

BloodHound Enterprise FedRAMP® High Authorized Identity Attack Path Management

Protecting Mission-Critical Assets from Unseen Threats

Identity relationships chain together in ways defenders never intended. Privileges, group memberships, and configurations across hybrid environments create attack paths that are easy for adversaries to exploit but nearly impossible to understand. Attackers move laterally and escalate privileges across Active Directory, Entra ID, and the systems connected to them without advanced tactics or malware. These attack paths bypass traditional defenses like EDR, PAM, and IGA entirely.

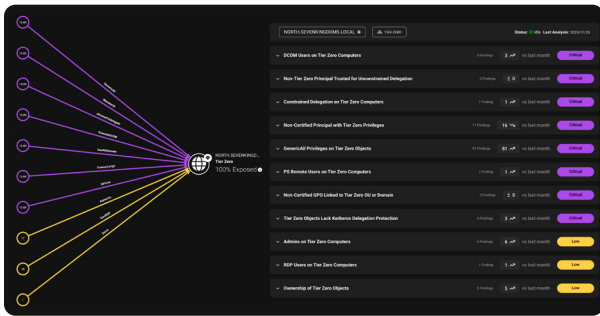
Federal environments amplify this complexity. Decades of technical debt, interconnected trust boundaries, and environments grown through organizational changes leave most agencies blind to how identity relationships collide across systems. **Understanding these cross-system attack paths is essential to protecting mission-critical assets.**

Federal agencies operate some of the most targeted environments in the world, where identity-based attacks against mission-critical systems are a persistent and growing threat. BloodHound Enterprise gives federal security teams the attacker perspective of how identities flow across on-premises AD, cloud, and SaaS environments, surfacing the attack paths adversaries will use to reach critical systems. As a FedRAMP High authorized solution, **BloodHound Enterprise is built to meet the security and compliance demands of the most sensitive civilian and DoD environments.**

- ✓ 97% of breaches leverage an identity attack path.
- ✓ 70%+ of users in an AD domain have at least one attack path to Tier Zero and control over the enterprise.
- ✓ 300,000 attack paths can be eliminated by fixing a single priority choke point.

Key Benefits for Government Security & Identity Teams

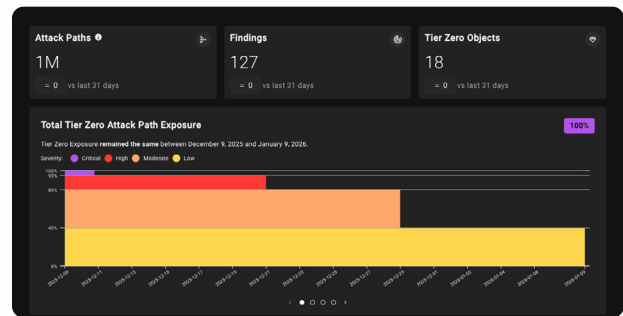
- **Eliminate years of accumulated identity risk** across on-premises AD, cloud, and SaaS environments, establishing a stronger security posture and reducing the attack surface adversaries rely on to reach mission-critical systems.
- **Continuously monitor identity attack paths** across your hybrid environment and remediate them with confidence. Detailed, step-by-step guidance gives identity and security teams the knowhow to act decisively without disrupting mission-critical operations.
- **Extend the value of BloodHound Enterprise** across your entire security stack—native integrations with Splunk, Cortex XSOAR, Cisco Duo, ServiceNow IR, and Vulnerability Response enrich every downstream tool and process with the identity context only attack path management can provide.
- **Support continuous compliance** with NIST CSF, NIST 800-171, and NIST 800-53 through continuous monitoring of identity attack path exposure, giving agencies the evidence and visibility to meet their most demanding regulatory requirements.



See Attack Paths Across Your Entire Identity Ecosystem

Attack paths don't stop at Active Directory or Entra ID boundaries. OpenGraph extends the same attack graph across cloud identity, cloud infrastructure, code repositories, and endpoint management, with built-in coverage for platforms like Okta, AWS GitHub, and Jamf. Federal security teams see how privileges chain across entire identity estate, from the seams between cloud and on-premises identity to the permissions guarding sensitive code and production systems.

The open architecture lets coverage grow to any system where identity relationships create risk.



Extend Protection Beyond Tier Zero

Federal agencies operate systems where compromise would be catastrophic even if they fall outside traditional Tier Zero definitions. Privilege Zones give you the ability to define what critical means for your mission, whether that's classified intelligence repositories, personnel security databases, background investigation systems, or clearance management platforms.

Identify every attack path leading to these assets, segment them with precision, and eliminate exposure before adversaries can reach the systems your mission depends on.

Learn More

Federal agencies can now adopt Identity Attack Path Management as a continuous security practice within their operational constraints. BloodHound Enterprise provides the visibility your security teams need, the controls your compliance framework demands, and the FedRAMP High authorization your environment requires. Scentry expert-led services help agencies operationalize BloodHound Enterprise and mature their attack path management practice, from remediation strategy to compliance reporting.

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/get-a-demo



Access Scoped to Your Mission

Environmental Targeted Access Control (ETAC) segments BloodHound Enterprise access so each team sees only the portion of the environment it manages, even across multiple trust boundaries and organizational divisions.