illusive

Goodbye anomaly detection.
Hello distributed deception.

#stopsidewaysattacks

Attackers have the advantage. Using AI tools and automation, threat actors have evolved their evasion techniques beyond the defenses of traditional ‘find the needle in the haystack’ security technologies. Unfortunately, SOC IR teams continue to spend invaluable time and resources mired in the turmoil of triaging an avalanche of alerts and false positives—and accepting the sinking likelihood that they are still missing attacks dwelling in the shadows. Current approaches aren’t enough. It’s time to flip the dynamic.

SIEM
AV
NTA
PAM
UEBA
EDR
Attackers only need to be right once
Defenders must be right every time

Flip cyber asymmetry and force attackers to reveal themselves

Instead of building walls and restrictive controls around your assets, Illusive disarms the attacker—destroying their decision-making and depriving them of the means to reach their targets. It’s a simple, adaptive approach that empowers your defenders to stop cyberthreats that could otherwise exist in your environment for months or years.

What you see

Environment as typical network diagram

What attackers see

Environment as opportunity to move sideways

- Hidden credentials
- Connections
- Pathways

Get Ahead of the Bad Guys

Illusive combats attackers by cleaning the environment and then introducing a dense web of inescapable deceptions across the network tailored to mimic real data, credentials, and connections that an attacker needs to move within the network. Confronted with a distorted view of reality, it becomes impossible to choose a real path forward. Unknown to the attacker, one wrong step triggers an event notification capturing real-time forensic data from the system where the attacker is operating, allowing rapid response.

Prevent, detect and stop.

Create a hostile environment for attackers.

Built by Defenders, for Defenders

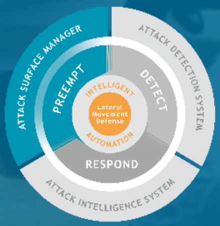
Illusive has beaten well over 100 of the world's most advanced and aggressive Red Teams! How? The Illusive platform is engineered by people steeped in nation-state cyber intelligence and defense with tactical understanding of how attackers operate. Purpose-built to help you simply and easily identify real threats, Illusive's three core elements work in tandem to help you paralyze attackers and stop them in their tracks.

Cloud Security • Insider Threat Defense • M&A Security • SOC Efficiency • Unsecurable System Protection

Perpetually remove attack pathways

- Gain unprecedented, risk-focused visibility to errant access
- Continuously minimize your attack surface; improve cyber agility

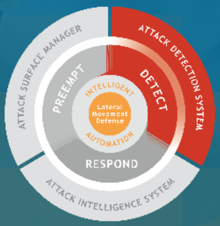
Attack Surface Manager (ASM) Preempts attacks by continuously identifying and removing errant credentials, connections and pathways attackers leverage to move sideways on a network, as well as the data they use to fuel their attacks. A clean cyber environment denies attackers the keys they need to move forward.



Your environment becomes a trap

- Detect attackers at "Patient Zero" before damage is done
- Reduce false positives—a tripped deception means game on!

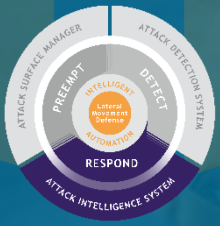
Attack Detection System replaces the real data that was found and removed by ASM and blankets the network with deceptive data that authentically mimics data attackers expect to see, disorienting the attacker with no choice but to engage with deceptive data---revealing their presence. The odds now shift in favor of the defenders.



Remediate with real-time forensics

- Make quick and smart response decisions under fire
- Magnify the power of limited IR resources

Attack Intelligence System springs into action when a deception is tripped to deliver rich, real-time source and target forensics that pinpoint the attacker's location and violation, providing the SOC with a fully-formed incident notification that cuts research and investigation time by two-thirds.



Visit us at www.illusivenetworks.com

Email us at info@illusivenetworks.com

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

Illusive Networks stops cyberattacks by destroying attackers' ability to make safe decisions as they attempt to move toward their targets. Using Illusive, organizations eliminate high-risk pathways to critical systems, detect attackers early in the attack process, and capture real-time forensics that focus and accelerate incident response and improve resilience. Through simple, agentless technology, Illusive provides nimble, easy-to-use solutions that enable organizations to continuously improve their cyber risk posture and function with greater confidence and agility.