Strengthen Your Privileged Access Management Solution with Attack Path Management

Get full visibility into your identity network and help the rest of your identity-related tech stack operate efficiently.

PROBLEM

Identity is a prime target for adversaries. Once a privileged account is compromised, attackers can quickly seize control of critical assets. To protect sensitive systems and data, organizations often implement a Privileged Access Management solution (PAM).

PAM solutions provide controlled, elevated access through systematic management and protection of privileged accounts, credentials, and commands used to administer critical systems and applications. When properly deployed, these solutions significantly limit an attacker's ability to move laterally through your network and escalate privileges.

However, while organizations can typically identify and protect explicitly granted privileges, it's the **incidental privilege**—unintended access rights granted through complex group memberships, inheritances, and role assignments—where critical security gaps emerge across Active Directory and Entra ID environments. This oversight can leave open doors for attackers.

Before you can protect your organization's critical identities and resources, you must first understand where those assets are within your environment and how they can be accessed—directly or indirectly.

SOLUTION

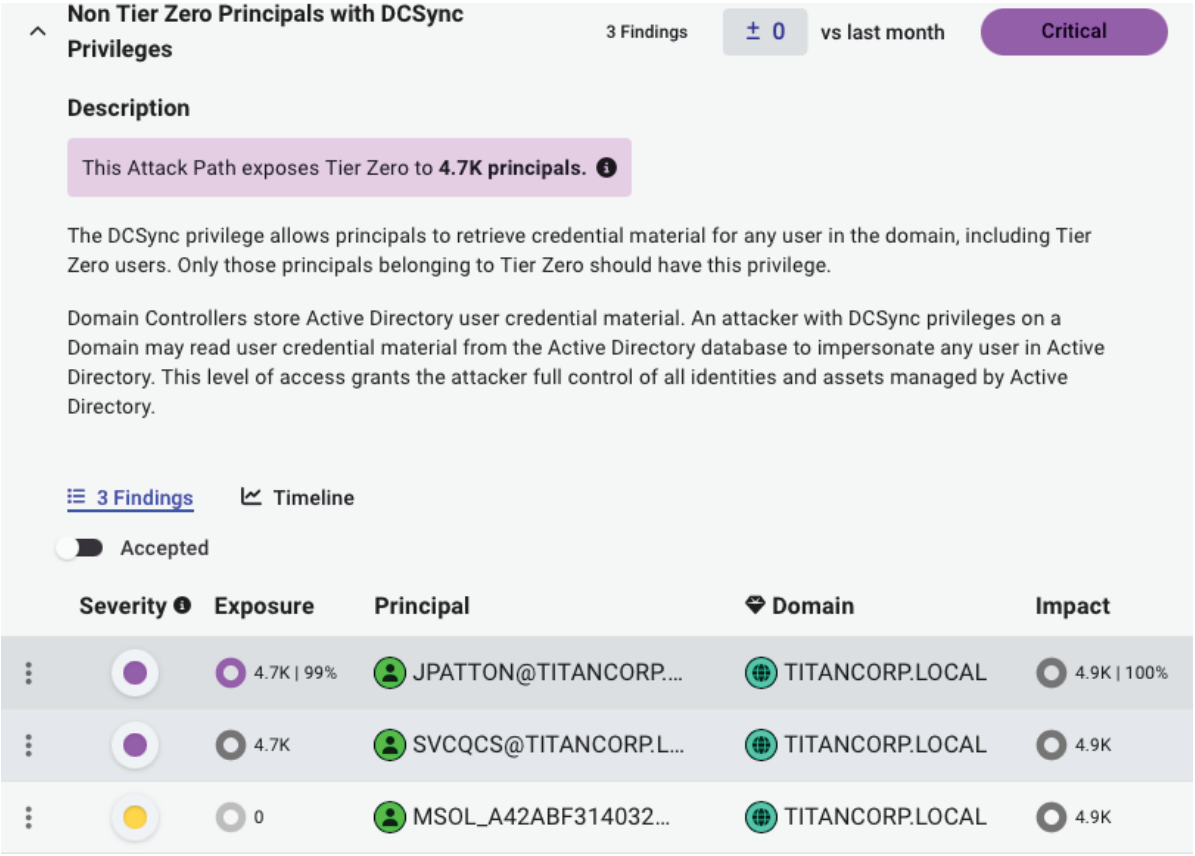
BloodHound Enterprise quickly maps your AD and Entra ID systems to uncover the Identity Attack Paths that attackers could exploit to move laterally, escalate privileges, and create persistent backdoors for future access.

BloodHound Enterprise highlights the obvious Tier Zero principles like Domain Admins and Enterprise Admins, but it also captures Tier Zero accounts that have elevated privileges by delegation.

In the example on the next page, three Active Directory accounts are granted DS-Replication-Get-Changes and DSReplication-Get-Changes-All. These privileges are often granted to service accounts to sync Active Directory objects to other locations. However, they can also be used by attackers to execute the DCSYNC attack and impersonate any user.

BLOODHOUND ENTERPRISE

Powered by SPECTEROPS



The SVC and MSOL accounts should be managed with a PAM solution, as their privilege is granted by design. To explain further: the MSOL account is utilized to sync directory objects between AD and Azure. Removing these privileges would break the sync between directories. These accounts are Tier Zero identities and should be included in the scope of identities protected by your PAM solution.

However, JPATTON should be remediated, as it is not an administrative account. This excessive privilege could allow an attacker to compromise the environment. This is just one example of the incidental privilege that plagues many organizations and represents an essential but often overlooked source of identity risk.

As you begin implementing your privileged access solution, you can leverage this information to develop a phased approach to onboarding groups based on their risk and criticality. This data also supports cooperation between operational and security teams to manage and eliminate privilege sprawl and detect when new privileged access paths emerge that bypass your PAM program controls. By doing so, you address the tech debt that plagues nearly all AD and Hybrid Entra ID environments.

Entropy is inevitable in any complex system, and identity infrastructures are no exception. A fundamental pillar of an effective PAM strategy is recognizing that discovery must be a continuous process, not a one-time event.

HOW IT WORKS

1. Identify – Discover your critical assets and the attack paths an adversary is most likely to exploit to give you a more accurate understanding of abusable privilege.

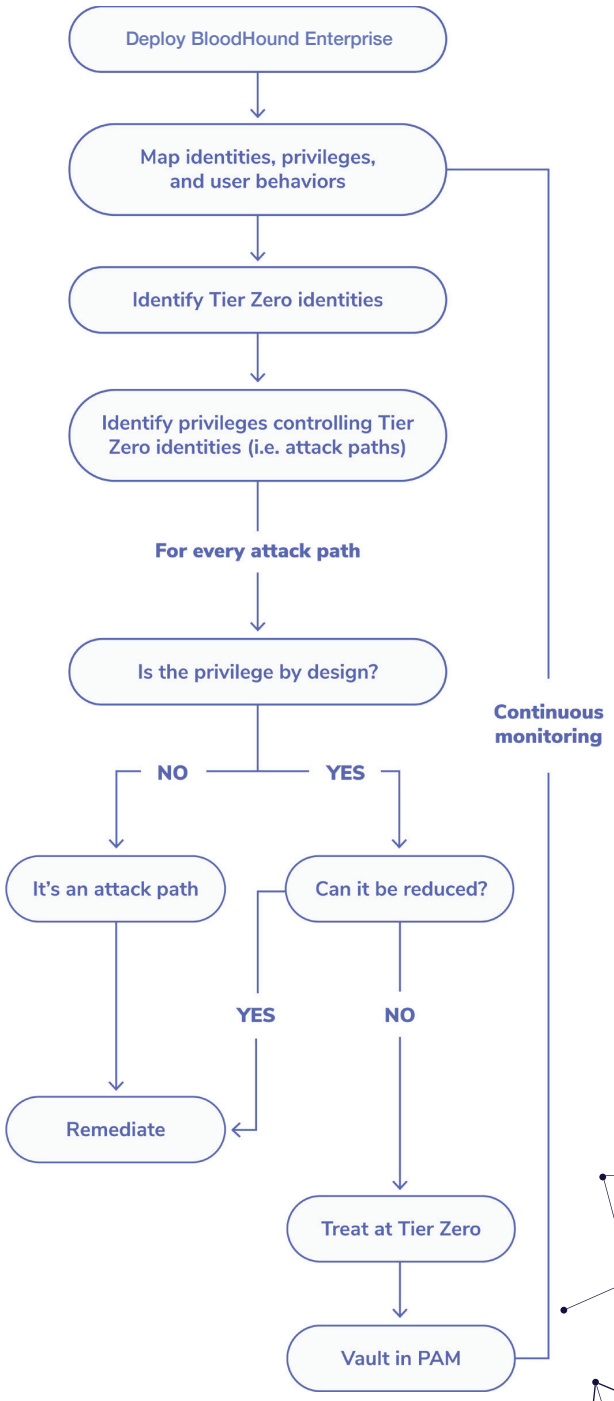
2. Prioritize – Assess exposure by identifying how many principals have paths through a particular node and use this insight to determine the most critical paths for strengthening privileged access management.

3. Remediate – Follow proven remediation guidance to reduce risk and eliminate unnecessary privilege without causing costly disruptions to business operations.

4. Report – Demonstrate the efficacy of remediations and a reduction in identity risk across your Identity Attack Path and PAM programs.

5. Operationalize through Integration – Incorporate BloodHound Enterprise into your PAM program's ongoing discovery process to confirm privileged access remains properly managed as your environment evolves.

The security challenges that privileged accounts represent extend far beyond what a PAM solution alone can address. By implementing complementary APM and PAM approaches, organizations can significantly reduce their identity risk exposure while enhancing the integrity of their privileged access security programs at all stages of maturity.



To learn more about BloodHound Enterprise, visit specterops.io/get-a-demo