Illusive Networks for Insider Threat Defense

A deception-based approach to preempt, detect, and respond to attacks

Insider incidents represent approximately 34%* of electronic attacks and present several unique challenges. Insiders can operate more silently and inflict more damage than outsiders because they already have some trusted access and insight into an organization's valuable assets. But in many cases, malicious insiders must also snoop around file systems and acquire credentials and connections to systems and applications they don't have authorized access to—in other words, they must conduct lateral movement just as an external attacker would.

Do you know how attackers can move sideways once they are inside your network?

With Illusive's deception-based technology, organizations can protect against malicious insiders while maintaining an internal culture of trust and respect.

The Illusive platform helps companies to:

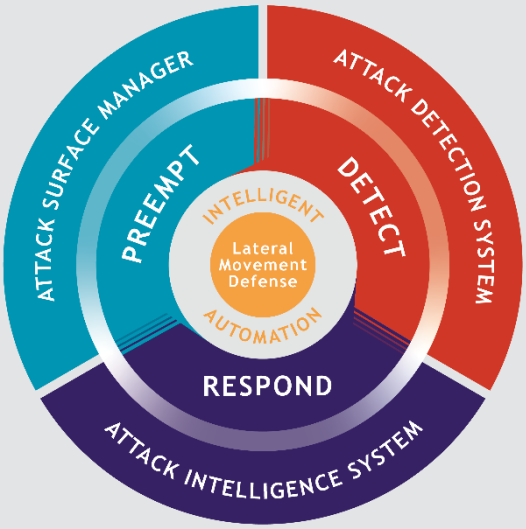
- **Non-intrusively detect suspicious insider threat activity**
- **Make it harder for insiders to get where they don't belong**
- **Quickly gather the forensic evidence—both source and target—needed to expedite investigations and take appropriate action**
- **Immediately know how close a potential attacker is to critical systems and domain admin credentials**

While a deception-based platform is just one part of an insider threat program, Illusive provides a critical piece that has been missing until now by providing the means to detect and deter the silent malicious activity of trusted users.

By hardening the network against advanced techniques, detecting the earliest signs of suspicious activity, and providing the tools to prioritize, investigate, and respond, Illusive helps to reduce the risk of insider threats, so that businesses can thrive in an increasingly complex IT landscape.

*Verizon 2019 Data Breach Investigations Report

The Illusive Platform provides centralized management across even the largest and most distributed environments. Three modular components can work together or be operated separately to preempt, detect, and respond to cyberattacks.



Changing the math for early attack detection

Reducing the number of real artifacts while saturating endpoints with deceptive ones increases the odds that attackers will choose deceptions—and be instantly caught.

How the Illusive Platform Detects Malicious Insiders:

- **Attack Surface Manager:** Finds and removes errant high-privilege credentials, connections, and attack pathways to deter unauthorized lateral movement from one endpoint to another.
- **Pathways:** A feature that automatically reveals attack paths from any machine to high-value targets, provides drill-down details on the systems in each path, and enables point-and-click elimination of excess connectivity, leveraging risk and connectivity ratings.
- **Attack Detection System:** Distributes deceptive data on every endpoint across the network, forcing attackers to reveal themselves early in the attack process by disorienting and manipulating their decision-making. As soon as an attacker interacts with a deception, an immediate notification is sent to the security team, along with detailed forensics (see below).
- **Attacker View:** Shows real-time proximity of attackers to Crown Jewel systems and high-privilege credentials.
- **Deceptive Microsoft Office Beacon Files:** Automates the creation and customization of deceptive Word and Excel documents that are indistinguishable from the genuine article. These deceptive Office documents can be loaded with fake data that notifies the SOC team once an attacker tries to use the information to gain access. Additionally, both real and deceptive Office files can be beaconized to immediately alert organizations to the presence of malicious insiders as soon as they interact with the deceptive file.
- **Attack Intelligence System:** Empowers Incident Response teams with easy-to-use, precision forensics — both source-based and from high-interaction decoys — so they can rapidly determine the best course of action to minimize business damage and improve future cyber resilience.
- **Forensics Timeline:** A unified, sortable per-incident chronology of forensic data.
- **FirstMove Services:** Assistance in planning deployments, use case development and interpretation of security notifications.

The Fastest and Most Effective Strategy for Insider Defense

- See exactly how insiders could reach your critical assets by uncovering invisible conditions that enable lateral movement and easily remove them
- Ensure early attacker detection of malicious insiders—no matter where compromise begins
- Reduce noise in the SOC by focusing attention on high-fidelity notifications
- Agentless technology deploys in days with little IT involvement
- Gain efficiency under fire. At the moment of detection, responders have comprehensive insight to quickly determine the best course of action
- Proven to scale across networks of more than 500,000 endpoints

> *"Illusive **cut investigation time by two-thirds**. The graphical dashboard shows us where the attacker is in relation to crown jewels. We can quickly drill down to specific details, and Illusive automatically gives us a timeline of what has happened on the endpoint. It's invaluable."*
>
> *Information Security Manager, Energy Company*

Illusive Networks empowers security teams to reduce the business risk created by today's advanced, targeted threats by destroying an attacker's ability to move sideways toward critical assets. Illusive reduces the attack surface to preempt attacks, detects unauthorized lateral movement early in the attack cycle, and provides rich, real-time forensics that enhance response and inform cyber resilience efforts. Agentless and intelligence-driven, Illusive technology enables organizations to avoid operational disruption and business losses by proactively intervening in the attack process so they can function with greater confidence in today's complex, hyper-connected world

Visit us: www.illusivenetworks.com

Email us: info@illusivenetworks.com

Call us:: US: +1 844.455.8748

EMEA / AsiaPac: +972 73.272.4006

Find us: