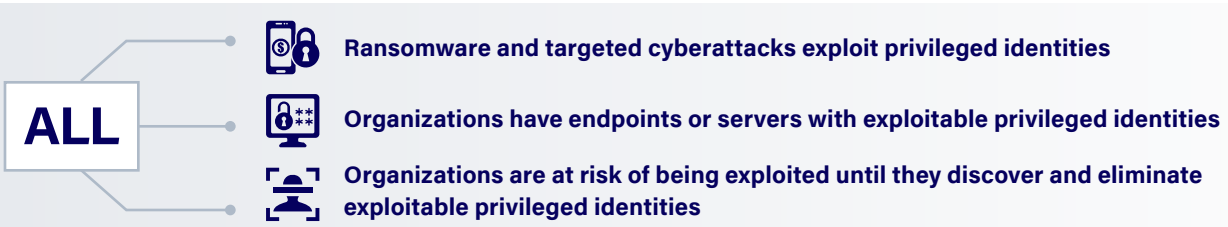
The Risks and Solutions for Privileged Identities

Prevent Cyberattacks by Eliminating Exploitable Privileged Identities



Ransomware Exploits Privileged Identities

Privileged identities are the number 1 target 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 near endless supply of attack tools like Bloodhound, Cobalt Strike, Mimikatz, and ADFind, making it easy to exploit privileged credentials resident in all organizations. It's not surprising that 79% of organizations have had an identity-related breach in the past 2 years[1].

Exploitable Privileged 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 privileged identity risk.

CNA Insurance: *Ransomware operator utilizes a credential stuffing to access the network via RDP. The initial stolen credentials were used for initial access and from there the attacker escalate privileges to Domain Admin to exfiltrate and encrypt data. CNA ultimately paid a $40M ransom to recover from the attack.*

The following privileged identity risk taxonomy describes the risk categories as unmanaged, misconfigured, and exploitable. Each of the category examples represent situations not adequately managed by existing identity management systems.

Identities at Risk

UNMANAGED

- Local Admins
- Legacy Apps & Shadow SaaS
- Accounts Not in PAM, No MFA

MISCONFIGURED

- Shadow Admins
- Kerberoastable Service Accounts
- Identity & Password Re-Use

EXPLOITABLE

- Cached Credentials
- Stored Cloud Tokens
- In-App Stored Credentials

Many of the privileged 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 inadvertently captured in browser history
- Domain admin credentials can be retained in system memory after a remote support session
- User privileges are accidentally escalated due to complexity inherent in a corporate IT directory

Consequently, the optimal remediation measures need to be continuous and automated. Failure to discover and mitigate ongoing stream of privileged identity risks makes it way too easy for attackers to escalate privilege and achieve their mission.

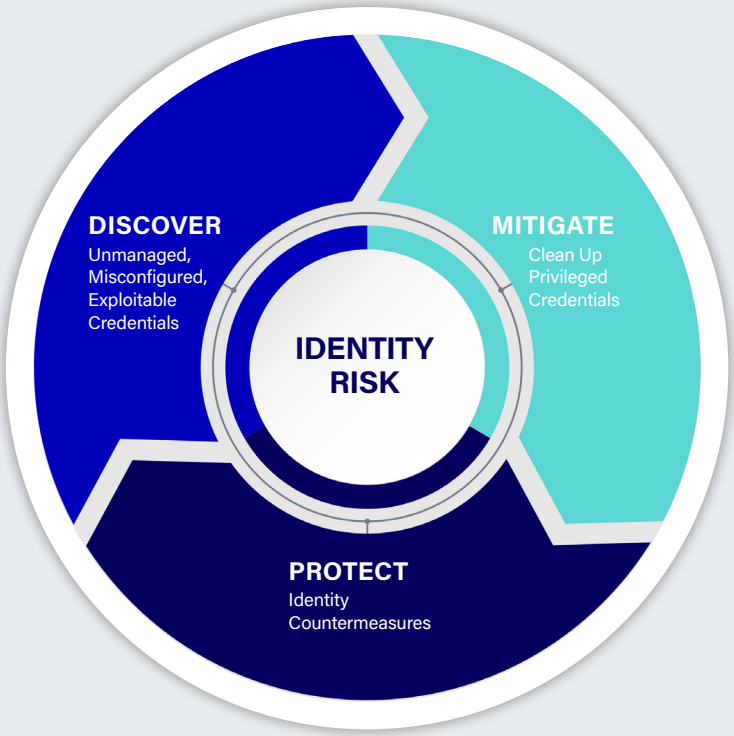
[1] Source: Dimensional Research - Identity Security: A Work in Progress

Continuous Discovery and Mitigation of Privileged Identity Policy Violations

Illusive helps organizations improve their security posture by proactively discovering and mitigating privileged identity risks attackers exploit for ransomware and other cyberattacks. For identity risks that can't be easily eliminated, Illusive can deploy compensating deceptive artifacts directly to endpoint and server systems, where the attacker operates, to detect attempts to exploit privileged identities to move laterally and access crown jewels.

Illusive's Discover – Mitigate – Protect privileged identity risk methodology makes it more difficult for attackers to "live off the land" and evade defenses by discovering, mitigating, and protecting against unmanaged, misconfigured, and exploitable privileged identities such as shadow admins, cached privileged account credentials, and local admins.

- **Discover** – Gain a complete understanding of current privileged identity risk.
- **Mitigate** – Easy and continuous clean up for identified privileged identity risks and policy violations.
- **Protect** – Compensating controls (e.g., Deceptions) for privileged identity risks that can't be mitigated.



Privileged Identity Risk Audit

To get started in understanding the privileged identity risks in your environment, we can run a Privileged Identity Risk Audit report, to Discover specific identity risks, and offer actionable insights into the identity risks and the associated lateral movement exposure. The comprehensive report will reveal any high risk privileged identity and lateral movement issues such as:

- Shadow 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 privilege identity risk policy violations to disrupt the lateral movement that ransomware and other cyberattacks used to access critical assets. Despite significant investments, it's still difficult to see and stop attackers moving inside your environment. Illusive enables organizations to create a hostile environment for attackers by discovering privileged identity risks, mitigating policy violations, leveraging deceptive controls to detect attacker actions associated with identity risk not easily mitigated, and delivering on-demand visibility into nefarious attacker activities.

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 global pharmaceuticals. Illusive has participated in over 130+ red team exercises and has never lost one!