Illusive Spotlight™

Automatically discover and remediate identity vulnerabilities before attackers exploit them

Identity Threat Detection & Response (ITDR) is Critical to Protect Against the #1 Vector for Attack

The global increase in cyberattacks has been enabled by attackers shifting their focus from system to identity-based attacks, such as account takeover attacks (ATOs). These attacks are often completed in only days and go undetected without leaving any indicators of compromise or evidence of malware.

Identity is the New Vulnerability

Despite the deployment of privileged account management (PAM) and multi-factor authentication (MFA), vulnerable identities exist on 1 in 6 enterprise endpoints. Privileged identities are the number one vector for ransomware and other targeted cyberattacks. When an attacker first lands on a host, it's very rarely their end target, so they must escalate privilege, and move laterally to achieve their objectives. Attackers have access to a wide variety of attack tools such as Bloodhound, Cobalt Strike, Mimikatz, and ADFind, making it fast, easy, and effective for them to exploit privileged credentials — and hard for organizations to detect. It's not surprising that 84% of organizations have had an identity-related breach in the past year[1] and that ransomware has surged to record-breaking levels.

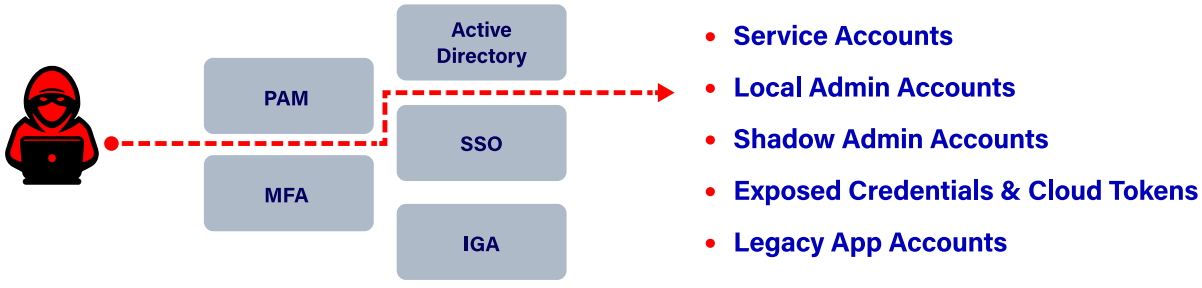
An example attack at CNA Insurance:

A ransomware operator used credential stuffing to access the network via RDP. Stolen credentials were used for initial access, and from there the attacker escalated privileges to Domain Admin, then encrypted critical data, exfiltrating some of it. CNA ultimately paid a $40M ransom to recover from the attack.

Every Organization has Vulnerable Identities

The complexity of identity and access management system deployments, the constant pace of changes to identities, and the lack of any continuous visibility into the gaps that exist in the environment are the cause of identities becoming vulnerable.

- Service Account, Local Admin, and privileged Domain credentials have gone unmanaged by PAM
- Shadow Admin accounts get unintentionally created with excessive privileges
- RDP sessions aren't always properly terminated
- Credentials and cloud access tokens are commonly cached on endpoints by user applications, such as browsers, SSH, FTP, PuTTY, databases

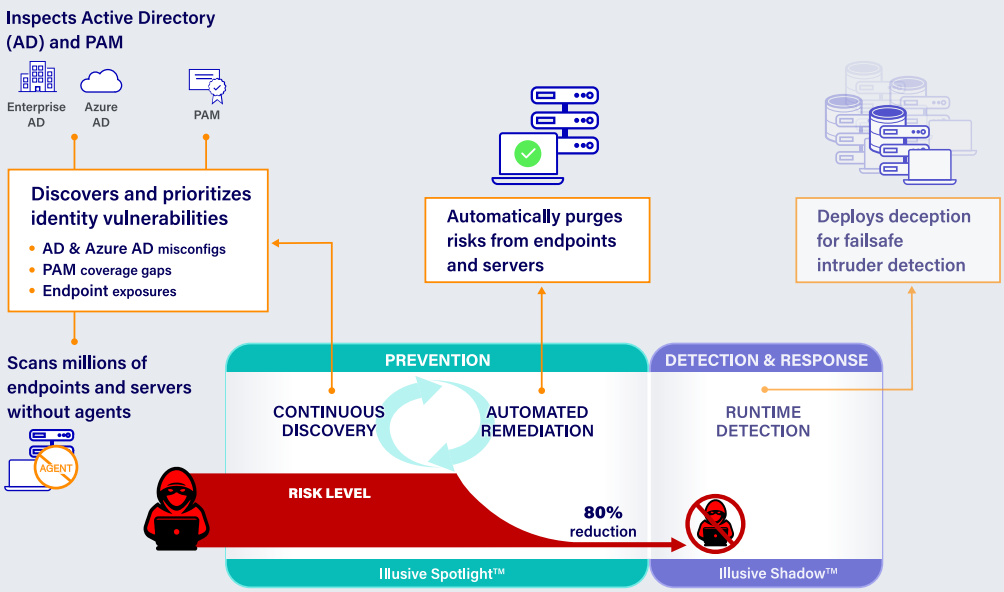


Find and Fix Vulnerable Identities

Illusive's agentless approach delivers unparalleled visibility into vulnerable identities by scanning directory structures (e.g., Active Directory), privileged access management (PAM) solutions (e.g., CyberArk, Delinea), endpoints, servers and services, revealing the gaps between the intention of an organization's identity security policies and the reality of their environment. Illusive prevents attacks by taking away what attackers need to complete their crime: privileged account access.

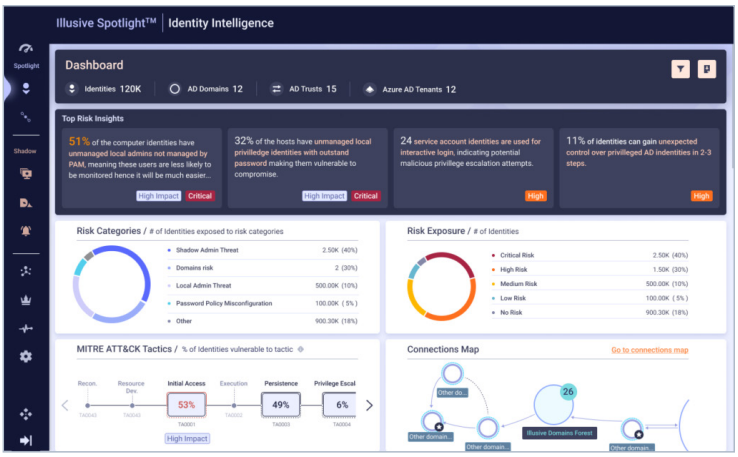
Continuous Discovery and Remediation of Privileged Identity Vulnerabilities and Policy Violations

- **Continuously Discover**
  Comprehensive discovery of identity vulnerabilities
- **Automatically Remediate**
  Ease cleanup of identity vulnerabilities
- **Accurately Detect and Respond**
  Detects identity threats that evade traditional defenses



Spotlight Enables:

- CISO and security leaders with identity risk dashboard
- Vulnerability management teams to harden their identity security posture
- SOC and IR teams to effectively detect privilege escalation and lateral movement
- Security M&A teams to properly assess the risk of newly acquired environments
- Identity teams to automate evidence collection for identity audits and compliance



About Illusive

Illusive discovers and remediates privileged identity risk policy violations that are exploited in all ransomware and other cyberattacks. Despite significant investment to protect identities, including deployment of PAM and MFA solutions, every organization has exploitable identities. Illusive makes it easy to find these previously unknown vulnerable identities sprawled across an organization's endpoints and servers, then eliminate them or deploy proven identity compromise detection techniques to stop attackers. Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help companies protect their critical assets, including the largest global financials and pharmaceuticals. Illusive has participated in over 140 red team exercises and has never lost one.

[1] https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/