BLOODHOUND ENTERPRISE

DATASHEET

BloodHound Enterprise

Uncover and Eliminate the Critical Identity Risk You Can't See

95% of Fortune 1000
organizations have attack paths reachable via AD and Entra ID

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

97% of breaches
leverage an identity attack path

The SpecterOps Difference

BloodHound Enterprise is more than another security product. It's a platform that brings together the decades of offensive and defensive security experience[1] across our teams, thousands of red team engagements around the globe,[2] and tireless work of our research team[3] to find novel identity exploits and the defensive actions needed to prevent or eliminate them.

This knowledge continuously feeds BloodHound Enterprise to make it the most expansive and reliable view of identity security available.

Attackers use identity attack paths to find the most effective way to silently advance through an environment, bypassing detections and alerts to reach their targets: critical IT infrastructure, protected customer and regulatory data, vital business services and applications, and other key resources.

BloodHound Enterprise uncovers your identity attack paths, mapping out how an adversary would leverage often-hidden relationships to reach critical assets, and helps reduce identity risk through tailored remediation guidance, and exposure risk tracking to strengthen your identity overall security posture.

Adversaries live in the gaps between identity systems, overlooked privileges, and misconfigurations, chaining together unintended relationships and evading detection through critical attack paths. **BloodHound Enterprise gives you the attacker perspective to proactively understand these gaps and secure them before they are exploited.**

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.

1. specterops.io/about
2. specterops.io/services/#red-team-engagements
3. specterops.io/blog/category/research

Why BloodHound Enterprise

Visualize complex identity connections and relationships to understand where unseen misconfigurations have exposed your organization's most vital assets.

Continuous Attack Path Mapping

Discover your most critical assets and continuously identify the attack paths adversaries use to move throughout your environment. BloodHound Enterprise is the foundation of your Attack Path Management program, adding critical context around the gaps adversaries exploit.

Prioritized Attack Path Choke Points

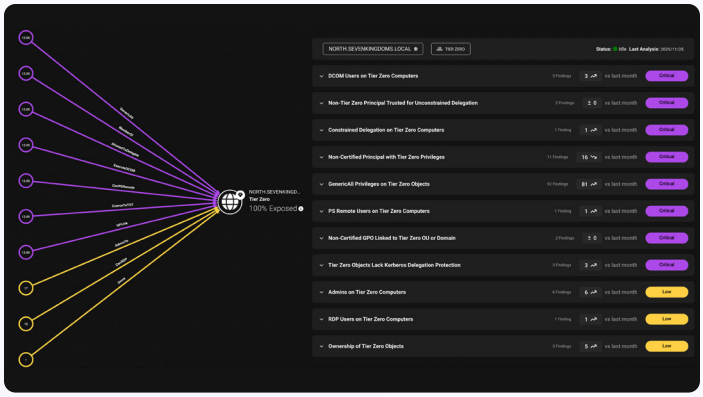
Analyze the millions of attack paths within your environment, identify the choke points that enable rapid risk reduction, and prioritize them based on the risk presented to your organization. Eliminate the most risk with each remediation. On average, a single remediation cuts up to 17,000 attack paths.

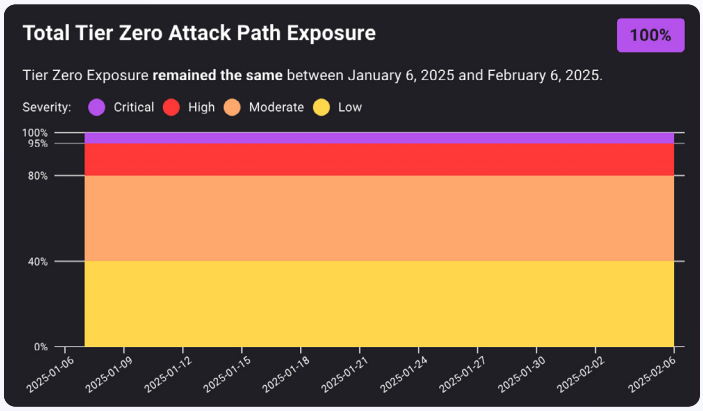
Practical, Step-by-Step Remediations

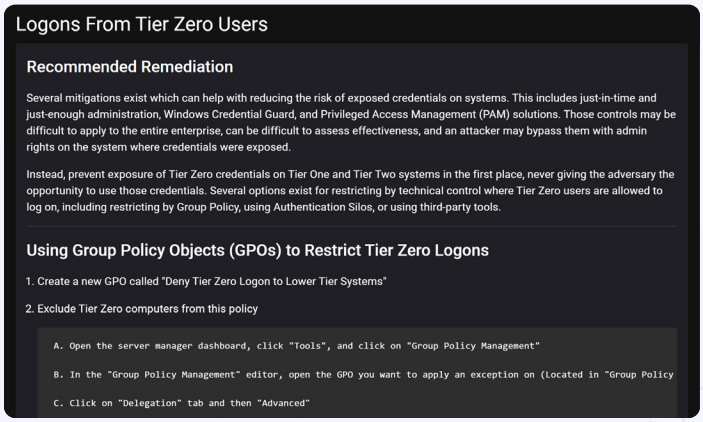
Remove misconfiguration debt using guided remediations that walk your administrators through resolution processes screen-by-screen, eliminating the guesswork and ensuring practical and safe remediation.

Protect What Matters Most with Privilege Zones

BloodHound Enterprise Privilege Zones gives you the ability to accurately segment assets and understand where attack paths provide adversaries with access points, so you can eliminate them. Apply least privilege with the visibility to confidently enforce them.







> **In today's complex enterprise environments, identity-based attack paths are like needles buried in a haystack of permissions, trust relationships, and misconfigurations – especially around Tier Zero resources. BloodHound Enterprise goes beyond detection: It continuously maps and prioritizes the most exploitable paths in AD and Entra ID, empowering engineering teams to respond decisively and safeguard the keys to the kingdom before adversaries can act.***

– Jason Krolak, Principal Group Engineering Manager, Microsoft

* Legal Disclaimer (CELA): The quote above reflects my personal opinion and does not represent the view of Microsoft or its affiliates.

Learn more at specterops.io ›