BloodHound Enterprise - FedRAMP® High Authorized

Reduce Risk in Your Identity and Directory Environments

Identity is a prime target for adversaries. Once a privileged account is compromised, attackers can quickly seize control of an organization's critical assets. Identity Attack Paths are easy for threat actors to exploit but hard for defenders to detect, posing major risks in Active Directory (AD), Active Directory Certificate Services (ADCS), and Entra ID environments.

Attackers use these paths to move laterally, escalate privileges, and evade detection, aiming for privileged access (known as Tier Zero) control. Since AD, Entra ID, and Azure underpin most systems, understanding Attack Paths and directory hygiene is crucial to mitigating identity risk.

However, the complexity of organizations' hybrid identity footprint, years of technical debt, and constant organizational changes leave most companies blind to these vulnerabilities—making it easier for attackers to breach critical assets.

97% of breaches leverage an Identity Attack Path

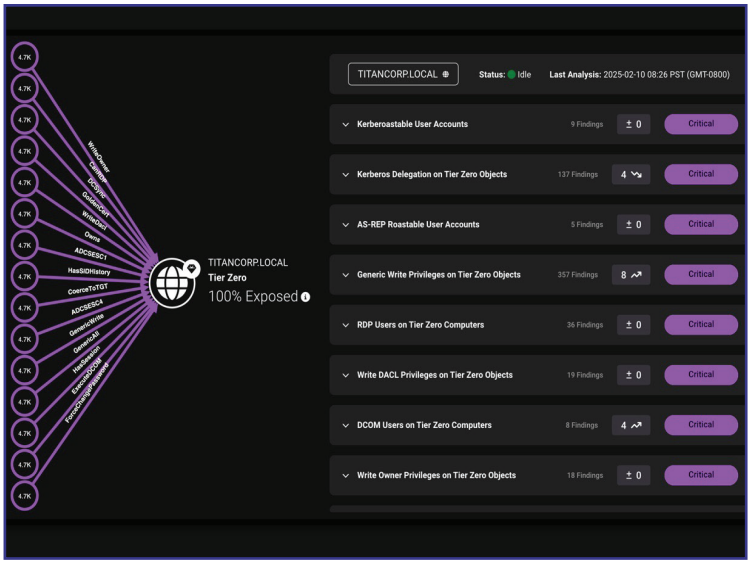
Over 70% of users in an AD domain have at least one attack path to Tier Zero and control over the enterprise

Fixing a single priority choke point can remove 300,000 attack paths

SpecterOps pioneered the concept of Attack Path Management (APM) by creating and maintaining BloodHound since 2017.

BloodHound Enterprise (BHE) provides an adversarial perspective on Identity risk in AD, Entra ID, and hybrid environments. This fully managed SaaS solution visualizes Attack Paths, offers remediation guidance, and tracks improvements over time.

BHE continuously maps and quantifies Attack Paths, identifies misconfigurations, and reduces the impact of targeting identities as the preferred attack vector.

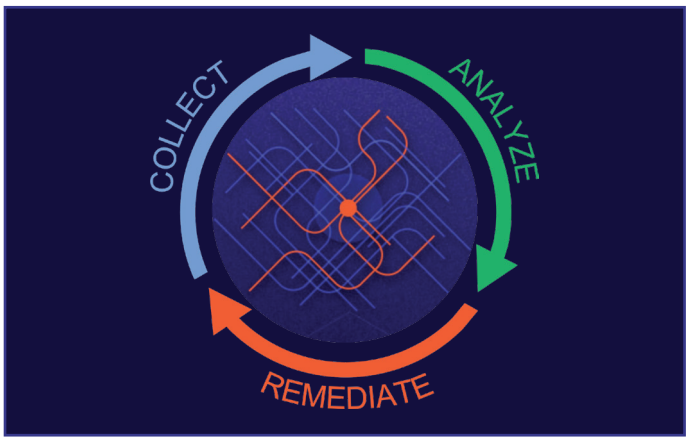


Visualize the complex connections and relationships in AD and Azure to understand where misconfigurations have exposed your organization's most valuable assets.

Key Benefits for Government Security & Identity Teams

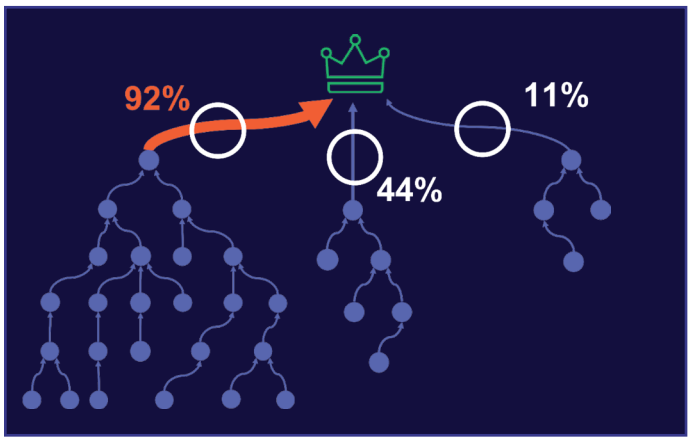
- Gain visibility into your Identity risk and exposure across your entire AD, ADCS, Entra ID, and hybrid environment enabling security teams to enforce consistent policies and control.
- Helps agencies meet critical compliance requirements (such as, NIST CSF, NIST 800-171, and NIST 800-53) through continuous monitoring of Identity Attack Path exposure.
- Get insights on Attack Path risk and remediation progress over time
- Enable agencies that require FedRAMP High Authorization (achieved December 2024 via Palantir FedStart) to utilize BHE at scale to enhance their mission in protecting high-value assets

Why BloodHound Enterprise



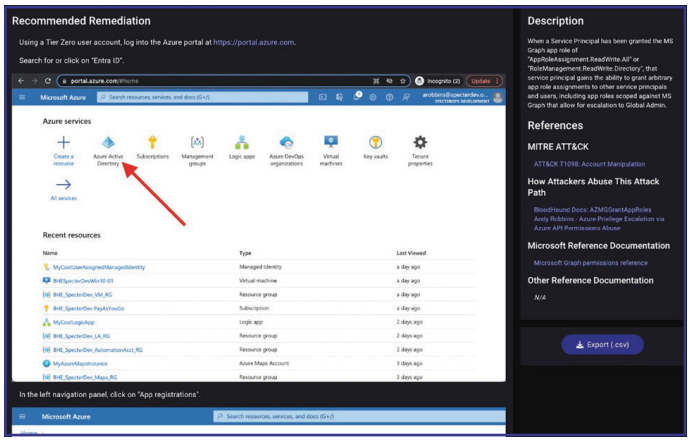
Continuous Attack Path Mapping

Identify your most critical Tier Zero or Control Plane assets, and then continuously identify every available Attack Path to understand how adversaries can move laterally and escalate privileges to compromise your environment.



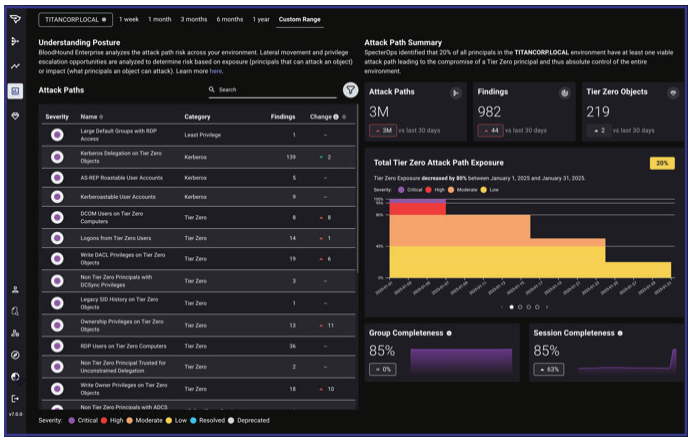
Prioritized Attack Path Choke Points

Analyze the millions of Attack Paths within your environment and prioritize the choke points that enable rapid risk reduction. This allows you to eliminate the largest amount of Attack Path risk with a single remediation.



Practical, Step-by-Step Remediations

Remove misconfiguration debt using guided remediations that walks your administrators through resolution processes screen-by-screen, eliminating the guesswork and ensuring practical and safe remediation.



Security Posture Measurement

Establish a baseline of your identity security posture, reassess risk and track improvements across all your directory environments over time.

To learn more, contact your SpecterOps representative or sign up for a demo to see how BloodHound Enterprise can help protect your organization's most critical assets:

SPECTEROPS.IO

"The BloodHound Enterprise team approached the problem differently, focusing first on Attack Path exposure to Tier Zero. They used the same language as our assessment experts, prioritized issues on risk, and included detailed remediation advice in each finding."

– Ryan Gray, Security Engineering Manager, Woodside Energy

©2025 SPECTER OPS, INC.