BLOODHOUND ENTERPRISE

DATASHEET

BloodHound Enterprise

FedRAMP® High Authorized Identity Attack Path Management

Protecting Mission-Critical Assets from Identity Threats

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.

Identity relationships can chain together access in ways identity teams 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. As a result, attackers can move laterally and escalate privileges to access critical assets across Active Directory, Entra ID, and the myriad resources connected to them without advanced tactics or malware.

Identity attack paths provide all the reach they need, and often these attack paths bypass traditional defenses like EDR, PAM, and IGA entirely.

Decades of technical debt, interconnected trust boundaries, and environments grown through organizational changes leave most agencies unaware of how identity relationships collide across systems.

BloodHound Enterprise gives federal security teams the attacker perspective of how identities flow across perceived boundaries, 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.

Enterprise Controls for Sensitive Environments

Environmental Targeted Access Control (ETAC)

Segment access so users only see their portion of complex federal environments with multiple trust boundaries or federated structures.

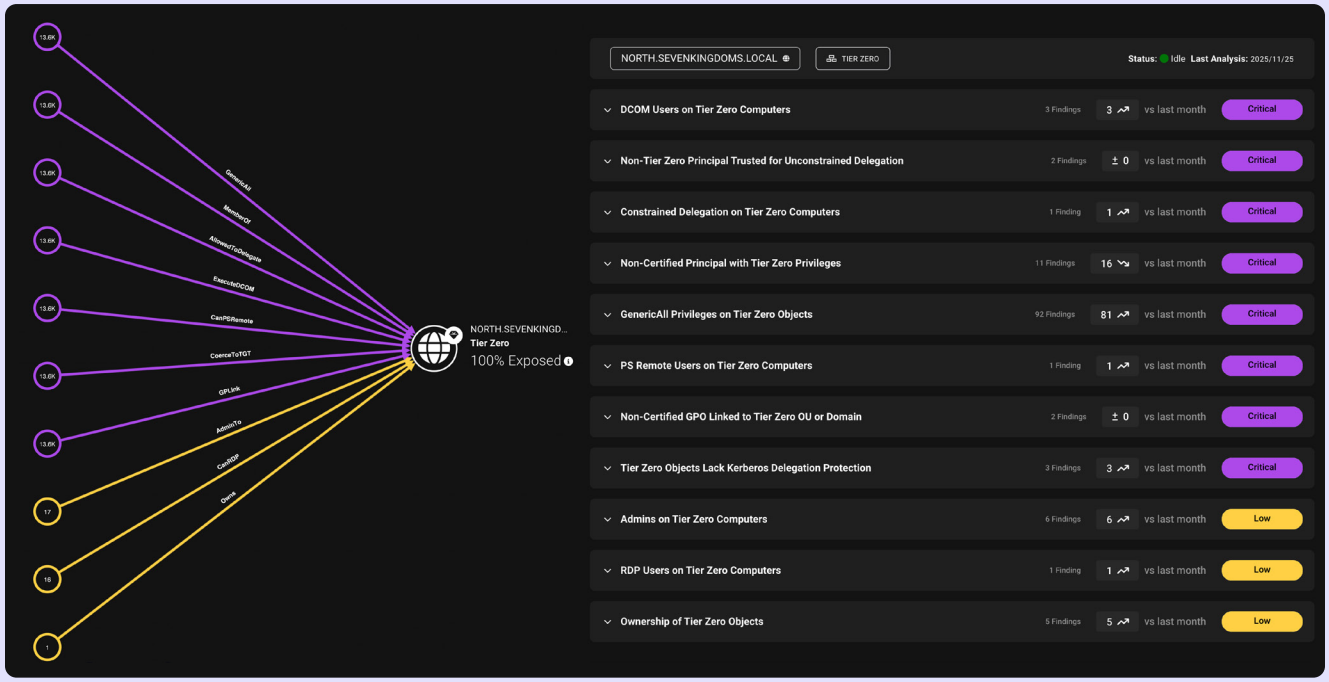
Bring Your Own Key (BYOK)

Control your own encryption keys for attack path data, keeping the complete map of identity vulnerabilities exclusively under your agency's control.

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 elminated by fixing a single priority choke point



Visualize complex identity connections and relationships to understand where misconfigurations have exposed your organization's most valuable assets.

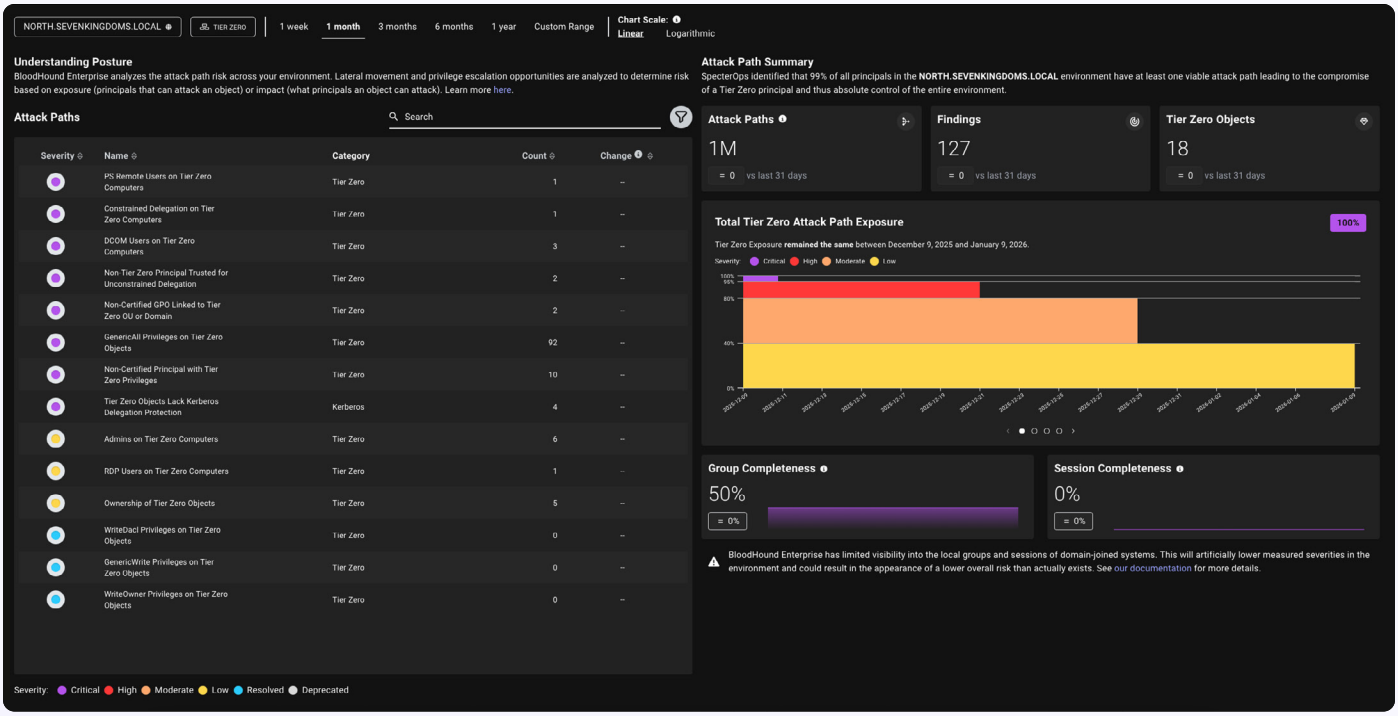
Key Benefits for Government Security & Identity Teams

- **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 ability to act decisively without disrupting mission-critical operations.
- **Extend the value of BloodHound Enterprise** across your entire security stack. Native integrations with Splunk, ServiceNow IR and Vulnerability Response, Cortex XSOAR, and 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 visibility across the identity systems federal agencies depend on, revealing how privileges chain together across different platforms, such as Okta, GitHub, and Jamf-managed Macs to create paths adversaries will exploit.

- **Okta** integration exposes cross-boundary attack paths between cloud identity providers and on-premises directories, revealing lateral movement opportunities that exist in hybrid identity architectures federal agencies rely on.
- **GitHub** coverage protects the software supply chain by mapping how repository permissions and organizational access create pathways to sensitive code and production environments.
- **macOS** visibility discovers local privilege relationships on Jamf-managed Mac endpoints that create entry points adversaries exploit to gain initial access or move laterally through the enterprise.



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 gives 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

Contact your SpecterOps representative or sign up for a demo to see how BloodHound Enterprise can help protect your organization's most critical assets.

Learn more at specterops.io ›