A practical approach to cyber resiliency

Efficiently secure the critical assets in your hybrid Active Directory with attack path management.

Quest

Introduction

Organizations today are keenly aware of the need to improve cybersecurity. However, finding an effective and efficient strategy for achieving that goal often feels elusive. Adversaries are constantly inventing new tactics and techniques, leaving IT scrambling to fight the latest fire.

However, there is a practical way to get ahead of the onslaught of cyberattacks: Think like an adversary. For years, hackers have been using a free open-source tool called BloodHound to find the quickest path to take over an environment once they've compromised an ordinary user account. To keep up, IT teams need to proactively map out all these attack paths that hackers could exploit and — critically — pinpoint the key remediation measures that will shut off hundreds or thousands of those attack paths at once.

Now they have a tool that makes effective attack path management easy: SpecterOps BloodHound Enterprise. This white paper explains how attack path management works and why it is a practical approach to modern cybersecurity. Then, it explains how to complement attack path management with other key strategies to achieve not just cyber security, but cyber resiliency.

Understanding your critical assets

Classifying critical assets in an on-premises environment

A vital first step in protecting your IT environment is understanding your most critical IT assets. In an on-premises environment, IT pros classify assets into the following tiers, which are illustrated in Figure 1:

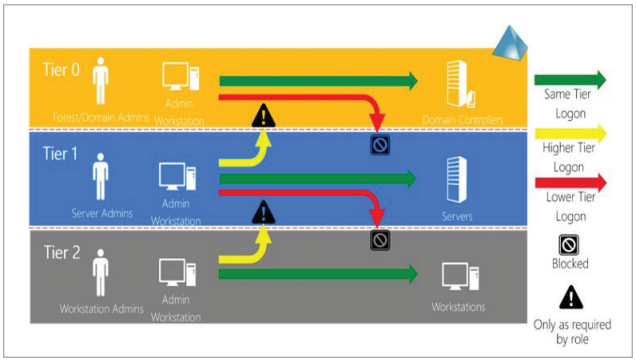

Figure 1. Classifying critical assets in an on-prem environment (Image credit: Microsoft)

Tier 0 (the control plane) comprises your most sensitive assets, such as Domain Admins, domain controllers and administrative workstations.

- **Tier 0 —** Tier 0, or the **control plane**, comprises your most sensitive assets, such as forest and domain admins, domain controllers, and administrative workstations.
- **Tier 1 —** The next tier comprises your slightly less sensitive assets, such as server admins and their workstations. More generally, it includes the following two planes:
  - **Management plane —** For enterprise-wide IT management functions
  - **Data/workload plane —** For per-workload management, which can be performed by either IT personnel or business units
- **Tier 2 —** Tier 2 includes assets like workstation admins and their workstations. It controls both **user access** and **application access**.

Classifying critical assets in a hybrid environment

This model can be expanded from on-premises Active Directory to cover hybrid environments that include Azure AD, as illustrated in Figure 2. As you can see, the model includes the same components described above: control plane, management plane, data/workload plane, user access, and app access.

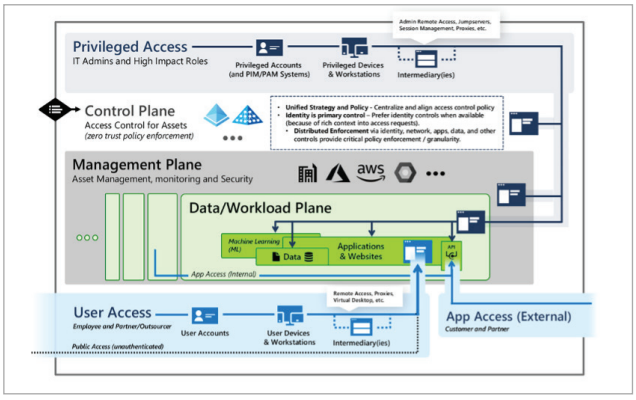

Figure 2. Classifying critical assets in an on-prem environment (Image credit: Microsoft)

Quest

It's important to note that several critical security principles apply across both of these models. First and foremost, nothing should be able to control anything in a higher tier. In particular, assets in the control plane should never be controlled by assets in the management plane or the data/workload plane. In addition, whenever there is a legitimate need to access resources using privileged access, the user should use a dedicated privileged user account and a dedicated privileged access workstation (PAW).

> **Assets in the control plane should never be controlled by assets in the management or data/ workload planes.**

Key examples of critical assets

It's important to understand that critical assets are not limited to highly privileged accounts like Domain Admins and Server Admins. Other examples include:

- Domain controllers (DCs), which hold all the credentials for all AD user accounts
- Group Policy objects (GPOs) that affect Tier 0 assets
- Your Azure AD Connect server and the associated service account
- ADFS
- Certificate Authority (CA) and public key infrastructure (PKI) servers, since an adversary who compromise them can generate certificates that they can use to log on as any user without knowing their password
- Active Directory backups
- Privileged access workstations

Uncovering the attack paths that put your critical assets at risk

Adversaries are, of course, eager to gain access to your critical assets — compromising those assets enables them to achieve their ultimate goal, whether that's to steal your most valuable data, unleash ransomware across the environment and corrupt your AD backups to increase the odds you'll pay the ransom, plant back doors to enable future access, or something else.

However, adversaries generally can't compromise your Tier 0 assets in their initial assault. Instead, they usually use phishing, password-based attacks and other techniques to take over an ordinary user account. Once they have established that foothold, they can use an open-source tool called BloodHound to discover a series of steps they can take to gain control of Tier 0 assets. Such a series of steps is called an **attack path**.

> **An attack path is a series of steps that enables an adversary who has compromised an ordinary user account to gain access to your control plane.**

An attack path is not a simple missing security update or suboptimal configuration that can be handled through effective patching and vulnerability management. Rather, an attack path is a series of steps that takes advantage of a combination of factors such as concealed permissions, nested group membership, misconfigured Group Policy, inherent security gaps in AD architecture, and complex relationships in Active Directory and Azure.

The best way to explain attack paths is through an example. Figure 3 illustrates one attack path. Its root is an ordinary user account, Alex. However, that user account is a member of the HelpDesk group, which in turn is a member of another group, Tier Two support. (Such group nesting is very common in AD.) And the Tier Two support group has local admin rights on the computer Payment-01. According, Alex — or an adversary who compromises Alex's account — has local admin rights on that machine, where a service account (SVC_PAYADMIN) is logged on.

As a result, Alex (or the adversary) can use the Alex account's local admin rights to log into the Payment-01 computer and run a tool like mimikatz to promptly dump the credentials of the service account and act on behalf of that account. And the service account has the right to add members to the Domain Admins group, a Tier 0 asset that grants full control over the environment.

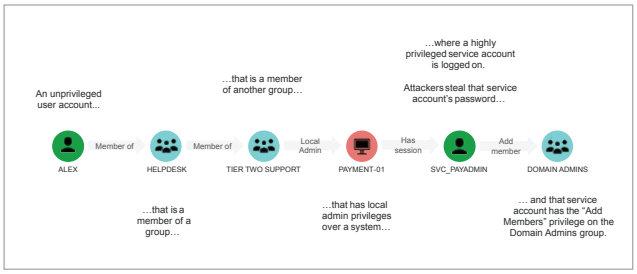

Figure 3. An example of an attack path in Active Directory

Attack path management

Mapping attack paths

The example above illustrates just one attack path in an environment — most environments have hundred or even thousands of attack paths that enable an adversary who gains control of an ordinary user account to compromise the control plane.

The open-source version of BloodHound typically shows only the shortest attack paths in the environment. It's like Google Maps — if you're driving from Seattle to Manhattan, Google Maps will provide the top two or three routes for completing your trip. But while getting only the top few routes from Google Maps is typically good enough, security teams need to know about all the attack paths in their environment, and not just the simplest ones.

Happily, there is now a version of the tool built specifically for security teams, SpecterOps BloodHound Enterprise, that can automatically map out all the attack paths that lead to your critical assets. BloodHound Enterprise analyzes all of the relationships throughout your domain and identifies every way that an adversary could abuse them to get to your control plane, as illustrated in Figure 4. Even better, it presents those attack paths in a clear graphical format.

SpecterOps BloodHound Enterprise will automatically map out all the attack paths that lead to your critical assets.

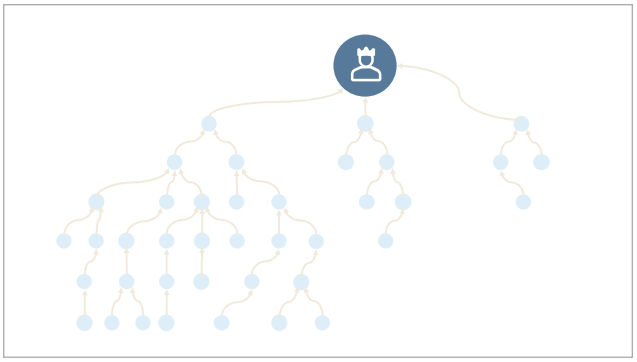

Figure 4. BloodHound Enterprise maps all of the attack paths that lead to your control plane.

Identifying and mitigating the choke points

Of course, mitigating hundreds or even thousands of attack paths one by one would be an overwhelming task for even the most well-staffed IT team. It would be like trying to block every possible route from Seattle to Manhattan. As you block one route, adversaries will simply pick another. Moreover, the roadblocks you're erecting all over would disrupt legitimate traffic in your environment, potentially even bringing the business to a virtual standstill.

Fortunately, BloodHound Enterprise provides a far more effective option than a scattershot defense strategy. It assembles the attack paths it uncovers into a single coherent picture, grouping all the attack paths that share the same final step, the **choke point**. Even organizations with thousands of attack paths generally have only a handful of choke points.

BloodHound Enterprise even quantifies the choke points, telling you with a high degree of certainty what percentage of your accounts are the starting point for an attack path that depends upon the same final step, or choke point. For example, Figure 5 illustrates an environment with three choke points. The one on the left is the final step in attack paths that affect 92% of all accounts. The percentages total more than 100% because a given account can be the root of more than one attack path.

Quest

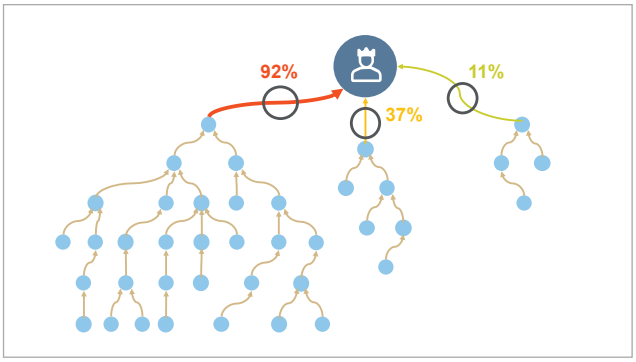

Figure 5. BloodHound Enterprise identifies the choke points that multiple attack paths have in common.

BloodHound Enterprise identifies the choke points shared by multiple attack paths, so you can block hundreds of them at one.

By mitigating a choke point, you block every attack path that relies upon it. And BloodHound Enterprise details the specific actions you need to take, such as removing a particular permission or instance of nested group membership.

Attack path monitoring

Sometimes, however, organizations cannot quickly remediate certain choke points because there's so much technical debt in their Active Directory — relationships, group memberships, permissions and so on are so complex that making changes introduces the risk of breaking things, such as a critical application that relies on a particular permission.

Therefore, it's crucial to combine the attack path management with **attack path monitoring** — continuously watching to see if any attack paths that you have yet to mitigate are being leveraged, so you can respond promptly. Quest Change Auditor and On Demand Audit complement BloodHound Enterprise by:

- Monitoring Active Directory in real time for active attacks and indicators of compromise (IOCs)
- Blocking adversaries from leveraging attack paths by preventing changes and access to critical assets, such as adding themselves to Domain Admins or another privileged groups
- Auditing security changes across your Active Directory and Azure AD environments

It's critical to continuously monitor all attack paths you have not yet been able to mitigate.

Beyond cybersecurity: cyber resiliency

Attack path management and attack path monitoring can dramatically strengthen cybersecurity. But organizations today need **cyber resiliency**, which includes both minimizing cyber risks and ensuring that they can get back up and running quickly even if disaster strikes. These Quest solutions can help:

GPOADmin

Group Policy merits special attention because GPOs can control settings across the domain and are therefore a major vector for attacks. GPOADmin® streamlines GPO management and security by helping you to:

- Ensure that proposed changes to GPOs adhere to your security policies before they are deployed
- Continually validate GPOs through automated attestation
- Quickly roll back an unapproved GPO change to an approved configuration

Recovery Manager Disaster Recovery Edition and On Demand Recovery

Recovery Manager for Active Directory and On Demand Recovery provide value in several areas. First, they facilitate choke path remediation by providing peace of mind if a change to configuration or permissions does cause issues, the IT team can immediately roll back the modification and return to a known good state.

Quest

More broadly, these solutions enable you to get your business back up and running as quickly as possible if you do suffer a successful attack or another type of disaster. They can:

- Promptly roll back changes to AD and Azure AD when remediation actions have unintended consequences
- Revert unapproved or otherwise unwanted changes to any object, including users, GPOs and AD configuration
- Quickly recover AD domains or an entire AD forest after an attack

Focus on cyber resiliency: ensuring you can get your business back up and running fast in case of a successful attack or a disaster.

Conclusion

Microsoft reports that 95 million Active Directory user accounts are under attack every day. Now you know why: By compromising an ordinary user account, an adversary is likely to be able to leverage an attack path that will get them to your Tier 0 assets in just a handful of steps, which the open-source version of BloodHound will quickly lay out for them. Fortunately, IT teams now have a solution that provides a practical way to cut off hundreds or even thousands of attack paths at once. SpecterOps BloodHound Enterprise will map out the attack paths in your AD, prioritize them according to risk and provide clear guidance on remediation.

For a robust strategy that delivers not just cyber security but cyber resiliency, be sure to complement BloodHound Enterprise with Quest Change Auditor and On Demand Audit for effective attack path monitoring, GPOADmin for streamlined Group Policy management and security, and Recovery Manager for Active Directory and On Demand Recovery for quick and reliable backup and recovery.

Schedule a free Active Directory security assessment to review your current security posture and uncover the attack paths that put your most critical assets at risk.

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 Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.