VECTRA®

Check Point® SOFTWARE TECHNOLOGIES LTD.

# Gain continuous threat visibility and enforcement with Check Point and Vectra

## CHALLENGE

Security teams must continuously monitor for threat activity across all environments and contain and block threats immediately.

## SOLUTION

Integration of the Cognito automated threat detection and response platform from Vectra with Check Point Next Generation Firewalls empowers security staff to quickly expose hidden attacker behaviors, pinpoint specific hosts involved in a cyberattack, and contain threats before data is lost.

## BENEFITS

- Prevent zero-day threats by deploying security that detects and prevents threats first
- Automate threat response by combining behavior-based threat detection with real-time enforcement
- Empower security analysts to respond to threats using simple event tags
- Take focused blocking actions, such as blocking based on type of threat, risk and certainty

## Detect and stop threats continuously

Threats are stealthy and can stay hidden over long periods of time while they exfiltrate data within allowed traffic channels. With increasingly sophisticated threats, security teams need accurate and continuous monitoring for threat activity across all environments.

The success or failure of a security team often boils down to time-to-response. Once identified, threats must be contained immediately and malicious activity blocked.

Even after the detection, response may require hours or days of investigation from highly trained security analysts to stop the damage and return to normal operations.

## Continuous, real-time threat prevention

The integration between the Cognito™ automated network detection and response platform from Vectra® and Check Point Next Generation Firewalls empowers security staff to quickly expose hidden attacker behaviors, pinpoint specific hosts involved in a cyberattack and contain threats before data is lost.

The Vectra and Check Point partnership combines behavioral threat detection and real-time enforcement. Joint customers can integrate Check Point Next Generation Firewalls with the Cognito platform in a matter of minutes. The joint solution provides the protection, visibility and enforcement tools security teams need.

Timely response to threats starts with Check Point SandBlast Zero-day Protection. Check Point SandBlast Zero-Day Protection is a cloud-based sandboxing technology where files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before they enter the network. SandBlast detects malware at the exploit phase, even before attackers can apply evasion techniques attempting to bypass the sandbox.

## Intelligent threat detection

Enterprises can augment Check Point prevent-first security with Vectra. The Cognito platform accelerates customer threat detection and investigation using sophisticated artificial intelligence to collect, store and enrich network metadata with insightful context to detect, hunt and investigate known and unknown threats in real time. Cognito integrates seamlessly with Check Point Next Generation Firewalls, dynamically blocking malicious traffic.

Blocking can be fully automated based on the type of threat, as well as threat and certainty scores of specific hosts, such as hosts subject to Payment Card Industry (PCI) regulations.

With Check Point prevent-first Next Generation Firewalls augmented with Cognito automated threat detection and response, security teams can condense weeks of work into seconds and take action before damage is done.

## Empower analysts to stop attacks

Finding and retaining qualified security staff is a challenge for most organizations. Even in the best of cases, most networks generate more security alerts than staff have the time to analyze.

The powerful combination of Cognito threat detection and response with Check Point Next Generation Firewall prevent-first enforcement makes the best use of time and talent.

Security teams can quickly pinpoint the hosts involved in an active cyberattack, verify the threat with on-demand forensics and trigger a dynamic containment of the affected devices—all from within the intuitive Cognito user interface.

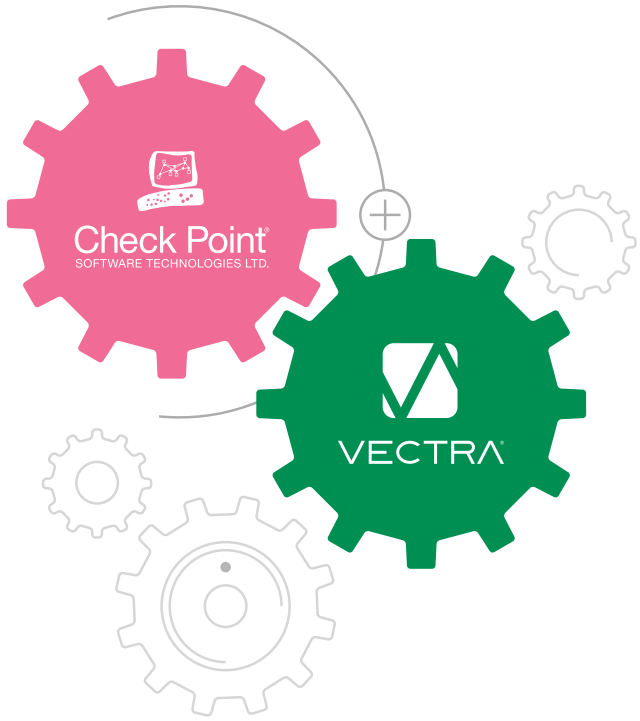
Automation empowers staff to find and resolve issues quickly, saving time and money.

## Automate containment based on risk and certainty

Many behavioral analysis solutions simply flag anomalies, which then require extensive analysis and follow-up to determine an appropriate response. This leads to a bottleneck from human analysis and security staff who suffer from alert fatigue. Ultimately, delayed responses and missed alerts can result in attackers successfully exfiltrating company data.

In addition to automating the hunt for threats, the Cognito platform automatically scores each detection and affected host in terms of risk to the network and the certainty of the attack. These scores retain context over time and correlate the progression of an attack, allowing staff to prioritize the most urgent issues first.

Security staff can use Cognito threat-level and certainty scores to drive dynamic blocking rules aligning to the risk profile of the organization.




## About Vectra

Vectra® is the leader in network detection and response – from cloud and data center workloads to user and IoT devices. Its Cognito® platform accelerates threat detection and investigation using artificial intelligence to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers three applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. For more information, visit vectra.ai.

## About Check Point

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes. For more information, visit www.checkpoint.com.

VECTRA®
Security that thinks®

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