BLOODHOUND ENTERPRISE

OVERVIEW

# Introducing BloodHound Scentry

## Accelerate Your Attack Path Management Practice with Expert Guidance and Extended Team Capacity

Adopting a new practice into a security program often leads to important questions. How does this align with other security tooling? How do we build internal processes that scale across organizations? How do we measure success? These program maturity challenges span people, processes, and technology—and often require expert guidance and assistance.

BloodHound Enterprise provides the foundation for identity Attack Path Management (APM), continuously mapping and analyzing the paths that attackers take to your critical assets and providing prioritized remediation guidance to reduce risk. **BloodHound Scentry is designed to help organizations build and sustain a world-class APM practice: operationalize the program, scale adoption of new capabilities, and make progress measurable over time. Scentry leverages the proven expertise of the SpecterOps team to accelerate your identity APM program and protect your most critical assets.**

## What's Included

### Attack Path Remediation

Every environment has unique requirements, constraints, and technical debt. Scentry experts assess your identity environment (including Active Directory and Entra ID), identify high-impact attack paths and priority actions, and deliver tailored remediation guidance aligned to your identity model—reducing risk from misconfigurations, excessive privileges, and unintended access paths.

### Expert Analysis

Scentry experts provide monthly analysis of identity attack paths, trends, and key risk drivers across your environment. We share clear findings, prioritized recommendations, and practical next steps, and investigate emerging threats and adversary techniques when your organization or industry faces elevated identity risk.

### Privilege Zone Design

BloodHound Enterprise lets you create Privilege Zones around your most critical assets. Scentry experts identify and prioritize high-value identity assets, configure effective Privilege Zones and access boundaries, and track ongoing governance, certification, and control effectiveness over time.

## Why BloodHound Scentry Matters

Built on years of adversary tradecraft and real-world experience protecting Fortune 100 organizations, Scentry helps your team identify, prioritize, and remove high-impact identity attack paths—reducing risk from misconfigurations, excessive privileges, and unintended attack paths.

You'll protect critical assets through Privilege Zones and follow a clear, repeatable program with defined deliverables and measurable progress.

**BloodHound Scentry from SpecterOps ensures you can translate that visibility into measurable risk reduction and sustained program success. Operationalizing an APM practice creates consistent, repeatable, and measurable attack path reduction.**

### BloodHound OpenGraph Support

BloodHound OpenGraph expands attack path coverage across any platform, repository, or application, including hybrid identity systems and custom applications. Scentry experts help you design, build, and validate OpenGraph extensions to meet your coverage requirements and continuously map new identity relationships, privileges, and attack paths as your environment changes.

### Customized Reporting

Scentry tracks the progress of your identity Attack Path Management practice with tailored reporting, including identity hygiene reports and quarterly executive packages. These reports connect attack path remediation and Privilege Zone adoption to measurable improvements in identity security posture, operational risk reduction, and business outcomes.

---

## Outcome

**BloodHound Scentry helps you rapidly build, scale, and mature your identity Attack Path Management practice. Advance from tactical remediation to strategic risk reduction with expert guidance and optimized processes that integrate into your existing security operations.**

## BloodHound Scentry enables your team to:

- **Establish workflows to review, prioritize, and track attack paths using BloodHound Enterprise and OpenGraph data**
- **Coordinate remediation across Security, Identity/IAM, and IT with clear ownership and accountability**
- **Identify critical assets, implement Privilege Zones, and reduce privilege escalation and lateral movement risk**
- **Set risk-aligned SLAs and measure progress with consistent metrics and reporting rhythms**
- **Communicate remediation outcomes to stakeholders and leadership in business-relevant terms**

**The difference between knowing what to fix and consistently reducing attack path risk is where BloodHound Scentry bridges the gap—combining SpecterOps expertise with BloodHound Enterprise to accelerate maturity and expand protection for critical assets.**

## Getting Started

Whether you are an existing BloodHound Enterprise user who is looking to optimize and expand your identity APM practice or a new customer looking to jumpstart your practice with expert help, SpecterOps can help.

Through interactive and collaborative workshops sessions with your BloodHound Scentry team, you will set a plan for your APM practice with a focus on understanding your graph and analyzing risk, determining the best remediation strategies, identifying newly emerging threats outside standard BloodHound Enterprise views, and expanding APM to protect your most critical assets and applications through Privilege Zones and OpenGraph extensions.

**Contact your account team to learn more about BloodHound Scentry.**

## 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** ›