BLOODHOUND ENTERPRISE

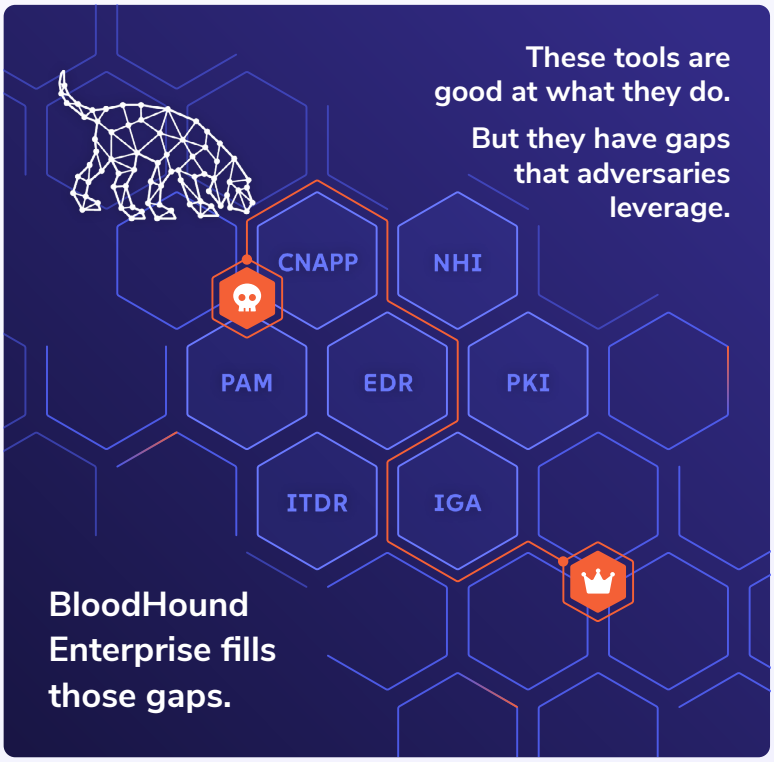
DATASHEET

BloodHound Enterprise Fills Critical Gaps in Identity Security

Attack Path Management Provides Full Visibility

Modern enterprises deploy advanced security solutions to combat cybercrime, yet sophisticated attacks still succeed. Why? These tools have critical blind spots that leave defenders in the dark. Adversaries exploit legitimate identities, cascading privileges, and hidden relationships that traditional solutions cannot see.

BloodHound Enterprise provides the missing layer: a comprehensive identity attack graph revealing how attackers pivot from any compromised identity to critical assets—enabling proactive remediation before exploitation.



ITDR / EDR (Identity Threat Detection & Response / Endpoint Detect & Respond): Finding the Signal in the Noise

What They Miss

- Operates after abuse starts, not before
- Cannot see the identity graph and hidden attack paths
- Miss lateral movement using valid credentials and native tools
- Don't address identity technical debt creating attack opportunities

BloodHound Enterprise

Maps the complete identity graph showing **who can become who** through cascading control, to understand the impact of fraudulently obtained credentials. Eliminates structural attack paths before exploitation, without waiting for an alert.

PAM (Privileged Access Management): Beyond Initial Access Control

What It Misses

- Ineffective after credentials are granted
- Cannot discover hidden privilege through GPOs, OUs, Resource Groups
- Coverage gaps from difficulty identifying all privileged paths
- Misses accounts with abusable permissions enabling lateral movement

BloodHound Enterprise

Discovers **all forms of privilege**—explicit admin rights and implicit control relationships. Identifies shadow admin accounts and dangerous permissions, ensuring comprehensive PAM coverage beyond obvious administrative accounts.

IGA (Identity Governance & Administration): Who Can Become Whom?

What It Misses

- Shows who can access what, not who attackers can become
- Cannot model cascading privileges or transitive control
- Focuses on direct entitlements, not privilege escalation chains

BloodHound Enterprise

While IGA answers "who has access?", BloodHound answers "who can become who?" revealing how low-privilege accounts pivot through multiple identities to reach critical assets. Adds the adversary perspective to IGA's provisioning data.

CNAPP (Cloud Native Application Protection Platform): Bridging the Hybrid Gap

What They Miss

- Disconnected from on-premises identity risks
- Cannot trace hybrid attack paths between AD and cloud
- Miss how cascading control enables identity takeover
- Lack adversary perspective on identity relationships

BloodHound Enterprise

Unified visibility across hybrid environments, mapping attack paths from on-premises AD through Entra ID to cloud resources reveals how on-prem technical debt enables cloud tenant takeover.

The Attack Path Management Advantage

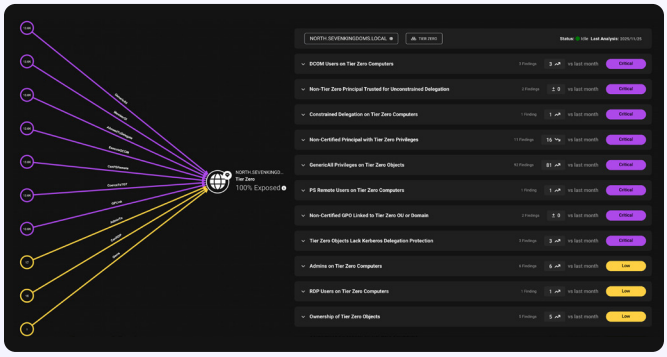
BloodHound Enterprise strengthens your security stack with:

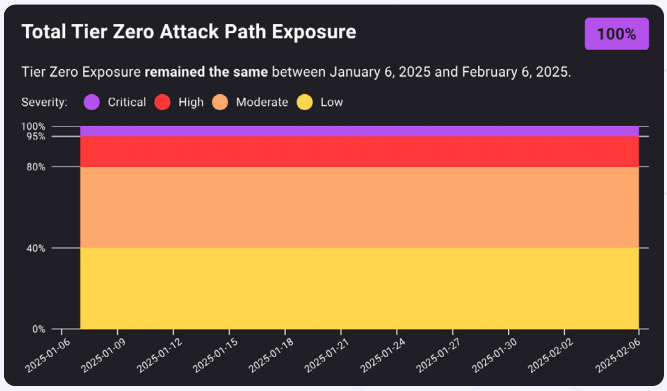
Comprehensive Attack Graphs
Maps identities, permissions, and trust relationships across AD, Azure/Entra ID, and cloud platforms

Adversary-Focused Prioritization
Identifies highest-risk paths to critical assets and quantifies impact to determine priority

Proactive Remediation
Prescribes targeted fixes that break attack paths without disrupting business

Continuous Hardening
Integrates into change control to prevent new attack paths from emerging





Stop playing defense. Eliminate the paths.

This is a brief overview from an extended Solution Brief. Please ask your sales representative for the full version.