Illusive Networks for Microsoft Azure Active Directory

Defend privileged identities and block malicious lateral movement

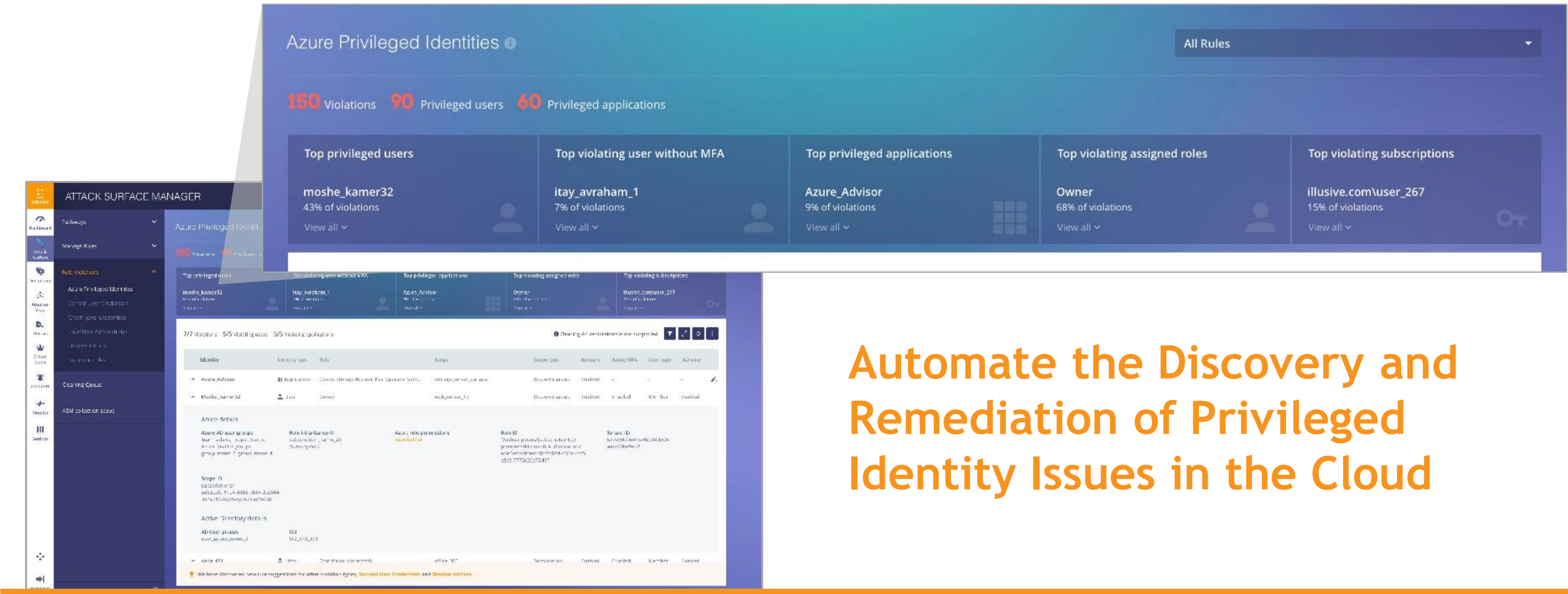
90% of global enterprise organizations use Microsoft Active Directory (AD) as their primary method of authentication and user authorization. These organizations often find it a challenge to adapt on-premise cyber defenses when moving to the cloud, as migration expands the potential attack surface and exacerbates security flaws in existing on-premise protection. This creates discrepancies between AD and Azure identity policies that lead to unauthorized access and prolonged attacker dwell times in search of high-value assets. Illusive Networks for Microsoft Azure Active Directory (AAD) gives organizations the tools they need to protect privileged user identities in the cloud from attacker abuse.

Secure Pathways to and from Azure Active Directory

The Illusive Platform safeguards privileged identities in Azure Active Directory by identifying and eliminating pathways and credentials that attackers might leverage to move towards critical data stored there. This attack surface management for AAD reduces account takeovers, lowers the mean time to identify and remediate misconfigurations, catches malicious insiders, and closes cloud security and attack surface visibility gaps. Additionally, Illusive can create deceptive objects based on the extraneous connections and credentials it has cleaned, which fool attackers into revealing their malicious presence in your AAD environment upon engagement. Don’t let security worries slow your organization’s digital transformation-accelerate it with protection that gives you the visibility to stop attacker movement no matter where it is occurring in your AD environment.

The Benefits of Protecting Azure Active Directory (AAD) with Illusive:

- Security & threat visibility on Active Directory and Azure
- Visualize and automate the discovery of critical assets in AAD
- Detect AAD misconfigurations for rapid remediation before attackers can take advantage
- Detect insider threats attempting to leverage policy gaps between AD and AAD
- Expose connections between privileged users on-premise and in the cloud
- Create AAD deceptions that provide high-fidelity threat detection



Azure Privileged Identities

All Rules

150 Violations 90 Privileged users 60 Privileged applications

Top privileged users	Top violating user without MFA	Top privileged applications	Top violating assigned roles	Top violating subscriptions
moshe_kamer32 43% of violations View all	itay_avraham_1 7% of violations View all	Azure_Advisor 9% of violations View all	Owner 68% of violations View all	illusive.com\user_267 15% of violations View all

Automate the Discovery and Remediation of Privileged Identity Issues in the Cloud

Illusive Networks for Azure Active Directory: Key Features

Attack Surface Management in the Cloud: Visualize and automate the discovery of which cloud data is a "crown jewel" that needs to be protected. Find and eliminate common attacker pathways towards critical information. Gain visibility into insecure usage and users across Active Directory and Azure.

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.

Privileged Cloud Credential & IAM Violation Discovery: Surface potential privileged identity blind spots and mitigate vulnerabilities created by shadow admins and other extraneous domain users.

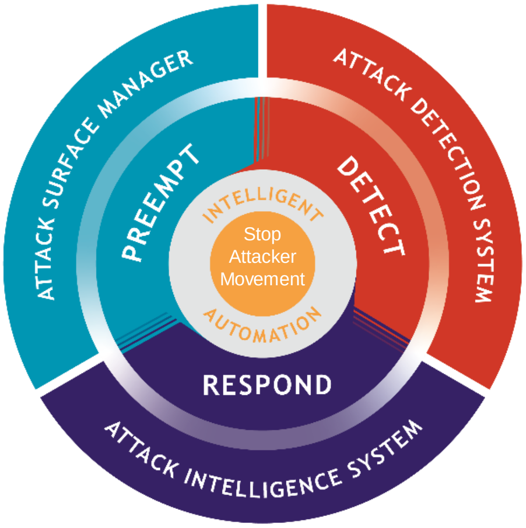
Cloud Deceptions: Customers can complement Illusive attack surface management for AAD with an extensive selection of in-cloud data deceptions. These deceptions seem like authentic pieces of valuable information to attackers and malicious insiders, tricking them into engagement, and forcing them to reveal their unauthorized presence to defenders in AAD. Cloud deceptions include deceptive SaaS application data, SSH and RDP deceptions, fake credentials, and much more.

Server Deceptions: The Illusive Platform offers highly-authentic deceptions based on commonly-used web and CI/CD servers, such as Tomcat, IIS and Jenkins servers. These are complemented by a slate of server-to-server deceptions that are designed to find and stop attacker movement between those servers.

Microsoft Office Word and Excel Beacon Files: Organizations can automate the customized creation of hundreds of thousands of deceptive Word and Excel documents. Real and deceptive Word and Excel documents can be also beaconized to immediately alert organizations to the usage of sensitive documents by malicious insiders or external attackers.

Standalone Decoys: Lightweight, hardware-free deceptive systems that can live in the cloud and turn any local host into a decoy that collects insight about attacker tactics and practices with zero additional operational overhead.

The Illusive Platform provides centralized management across even the largest and most distributed environments. Three modular components can work together or be operated separately to preempt, detect, and respond to cyberattacks.



Attacks come from all directions – from phishing emails to cloud account takeovers. The key to foiling attackers is stopping the attacker's ability to move anywhere they might be.

Stopping attack movement means stopping lateral movement in the data center environment, vertical movement to and from cloud, and movement across and within clouds. Illusive does all three, providing a comprehensive platform for stopping attacker movement no matter where they start or end up.

Illusive Networks stops attack movement from anywhere to anywhere by creating a hostile environment for attackers. Illusive shrinks the true attack surface to preempt attacks, creates the illusion of an expanded attack surface with deceptions for early detection of attacks in motion, and provides rich, real-time forensics that speeds response with actionable insights.

Agentless and intelligence-driven, Illusive deception technology enables organizations to avoid operational disruption and business losses by proactively intervening in the attack process so they can function with greater confidence in today's complex, hyper-connected world.

Visit us: www.illusivenetworks.com

Email us: info@illusivenetworks.com

Call us:: US: +1 844.455.8748
EMEA / AsiaPac: +972 73.272.4006

Find us: