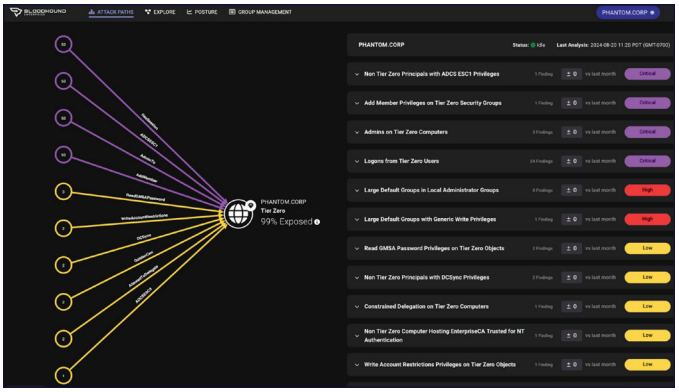
Attack Path Management in a FedRAMP High Environment

Reduce Risk to Your Mission in Identity and Directory Environments

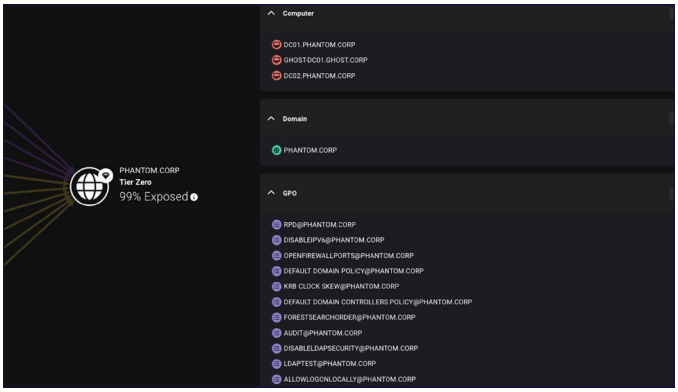
In cybersecurity, you can't fix what you can't see. And yet, adversaries have been exploiting Identity for decades. Identity Attack Paths are trivial for attackers to abuse, and the root cause of significant risk within Active Directory and Entra ID (formerly Azure AD). Adversaries use these Attack Paths to move laterally and escalate privilege, evading detection with ease. When Active Directory, Entra ID and Azure are the backbone to nearly everything in your stack, guided visibility of your identity attack paths and directory hygiene failures is critical.

Nearly all government organizations have Attack Paths reachable via Active Directory and Entra ID. SpecterOps has pioneered the concept of Attack Path Managements by creating and maintaining BloodHound for the last decade.

Now, with BloodHound Enterprise, the adversarial view of how to exploit (and proactively manage) Identity risk in your Active Directory, Entra ID and hybrid environments can be visualized in a fully-managed SaaS tool with remediation guidance, and improvements can be shown over time. BloodHound Enterprise is designated FedRAMP High via the Palantir FedStart Program.



Identify and quantify the Attack Path choke points that will eliminate the most risk to your critical assets.

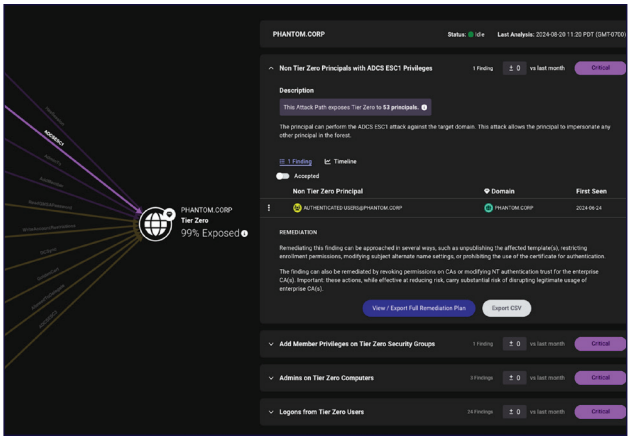


Visualize the complex connections and relationships in AD and Azure to understand where misconfigurations have exposed your organization's most valuable assets.

Benefits:

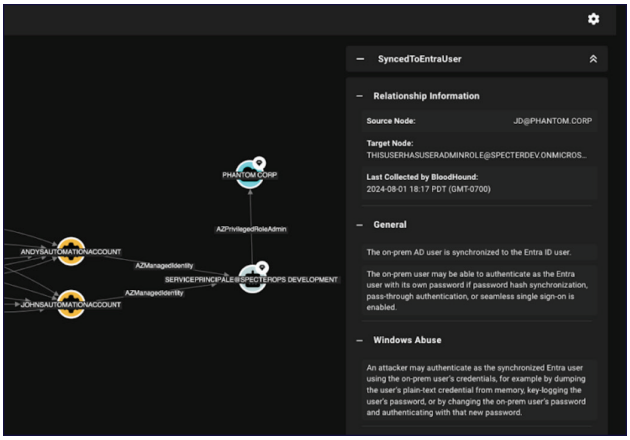
- Measure your Identity risk and exposure in Active Directory, Entra ID and hybrid environments
- Identify Choke Points to remediate millions of Attack Paths with individual fixes
- Eliminate years of technical debt
- Continuously audit for new Identity risk introduced into your environment

"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*



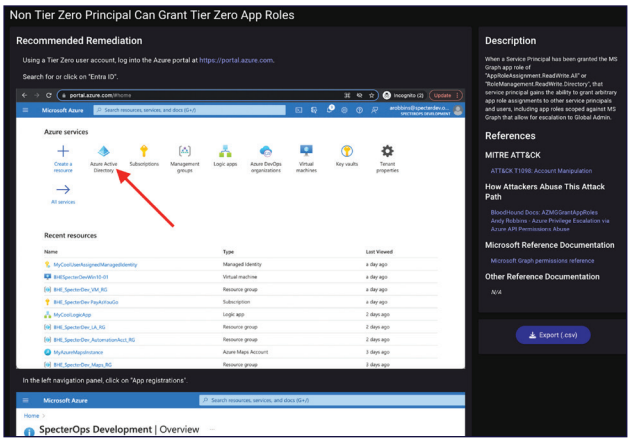
Continuous Attack Path Mapping

After automatically identifying critical Tier Zero or Control Plane assets, BloodHound Enterprise continuously identifies every available Attack Path to understand how adversaries can move laterally and escalate privilege to compromise your environment. BloodHound Enterprise's Attack Path Management covers Active Directory, Entra ID, as well as hybrid environments.



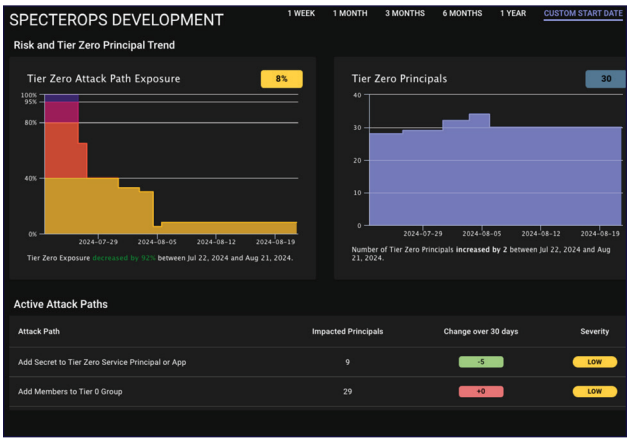
Prioritized Attack Path Choke Points

BloodHound Enterprise analyzes the millions of Attack Paths in your environment, identifies the choke points that enable rapid risk reduction, and prioritizes them based on the risk presented to your organization. This allows you to eliminate the largest amount of Attack Path risk with a single fix.



Practical, Step-by-Step Remediations

Remove misconfiguration debt rapidly using the guided remediations that walk administrators through resolution screen by screen.



Security Posture Measurement

Establish a baseline and track progress as administrators change Azure and Active Directory, reassessing risk over time.

Breaches are inevitable, but impactful breaches are not. Sign up for a demo at

BLOODHOUNDENTERPRISE.IO

bloodhoundenterprise.io