Attack Detection System™

Create the illusion of an expanded attack surface with agentless deceptions that fool attackers into revealing their presence.

Cyberattacks are inevitable—and attackers are more savvy 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. Illusive Networks Attack Detection System uses the attackers' own lateral movement process to force them to reveal themselves.

Attackers are human

After establishing a foothold, the attacker's next step is to understand their surroundings and decide where they'll try to move next. Though they may use automated attack tools to shortcut the process, they cannot avoid undertaking an iterative, human decision-making process to move from system to system to reach their targets.

Reversing the risk equation

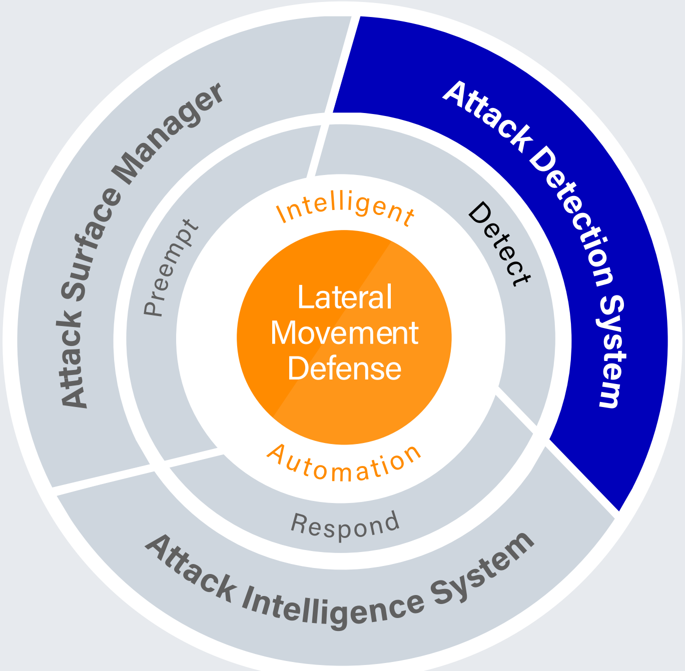
Illusive plants featherweight deceptions on every endpoint to mimic the real data, credentials, and connections the attacker needs. Confronted with a distorted view of reality, the attacker is overcome by the odds: it is impossible to choose a real path forward without activating a deception.

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 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.

The Attack Detection System is part of Illusive's comprehensive portfolio to undermine the lateral movement process— before, during, and after the attack by stopping an attackers ability to make decisions.



Attack Detection System components

17 Deception families

Deceptions use over 50 techniques to mimic credentials, connections, data, systems, and other artifacts that appear useful to the attacker. Deceptions are invisible to legitimate users and are, to the attacker, indistinguishable from real artifacts.

Deception Management System (DMS)

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

Trap Server

The Trap Server invisibly Interacts with attackers and manages collection of real-time host forensics when deceptions are activated.

Attacker View

The management console shows proximity of attackers to Crown Jewel systems and high-privilege credentials.

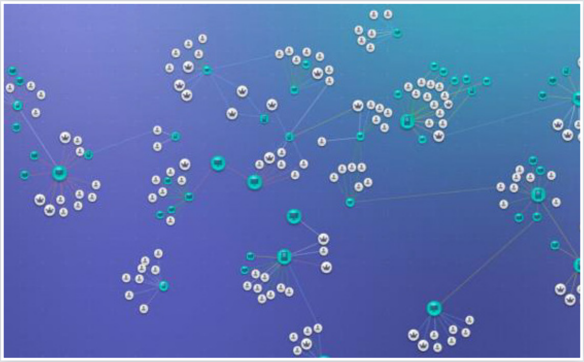
Forensics Timeline

A unified, sortable per-incident chronology of forensic data.

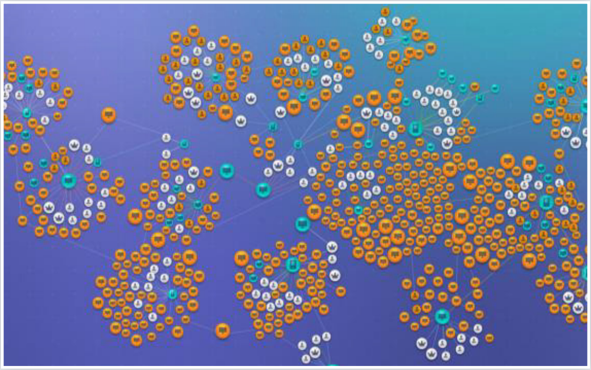
FirstMove Services

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.

A typical network environment



A network with deceptions deployed



The simplest way to detect stealth attackers

- **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 500,000 endpoints.

To be effective, deceptions must appear authentic within each unique organization. DMS learns relevant characteristics of the environment and automatically designs, deploys and manages a web of tailored deceptions.