Illusive Active Defense for Microsoft Defender for Endpoint

Illusive Active Defense and Microsoft Defender for Endpoint are complementary solutions that, when deployed together, offer improved threat detection effectiveness for nation-state and targeted ransomware (human-operated) attacks. The integrated solution represents a new diversified threat detection strategy, combining deterministic active defense, anomaly-based detection, and automated response in a single view.

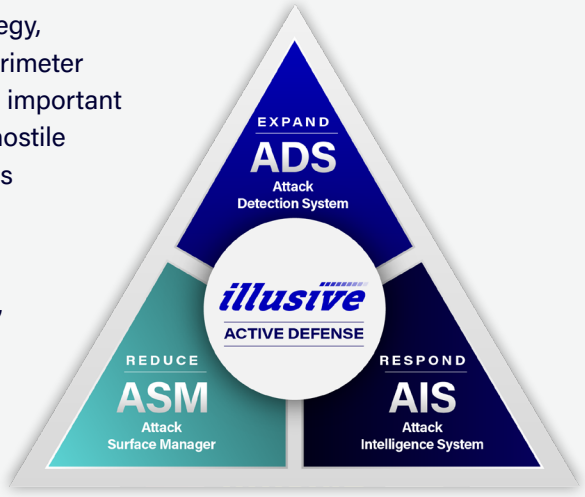
Today's prevalent and sophisticated human-operated attacks are wreaking havoc across industries, leveraging advanced attack techniques that can go undetected by current security controls. The attacker gains a beachhead on a host, harvests any available privileged identities, then moves laterally with precision towards high-value assets. A more diversified detection strategy, enabled by the integration of Illusive and Microsoft solutions, reduces risk by protecting privileged identities and endpoints, and automating response to contain the threat before targeted data and assets (crown jewels) are accessed.

Benefits of Illusive Active Defense for Microsoft Defender for Endpoint

- Unified deterministic and behavioral detection to prevent attackers from reaching high value assets
- Single pane of glass increases efficacy of threat detection and response operations
- Visualized and automated remediation of high-risk access pathways to crown jewels
- Shared crown jewel definitions provide proximity context for increased alert efficacy
- Automated response to detected threats
- Simplified deployment and operations

In the same way attackers have discovered ways to evade past detection controls like signature detection and behavioral analysis, they are now employing tactics to circumvent endpoint detection and response (EDR), a recent addition to many organizations' suite of security controls. EDR is an important advancement in endpoint detection controls, but the attack surface scope and growing attacker sophistication require a more diversified detection strategy. Combining the endpoint detection capabilities of Microsoft Defender for Endpoint with Illusive's offensively leaning Active Defense solution provides organizations the required diversified detection system. The integrated solution offers the industry's only behavioral and deterministic detection solution that identifies unusual behavior and transforms endpoints into an array of deceptions, making it nearly impossible for the attacker to move laterally without detection.

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.



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.

Illusive Active Defense and Microsoft Defender for Endpoint

The integrated solution is the first to combine deterministic active defense countermeasures, anomaly-based detection, and automated response in a single user interface to cover all phases of the MITRE ATT&CK and SHIELD frameworks. By pairing Illusive's deterministic detection with Microsoft's ability to quickly contain a compromised host, organizations can finally gain a tactical advantage against attackers, reducing risk and saving significant time in investigation and response efforts.

MITRE ATT&CK

1 Initial Access	2 Execution	3 Persistence	4 Privilege Escalation	5 Defense Evasion	6 Credential Access	7 Discovery	8 Lateral Movement	9 Collection	10 Command & Control	11 Exfiltration
Microsoft					**Illusive**				Microsoft	

MITRE Shield

1 Channel	2 Collect	3 Contain	4 Detect	5 Disrupt	6 Facilitate	7 Legitimize	8 Test
Illusive							

The unified system also leverages a diversified implementation strategy, combining agent and agentless detection architectures to maximize resilience against increasingly sophisticated attacker tactics. From the recent SolarWinds/Solarigate attacks, we have learned attackers are now employing advanced techniques to disable endpoint detection and monitoring solutions. Illusive's agentless detection architecture makes it impossible for the attacker to detect the presence of or disable Active Defense, so attacker activities are still detected and captured. The diagram of a unified Illusive and Microsoft solution below outlines the detection process from deployment of an Active Defense deception framework from attack through response.