Illusive Shadow™

Detect and respond to identity threats to stop privilege escalation and lateral movement to your critical assets

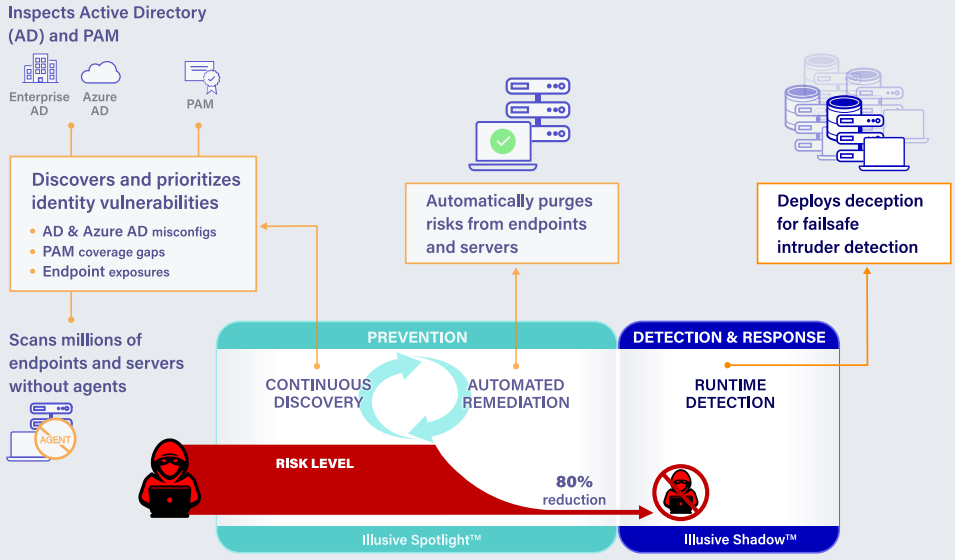
Identity Threat Detection & Response (ITDR) is Critical to Protect Against the #1 Vector for Attack

The global increase in cyberattacks has been enabled by attackers shifting their focus from system to identity-based attacks, such as account takeover attacks (ATOs). These attacks are often completed in only days and go undetected without leaving any indicators of compromise or evidence of malware.

From Probabilistic to Deterministic Detection

The probabilistic approaches to detection, using signatures or behavioral analysis, don't accurately detect account takeover attacks, or privilege escalation and lateral movement activities. They also often overwhelm security teams with false positives. To consistently detect attacks that bypass signature and behavioral approaches to detection, a deterministic approach is needed. Deceptive techniques are proven at enabling high-fidelity detection of privilege escalation and lateral movement. Unlike the outdated honeypots that use deception to lure attackers away from critical assets to gain threat intelligence, Illusive Shadow™ actively engages attackers in the organization's production environments for the sole purpose of detecting their existence. Believable, automatically customized, and featherweight deceptive "stories" are planted on endpoints, that mimic real data, credentials, and connections attackers look for during their attack. Unknown to the attacker, they unwittingly trigger an alert to the security team. With real-time source forensics in hand, the security team can take informed actions to stop the attack and avert business impact.

Illusive Shadow™ is part of Illusive's comprehensive ITDR solution



Illusive Shadow™ Features and Benefits

75+ Deception Techniques

Utilize active deception 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.

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. Illusive Shadow™ 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.

A View from the Attacker's Perspective

The Illusive Shadow™ 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.

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.

The simplest way to detect the stealthiest attackers

Illusive Shadow™ makes it impossible for attackers to move laterally by transforming every endpoint into a web of deceptions. It 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. Illusive is undefeated in over 140 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 a million endpoints
- **Fills in the gaps** left by signature and baseline-based threat detection approaches so that previously unidentified attacks can be detected and stopped

About Illusive

Illusive discovers and remediates privileged identity risk policy violations that are exploited in all ransomware and other cyberattacks. Despite significant investment to protect identities, including deployment of PAM and MFA solutions, every organization has exploitable identities. Illusive makes it easy to find these previously unknown vulnerable identities sprawled across an organization's endpoints and servers, then eliminate them or deploy proven identity compromise detection techniques to stop attackers. Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help companies protect their critical assets, including the largest global financials and pharmaceuticals. Illusive has participated in over 140 red team exercises and has never lost one.

[1]https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/