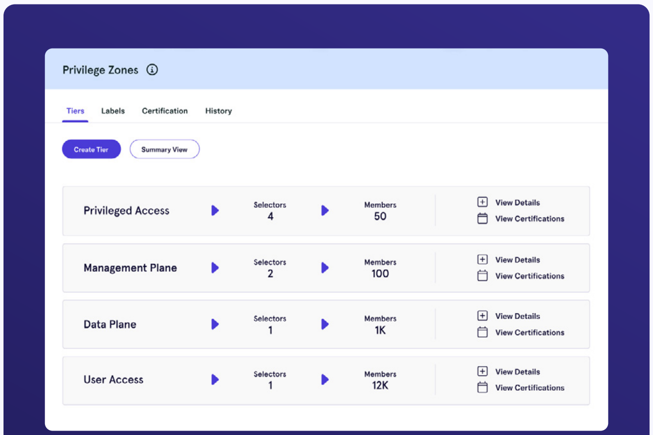
BLOODHOUND
ENTERPRISE

DATASHEET

Go Beyond Traditional Boundaries

with Privilege Zones in BloodHound



Privileged Access	Selectors 4	Members 50	View Details View Certifications
Management Plane	Selectors 2	Members 100	View Details View Certifications
Data Plane	Selectors 1	Members 1K	View Details View Certifications
User Access	Selectors 1	Members 12K	View Details View Certifications

Privilege Zones Enable Customers to Go Further Into the Attack Graph

- Enable the principle of least privilege across your environment.
- Segment assets based on your business priorities and environment.
- Protect any asset with BloodHound Enterprise's (BHE) rigorous analysis and visualization.
- New views to understand potential attack paths and quantify security risks across defined Privilege Zones.

Identity security practices have long supported a model of separating assets into secure management categories as part of a privileged access strategy, whether those be legacy directory services systems or modern hybrid or cloud environments. The most critical assets are often classified as Tier Zero (or the Control Plane).

Securing this traditional boundary is fundamental to identity security and a priority for practitioners and security leaders to protect and prevent consequential data breaches, escalation of an attacker within directory environments, or other malicious activity designed to take down an organization.

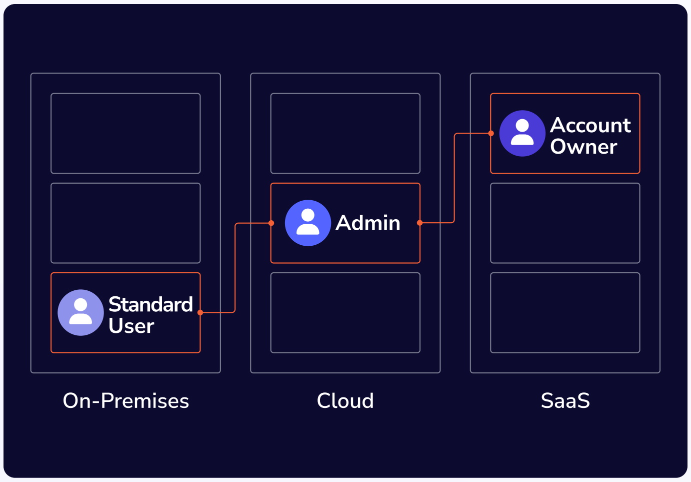
However, other business critical assets likely require similar scrutiny and visibility. For example, health records at a regional hospital or a code repository at a tech company. **These assets deserve as much scrutiny as traditional "crown jewels" to reduce business risk, such as loss of reputation or loss of revenue, which is why we're introducing Privilege Zones.**

While there will continue to be a segregated group of critical assets for attack path analysis, Privilege Zones allows teams to add zones unique to each organization's priorities. Zone One assets may include things like HIPAA servers, databases with customer information, or PCI DSS payment systems that require 100% uptime.

With Privilege Zones, teams can identify an asset, determine its appropriate zone, and apply the correct label.

The analysis will:

- ✓ Include a risk score
- ✓ Classify the attack path
- ✓ Offer remediation guidance
- ✓ Assess severity
- ✓ Highlight any connections to more critical zones



Built for Hybrid Environments

In hybrid environments, users often exist in multiple identity systems: On-prem, Cloud, and SaaS platforms (such as GitHub or Salesforce). While these accounts may look separate—attackers see the connections. A single employee may have identities that span multiple systems with escalating privileges—signifying poor hygiene and a zone violation across systems.

Privilege Zones detects these hybrid attack paths, allowing Identity and security teams to enforce cross-system privilege separation that scales for hybrid environments.

Getting Started

Privilege Zones includes two components:

- Management
- Analysis

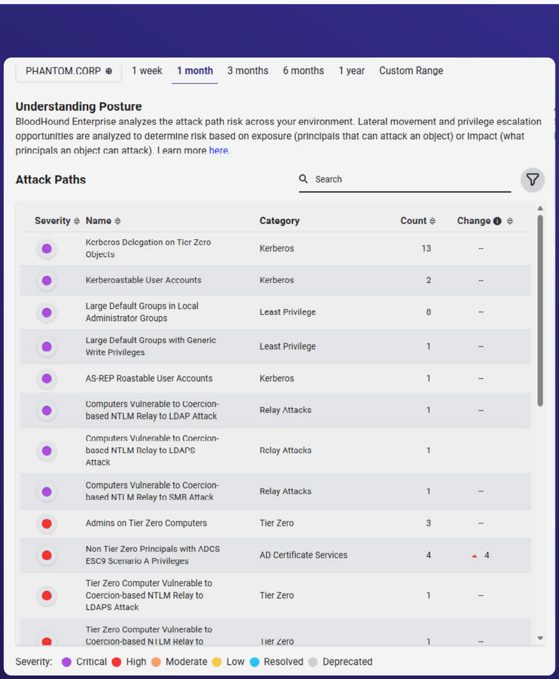
Privilege Zones Management will allow users to create additional protective privilege zones outside of Tier Zero and apply labels to group assets into additional zones. This functionality will be available to all users of BloodHound.

Privilege Zones Analysis will follow later in the year. Once all the assets outside of Tier Zero that need to be protected have been identified, those assets can be analyzed for potential attack paths, just like Tier Zero assets. With a subscription to Privilege Zones Analysis, BloodHound Enterprise customers will be able to view assets and attack paths by zone to shore up adequate security measures.

Summary

Privilege Zones introduces the technical control to validate and defend your access model—on-prem, in the cloud, and everywhere in between. Enforce the boundaries your policies assume and finally implement Least Privilege in your BloodHound Enterprise account today.

Learn more at specterops.io/get-a-demo



Understanding Posture

BloodHound Enterprise analyzes the attack path risk across your environment. Lateral movement and privilege escalation opportunities are analyzed to determine risk based on exposure (principals that can attack an object) or impact (what principals an object can attack). Learn more here.

Attack Paths

Severity	Name	Category	Count	Change
●	Kerberos Delegation on Tier Zero Objects	Kerberos	13	--
●	Kerberoastable User Accounts	Kerberos	2	--
●	Large Default Groups in Local Administrator Groups	Least Privilege	8	--
●	Large Default Groups with Generic Write Privileges	Least Privilege	1	--
●	AS-REP Roastable User Accounts	Kerberos	1	--
●	Computers Vulnerable to Coercion-based NTLM Relay to LDAP Attack	Relay Attacks	1	--
●	Computers Vulnerable to Coercion-based NTLM Relay to LDAPS Attack	Relay Attacks	1	
●	Computers Vulnerable to Coercion-based NTLM Relay to SMB Attack	Relay Attacks	1	--
●	Admins on Tier Zero Computers	Tier Zero	3	--
●	Non Tier Zero Principals with ADCS ESC9 Scenario A Privileges	AD Certificate Services	4	▲ 4
●	Tier Zero Computer Vulnerable to Coercion-based NTLM Relay to LDAPS Attack	Tier Zero	1	--
●	Tier Zero Computer Vulnerable to Coercion-based NTLM Relay to	Tier Zero	1	--

Severity: ● Critical ● High ● Moderate ● Low ● Resolved ● Deprecated

Privilege Zones Attack Path Analysis

- Analyze Attack Paths across Zones.
- Identify choke points where attackers can bypass security boundaries.
- Ensure your tiered architecture works as designed—no gaps, no blind spots.

SPECTEROPS