



## SOLUTION BRIEF

### BloodHound Enterprise: Effective Attack Path Management for All

As a largely unseen, unmanaged, and growing problem for enterprises, Active Directory (AD) Attack Paths are used by attackers to gain control of systems and data, impersonate users, abuse legitimate access to non-AD systems and much more. This problem is compounded by mountains of misconfiguration debt in AD, making it difficult to improve your security posture. With IT Ops and SecOps needing better Attack Path Management tools, BloodHound Enterprise helps organizations proactively and continuously identify, manage, and remediate millions of AD Attack Paths, dramatically and measurably improving AD security with minimal effort.

#### The Problem BloodHound Enterprise Solves

Adversaries have been targeting AD Attack Paths for decades. From an adversary's perspective, Active Directory is:



**FOUNDATIONAL.** Organizations are built on top of AD. While taking control of AD isn't the end goal, it virtually guarantees achieving the adversary's true objective.



**UBIQUITOUS.** AD is used by nearly every enterprise; adversaries can use skills used to abuse organizations universally across their victims.



**POWERFUL.** The same advanced administrative power features in AD are used by adversaries to persist and complete their objective without the use of exploits.

Enterprise defenders and IT architects do their best to eliminate risk, but their AD environment:

- **Provides Zero Visibility:** Windows and AD make it nearly impossible to audit privileges.
- **Constantly Evolves:** New users, new machines, new environments, and user logins all add to and create new Attack Paths.
- **Is Buried in Debt:** Years of misconfiguration debt add Attack Paths and hide adversary activities.

#### Redefining AD Security by Enabling Attack Path Management



##### Unprecedented Visibility into Active Directory

Visualize all privileges for instant clarity on your AD structure and architecture.



##### Impractical Best Practices Made Practical

Tiered Administration, Least Privilege, and Credential Hygiene are now possible.



##### Active Directory Security for Everyone

Harden Active Directory against abuse and improve directory services availability.



##### Elimination of 'Band-Aid' Fixes

Directly address the risk of Attack Paths at precise Choke Points rather than fighting misconfiguration debt.



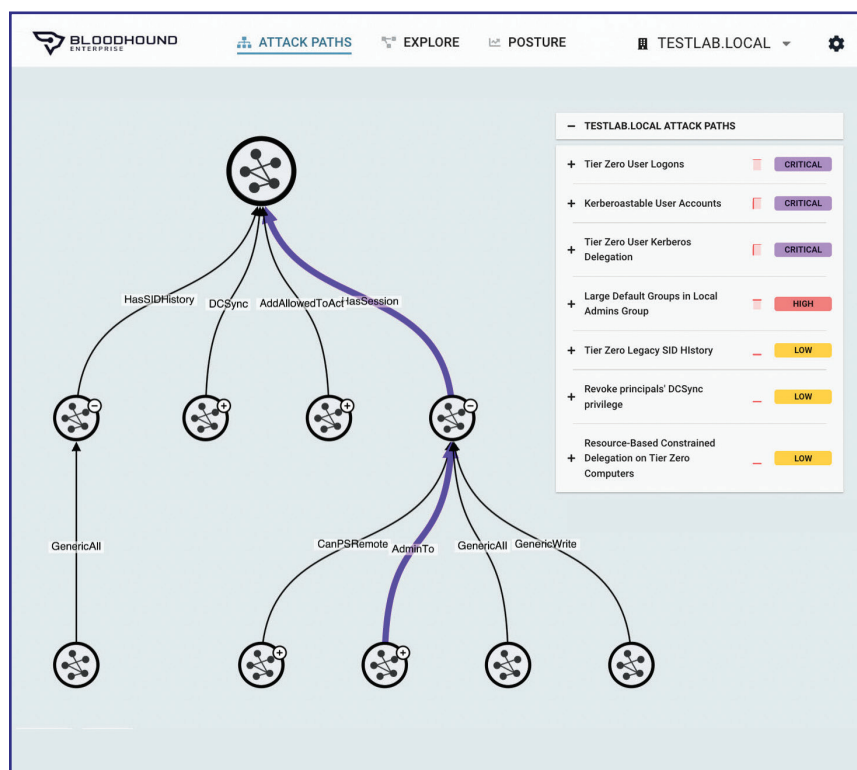
##### Measurably Improve Security Posture

Meaningful and transparent measurements that illustrate the risk reduction gained from Attack Path Management.

FOR MORE INFORMATION, PLEASE VISIT **BLOODHOUNDENTERPRISE.IO**

## A Profoundly Different Approach to Attack Path Management

Current AD security solutions are not addressing the root problem. Listing thousands of generic configuration issues solves nothing. BloodHound Enterprise's Attack Path Management solution takes a different and fundamentally more strategic approach to addressing the problem. BloodHound Enterprise flips the focus from listing all misconfigurations in AD to identifying and prioritizing the most critical 'choke points' to your high-value targets, eliminating millions of attack paths at once.



## BLOODHOUND ENTERPRISE IS BUILT ON FOUR CORE TENETS



### CONTINUOUS ATTACK PATH MAPPING

As connections and behaviors that form Attack Paths are continuously changing, BloodHound Enterprise:

- Continuously charts every relationship and connection
- Reveals full understanding of real permissions
- Exposes new and existing hidden Attack Paths



### REAL-WORLD REMEDIATION GUIDANCE

By understanding the true privileges of users and the pathways they create, BloodHound Enterprise:

- Delivers practical remediations without negative impact
- Provides comprehensive guidance using unambiguous language
- Informs how to validate privileges being removed are not required



### CHOKE POINT ENUMERATION & PRIORITIZATION

To eliminate the largest number of Attack Paths with the minimal amount of work, BloodHound Enterprise:

- Measures the impact of any point in an Attack Path
- Identifies optimal locations to block the most pathways
- Ranks choke points by collective risk reduction



### CONTINUOUS SECURITY POSTURE IMPROVEMENT

To provide comprehensive measurement of Attack Path risks, BloodHound Enterprise:

- Establishes a baseline of AD, identifying Attack Paths and their accumulated risks
- Measures continuously as changes to AD occur, reassessing risk
- As Choke Points are eliminated, significant security posture improvements are observed