Illusive for Microsoft 365 E5

Lateral Movement Threat Detection to Enhance Security Consolidation

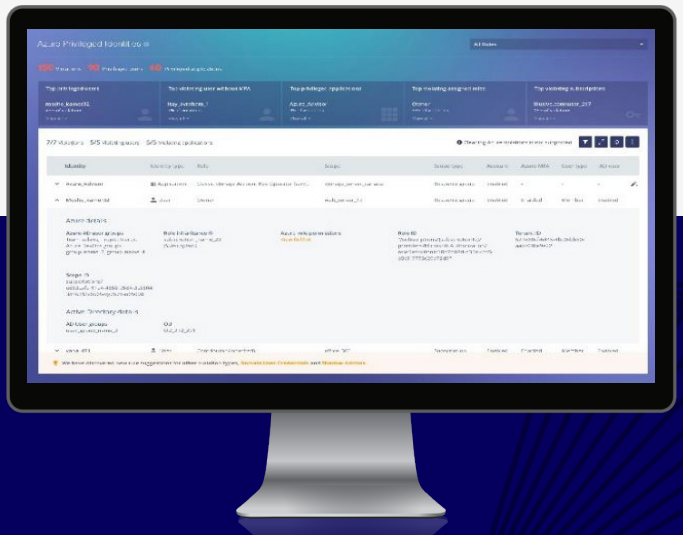
Combining many different cybersecurity solutions under one trusted vendor is a great way to make defending the enterprise more productive and cost-efficient. However, as advanced persistent threats and massive shifts to working from home continue to evolve, it remains a best practice to defend in depth and bolster consolidated security solutions with targeted protection designed to work with your existing stack. The Illusive Active Defense Suite is architected and engineered to provide attack surface management, high-fidelity threat detection and precision forensic cybersecurity intelligence both within and alongside Microsoft's 365 E5 suite of cloud-based productivity, security and compliance applications.

Malicious Lateral Movement Management for Microsoft and Beyond

Illusive combats attackers by cleaning the environment and then introducing a dense web of inescapable deceptions across the network tailored to mimic real data, credentials, and connections that an attacker needs to move laterally. Confronted with a distorted view of reality, it becomes impossible to choose a real path forward. Unknown to the attacker, one wrong step triggers an event notification capturing real-time forensic data from the system where the attacker is operating, allowing rapid response. Illusive provides comprehensive lateral threat management prevention, detection, and response capabilities through a uniquely effective threat intelligence and mitigation strategy designed to safeguard Microsoft-enabled environments.

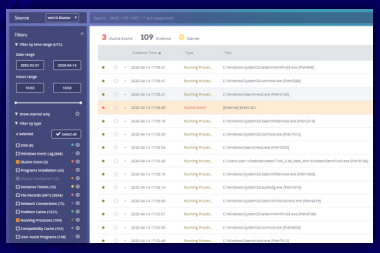
Benefits of Illusive with Microsoft 365 E5

- Enhance attack surface management and deception in Microsoft 365 E5 Security environments
- Integrations for Azure AD and Azure Sentinel that block malicious lateral movement in Microsoft environments
- Continuously monitor and detect vulnerable identities and shadow admins outside the scope of PIM
- Boost AD honeytoken capabilities with a full deception platform that tricks attackers into revealing their presence
- Protect environments beyond Microsoft including Linux, IoT, OT and ICS/SCADA
- Actionable threat analytics and forensics that make incident triage more efficient



Malicious Lateral Movement Management for Microsoft and Beyond

Forensics Timeline Speeds Incident Triage



Illusive for Microsoft 365 E5 Key Features

End-to-End Microsoft Tools Support
Illusive contains out-of-the-box integrations with Azure AD and Azure Sentinel. It also has been engineered to run seamlessly alongside other Microsoft 365 E5 Security components to allow for a full deployment of the Illusive Active Defense Suite's high-fidelity threat detection and attack surface management in Microsoft-secured environments.

Enhanced Threat Visibility through Attack Surface Manager
Illusive's Attack Surface Manager (ASM), a part of the Illusive Active Defense Suite, integrates with Microsoft Privileged Identity Manger to enhance the visibility and monitoring of potentially vulnerable privileged identities. Get crucial intelligence to remediate accounts with excessively elevated privileges, identify and remove unnecessarily cached credentials, and disable excess connectivity before attackers can take advantage.

Reduce Cloud Identity Risk and Misconfigurations
Leveraging Azure AD, Illusive complements Microsoft Cloud App Security and Azure ATP by mapping on-prem user access levels to cloud access permissions. This helps to identify misconfigurations and leads to a more thorough review of security access to IaaS and PaaS environments. Illusive also identifies and removes risky credential and connection data to cloud environments and SaaS apps.

High-Fidelity Threat Detection
Illusive leverages a web of seemingly real but ultimately deceptive data placed all over the network to fool attackers into engagement. Once attackers interact with the deceptive data, Illusive provides crucial data about genuine in-progress attacks. This instant, high-fidelity threat reporting can be leveraged to immediately shut down threats before they are able to reach critical data, including in hard-to-secure environments like IoT, OT and ICS/SCADA.

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.