BloodHound Enterprise

Eliminate Hybrid and AI Identity Attack Paths to Your Critical Assets

Identity security is one of the greatest challenges defenders face in modern enterprises. Every user, workload, service account, AI agent, permission, and trust relationship represents a potential path to compromise. Years of digital transformation expanded access needs across Active Directory, Entra ID, Okta, AWS, GitHub, SaaS applications, cloud infrastructure, and AI services, and beyond, which created identity technical debt that traditional security tools cannot fully visualize.

Attackers exploit these identity relationships by chaining permissions across environments until they reach critical assets. BloodHound Enterprise reveals the attack paths that present the greatest organizational risk before they can be abused and pinpoints chokepoints for remediation where a single action can eliminate an entire class of attack paths, allowing organizations to **continuously identify, prioritize, and eliminate the identity conditions attackers depend on while reducing enterprise risk over time.**

"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

Built for the Modern Identity Ecosystem

BloodHound Enterprise unifies attack path visibility across environments while bringing valuable insights into your Security and AI workflows, allowing you to manage attack paths programmatically, with demonstrable risk reduction:

- **Identity:** Active Directory, Entra ID, Okta
- **Cloud:** AWS, Azure
- **Nonhuman Identities:** Service accounts, workload identities, AI agents
- **AI Platforms & Agentic AI:** Entra Agent ID, BloodHound Hunter
- **Endpoints:** Windows, Jamf-managed macOS
- **DevOps:** Git repositories, CI/CD platforms
- **Security Operations and Alerting:** Splunk SIEM & SOAR, Palo Alto Cortex XSOAR, CrowdStrike Falcon IT, Microsoft Sentinel, Google SecOps, Quest ChangeAuditor
- **Ticketing and Service Management:** ServiceNow Vulnerability Response and Security Incident Response, Jira

Along with 30+ more community-driven extensions and the ability to build custom extensions in your environment with the BloodHound Scentry service, and additional third-party integrations.

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

Secure the AI-Driven Identity Era

AI Is Accelerating Both Attack and Defense

In both cases the attack surface is expanding. Organizations are deploying AI agents, workload identities, and automation faster than governance can keep pace, while adversaries use AI to discover and exploit identity attack paths at unprecedented speeds. **BloodHound Enterprise helps organizations secure this expansive identity ecosystem by identifying attack paths across human, non-human, workload, and AI identities before they can be abused.**

Secure Every Identity

Map attack paths across human, non-human, workload, and AI identities to reveal how new trust relationships and privileges expose critical assets across hybrid environments.

Reduce Risk Before Attackers Exploit It

Models which repositories, branches, and workflows can be influenced, what can execute within them, and what that execution reaches downstream, including the build artifacts and distribution pipelines that connect internal code changes to external impact.

Extend Attack Path Intelligence into AI Workflows

BloodHound Hunter integrates attack path data with AI-enabled security workflows, helping teams investigate attack paths faster, translate attack path findings across teams, and make better security decisions with complete enterprise context.

Bring Attack Path Intelligence to AI with BloodHound Hunter

BloodHound Hunter is an MCP-based agent interface within BloodHound Enterprise, marrying BloodHound graph intelligence with critical enterprise context and security controls. Bloodhound Hunter securely connects approved AI assistants and enterprise knowledge sources to BloodHound Enterprise's attack path intelligence. Analysts can investigate identity risk using natural language, explain remediation priorities, identify critical assets, and accelerate decision making while maintaining enterprise context.

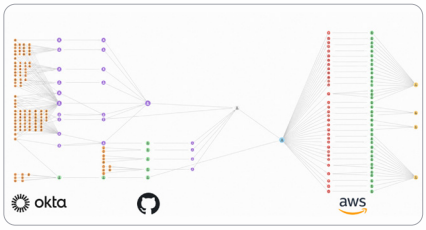
BloodHound Hunter helps customers:

- **Cut through noise**
  by focusing on the attack paths and findings that have the greatest impact on your environment.
- **Apply business context**
  to prioritization, using internal knowledge and trusted tools to inform decisions.
- **Support different stakeholders**
  by translating technical findings into language that is more useful for different teams and decision-makers.
- **Create more tailored workflows**
  for reporting, investigation, and analysis.
- **Lay the groundwork for future innovation**
  in operationalizing attack path data.

Operationalize Identity Attack Path Management

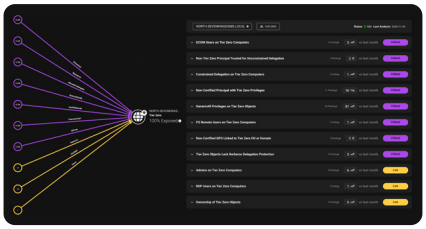
Map Your Complete Attack Surface

OpenGraph, BloodHound's extensible attack graph engine, expands attack graph visibility across new identity providers, cloud platforms, AI services, development environments, and enterprise technologies, so organizational APM practices can grow with the environment, and security teams can maintain a singular view of attack path risk to critical assets anywhere.



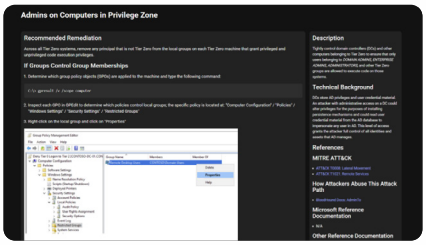
Prioritize Attack Path Choke Points

Across millions of attack paths, there are a small number of remediation actions that eliminate the greatest concentration of organizational risk. BloodHound Enterprise recalculates chokepoints as identities, cloud resources, AI agents, and workloads change, ensuring remediation efforts always focus on the attack paths that matter most.



Remediate with Confidence

BloodHound Enterprise goes beyond visibility into where attack paths exist. Guided remediation helps defenders and identity teams eliminate them at scale without impacting key systems, improving security posture and resolving decades of identity tech debt.



Protect Your Most Critical Assets with Privilege Zones

Not every identity or asset carries the same level of risk. BloodHound Enterprise Privilege Zones enable organizations to define the administrative and security boundaries that are critical to the business, then continuously find where identities, permissions, delegated administration, and trust relationships violate those boundaries. This extends the principles of least privilege and tiered administration beyond a single platform, providing a consistent process to secure critical assets across hybrid, cloud, SaaS, endpoint, and development environments. Privilege Zones can be defined around any high-value asset or administrative boundary, including:

Identity & Administrative Control

- Privileged users, groups, and administrative roles
- Executive users and executive groups
- Okta Core Identity Store

Critical Business Systems & Data

- Vital line-of-business applications
- Regulatory data, sensitive customer data, and PII
- Intellectual property

Development & Software Supply Chain

- Git repositories capable of influencing production
- CI/CD pipelines
- API tokens and other high-value credentials

Managed Endpoints

- Managed devices used by privileged administrators
- Devices assigned to executives, developers, and other high-impact users or groups
- Jamf-managed Mac OS environments

Rather than protecting technologies in isolation, BloodHound Enterprise reveals the identities that can cross administrative boundaries and the attack paths that connect them. This enables organizations to enforce least privilege, reduce identity-driven risk, and ensure their most critical assets remain isolated from unnecessary administrative influence.

Bring SpecterOps Expertise to Your APM Practice

BloodHound Scentry is a tradecraft-driven advisory service that extends the value of BloodHound Enterprise by applying SpecterOps' adversary research, attack path expertise, and real-world experience directly to your environment. Continuous expert analysis of your graph, tailored remediation strategies, and advanced guidance help you stay ahead of emerging threats as you grow and mature your APM practice.

Scentry can help you:

- **Discover**
  unknown or complex attack paths to your critical assets.
- **Understand**
  the adversary implications of those paths.
- **Develop**
  practical, environment-specific remediation strategies.
- **Build**
  Privilege Zones, extending APM to your most critical assets, identities, and resources.
- **Design**
  custom OpenGraph extensions for your most vital applications and environments.

For additional details, use cases and outcomes, check out the BloodHound Scentry data sheet.

Research-Driven, Adversary-Informed, Results Oriented

SpecterOps helps organizations defend against tomorrow's identity attacks by applying the same adversary tradecraft behind BloodHound, over 100 open-source solutions, and our industry-leading security research. Our Services teams expose real-world risk through red team operations, penetration testing, attack path assessments, web application security assessments, and AI security evaluations.

We also help organizations mature security programs through advisory, assessments, and purple team engagements, while our hands-on Training equips defenders with practical expertise in identity security, offensive tradecraft, detection engineering, Active Directory, Azure, and enterprise-scale lab environments. SpecterOps has trained over 10,000 security practitioners worldwide.

The research, training, and service engagements directly guide BloodHound Enterprise, helping organizations validate attack paths, accelerate remediation, and strengthen their security posture.

To learn more about our Offensive Security Services, Security Program Development & Maturity offerings, or Training programs, click here.

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 ›

SPECTEROPS ©2026 Specter Ops, Inc.