Check Point SOFTWARE TECHNOLOGIES LTD. | VECTRA™

WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT + VECTRA

CONTINUOS THREAT VISIBILITY AND ENFORCEMENT

CONTINUOUS, REAL-TIME THREAT PREVENTION

Benefits

- **Prevent Zero-day Threats:** deploy security that detects and also prevents threats first
- **Automate Threat Response:** combine behavior-based threat detection with real-time enforcement
- **Empower Security Analysts:** respond to threats using simple event tags
- **Focused Blocking Actions:** block threats based on type of threat, risk and certainty

INSIGHTS

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.

VECTRA COGNITO AND CHECK POINT

The integration between Vectra and Check Point enables 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 Vectra Cognito in a matter of minutes. The joint solution provides the protection, visibility and enforcement tools security teams need.

- Timely response to threats first 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 hackers can apply evasion techniques attempting to bypass the sandbox.
- Augment Check Point prevent-first security with Vectra Cognito. 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.

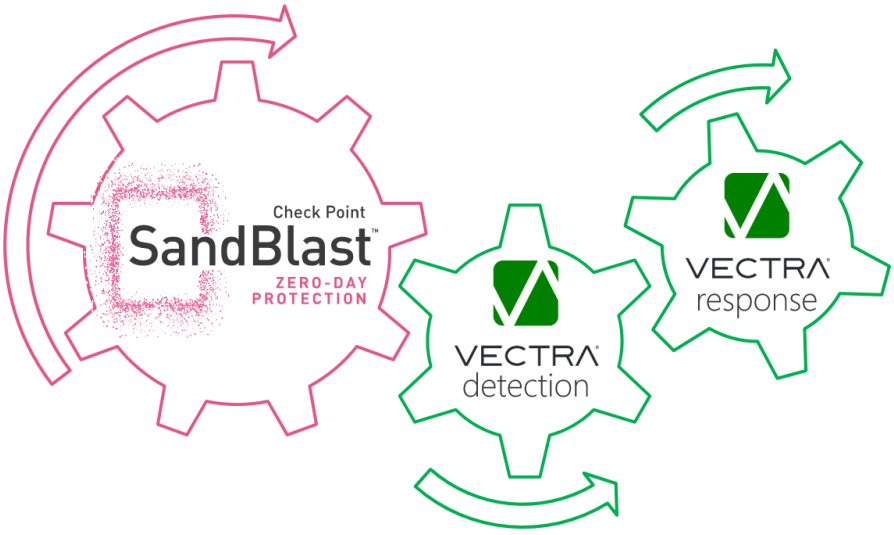
Cognito integrates seamlessly with Check Point Next Generation Firewalls, dynamically blocking malicious traffic. Blocking can further be fully automated based on the type of threat, as well as threat and certainty scores of specific hosts, e.g. hosts subject to Payment Card Industry (PCI) regulations. With Check Point prevent-first Next Generation Firewalls augmented with Vectra Cognito automated analysis and response, security teams condense weeks of work into seconds and take action before damage is done.

EMPOWERING 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 combination of Vectra 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 Cognito user interface. This automation empowers staff to find and resolve issues quickly, saving time and money.

AUTOMATE CONTAINMENT BASED ON RISK-LEVEL AND CERTAINTY

Many behavioral analysis solutions simply flag anomalies, which 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, Cognito 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. Staff can use these threat-level and certainty scores to drive dynamic blocking rules aligning to the risk profile of the organization.



ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) 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.

ABOUT VECTRA

Vectra Cognito provides the fastest, most efficient way to find and stop attackers once they are inside a network. Cognito delivers real-time attack visibility across your entire network and puts attack details at your fingertips to empower immediate action. Leveraging artificial intelligence, Cognito performs automated threat hunting with always-learning behavioral models to quickly and efficiently find hidden attackers before they do damage. Cognito also delivers blind-spot-free threat detection by directly analyzing all network traffic for high-fidelity visibility into the actions of all devices. With visibility into traffic from cloud and data center workloads to user and IoT devices, attackers have nowhere to hide.

CONTACT US
Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | www.checkpoint.com