Partner Brief

The Illusive Active Defense Suite and Splunk Enterprise Security

Real-Time Post-Breach Threat Detection and Management

Illusive Active Defense Suite integrates with Splunk to help organizations gain continuous visibility into their attack surface risk, provide real-time threat detection, and automate incident response to attacks from ransomware, nation-state threat actors and insiders. Illusive's attack surface hygiene and deception products deliver risk data and high-fidelity alerts that Splunk customers can leverage to reduce the risk of attack and shrink the time and overhead required to identify, analyze and remediate high risk conditions. With the power of Illusive and Splunk working together, your organization can reduce risk and increase IR and SOC efficiency, improve threat visibility and ultimately harden your overall security posture.

With Illusive and Splunk working in tandem, your organization reaps the following advantages:

- Visibility into risk of attacker credential harvesting and lateral movement
- Detect the most sophisticated ransomware and nation-state attackers and insiders
- Comprehensive forensic data about attackers and endpoints
- On-demand Illusive forensic collection through Splunk playbooks
- View high-fidelity Illusive detection alerts within Splunk

How Illusive and Splunk Work Together to Identify and Manage Threats

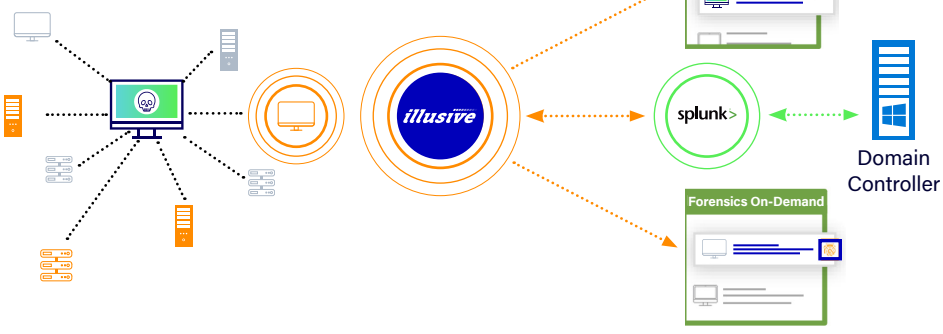
1

Illusive provides attack risk data and early detection of lateral movement by humans or malware on the endpoint

2

Attacker unknowingly accesses a highly authentic endpoint deception

Illusive sends high-fidelity attack risk, alert and forensic data for **Splunk** to leverage



Ensure Attack Surface Hygiene

Illusive identifies and removes unnecessary credential, connections, and pathways to crown jewel resources.

Early Breach Detection through Deception

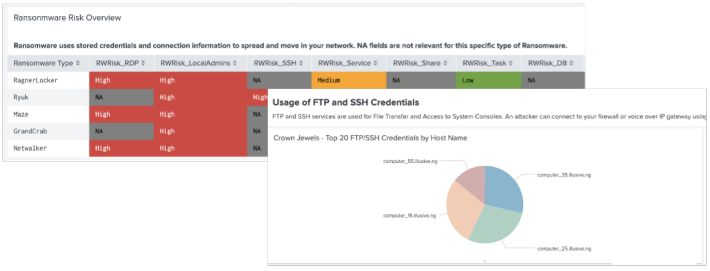
Illusive spreads inescapable deceptions throughout your network that are indistinguishable from the sensitive materials cybercriminals seek to help them move sideways after a breach. Once attackers inevitably interact with one of these deceptions, they provide a high-fidelity incident notification of their malicious presence.

Powerful Source-Based Forensics

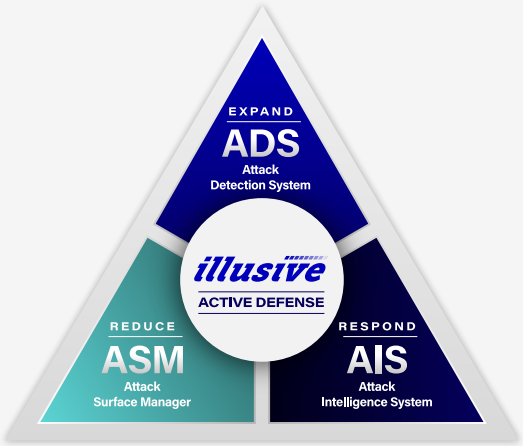
Rich forensics about threats and attackers get captured and can be automated as an integral part of your Splunk playbooks. Splunk also enables additional deception techniques, leveraging Splunk Enterprise Security's communication with your Active Directory to trick attackers into stealing fake credentials, which then act as a beacon that warns of an attacker's presence.

Illusive and Splunk in Collaboration: Key Benefits

- Identify unnecessary credentials and pathways that fuel attackers
- Detect and isolate attackers early in the threat lifecycle
- Halt vertical movement between hybrid and multi-cloud ecosystems
- Improve efficiency of shorthanded limited SOC and IR teams
- Expand incident playbook automation scenarios within Splunk
- Strengthen your security posture with advanced deception techniques



The **Illusive Active Defense Suite** provides centralized management across even the largest and most distributed environments. Three products work together to protect organizations against today's most sophisticated cyberattacks.



ASM: Attack Surface Manager continuously analyzes and removes unnecessary credentials and pathways, reducing the attack surface.

ADS: **Attack Detection System** makes it impossible for attackers to move laterally by transforming every endpoint into a web of deceptions.

AIS: **Attack Intelligence System** delivers human readable on-demand telemetry for current attacker activities to speed investigation and remediation.

Illusive's 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 for an attacker that has established a beachhead.

About Illusive

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

About Splunk

Splunk is the world's first Data-to-Everything Platform.

Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver.

Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future.

With more than 5,000 employees in 27 offices worldwide, we're focused on creating lasting data outcomes for our customers.