



Active Defense: TrapX® DeceptionGrid® and Carbon Black Cb Response®

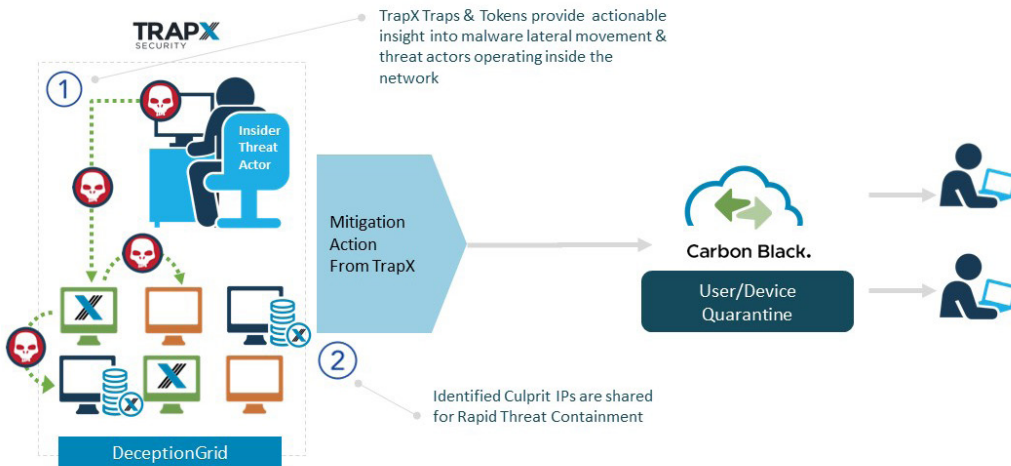
TrapX Security® and Carbon Black® have joined forces to provide real-time visibility and threat detection, improved incident response and rapid threat containment.

The Joint Solution

Carbon Black Cb Response is a highly scalable, real-time Endpoint Detection and Response (EDR) solution with unparalleled visibility for top security operations centers and incident response teams.

This integration enables the DeceptionGrid to provide actionable threat intelligence and initiate rapid threat containment actions or interdiction throughout the Carbon Black security ecosystem.

Real-Time Adaptive Deception - Rapid Threat Containment



How will you know if one of your endpoints has been compromised?

How quickly will you know your current security tools have failed?

How quickly can you isolate and shut down the attack, and return to normal operations?

Carbon Black

The joint solution offers customers early detection capabilities for advanced targeted attacks, zero-day malware, and human threat actors operating on endpoints, along with the ability to quickly and proactively isolate compromised assets, thereby shutting down attackers in real time.

TrapX's DeceptionGrid

DeceptionGrid is based on our TrapX Deception-in-Depth architecture, which combines wide-ranging deception capabilities to bait, engage, and trap attackers. The DeceptionGrid's multi-tier architecture presents deception attack surfaces that match attacker activity adaptively, creating a tempting environment for attackers on various types of endpoints.

DeceptionGrid baits attackers by deploying automated, camouflaged deception Tokens (lures) with the addition of medium and high-interaction Traps (decoys) among authentic IT resources. The Traps appear identical in every way to authentic IT assets and connected Internet of Things (IoT) devices. The attacker sees an array of camouflaged Traps which appear as tempting medical devices, servers, automated teller machines, retail point of sale workstations, switches, industrial control system components and many other devices. DeceptionGrid even maintains a facade of convincing network traffic among the Traps, thereby enhancing the illusion of authenticity and further engaging sophisticated attackers.

The Use Case

When malicious activity is identified by one of the DeceptionGrid's sophisticated traps, an alert is sent automatically to Cb Response for isolation based on policy (risk-based) rules. Users can also isolate the endpoint manually with Cb Response through the TrapX Security Operations Console (TSOC).

After the malware or human threat actor is completely shut down, security teams can leverage Cb Response to take remediation actions including enterprise-wide hash banning, drilling down to root cause and the ability to create automated watchlists to alert on similar malicious techniques in the future.

Benefits for Your Organization by Deploying the DeceptionGrid

- » **Reduced time-to-breach detection** – DeceptionGrid detects malware and human threat actor movements inside the perimeter immediately.
- » **Powerful situational awareness** – DeceptionGrid detects lateral movements that are often missed by other types of cyber tools and defenses.



- » **Highest-fidelity alerts** – DeceptionGrid generates a very low volume of highly accurate alerts.
- » **Deception-in-Depth integrated product platform** – Deception in Depth brings the industry's most comprehensive and powerful suite of deception techniques together in one multi-tier architecture to bait, engage, and trap attackers.
- » **Ease-of-deployment** – DeceptionGrid deployment is simple and fast, using custom-built proprietary emulations and powerful automation.
- » **Actionable intelligence** – Information flows across the integrated network to leverage discovery and uncover hidden threats that target critical assets in both IT and OT infrastructures.
- » **Deep visibility into internal endpoints** – The DeceptionGrid/Carbon Black joint solution provides augmented and actionable real-time visibility into lateral movements from attackers, targeting special endpoints including IoT, SCADA, ICS, POS, and medical devices.
- » **Carbon Black integration** – Cb Response integrates seamlessly with DeceptionGrid which results in fast deployment, trouble-free administration and automated rapid threat containment. TrapX provides MSSP partners that bring the expertise and skills needed to supplement constrained in-house teams.

About TrapX Security

TrapX Security is the leader in deception technology. Their DeceptionGrid solution rapidly detects, deceives, and defeats advanced cyberattacks and human attackers in real time. The DeceptionGrid also provides automated, highly accurate insight into malicious activity unseen by other types of cyber defenses. By deploying DeceptionGrid, you can create a proactive security posture, fundamentally halting the progression of an attack while changing the economics of cyberattacks by shifting the cost to the attacker. The TrapX Security customer-base includes Forbes Global 2000 commercial and government customers worldwide in sectors that include defense, healthcare, finance, energy, consumer products, and other key industries. Learn more at www.trapx.com.

About Carbon Black

Carbon Black is a leading provider of next-generation endpoint security. As a cyber-security innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. Learn more at www.carbonblack.com.

TrapX Security, Inc.
3031 Tisch Way
110 Plaza West
San Jose, California
95128
+1-855-249-4453
www.trapx.com
sales@trapx.com
partners@trapx.com
support@trapx.com