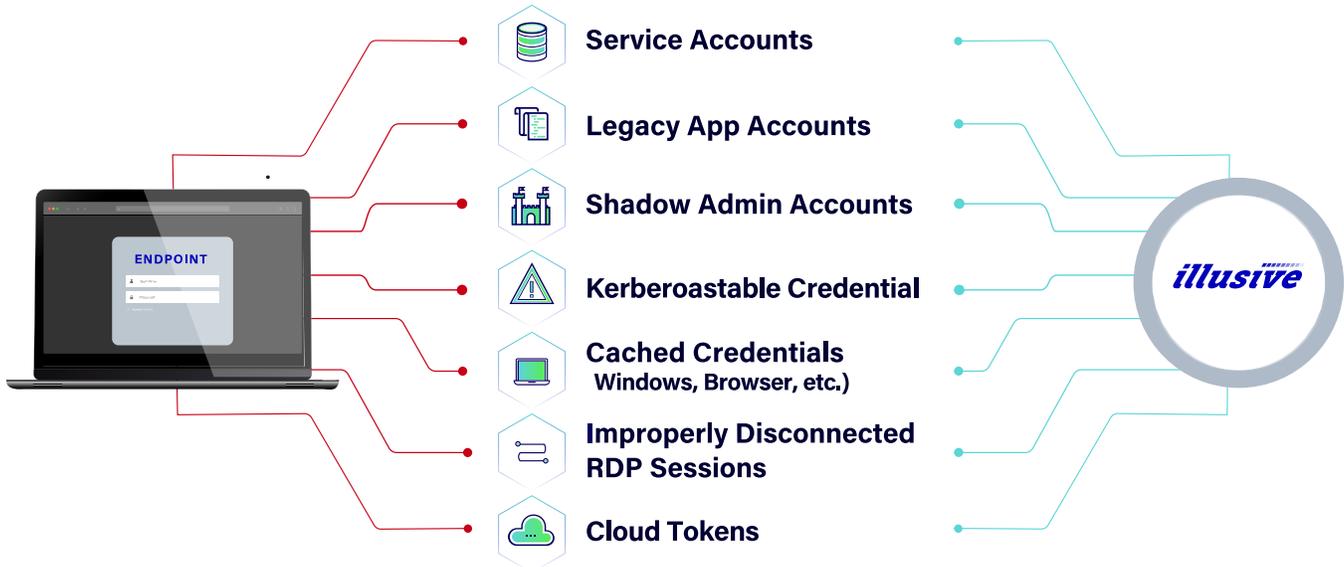# Identity Risk Assessment

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

Ransomware Exploits Privileged Identities

Despite the deployment of PAM and MFA solutions, **Illusive discovers privileged identity risks on 1 in every 6 enterprise endpoints.** Every organization is at risk of dramatic compromise until they discover and eliminate privileged identity risks, such as:

ENDPOINT

- **Service Accounts**
- **Legacy App Accounts**
- **Shadow Admin Accounts**
- **Kerberoastable Credential**
- **Cached Credentials** Windows, Browser, etc.)
- **Improperly Disconnected RDP Sessions**
- **Cloud Tokens**

Let Illusive Illuminate Your Security Blindspots – It's as Easy as 1-2-3!

Illusive has developed a frictionless, SaaS-delivered process to minimize your requirements while maximizing your value with actionable insights delivered within hours.

| 1 Provide **ONE** endpoint. | 2 Spend **TWO** hours. | 3 Receive **THREE** key insights. |

- Unmanaged local admin credentials, which are frequently used in ransomware attacks.
- Misconfigured privileged credentials, which are frequently used in APTs.
- Exposed admin accounts, which can be exploited in privilege escalation attacks.

Are one in six of your endpoints leaving you vulnerable to attack?

To get started, contact **info@illusive.com** or sign-up at **https://illusive.com/identity-risk-assessment**