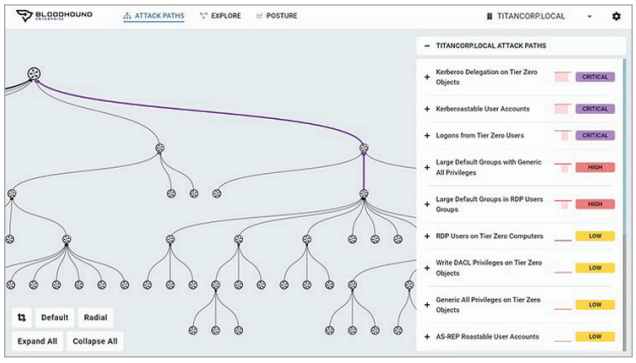
Active Directory Security Assessment

Minimize attack paths and secure Active Directory and Azure with SpecterOps BloodHound Enterprise

A critical component of defending Active Directory (AD) and Azure from cyberattacks is to identify and secure the attack paths attackers could use to infiltrate your AD environment. And that should be no surprise considering more than 95 million AD user accounts are under attack every day. But how do you prioritize which attack paths to secure first?

While most people who defend IT networks think in terms of lists — checking thousands of generic configuration issues — attackers often think in graphs in order to more quickly find a path to an organization's control plane or Tier Zero assets. That's where SpecterOps BloodHound Enterprise can help.

With our AD Security Assessment using BloodHound Enterprise, we're able to provide critical insight into the security of your hybrid AD environment, showing you a superset of your critical assets in AD and Azure (Azure AD and Azure Resource Manager) – the assets that would mean game over if a cyber attacker got control of them. With the Active Directory Security Assessment, you'll visually see the potential paths an attacker could use to gain access to the crown jewels of your environment.



Identify and quantify the attack path choke points that will eliminate the most attack paths to your critical assets.

Find and remove the choke points – the top-level attack paths – to increase your security posture.

How does it work?

First, one of our experienced solutions architects will consult with your team to set up BloodHound Enterprise and complete the initial scan of your environment. From there, we help you understand every possible route to your Tier Zero assets and identify every relationship throughout your hybrid environment that an attacker could abuse to gain access. With BloodHound Enterprise, we'll measure every attack path — and the corresponding choke points on those attack paths — to give you an overall view of the risk your organization is carrying in your

Benefits:

- Measures the impact of any point in an attack path
- Identifies the optimal location to block the largest number of pathways
- Ranks these finite set of choke points by collective risk reduction
- Minimizes remediation efforts and eliminating misconfiguration debt cleanup

hybrid AD environment. And as you improve your attack path management by eliminating these choke points, you'll also be able to see the effect these changes will have on your overall security posture.

Continuous assessment

Enterprise networks, user privileges, application permissions and security group memberships are dynamic. For every system a privileged user logs into, the user leaves behind tokens and credentials for adversaries to try to obtain. Because the connections and behaviors that form attack paths are continuously changing, the attack paths themselves must also be continuously mapped. With BloodHound Enterprise, you can continuously:

- Chart every relationship and connection
- Reveal full understanding of real permissions
- Expose new and existing hidden attack paths in AD and Azure AD
- Ensure your team is meeting the ongoing security needs of your organization

Areas of focus

The AD security assessment will:

- Deliver practical remediations without drastic changes to AD / Azure AD or negative impact
- Provide precise and comprehensive guidance to help you eliminate attack paths
- Furnish instructions on how to validate that the privileges being removed are not required
- Provide visibility to all AD attack paths
  - Enumerate and uncover all attack paths available to attackers for lateral movement and privileged escalation
- Prioritize choke points with practical remediations
  - Identify how you can remove millions of attack paths with the minimum amount of effort and do so within your existing AD architecture
- Measure your AD security posture improvements over time
- Identify your exposure level of high-value targets and track remediation effectiveness

Next steps

While SpecterOps BloodHound Enterprise helps chart and identify the attack paths and choke points across your hybrid AD environment, it's up to you to eliminate the identified choke points and set parameters to ensure the ongoing security of your environment. Quest can help there, too.

Comprehensive risk assessment and threat monitoring

Pair SpecterOps BloodHound Enterprise with Change Auditor and On Demand Audit for a comprehensive risk assessment and threat monitoring solution. Together, you'll be able to fully audit all security changes across your AD and Azure AD environments, including user and group changes, and detect exploits early such as exfiltration of the AD database via offline copy or unauthorized domain replication. You'll also be able to block attackers' access to paths – including privileged groups, GPOs and exfiltration of your AD database to mitigate and avoid costly ransomware attacks.

Attack path mitigation via securing GPOs

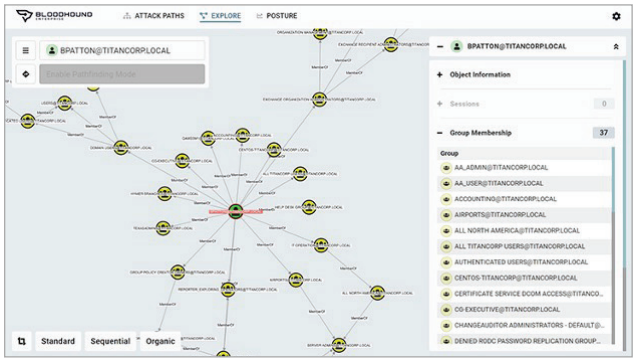
When you use SpecterOps BloodHound Enterprise with GPOADmin, you'll be able to improve attack path management by securing GPOs. These solutions allow you to ensure that any changes adhere to change management best practices prior to deployment, a critical step in Active Directory group policy management. Moreover, you'll be able to continually validate GPOs through automated attestation — a must for any third-party group policy management solution. Furthermore, you'll be able to quickly revert back to a working GPO in the event that a GPO change has an undesired effect, allowing you to get your environment running smoothly again in seconds.

Risk protection and remediation insurance

For true risk protection and remediation insurance, combine SpecterOps BloodHound Enterprise with Recovery Manager for Active Directory Disaster Recovery Edition and On Demand Recovery. This product combination gives you comprehensive capabilities when it comes to backing up hybrid Active Directory and quickly recovering from any mistakes, corruption or disaster. Moreover, you'll be able to highlight any changes made since the last backup by comparing the online state of AD with its backup (or multiple backups). Furthermore, you'll be able to restore any object in AD, including users, attributes, organizational units (OUs), computers, subnets, sites, configurations and Group Policy Objects (GPOs).

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.



Visualize the complex connections and relationships in AD and Azure to understand where misconfigurations have exposed your organization's most valuable assets

SYSTEM REQUIREMENTS

System

- Windows Server 2012+
- 16GB RAM
- 100GB hard disk space
- .NET 4.5.2+

Network

- TLS on 443/TCP to your tenant URL (provided by your account team)
- TLS on 443/TCP to Azure tenant (if applicable)

Permissions

SharpHound (on-premises Active Directory collection)

- Service account added to local Administrators group

AzureHound (Azure collection)

- Directory Reader on Azure AD Tenant
- Reader on all Azure Subscriptions
- Microsoft Graph
  - AppRoleAssignment.ReadWrite.All
  - RoleManagement.Read.All