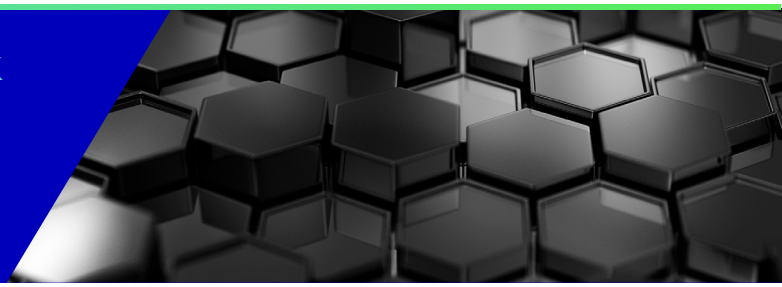
Illusive Integration with CyberArk Privileged Access Security

Find and Remove Exploitable Accessible Privileged Credentials



Attackers actively seek and leverage privileged credentials to gain access to network resources and ultimately, the "crown jewels" of the organization. It's critically important to both identify and manage privileged accounts and credentials to ensure any unmonitored accounts discovered in your Illusive scan are secured by CyberArk moving forward.

The Challenge

Most attacks originate on the endpoint where threat actors seek out accessible privileged credentials for exploit and the residue of left behind connections. As access footprints change on a daily basis, visibility of this attack exposure is often unknown, significantly expanding security blind spots and risk. To be effective, removal of these credentials and connections must be prioritized, easy and automated, performed continuously, and constantly monitored to mitigate risk.

An Integrated Solution

Exploding attack surfaces increase risk of breach to the enterprise. Illusive continuously conducts privileged account discovery, surfacing risky credentials sought after by attackers. The Illusive integration with CyberArk Privileged Access Security identifies accounts that are both managed and unmanaged by CyberArk, enabling updates of CyberArk coverage to provide continual protection of unmonitored accounts that appear as access footprints change.

Working Together

Once Illusive discovers a Local Admin user, it checks against CyberArk to identify if it's managed or unmanaged. If it's found to be managed on some endpoints, but unmanaged on others, the user is marked as a "Partially Managed" account—a potential attack risk—thus allowing for appropriate remediation.

Working Together

Illusive and CyberArk Privileged Access Security

1. Illusive continuously scans the attack surface for errant credentials, connectivity and attack pathways

2. Discovery of an Admin initiates a check against CyberArk to confirm if the account is managed or unmanaged—identifying a potential security blind spot

3. Some Admins may be the same across the organization. Unmanaged Admins may be on purpose or a security risk. Illusive surfaces these insights for review and action as appropriate

Key Benefits

High-impact cyberattacks have a phase in which attackers must move laterally towards their target, requiring credentials and connections between systems. Defenders often lack the ability to get ahead of this evasive process. The Illusive and CyberArk integration helps identify and remove high-risk credentials and rogue connections at scale. Together, organizations can finally manage the attack surface perpetually to preemptively cut off malicious access to an organization's "crown jewels."

CyberArk's Privileged Access Security solution is a full life-cycle solution for managing the most privileged accounts and SSH Keys in the enterprise. It enables organizations to secure, provision, manage, control and monitor all activities associated with all types of privileged identities.

Illusive's Attack Surface Manager deprives attackers of their means to attack. Illusive identifies and removes attack surface risks, like errant credentials, connections, and pathways that attackers expect and leverage to move laterally towards the organization's "crown jewels." Additionally, the solution identifies and ranks surface risk to provide business context for incident response.

Discover and minimize attack surface risk to eradicate "Living off the Land" lateral/ vertical movement

Find and remove accessible risky credentials, and onboard unmonitored privileged accounts residing on endpoints that are discovered by Illusive into the CyberArk solution

Uncover and remediate partially managed local administrator accounts

Dramatically reduce the time to accelerate incident response and threat remediation

Beat the Red Team every time—your flag will never be captured again!

About Illusive

Illusive reduces cyber risk by shrinking the attack surface and stopping attacker movement. Despite significant investments, it's still difficult to see and stop attackers moving inside your environment. Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help Fortune 100 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! To learn more, visit **www.illusive.com**

About CyberArk

CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500. To learn more, visit **www.cyberark.com**