illusive®

Deception Management System

Solution Brief

illusive

The Art of Deception: Creating an alternate reality

When advanced attackers compromise a network, they relentlessly inch towards a clearly defined target. To reach their goal, these persistent and highly skilled attackers iteratively collect data, analyze it, and use it to move laterally.

Deception technology is the most effective way to detect advanced attackers as it uses their tactics against them. Deception technology takes advantage of attackers' persistence and their iterative method to detect advanced attacks early. Using fake information such as user-credentials, servers, and websites, you can detect attackers before they reach sensitive data.

To stop even the most advanced attacks, planted deceptions must blend perfectly into a network and agentlessly adapt as the environment changes. Sophisticated attackers can identify and avoid manually managed deceptions as they are scattered, outdated, or dissimilar to real information. To remain one step ahead, state-of-the-art, network-optimized deceptions automatically and dynamically construct a deceptive layer over your entire network, with zero IT footprint. By constantly creating an environment where attackers cannot tell real information from fake information, deceptions ensure that the data attackers collect is always unreliable. And if attackers cannot rely on collected data, they cannot proceed.

Due to the growth of the Crime-as-a-Service model, Europol's 2016 Internet Organized Crime Threat Assessment report stated that APT attacks are expected to continue increasing, targeting a growing number of industries. These attacks pose not only a financial threat to targeted companies, but also a fundamental threat to their brands. For example, excluding legal costs, Target's 2013 APT cost the retail giant $162 million while Forbes business magazine reported that, for that year's final quarter, sales declined by almost 50% and up to 10% of customers indicated that they would never shop there again.

The illusive Deception Management System: Agentless, automatically manufactured deceptions to best-fit your network

The illusive Deception Management System™ (DMS) is an evolutionary breakthrough in the agentless illusive Deceptions Everywhere® solution. Using advanced machine-learning, the DMS preemptively identifies attack vectors and autonomously crafts best-fit deceptions for optimal cyberattack protection.

In an industry-leading advancement, the DMS automatically creates an optimized deceptive environment for your network. DMS handles the creation, diversification, placement, and dynamic modification of deceptions, planting them across the network without infrastructure, to construct the most effective deceptive layer.

Though deceptions are invisible to authorized users, they are unavoidable to attackers. In an attack's early stages, when an attacker attempts a lateral movement, illusive produces high-fidelity alerts and gathers source-based forensics in real-time. Reliable alerts enable automatic mitigation, while immediate forensic-gathering enables easier incident response.

What is the Deception Management System?

The illusive Deception Management System™ is the first-of-its-kind solution that uses advanced machine-learning to foresee and preempt cyberattack vectors, automatically creating, deploying, and updating optimized deceptions across your network.

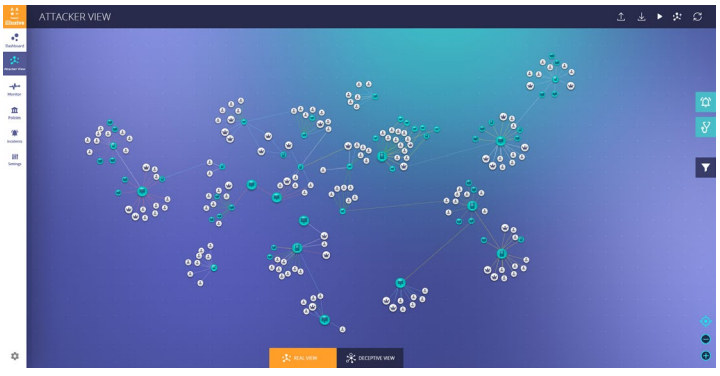
Automated Deception Management: Smart protection made simple

To benefit from trustworthy and actionable alerts, illusive offers made-to-measure deceptions without interrupting your IT team's productivity. An efficient plug-and-play solution, the automatic network-discovery, immediate network analysis, instant deception-creation, and "one-click" agentless deployment ensure zero disruptions to users.

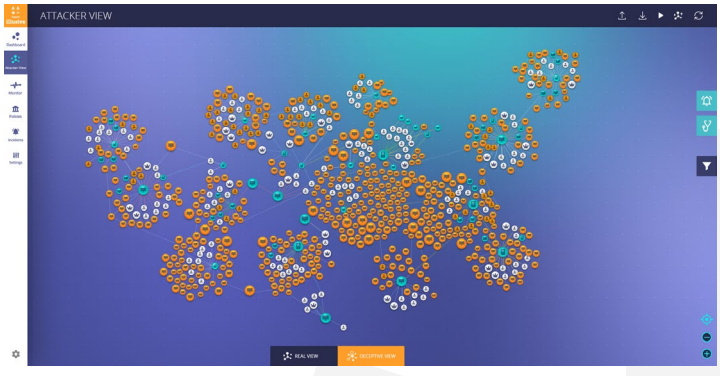
To ensure attackers find fake data indistinguishable from real data, the illusive DMS autonomously discovers network connections, conventions, data, and attack-risks. This information is then used to create tailor-made deceptions for each attack-vector. For every network location, you can gain penetrating insight into network risks and plant deceptions whose names, data, connections, and access-privileges follow the customer-specific reality.

illusive protection is proactive, not reactive. Advanced machine-learning techniques ensure that hidden attack vectors are identified and protected before attacks occur.

As your organization shifts and develops, illusive adapts to ensure attacks are detected in their infancy. By deploying realistic deceptions in new locations and updating them to adjust to changes, illusive constantly monitors your network and adapts protection to provide a solution that evolves alongside your network.



Real Network



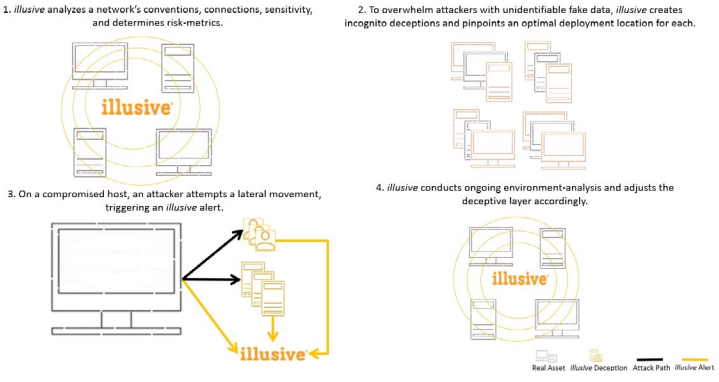
Network with Deceptions

Benefits

- *Agentless*
- *Automatically identifies and neutralizes attack vectors*
- *Makes it impossible for attackers to tell what is real and what is fake*
- *Increases attack detection via optimal deception-deployment*
- *Continuously monitors your network and applies adaptive protection*
- *Requires zero maintenance or business disruption*
- *Involves minimal IT investment*
- *Engages autonomous systems without reliance on other tools*
- *Offers "one-click" deception deployment*
- *No IT footprint*

"illusive networks is a perfect example of the kind of 'out of the box' thinking necessary to challenge the growing threat of targeted attacks."

Eric Schmidt, Google Chairman and Founding Partner at Innovation Endeavors



illusive

The illusive difference: Deceptions Everywhere

illusive exposes attackers by turning their strengths into weaknesses. The revolutionary illusive networks Deceptions Everywhere® solution weaves a deceptive layer over your entire network, creating an environment where attackers cannot rely on the information they collect. If attackers cannot collect reliable data, they cannot make decisions. And if they cannot make decisions, the attack is paralyzed.

As deceptions are invisible to authorized users, no false-positive alerts are triggered; every notification of deception-use is a high-fidelity indication of an attack. With zero false-positives, you can reliably configure automatic mitigation.

illusive's actionable alerts provide the real-time forensic information needed to investigate and contain attacks. Information is collected from compromised hosts at the exact moment that attackers use false data, before they have time to clean their tracks, saving Incident Response teams precious time and energy.

Using the illusive Deception Management System™ (DMS), deceptions are automatically optimized, instantly diversified, and constantly monitored. The agentless technology ensures zero-impact to business operations and working environments.

Revolutionary visibility: Attacker View

The illusive Attacker View™ is a powerful application that displays your network as attackers see it. The Attacker View is a groundbreaking tool, enabling you to evaluate your network's cyberattack risk-status, map discoverable and reachable sensitive assets, minimize attack-paths, monitor attacker movements, and mitigate remaining risks via deception policies. Additionally, the Attacker View produces an Attack-Risk Report to help you manage your organization's safety.

"By 2019, continued weaknesses in prevention will drive at least 10% of large enterprises to adopt deception-enabled tools and tactics (up from just 5% in 2016), improving detection and response, and shifting some of the economic burden to attackers."

Gartner Competitive Landscape: Distributed Deception, August 2016

A Unique Approach

- *Agentless operation ensures zero disruptions to business*
- *illusive offers the earliest attack-alerts in the industry*
- *Incidents trigger the highest-fidelity alerts available, enabling automatic mitigation*
- *illusive automatically manages, distributes, and monitors dynamic deceptions*
- *Attackers reveal themselves long before reaching sensitive data*
- *The Attacker View™ reveals hidden attack-paths before attacks occur*
- *illusive collects the most detailed, real-time source-based forensics attainable*

About illusive networks

illusive networks is a global pioneer of deception technology – the most effective protection against advanced attacks. To lead the Distributed Deception Platform, top cyber-attack specialists from Israel's elite cybersecurity Intelligence Corps (unit 8200) were brought together with pioneering experts and entrepreneurs with over 50 years of combined experience in cyber-warfare and cyber-security.

With offices in Tel Aviv and New York, illusive networks changes the asymmetry of cyber-warfare by focusing on the weakest link in a targeted attack – the human team behind it.

For more details, visit www.illusivenetworks.com or contact info@illusivenetworks.com.