illusive | Azure Sentinel

Partner Brief

Illusive for Microsoft Azure Sentinel

High-Fidelity Attack Detection, Incident Enrichment & Threat Intelligence

Recent events have redefined the meaning of "normal user activity," and cybersecurity approaches must follow suit. With the massive shift to working from home, and its subsequent uptick in alert volume, organizations need tools that will help them quickly determine which alerts should be prioritized for mitigation. The Illusive Active Defense Suite integration with Microsoft Azure Sentinel provides high-fidelity notification and full intelligence about attack surface risk and the most dangerous in-network threats so they can be stopped early before damage can be done.

Stop the Lateral Movement that Enables Attacks

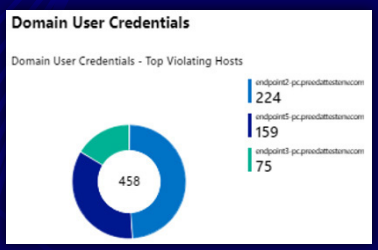
Illusive attack surface management identifies and removes leftover credentials and connections that attackers leverage to move from machine to machine as they laterally move towards the critical assets they seek to steal. Then, Illusive replaces those credentials and connections with deceptive versions that attackers would expect to encounter and exploit. Once attackers engage with this deceptive data, organizations receive full forensics on attacker activity and can take any necessary steps to remediate the threat.

Through the Illusive Attack Management System data connector, organizations can share Illusive's attack surface analysis data and incident logs with Azure Sentinel. This information can be viewed from dedicated dashboards especially designed for Azure Sentinel that provide actionable insight into attack surface risk and that provide high-fidelity notification of unauthorized lateral movement in your organization's network.

The Benefits of Integrating Illusive with Azure Sentinel

- Incorporate Illusive attack surface management and high-fidelity threat detection within Azure Sentinel
- Detect malicious lateral movement from anywhere to anywhere in hybrid cloud environments
- Find imminent threats that behavioral- based detection often misses
- Map and secure network pathways to critical assets
- Reduce false positives to make threat investigations quicker
- Get enriched Illusive forensic intelligence for any alert Azure Sentinel aggregates
- Custom playbooks and APIs for Sentinel that automate additional attack intelligence and forensics
- Leverage detailed threat analytics to make incident triage more efficient

Detailed east-west lateral movement risk and attack intelligence from within Azure Sentinel



Illusive for Azure Sentinel Key Features

CEF Connector and Dashboards
Ingest Illusive attack surface management and threat detection data into Azure Sentinel. A series of dashboards with full analytics about potential attack risks and current threats provides intelligence about the most dangerous threats, their distance from critical assets, attacker behavior, and much more.

End-to-End Microsoft Cloud Tools Support
Out-of-the-box integrations with Azure AD, Intune and Microsoft Managed Desktop (MMD) allow for a full Illusive deployment in Microsoft- enabled cloud environments.

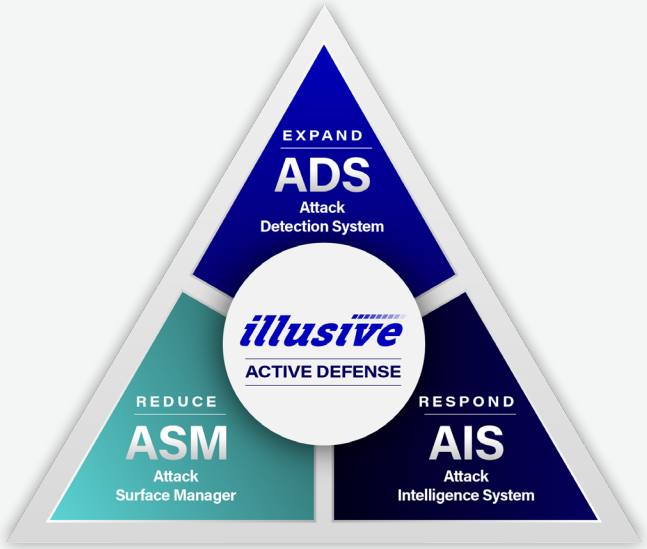
Illusive Playbooks Designed for Sentinel
Enhance Security Operations Center (SOC) efficiency for any event detected by Sentinel. Get full Illusive forensics for all incidents, including a chronological timeline of all events on a specific host, and automate attack surface reduction as new potentially risky attacker pathways appear.

Enhanced Threat Visibility through Attack Surface Manager
Illusive's Attack Surface Manager, a part of the Illusive Active Defense Suite, provides increased visibility into the potential ways that attackers can move laterally towards critical data on your network. Get crucial intelligence about your crown jewel assets, how many hops it would take to reach them, which machines have admin credentials stored on them, and much more.

Launch Automated Deception Campaigns When Risk Is Detected
The Illusive Active Defense Suite boasts a full array of data-based network deceptions, device emulations and full decoy environments. Network deceptions and emulations can be triggered to launch when threats are detected to instantly block malicious lateral movement.

Comprehensive Forensics that Increase SOC Efficiency
With Illusive's detailed forensics about attack surface risks, impending threats and attacker behavior, organizations are able to empower lower tier analysts and improve the quality of their escalations, freeing upper-tier analysts to focus on the most urgent threats and waste less time on false positives.

Illusive's Active Defense Suite 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.



The Illusive Active Defense Suite consists of three complementary security technologies:

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

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

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