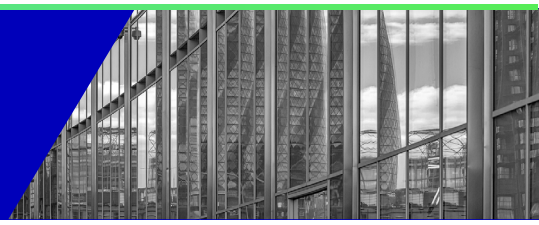
Illusive For Protection of Active Directory (AD) and Azure AD

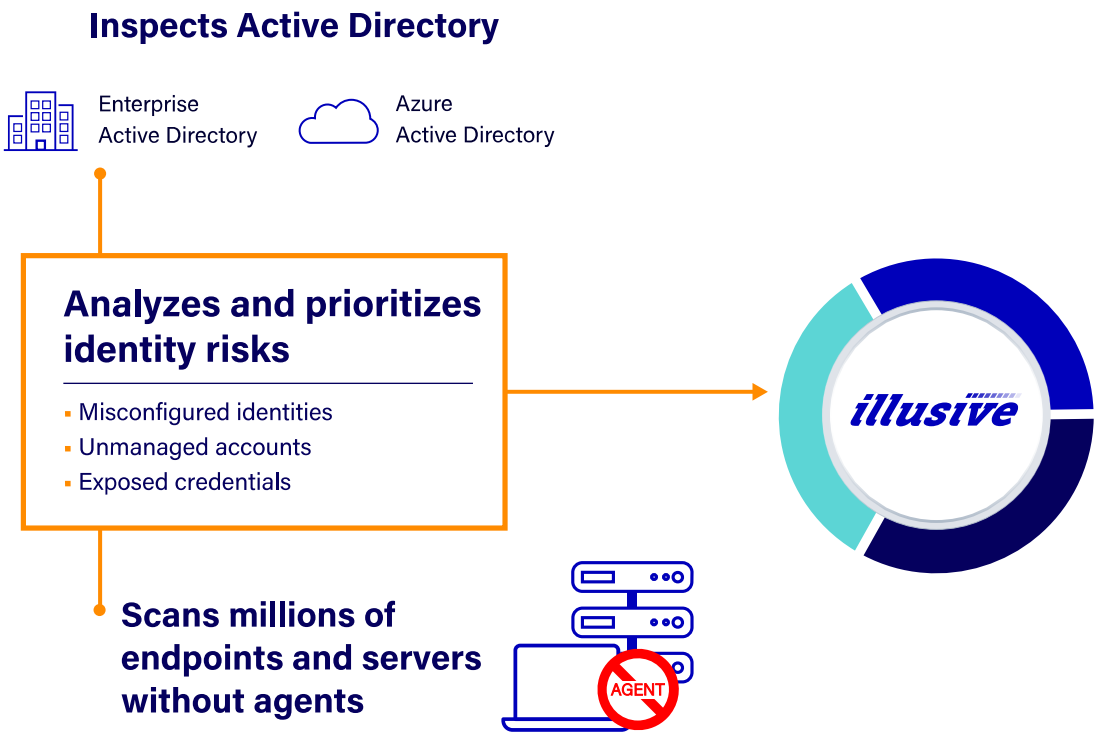


It's estimated that over 90% of organizations worldwide use Active Directory. AD and Azure AD provide the directory services that control most authentication and authorization activities for most companies, making them "the keys to the castle" in the IT world. Accordingly, AD is an irresistible target for cyber attack.

Unfortunately, AD is a complex legacy application that organizations have implemented for many years, accumulating technical debt that's difficult to pay down. Also, it doesn't always do a good job of handling situations such as application service accounts, where there's identity information unrelated to a user. As a result, there are security-related challenges, such as the following:

- Highly privileged users may not always have the security characteristics (such as MFA-enablement) that they should.
- As a result of nested groups, and the nuances of some privileges, "ordinary" users may have ways to become highly privileged, in unexpected ways.
- There may be service accounts with security weaknesses, including ones that are used for interactive login, when that should be disallowed.
- Local admin accounts that are supposed to be managed using LAPS may be misconfigured or completely unmanaged.
- The interaction between on-premise AD and Azure AD means vulnerabilities can cross between the environments in unexpected ways.

Taking an attacker-oriented approach, Illusive discovers AD identity vulnerabilities in on-premise AD, Azure AD, and individual endpoints — including pathways and credentials that attackers might leverage. 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 environment upon engagement.



Illusive Capabilities

Overall posture assessment
Illusive provides comprehensive environmental assessment, with trending, based upon risk-scored identity vulnerabilities—AD cross-referenced with endpoint assessment.

Attack paths
Illusive uncovers attack paths by number of steps required for privilege escalation, cross referenced with pathways to "crown jewel" systems and potential endpoint credential exposure.

Endpoint local admin
Illusive detects identity risk situations related to local admin accounts, such as accounts not registered in a PAM solution, accounts unused for lengthy periods, accounts with unchanged passwords for a lengthy period, etc.

Endpoint exposed credentials
Illusive detects and remediates credentials exposed on endpoints in system memory, browser cache, files on disk, and many commonly-used administrative applications, such as PuTTY and SSH.

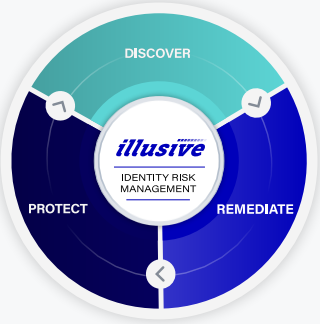
Risk scoring and prioritization
With each identity vulnerability, Illusive aggregates the vulnerabilities at the identity level, risk scores the results, and prioritizes the results so that the most important vulnerabilities are addressed first.

Automated remediation
Based upon policy, Illusive can automatically close privileged RDP sessions, clear exposed endpoint credentials, and disable local admin accounts.

Integration with MFA to deliver step-up authentication
Illusive can automatically enable multi-factor authentication (MFA) for privileged accounts as a remediation process, based upon policy.

Real-time attack detection and monitoring
Illusive Shadow™ lets you deploy a wide range of deception-based protection on endpoints, including deceptive AD account information that's monitored in real time for alerting. It can also deploy cloud deceptions including deceptive SaaS application data, SSH and RDP deceptions, fake credentials, and much more.

API Integrations
Illusive includes out-of-the-box integrations with AD, Azure AD, Intune and Microsoft Managed Desktop (MMD). Illusive's API integrates with SIEM, SOAR, and ticket systems.



About Illusive

Illusive takes away the one thing attackers need to be successful – access to privileged identities. Founded by nation-state attackers, Illusive protects customers against the attack vector exploited in all recent ransomware and targeted cyber attacks by discovering and automatically remediating privileged identity risk. Illusive provides security teams with the visibility they need to prioritize risk remediation efforts, enable zero trust initiatives, and avoid red-team embarrassments and audit findings