
Prediction

The prediction category involves threat intelligence-gathering from hacker communities, marketplaces and bulletin boards. Threat intelligence gathered by security researchers can proactively minimize enterprise asset exposure and risk.

This is the charter and intent behind the Vectra Threat Labs™, a group of highly-skilled security researchers with a comprehensive understanding of how attacks work and how the threat landscape is continually shifting.

The primary responsibilities of the Vectra Threat Labs include:

- Analyzing the latest attack tools and methodologies.
- Developing new machine-learning detection capabilities.
- Dissecting malware propagation and exploitation techniques.
- Enumerating the threat landscape and labeling detected threats and their facilitators.



Security orchestration and automation platforms turn Cognito threat detections into action by integrating with other leading security solutions to stop attacker traffic or quarantine compromised host devices

Vectra Threat Labs operates at the precise intersection of security research and data science. Security researchers take unexplained phenomena seen in real-world networks and dig deeper to find the underlying reasons for the observed behavior.

Researchers in the Vectra Threat Labs zero-in on the attackers' goals, place them in the context of the broader campaign the attacker is waging, and provide insights into durable ways in which threats can be detected and mitigated.

This insight enables the improvement of existing threat-detection models and the creation of new models to efficiently and effectively find and stop an attacker using new techniques. As a result, Cognito enables organizations to quickly and proactively adapt their security protection strategies to anticipate future attacks.

Putting adaptive security to work

Operationally, Cognito complements the adaptive security architecture by providing continuous, pervasive monitoring and visibility at its core and ensuring that collected data is analyzed constantly for indications of compromise.

The Cognito cybersecurity platform delivers this essential core functionality, providing deep, continuous analysis of internal and Internet network traffic to automatically detect all phases of an attack in progress.

In addition, through its growing technology partner ecosystem, Cognito supports integration with robust threat response to ensure that host devices are quarantined, malicious processes are shut down, and other measures automatically occur to secure the enterprise.

By providing continuous automated threat detection and leveraging the prevention, response and orchestration tools that customers have in place, Cognito saves security teams time and effort and enables them to take prompt action before cyber attacks lead to data loss or damage.

VECTRA®
Security that thinks®

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