ILLUSIVE INTEGRATION BRIEF

Real-Time Deterministic Threat Identification and Containment

Illusive Integration with CrowdStrike Falcon

Illusive Networks and CrowdStrike have partnered to deliver real-time threat detection and instant isolation of compromised endpoints at the earliest point of attack. Illusive deception technology provides high-fidelity notifications that CrowdStrike customers can consume to automatically or manually isolate suspicious endpoints in milliseconds. Illusive and CrowdStrike help identify threats early in their life cycle, reduce response time, and gain the visibility needed to mitigate attacks before they get near critical assets.

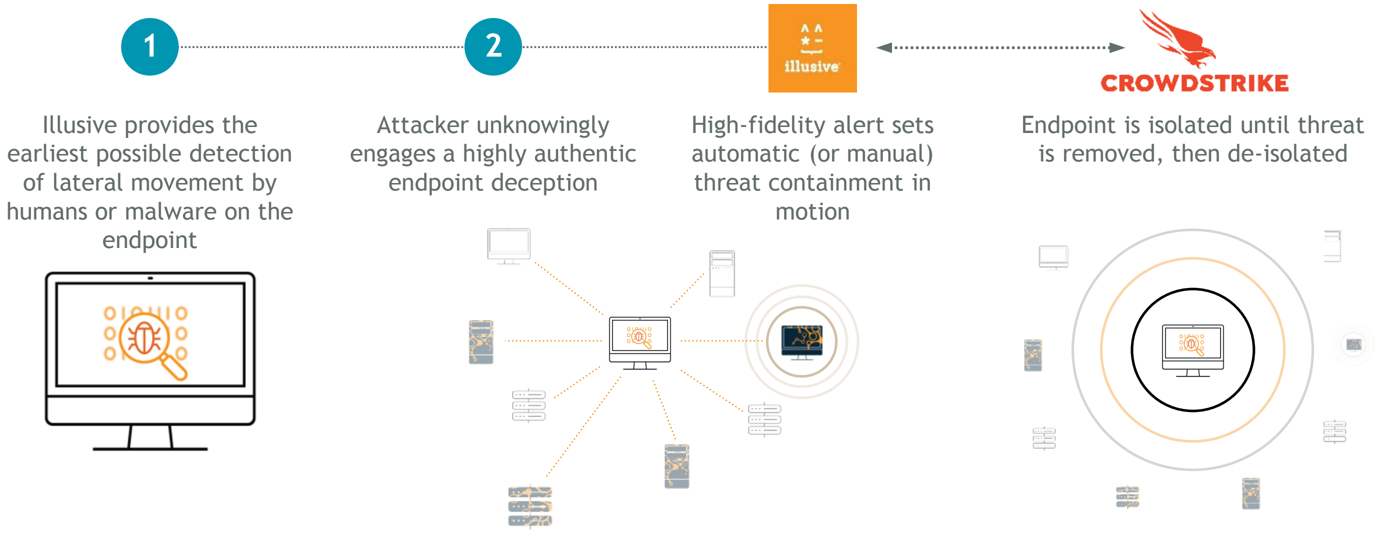
THE CHALLENGE

Attackers seek out (and expect) errant credentials and connectivity native to daily user activity to laterally move towards target systems—a technique often undetected because it appears ‘normal’ to most security tools. Defenders often lack ability to get ahead of this process, becoming mired chasing false positives while real threats dwell in the shadows.

AN INTEGRATED SOLUTION

The Illusive and CrowdStrike integration offers automatic and on-demand incident mitigation initiated from directly within Illusive. Upon receipt of an Illusive alert from the endpoint, users can isolate compromised hosts in real-time leveraging the CrowdStrike Falcon® platform. It’s the fastest way to stop an endpoint-based threat once it is reported by Illusive. On-demand incident mitigation allows you to manually take a host offline and freeze the situation, allowing time to consider consequences and other paths of remediation.

Working Together: Illusive and CrowdStrike Falcon



1 Illusive provides the earliest possible detection of lateral movement by humans or malware on the endpoint

2 Attacker unknowingly engages a highly authentic endpoint deception

High-fidelity alert sets automatic (or manual) threat containment in motion

Endpoint is isolated until threat is removed, then de-isolated

CrowdStrike Falcon stops breaches via a unified set of solutions that prevent all types of attacks. Today’s attackers increasingly rely on exploits, zero days, and hard-to-detect methods, such as PowerShell. CrowdStrike Falcon responds to those challenges with a lightweight solution that unifies next-generation antivirus, endpoint detection and response, cyber threat intelligence, managed threat hunting capabilities and security hygiene—that is cloud-managed and delivered.

WORKING TOGETHER

This integration pairs Illusive's deterministic alerting with CrowdStrike's Endpoint Detection and Response (EDR) solution to respond and contain a compromised host until the threat is removed. Illusive’s deterministic deception-based threat detection is not dependent on the existence of attack tools, malware or exploits, but on actual human engagement. This means that Illusive catches attacks to the endpoint, enhancing the view of anomaly-based EDR tools like CrowdStrike. Once a detection occurs, Illusive’s high-fidelity identification of an attack in motion, coupled with CrowdStrike’s immediate ability to isolate the compromised endpoint, accelerates response and mitigation to stop attacks early in their lifecycle. Many customers – especially those that lack extensive security resources – appreciate the option for full detection-response automation that combining Illusive and CrowdStrike allows.

KEY BENEFITS

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

Detect threats to the endpoint that circumvent anomaly-based detection tools

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 forensics

ABOUT ILLUSIVE

Illusive reduces cyber risk by shrinking the attack surface and stopping attacker movement. Illusive identifies and removes the vulnerable connections and credentials that enable attackers to move undetected, and then replaces them with deceptive versions that fool attackers into revealing their presence upon engagement. Unlike behavioral or anomaly-based threat detection, Illusive’s agentless approach captures deterministic proof of in-progress attacks and provides actionable forensics to empower a quick and effective response. To learn more, visit www.illusivenetworks.com

ABOUT CROWDSTRIKE

CrowdStrike Inc. (Nasdaq: CRWD), is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform’s lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility, preventing attacks on endpoints on or off the network. CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time, fueling one of the most advanced data platforms for security. Customers benefit from better protection, performance and immediate time-to-value. Learn more: https://www.crowdstrike.com

We are here to help! See a demo or discuss steps for a free Attack Risk Assessment at info@illusivenetworks.com

Visit us at www.illusivenetworks.com

Call us at +1 844.455.8748 (North America) or
+972 73.272.4006 (EMEA and AsiaPac)