BLOODHOUND ENTERPRISE

DATASHEET

BloodHound Enterprise

Eliminate hybrid identity attack paths to your critical assets

Identity security is one of the most complex challenges defenders face in modern enterprises. Every user, permission, group membership, and misconfiguration represents a potential path to compromise. Years of expanding IT operations mean identity and security teams constantly trading off system availability needs against a growing backlog of security debt. Security teams rarely have the bandwidth to address this identity tech debt and much of it is entirely unknown due to lack of visibility. Attackers know it—and exploit it.

Tier-0 protection is table stakes, but every organization has business critical systems beyond that boundary that carry just as much risk and receive far less scrutiny. BloodHound Enterprise surfaces this risk in the form of identity attack paths, offering your team the attacker perspective of how identities flow through environments, largely undetected. This allows organizations to proactively understand these gaps and secure them before they are exploited.

Attack Path Visibility Without Boundaries

Adversaries don't stop at AD and Entra and neither should your visibility. BloodHound Enterprise OpenGraph extends the power of attack path analysis across any system where identity relationships and privileges create risk. With built-in support for Okta, GitHub, and Mac systems, and the ability to extend coverage to any system in your environment, BloodHound Enterprise goes where your identities go.

OpenGraph Extension Coverage

Okta
Surface identity misconfigurations and privilege escalation paths within your cloud identity provider, including cross-platform paths that bridge Okta toon-premises AD and Entra ID.

GitHub
Identify how repository access and organization-level permissions can be abused as attack paths to sensitive code and downstream production systems.

MacOS
Discover local privilege relationships and misconfigurations on Mac endpoints that create hidden pathways into your broader enterprise environment.

> **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**

* The quote above reflects the personal opinion of the individual and does not represent the view of Microsoft or its affiliates.

This problem isn't theoretical

In modern hybrid environments:

Continuously identify and eliminate the attack paths adversaries use to reach your critical assets. Bloodhound Enterprise is the foundation of your Attack Path Management program, adding critical context around the gaps adversaries exploit, paired with remediation guidance to safely remove the risk without taking down the system.

- Thousands of identities can generate millions of potential paths. A large enterprise with tens of thousands of identities can generate well over ten million potential paths once effective privileges are mapped.
- Tools like IGA and PAM see the surface-level assigned entitlements, but miss the inherited, effective access across domains and platforms that attackers exploit.
- EDR and ITDR detect behavior after it happens; by the time an alert fires, the lateral move is usually complete.

What's made the problem worse is the explosive growth and diversity of systems, identities, and interconnections in today's enterprise. Hybrid environments introduce new privilege relationships spanning from legacy Active Directory environments to Azure Entra ID, PaaS, SaaS platforms, agentic AI, cloud IAM layers, and workloads.

Non-human identities (NHIs)—like service accounts, automation bots, and workload identities—further increase the attack surface, often with less oversight and more privilege than human users.

Understanding the Scope of the Problem

Additionally, commodity AI tooling has lowered the barrier to exploitation. What once required expert-level analysis or red team tradecraft can now be automated, customized, and scaled. AI will also expand the use of Non-Human Identities which creates even more attack paths.

Despite these trends, most organizations are still operating without any formal program for managing attack paths. They lack the visibility, ownership, and repeatable processes needed to reduce this form of risk; let alone prevent it. Even those with strong security tooling in place often underestimate how easily and quickly an intruder can traverse their environment. The result: a massive disconnect between perceived security and actual exposure.

Operationalize BloodHound Enterprise

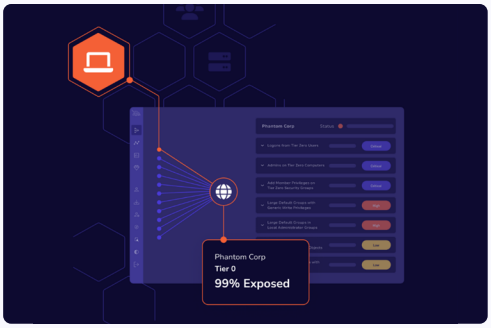
BloodHound Enterprise helps organizations continuously reduce identity risk across complex environments by pushing prioritized attack path findings directly into ticketing, alerting, and orchestration pipelines, accelerating mean time to remediation.

- Microsoft Sentinel SIEM & SOAR
- Palo Alto Cortex XSOAR
- ServiceNow SIR & VRM
- Splunk SIEM & SOAR
- Cisco Duo
- Quest ChangeAuditor

Deliver Real Results with BloodHound Enterprise

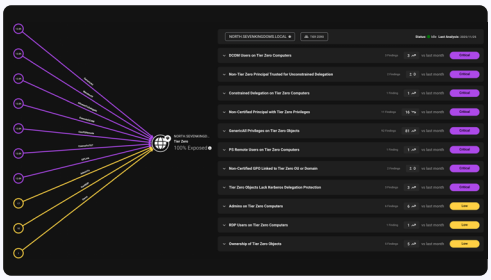
Map Your Complete Attack Surface

Continuously identify and eliminate the attack paths adversaries use to reach your critical assets. Bloodhound Enterprise is the foundation of your Attack Path Management program, adding critical context around the gaps adversaries exploit, paired with remediation guidance to safely remove the risk without taking down the system.



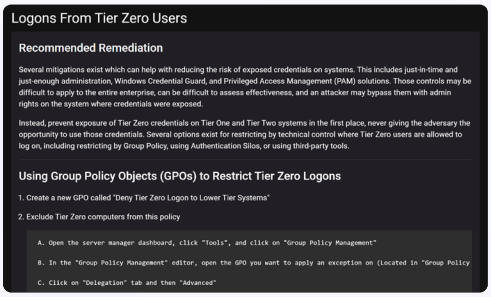
Prioritize Attack Path Choke Points

Analyze the millions of attack paths within your environment and identify the choke points that carry the highest concentration of risk to your critical assets. A single remediation of a choke point can collapse tens of thousands of attack paths at once—**on average up to 17,000 per chokepoint**—eliminating identity risk at scale and making every action count.



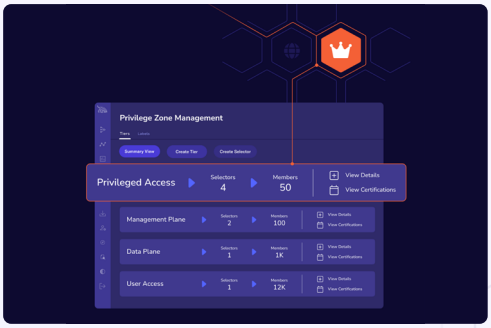
Remediate with Confidence

Guided remediations walk your teams through the resolution process screen-by-screen, turning uncertainty into decisive, measurable risk reduction. For teams balancing system availability against eliminating security debt, hesitation around large-scale changes has real security consequences, so knowing exactly what to do empowers your security team to take the next step.



Protect What Matters Most with Privilege Zones

Business critical systems extend far beyond the traditional administrative plane, and the attack paths that lead to them are equally dangerous. BloodHound Enterprise Privilege Zones lets you custom build zones for your organization's critical assets, surface the attack paths that lead to them, enforce least privilege with confidence, and eliminate risk before adversaries can exploit it. Our enhanced role-based access control model ensures that only authorized users have access to the specific domain they are responsible for securing.



About SpecterOps

SpecterOps pioneered the concept of Attack Path Management for Identity and created BloodHound, the industry-leading platform for identity security. Our team of experts have guided hundreds of organizations through their APM journey, from initial deployment to mature, continuously improving programs.

Learn more at specterops.io ›