BLOODHOUND ENTERPRISE

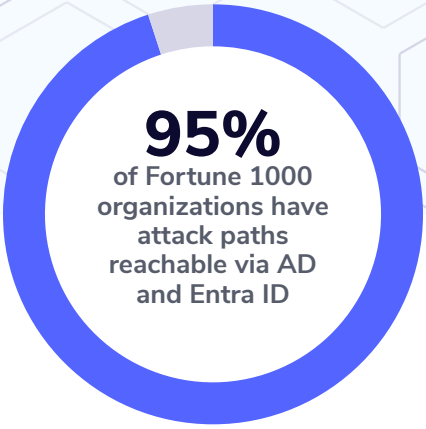
BloodHound Enterprise

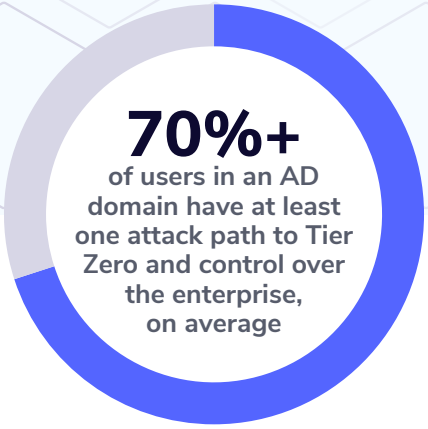
Reduce risk in your identity and directory environments

Identity and directory environments have become the preferred entry points for adversaries. Once a user with privileged access has been compromised, an attacker can easily orchestrate a cyberattack by taking control of an organization's critical assets. Identity attack paths are trivial for threat actors to exploit, yet difficult for defenders to detect, and the root cause of significant risk within Active Directory (AD), Active Directory Certificate Services (ADCS) and Entra ID (formerly Azure AD) environments.

Adversaries use identity attack paths to move laterally and escalate privilege, evading detection with ease as they attempt escalation to domain-level controls (known as Tier Zero). When AD, Entra ID and Azure are the backbone to nearly everything in your stack, guided visibility of your identity attack paths and knowing the gaps of your directory hygiene is essential.

Due to the complexity of AD environments, years of accumulated technical debt and constant org changes, most companies lack the insights needed to identify and remediate their identity attack path vulnerabilities. This opens the door for threat actors to easily compromise an organization's crown jewels.





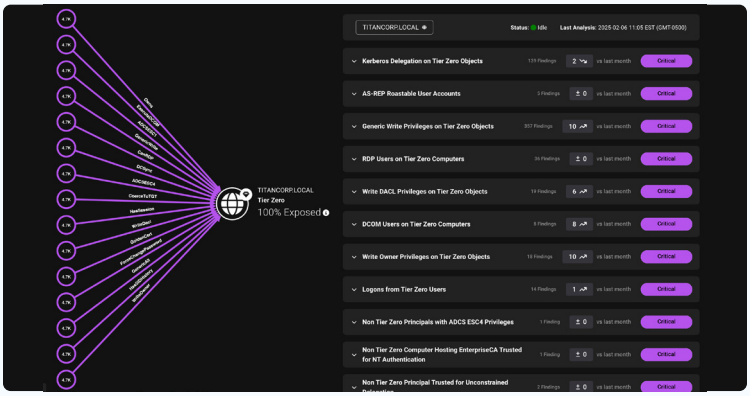
SpecterOps pioneered the concept of Attack Path Management (APM) by creating and maintaining BloodHound since 2017.

Now, with BloodHound Enterprise, an adversarial view of how to exploit (and proactively manage) Identity risk in your AD, Entra ID, and hybrid environments can be visualized in a fully managed SaaS tool with remediation guidance and improvements which are tracked over time.

BloodHound Enterprise continuously maps and quantifies attack paths within your existing architecture, exposes misconfigurations and reduces the allure of targeting directories as the preferred attack vector.

Key Benefits

- Gain visibility into your Identity risk and exposure across your AD, ADCS, Entra ID, and hybrid environments.
- Eliminate years of technical debt from multiple generations of AD Admins, on-prem AD / hybrid complexities, and mergers & acquisitions.
- Continuously audit for new Identity-based risks introduced into your environment.
- Get insights on attack path risk and remediation progress over time.



Visualize the complex connections and relationships in AD and Azure to understand where misconfigurations have exposed your organization's most valuable 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. BloodHound Enterprise covers AD, Entra ID, and hybrid environments.

Prioritized Attack Path Choke Points

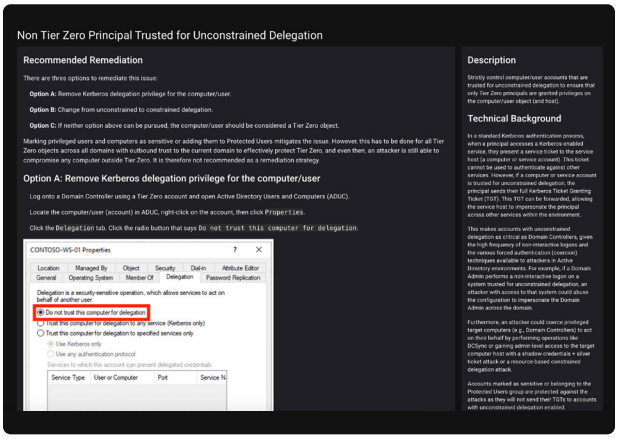
Analyze the millions of attack paths within your environment, identify the choke points that enable rapid risk reduction, and prioritize them based on the risk presented to your organization. This allows you to eliminate the largest amount of attack path risk with a single remediation.

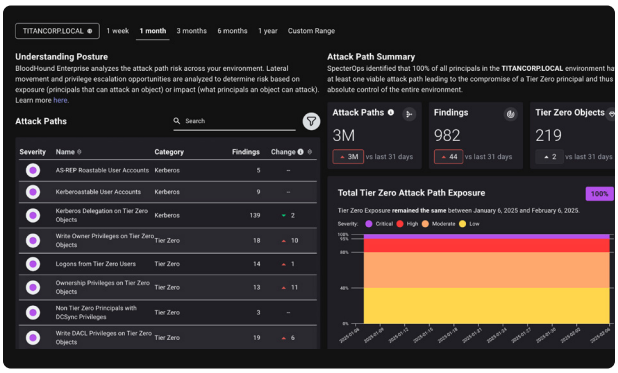
Practical, Step-by-Step Remediations

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 security posture, reassess risk and track improvements across all your directory environments over time.





> **"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

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