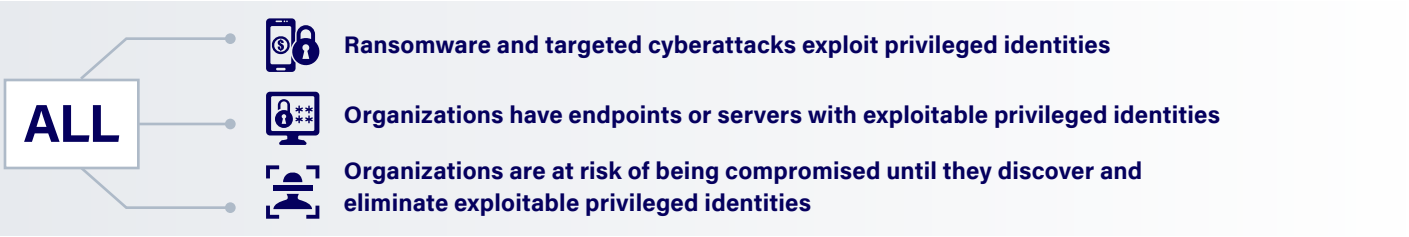
Illusive Spotlight™

Eliminate the #1 Vector for Cyberattacks: Access to Privileged Identities



Ransomware Exploits Privileged Identities

Despite the deployment of privileged account management (PAM) and multi-factor authentication (MFA), 1 in 6 enterprise endpoints and servers still have identity risks that let attackers gain the privileges they need. 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. It's not surprising that 79% of organizations have had an identity-related breach in the past two years[1] and that ransomware has surged to record-breaking levels.

Exploitable Identities are Commonplace

Privileged identities are more at risk than many realize. A close examination of a recent high-profile ransomware attack provides compelling evidence of the risk and potential costs of not fully understanding and mitigating exploitable identity risks.

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.*

Exploitable Identity Risks

[1] Source: Dimensional Research - Identity Security: A Work in Progress

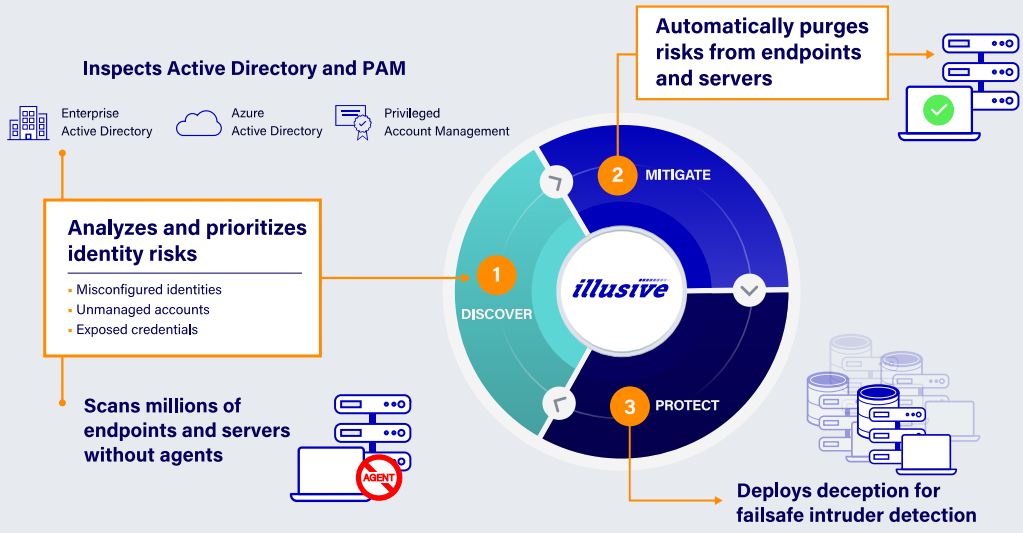
Many of these identity risks result from ordinary business and IT operational processes. The following are examples of some common processes that increase risk.

- Usernames and passwords are cached on endpoints by user applications, such as browsers, SSH, FTP, PuTTY, and databases, none of which are protected by PAM.
- Domain admin credentials are retained in system memory after a remote support session, or cached in a legacy application that's using a service account.
- Users are inadvertently extended with excessive 'shadow' privileges due to the complexity inherent in configuring identity directory objects and groups.

Continuous Discovery and Mitigation of Privileged Identity Policy Violations

Illusive's Discover – Mitigate – Protect approach to identity risk management makes it more difficult for attackers to "live off the land" and evade defenses.

- **Discover** – Continuous discovery of exploitable identity risks
- **Mitigate** – Automated cleanup of exploitable identity risks
- **Protect** – Deception-based detection provides compensating controls



Identity Risk Assessment

To get started in understanding the privileged identity risks in your environment, Illusive offers an Identity Risk Assessment that is as easy as 1-2-3: share one IT endpoint, spend two hours with Illusive's identity security experts, and receive three actionable insights specific to your organization. Illusive illuminates hidden identity risks, including:

- Unmanaged local admin accounts
- High risk connections to critical IT infrastructure and business assets
- Cached domain admin credentials contained on endpoints
- Unmonitored privileged users
- Improperly disconnected RDP sessions with heightened access
- Ambiguous shadow admins

About Illusive

Illusive discovers and mitigates 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. For most organizations, this means that 1 in 6 of their endpoints and servers hold service accounts, shadow admin accounts, improperly terminated RDP sessions, cached credentials or cloud access tokens that attackers can easily use to escalate privilege and move laterally to commit their crime. 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.