Attack Detection System™

Create a hostile environment for attackers with agentless deceptions that fool attackers into revealing their presence and stop lateral movement toward your critical assets.

Cyberattacks are inevitable—and nation-state and ransomware attackers are savvier than ever in "living off the land" and evading security monitoring and controls. You can't predict where an attacker will break in, or where malicious inside activity will break out, but you can detect attackers before a crisis occurs. And it doesn't have to be complex. The Attack Detection System uses the attackers' own lateral movement process to force them to reveal themselves.

From Reactive to Active Defense

Attackers are already inside your network, too often undetected by solutions focused on the perimeter or behavioral anomalies. The recently published MITRE Shield framework advocates that security teams adopt a more "active defense" strategy. Deception plays a primary component, and we are not referring to the old-fashioned honeypot approach. Attack Detection System actively engages the attacker once they have established a beachhead. By creating a hostile environment that traps the attacker unwittingly at every turn, Illusive slows the attacker down, and keeps them away from critical business assets.

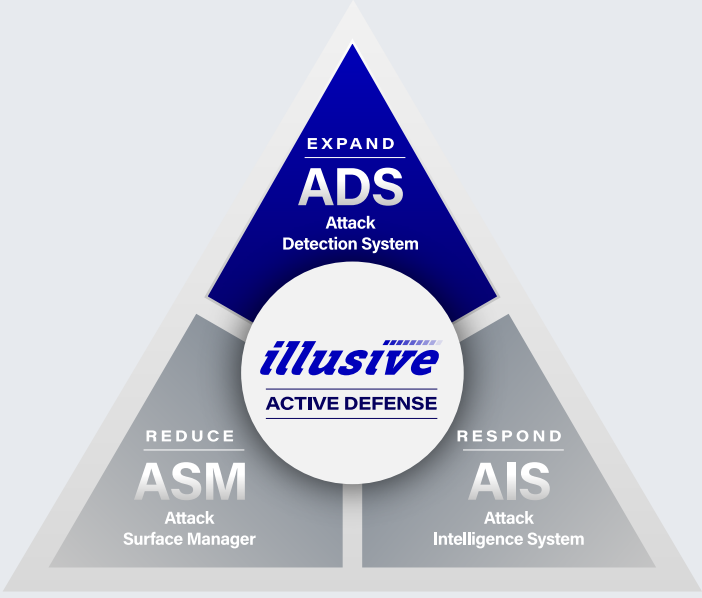
Reversing the Risk Equation

Illusive plants featherweight deceptions to mimic the real data, credentials, and connections the attacker needs. Confronted with a distorted view of reality, the attacker is overcome by the odds: it is impossible to choose a real path forward without activating a deception. Unknown to the attacker, one wrong choice triggers an alert. Incident responders can see how far the attacker is from critical business assets. With real-time source forensics in hand, they can take informed actions to stop the attack and avert business impact.

Detection as Agile as Your Business

By focusing on the attacker's process rather than on the tools or malware they're using, organizations are better protected from unknown, evolving threats, and can detect malicious behavior—regardless of what gaps may exist in their security controls. Enabled by intelligent automation, Illusive's approach scales and adapts—so the business can operate with greater confidence. Illusive is able to be deployed on-premise, or in cloud or hybrid cloud environments. Deceptions mimic cloud assets and protect cloud-based crown jewels.

The Attack Detection System is part of the Illusive Active Defense Suite to create an environment that is hostile to attacker activities. 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 of an attacker that has established a beachhead.



Attack Detection System Features and Benefits

75+ Deception Techniques

Utilize deception-powered Active Defense techniques to imitate credentials, connections, data, systems, and other artifacts that appear useful to the attacker. Ensure early attacker detection—both insiders and external attackers—no matter where compromise begins.

Agentless Detection and Protection

Illusive's unique agentless approach benefits both IT administrators and security teams. Built on intelligent automation, it is designed to have a light operational footprint to minimize the impact on IT and can't be disabled or circumvented by attackers like other agent-based solutions.

A View from the Attacker's Perspective

The Attack Detection System management console shows how close attackers are to critical assets, a full timeline of attacker activity once deceptions are engaged, full visibility into how attackers perceive the deceptive data, and much more intelligence on attacker activity.

Automated Deception Customized to Each Endpoint

An intelligent automation system enables a highly authentic deception environment that scales and adapts over time with very little human effort. ADS analyzes the endpoint landscape, designs tailored deceptions for each machine, deploys them through a one-click process, and manages the ongoing process of adjusting and managing deceptions over time.

Trap Server to Detour Ransomware and Other Threats

The Attack Detection System Trap Server invisibly interacts with attackers, moving them away from real data and critical assets and towards a completely imaginary attack surface.

Deceptive Microsoft Office Beacon Files

Organizations can automate the creation and customization of hundreds of thousands of deceptive Word and Excel documents that are indistinguishable from the genuine article, right down to the usage of company logos and letterhead. These fake but seemingly real Office documents can be loaded with fake data that sets off an alert as soon as an attacker tries to use the information to gain access.

FirstMove Services

Illusive provides a full scope of services to fill staffing gaps as needed, from assistance planning deployments to development of special use cases and interpretation of alerts.

The simplest way to detect the stealthiest attackers

Illusive's Attack Detection System (ADS) makes it impossible for attackers to move laterally by transforming every endpoint into a web of deceptions. ADS deterministically accelerates threat detection by identifying threats based on attacker interaction with deceptions, not probabilistic controls based on signatures or behaviors. Unlike other deception technologies that deploy agents or honeypots which can tip off or be exploited by the attacker, its agentless architecture prevents attacker detection. ADS is undefeated in over 130 red team exercises with some of the most sophisticated security organizations from Microsoft, Mandiant, US DoD, and Cisco.

- **Ensures early attacker detection**—both insiders and intruders—no matter where compromise begins.
- **Reduces noise in the SOC** by focusing attention on high- fidelity alerts.
- **Agentless technology deploys in days** with little IT involvement.
- **Provides continuous defense** by dynamically adjusting as the business environment changes.
- **Proven to scale** across networks of more than 1M endpoints.
- **Fills in the gaps left by signature and baseline-based threat detection** approaches so that previously unidentified attacks can be detected and stopped.

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 pharmaceuticals. Illusive has participated in over 130+ red team exercises and has never lost one!
To learn more, visit **www.illusive.com**