illusive | Microsoft

Partner Brief

Defend Microsoft Environments with Deterministic Threat Detection

What We Do at Illusive

Illusive protects enterprises with deterministic threat detection that paralyzes attackers:

REDUCE

Shrink the attack surface by finding and removing errant credentials, connections, and pathways that attackers use to reach crown jewel assets

EXPAND

Create the illusion of an expanded attack surface by filling the environment with deceptions that force engagement—thus revealing an attacker's presence early in the attack lifecycle

RESPOND

Speed incident response by instantly providing defenders with easily consumable contextual and telemetry data detailing the precise source and nature of the attack

Unlike anomalistic alerts that require extensive investigation to validate, if an Illusive alert goes off, there is a problem needing attention. Period.

End-to-End Protection for Microsoft-Enabled Environments

Customers are migrating to Microsoft Azure infrastructure and workplace productivity applications, and building security operations around Microsoft's 365 Defender suite of technologies. Illusive integrates with Microsoft to enrich the security of Microsoft-enabled hybrid cloud environments and augment the functionality of Microsoft's security stack. Illusive is a lightweight, agentless solution – comprised of a single binary – that can be deployed on premises or in the cloud with no hardware required.

Azure Active Directory

Azure AD
Defend Azure AD privileged identities & prevent attackers from leveraging stolen AD credentials

Cloud App Security
Automate attacker discovery and response in SaaS & cloud environments

Illusive + Microsoft
Defender Technologies

Extend Microsoft 365 E5 Security Bundle with Comprehensive Lateral Threat Management

Defender for Endpoint
Enhance risk exposure & streamline detection & response

Defender for Identity

Defender for Identity
Broaden threat detection beyond authentication to your entire on-premise ecosystem

Azure Sentinel
Enrich with specially designed high-fidelity threat notification and intelligence dashboards

Office 365

Defender for Office 365
Protect O365 via deceptive MS Office documents with beacons

Illusive and Microsoft Defender for Endpoint

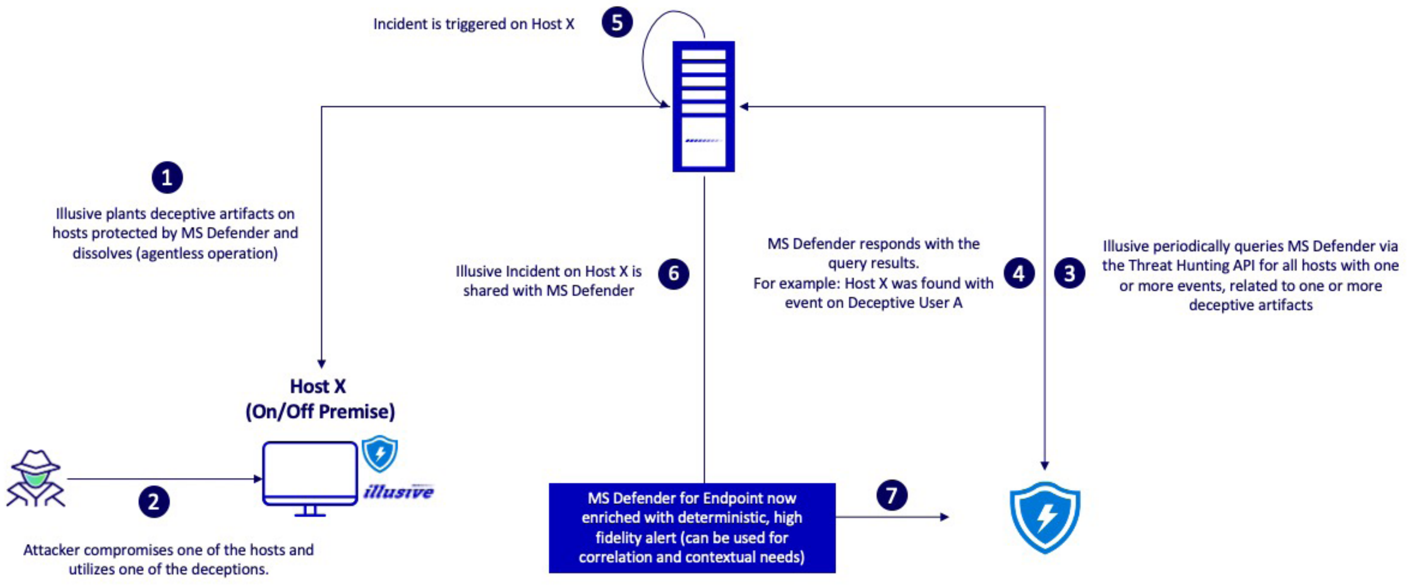
Combine deterministic active defense countermeasures, anomaly-based detection, and automated response on a single pane of glass. By pairing Illusive's deterministic detection with Microsoft's ability to quickly contain a compromised host, organizations can finally gain a tactical advantage against ransomware and nation-state attackers, reducing risk and saving significant time in investigation and response efforts.

Challenge

- 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.
- Once an attacker gains a beachhead on a host and harvests any available privileged identities they can find there, moving laterally and quietly with precision towards high-value assets becomes much easier.
- 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) solutions.

Better Together

- Lateral threat movement prevention, detection and response designed for multi-cloud and hybrid cloud environments
- Unified deterministic and behavioral detection with automated response prevents attackers from reaching high-value assets
- Near 0% false positive detection rate of human-derived malicious activity that often circumnavigates signature or anomaly-based tools
- Single user interface increases efficacy of threat detection and response operations
- Visualized and automated remediation of high-risk access pathways to crown jewel assets
- Shared crown jewel definitions provide proximity context for increased alert efficacy



1 Illusive plants deceptive artifacts on hosts protected by MS Defender and dissolves (agentless operation)

2 Attacker compromises one of the hosts and utilizes one of the deceptions.

3 Illusive periodically queries MS Defender via the Threat Hunting API for all hosts with one or more events, related to one or more deceptive artifacts

4 MS Defender responds with the query results. For example: Host X was found with event on Deceptive User A

5 Incident is triggered on Host X

6 Illusive Incident on Host X is shared with MS Defender

7 MS Defender for Endpoint now enriched with deterministic, high fidelity alert (can be used for correlation and contextual needs)

Illusive and Microsoft 365 E5 Security

Illusive provides high-fidelity threat detection and intelligence for customers of the Microsoft 365 E5 Suite of cloud-based productivity apps.

Challenge

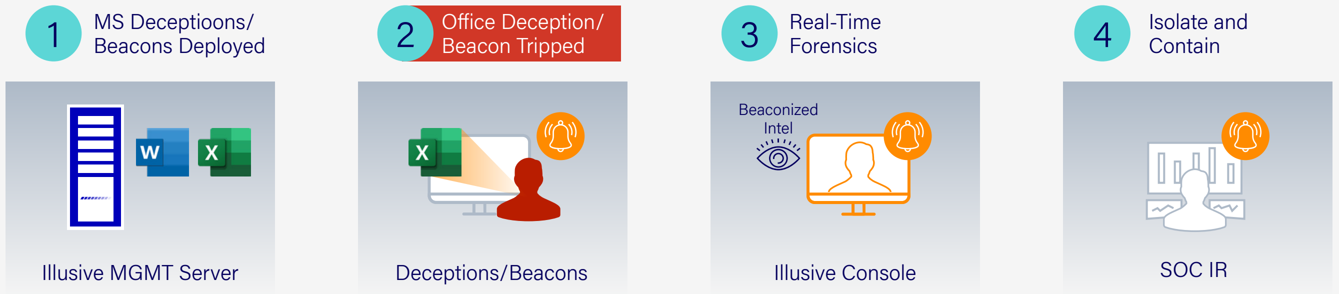
Customers are looking to reduce security stack complexity by consolidating security tools around Microsoft, but still catch ever-increasing and evolving ransomware and nation-state threats.

Better Together

Protect Enterprise Active Directory and Azure AD identities and SaaS applications from exploitation by surfacing risky identities and privileged identity misconfigurations in hybrid-cloud environments

- Enhance attack surface management and deception in Microsoft 365 E5 Security environments
- Continuously monitor and detect vulnerable identities and shadow admins outside the scope of Privileged Identity Management
- Stop ransomware, malicious insiders, nation-state attackers, and other threats attempting reconnaissance and data exfiltration
- Boost AD honeytoken capabilities with a full deception platform that tricks attackers into revealing their presence and data exfiltration
- Protect Office 365 from insider theft using deceptive Microsoft Office documents that entice attackers into engagement and provide beaconing technologies
- Illusive forensics-on demand provides fast, easy to understand real-time and historic incident timelines for any alerts including those from Microsoft security technologies

Deceptive Microsoft Office Beacon Files



Turn real or deceptive Word and Excel files into a beacon for early attack detection

Illusive and Microsoft Azure Sentinel

Illusive quickens preemption, detection and investigation of attacks for customers using Azure Sentinel. The Sentinel dashboards and data connector with Illusive provide the Sentinel user with attack surface risk data and deterministic alerts on endpoint breaches, identity compromise, or attacker movement in the network.

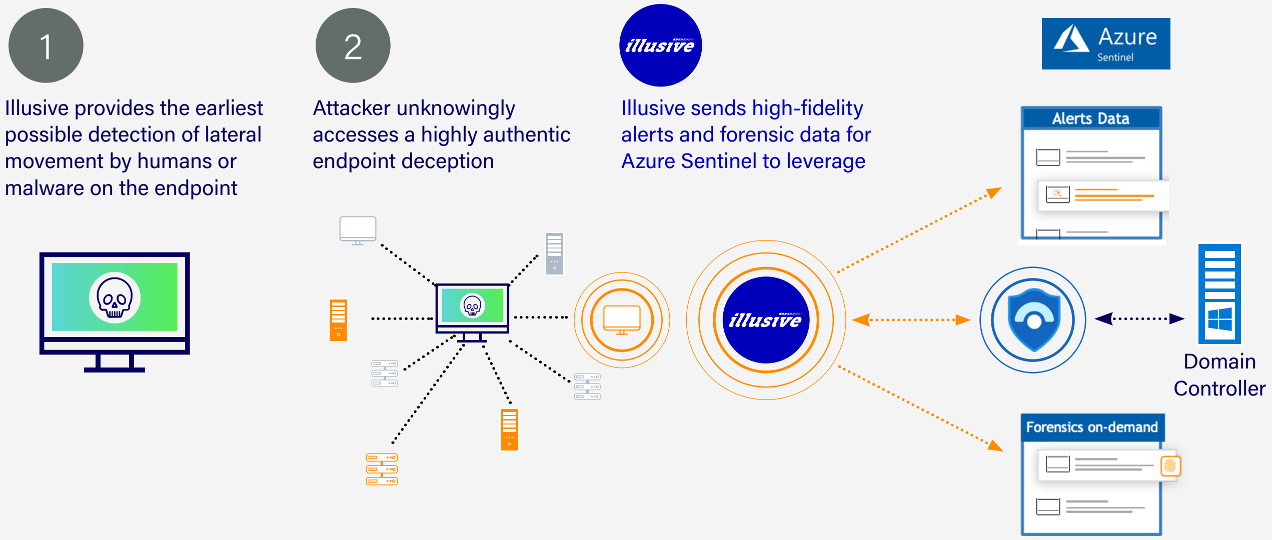
Challenge

- Customers desire more effective, efficient solutions for faster investigation
- Azure Sentinel customers want automated detection – detections that are 100% certain – to marry with Sentinel automation & orchestration response playbooks

Better Together

- Incorporate deterministic E-W/N-S detection in hybrid-cloud environments with Illusive dashboards designed for Azure Sentinel
- Illusive dashboards dynamically measure attack surface risk from within Azure Sentinel via Illusive remediation of risky credentials and connections
- Find imminent threats that behavioral-based detection often misses
- Complement Illusive's high-fidelity threat detection with Azure Sentinel's SOAR and remediation capabilities

Visualize your attack surface and deterministic alerts within Sentinel



1 Illusive provides the earliest possible detection of lateral movement by humans or malware on the endpoint

2 Attacker unknowingly accesses a highly authentic endpoint deception

Illusive sends high-fidelity alerts and forensic data for Azure Sentinel to leverage

Illusive and Microsoft Azure Cloud

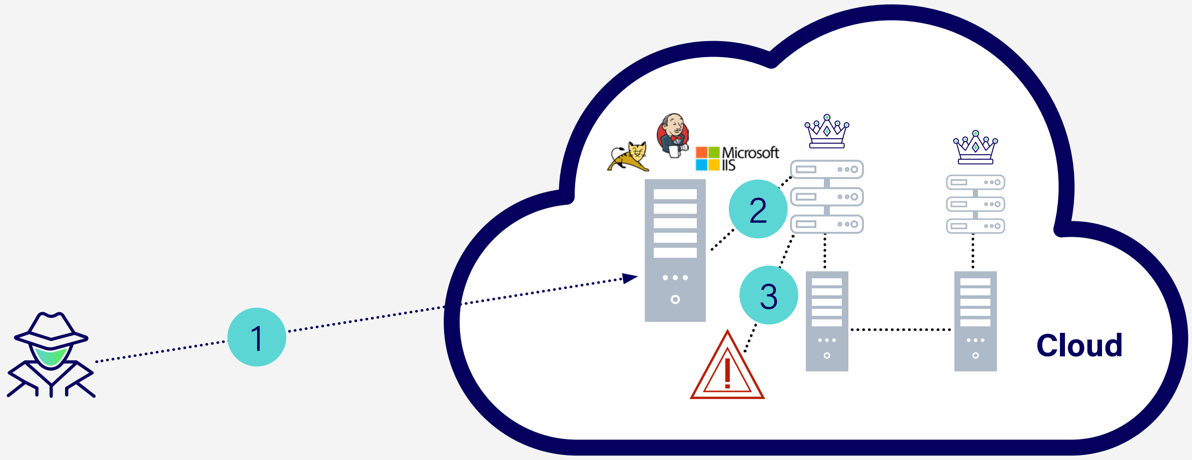
Illusive protects against lateral movement attacker behavior in the cloud by planting its web of cloud-based deceptions throughout Azure environments.

Challenge

- Lack of visibility into errant user credentials, connectivity, and attack pathways to SaaS-applications and cloud-based environments
- Malicious lateral movement bypasses anomaly-based tools
- Attacker activity may appear 'normal' in cloud environments, and existing security tools don't work as well

Better Together

- Create cloud-based deceptions that detect and stop attacker movement in hybrid-cloud (Azure) environments
- Identify insider threats coming from anywhere through a deterministic approach that avoids false positives
- Block unauthorized connections to Azure Cloud and Azure-based SaaS applications



1 Compromising Web app or CI/CD server

2 Deceptive configuration files with DB deceptive credentials/connections

3 Deterministic alert ► trapped!

For multi-cloud enabled environments, Illusive aligns with Microsoft's philosophy of extending services for protection of all assets across your ecosystem. Illusive's Microsoft integrations help customers further protect Azure and Microsoft users from today's most dangerous threats. Through attack surface management, deterministic threat detection and real-time source-based forensics, Illusive delivers end-to-end active defense to stop attacks no matter how they are carried out.

For additional resources, including solution specific integration briefs and videos, please visit the **Illusive + Microsoft integration page**.