BLOODHOUND ENTERPRISE

DATASHEET

BloodHound Enterprise

Attack Path Management for the Public Sector

Built for Complex, Open Environments

SLED security teams don't have the luxury of simple environments. They're asked to protect some of the most complex identity infrastructure, often with fewer resources than the threats they face.

State agencies manage thousands of employees and contractors across systems built over decades. Universities balance open research networks against sensitive data. K-12 districts operate under compliance mandates that stack up faster than lean security teams can address them.

Adversaries exploit exactly that complexity. They follow the trust relationships, misconfigurations, and credential connections that span those environments, moving through gaps no single team has visibility into.

BloodHound Enterprise gives lean security teams continuous visibility into those attack paths, so they can focus on what puts critical assets at risk rather than chasing alerts across disconnected systems.

Who We Serve

BloodHound Enterprise is purpose-built for identity environments that never stop changing.

- **State Agencies & Executive Branches**
- **Universities & Community Colleges**
- **State, County & Municipal Governments**
- **K-12 School Districts**
- **Judiciary & Court Systems**

BloodHound Enterprise

Adversaries live in the gaps between identity systems: overlooked privileges, misconfigurations, and unintended relationships chained together across your environment. BloodHound Enterprise gives you the attacker's perspective, so you can find and close those gaps before they are exploited.

Key Capabilities

- Continuous attack path mapping across AD, ADCS, Entra ID, and hybrid environments
- Prioritized choke point analysis—on average, a single remediation eliminates up to 17,000 attack paths
- Practical, step-by-step remediation guidance that walks administrators through screen by screen
- Ongoing auditing for new identity risks introduced as your environment changes
- Attack path risk and remediation progress reporting over time

Improving Device Management Configuration

Device management configurations—Group Policy Objects, Intune policies, and MDM settings—are rarely treated as identity security concerns. **In practice, they often determine what a machine trusts, what software runs with elevated rights, and which accounts hold effective control over endpoints across your environment.**

BloodHound Enterprise analyzes these configurations as part of the full attack path graph. A misconfigured GPO that grants excessive permissions, or an MDM policy that pushes scripts with admin rights, can create an attack path just as surely as a direct Active Directory misconfiguration. Surfacing those paths and connecting them to the identities and assets on either end is what allows your team to remediate the real risk rather than just the obvious one.

Privilege Zones: Enforcing the Boundaries Your Policies Assume

Identity security has long relied on separating assets into secure management categories, most commonly grouping the most critical infrastructure as Tier Zero. Privilege Zones extends that model so your team can apply the same rigorous analysis to the assets that matter most to your organization.

For SLED organizations, that means protecting the systems your communities depend on:

- Student lab and endpoint systems
- Faculty and staff workstations
- Research and grant networks
- Administrative and HR domains
- Financial, registrar, and records systems

With Privilege Zones, your team can identify an asset, determine its appropriate zone, and apply a label. Once defined, BloodHound Enterprise analyzes attack paths across those zones by assigning a risk score, assessing severity, classifying each path, offering remediation guidance, and flagging any connections to more critical zones.

Privilege Zones also identifies abusable hybrid attack paths. In environments where users have identities spanning on-prem Active Directory, cloud platforms, and SaaS systems like GitHub, attackers see the connections between those accounts even when administrators don't. **Privilege Zones surfaces those cross-system zone violations, so you can enforce privilege separation that scales across your entire environment.**

Expanding Coverage with OpenGraph

OpenGraph in BloodHound Enterprise extends attack path visibility across platforms including Okta, GitHub repositories, and Jamf-managed macOS endpoints.

With OpenGraph, attack paths are no longer invisible the moment they cross a platform boundary. Built in collaboration with the global BloodHound open-source community, BloodHound Enterprise brings the same continuous, prioritized analysis your team relies on for Active Directory to identity providers, developer environments, device management systems, and custom data sources. **Every environment adversaries move through, visible in a single graph.**

OpenGraph enables your team to:

- Connect compromised contractor or departmental identities to the critical infrastructure and regulated data they can reach
- Map attack paths across the hybrid mix of identity providers, developer platforms, and device management environments common in government and education
- Eliminate blind spots at platform boundaries where adversaries move between legacy and modern systems unseen
- Give lean security teams a prioritized view of the exposures that matter most, without chasing alerts across disconnected tools

Security Services & Training

Our security services, training, and research directly inform BloodHound Enterprise, enabling SLED organizations to continuously identify, measure, and eliminate identity-driven risk across modern enterprises.

Offensive Security Services & Program Development

SpecterOps offensive security services expose real-world risk through engagements designed to test your environment the way adversaries attack, not the way compliance frameworks and tools assume they will. Our security program development services build defensible processes, clear roadmaps, and capabilities your team owns and sustains independently.

Available Services

- Red team exercises
- Penetration testing
- Web application security assessments
- Attack path assessments
- Program development
- Maturity assessments
- Purple team assessments
- Custom solutions

Training

SpecterOps training equips your team with adversary expertise through hands-on courses, custom curriculum, and realistic lab environments, all designed by front-line practitioners. Courses are available as live public offerings, private and custom trainings, on-demand courses through our Tradecraft Academy, and at SO-CON and Specter Bash, two of our annual conferences. Additional offerings include realistic, enterprise-scale capture the flag environments for training teams and production-grade cyber ranges with the depth and complexity to enable AI model evaluations.

Available Courses

- Adversary Tactics: Detection
- Adversary Tactics: Identity-Driven Offensive Tradecraft
- Adversary Tactics: Red Team Operations
- Adversary Tactics: Tradecraft Analysis
- Adversary Perspectives: Active Directory
- Adversary Perspectives: Azure

> **In today's complex enterprise environments, identity-based attack paths are like needles buried in a haystack of permissions, trust relationships, and misconfigurations. 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.

Interested to Hear More?

Reach out to our head of SLED accounts at wjohnston@specterops.io.

Email Willie Johnston ›