illusive | Carbon Black.

Partner Brief

Illusive Platform with Carbon Black CB Response®
Real-Time Threat Detection and Endpoint Isolation

Illusive has joined forces with Carbon Black to provide real-time threat detection at breach beachheads and instant isolation of compromised endpoints. Illusive deception technology provides high-fidelity alerts that Carbon Black customers can leverage to automatically or manually isolate suspicious endpoints in milliseconds.

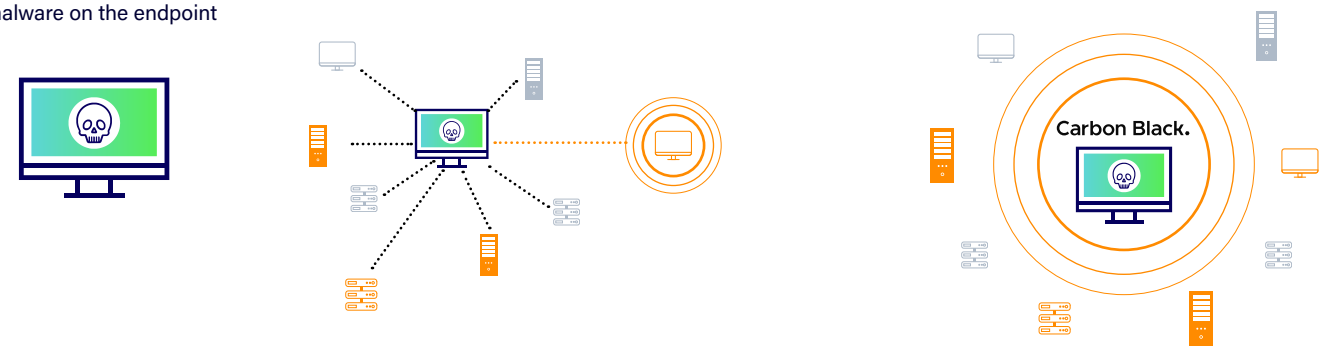
With the power of Illusive and Carbon Black working together, your organization can Identify threats earlier in their life cycle, accelerate response time, and gain the visibility you need to efficiently mitigate attacks before they ever get anywhere near your critical assets.

With Illusive and Carbon Black CB Response® working in tandem, your organization reaps the following advantages:

- Deterministically detect the most sophisticated human attackers, insiders, and malware
- Automatic or manual isolation of malicious IPs and hosts
- Comprehensive telemetry data about attackers and endpoints
- Simple de-isolation once investigation and mitigation are complete

How Illusive and Carbon Black Work Together to Identify and Stop Threats

1. Illusive provides the earliest possible detection of lateral movement by humans or malware on the endpoint
2. Attacker unknowingly accesses a highly authentic endpoint deception
3. illusive — High-fidelity alert sets automatic (or manual) threat containment in motion
4. Carbon Black. — Endpoint is isolated until threat is removed, then de-isolated



"A key aspect of threat-hunting is the use of deception technology to deploy traps in an organization's IT infrastructure to nab cyber adversaries and uncover their tactics, techniques & procedures."
– Tom Kellermann, Chief Cyber Security Officer, Carbon Black

Stopping Human-Driven Attacks with Illusive and Carbon Black

When an Illusive deception is activated, an alert is raised and automatically initiates defensive isolation and containment measures powered by Carbon Black.

Rich telemetry captured from the compromised machine give responders what they need to determine how to respond, such as terminating processes; deleting files; or disconnecting an endpoint from the network.

Further, analysts are provided visibility on how far the attacker is from critical business assets and Domain Admin credentials, offering insights on improvements to current security defenses.

Illusive and Carbon Black in Collaboration: Key Benefits

Illusive and Carbon Black integration provides organizations with more efficient detection of and automated response of sophisticated, human driven attacks. When pairing Illusive's deterministic, high-fidelity alerting with Carbon Black's instant ability to respond to and contain a compromised host until the threat is removed, organizations gain tactical advantage over adversaries armed with context-rich forensics that saves valuable hours of manual investigation efforts.

- Detect and isolate attackers early in the threat lifecycle
- Halt vertical movement between hybrid and multi-cloud ecosystems
- Amplify the power of limited SOC and IR resources
- Strengthen the security of your organization's critical assets
- Enhance attack intelligence and telemetry

The **Illusive Active Defense Suite** provides centralized management across even the largest and most distributed environments. Three products work together to protect organizations against today's most sophisticated cyberattacks.

ASM: Attack Surface Manager continuously analyzes and removes unnecessary credentials and pathways, reducing the attack surface.

ADS: **Attack Detection System** makes it impossible for attackers to move laterally by transforming every endpoint into a web of deceptions.

AIS: **Attack Intelligence System** delivers human readable on-demand telemetry for current attacker activities to speed investigation and remediation.

Illusive's Active Defense is a vital part of a diversified detection strategy, filling an important attacker lateral movement detection gap in existing perimeter defenses. Each of the products in the Illusive Active Defense Suite play an important role in preventing attackers from achieving their objectives by creating a hostile environment and accelerating the time to detection for an attacker that has established a beachhead.

About Illusive

Illusive reduces cyber risk by shrinking the attack surface and stopping attacker movement. Despite significant investments, it's still difficult to see and stop attackers moving inside your environment. Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help Fortune 100 companies protect their critical assets, including the largest global financials and global pharmaceuticals. Illusive has participated in over 130+ red team exercises and has never lost one! To learn more, visit **www.illusive.com**

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leader in cloud endpoint protection dedicated to keeping the world safe from cyberattacks.

The CB Predictive Security Cloud® (PSC) consolidates endpoint protection and IT operations into an extensible cloud platform that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations.

By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.