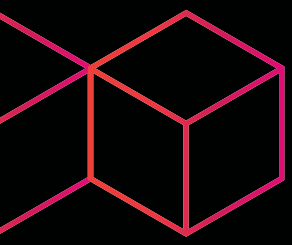
Securing Hybrid Active Directory Environments

September 30, 2021

BY DOUG DAVIS | Semperis Senior Product Manager

A practical guide to closing security gaps in Active Directory and Azure Active Directory.

Contents



Hybrid Active Directory Environments Are Under Attack

Many organizations are embracing a hybrid cloud journey—deploying the optimal mix of on-premises assets and cloud services for their needs. But with that flexibility comes complexity—especially in managing hybrid identity security in a Microsoft environment.

Securing Active Directory requires a different approach from securing Azure Active Directory: The tools, processes, and threats are distinct. Organizations struggle to effectively close security gaps in a hybrid environment—and cybercriminals are taking advantage of those vulnerabilities. Attackers are targeting hybrid Active Directory environments with increasing frequency, often using weak spots in on-premises Active Directory as an entry point, then moving to the cloud environment, as was the case in the SolarWinds attack.

"We see a lot of different challenges with protecting hybrid identity environments, starting with the basic fact that Active Directory and Azure Active Directory—outside of the name—have very few things in common," said Semperis CEO Mickey Bresman. "Azure AD provides a different stack of protocols, requiring a very different management approach—including protecting the identity system from cyberattacks. With a hybrid scenario, the potential attack surface expands for an adversary. It's a relatively common scenario to see attacks start on-prem and move to the cloud, or move from cloud to on-prem."

By understanding the fundamental differences between securing on-prem AD and Azure Active Directory, IT and security teams can close common attack vectors and strengthen their overall security posture while benefiting from the flexibility and efficiency of a hybrid AD environment.

> *With a hybrid scenario, the potential attack surface expands for an adversary.*
>
> **Mickey Bresman, Semperis CEO**

Security Risks to Watch for in Shifting to Hybrid Identity Management

It's easy to see why enterprises are gravitating toward a hybrid identity management model that promises the best of both worlds—a little bit in the cloud, and a little bit on-premises. In an Active Directory-centric environment, leveraging the cloud means integrating with Azure Active Directory.

Azure Active Directory (AAD), after all, is designed with an eye toward SaaS applications, providing single sign-on and access control. As cloud adoption increases, the ability to manage both on-premises and cloud access is becoming a business necessity. Leveraging AAD alongside Active Directory (AD) helps make hybrid identity management a reality.

As with anything in IT, however, the adage of look-before-you-leap still applies.

Monumental change with moving to the cloud

Moving any part of an IT operation to the cloud requires an adjustment. User authentication is no different. From a conceptual standpoint, organizations need to consider three critical issues.

1. A new authentication model

After 20 years of managing identity one way, adding AAD to the mix will be a critical adjustment. Going from using only on-premises AD to extending to cloud authentication requires a different mindset and approach. In AAD, there are no organizational units or forests, and no group policy objects. Concepts (and battle scars) about how to secure the identities in AD no longer apply in AAD.

> "Concepts (and battle scars) about how to secure the identities in AD **no longer apply in AAD**."

Many administrators start out believing that securing AAD is similar to securing AD, which is not the case. And you might already be using AAD without thinking much about it. If your organization is leveraging any Microsoft cloud services, such as Office 365, then AAD is already being used in the background. AAD is also leveraged heavily to connect to other non-Microsoft SaaS applications, such as Salesforce. All these factors introduce new considerations and choices. For example, should you keep AD and AAD separate or merge them using Azure AD Connect? Many new concepts need to be understood so you can make these decisions while keeping information systems secure.

2. The extension of the perimeter

Once an organization embraces the cloud, the notion of the traditional network perimeter ceases to exist. For IT administrators who have spent the last two decades running AD on-premises, this notion is a tremendous adjustment. In a hybrid identity environment, organizations now must be prepared to guard against an endless array of possible entry points.

3. Radical changes to the permission model

Moving to AAD also drastically changes the permissions model organizations need to secure. On-premises, it is fairly easy to control who has physical access to domain controllers, and overall management entry points are well-defined and documented. In a hybrid AD environment, identities are also now stored in the cloud, vulnerable to exploitation by anyone who has access to the internet. Suddenly, administrators are dealing with an inherently open model for initial access connections, which—when coupled with the larger number of services, roles, and permissions required—has a significant impact on risk.

Microsoft has actively tried to provide educational materials to prepare businesses for the changes caused by AAD adoption. However, many IT organizations are still failing to fully appreciate the implications of hybrid identity management. As more companies take a hybrid approach, attackers have expanded their modus operandi accordingly.

In September 2020, researchers at Mandiant (FireEye) noted they had seen an increase of incidents involving Microsoft 365 and Azure Active Directory, mostly tied to phishing emails attempting to entice victims into entering their Office 365 credentials into a phishing site. Mandiant researchers also observed attackers using a PowerShell module called AADInternals, which enables attackers to move from the on-premises environment to

AAD, create backdoors, steal passwords, and take other malicious actions. These threats will continue to grow with the exponential growth of interest in Azure and Office 365.

> Mandiant researchers observed attackers using a PowerShell module called AADInternals, which enables attackers to move from the on-premises environment to AAD.

Permissions, permissions, permissions

By far, of the three subjects mentioned above, the biggest security risk is caused by the changes to the permissions model. There are a huge number of services available when organizations move to a hybrid identity environment. Instead of a well-defined set of administrative groups in Active Directory, you now have roles in Azure AD, which will be unfamiliar. You can see this list of roles here. Each role has a lengthy list of assigned permissions. It is hard to understand the permissions assigned to each role just from the description, but many have a high level of access that isn't apparent.

Also, linking any SaaS service to AAD, which is probably why you added AAD to the mix, adds permission models that need to be managed. Microsoft Teams, for example, uses SharePoint integration at the back end. With the wrong configurations, adding a guest to Teams might create a situation where this new user now has access to files stored on SharePoint for Teams. Folks might not be aware that these files are now available to guest users who were added to their channel only for a quick chat. In addition, the ability to add Apps in Teams effectively extends the permission model to these third-party tools. This is just one example of the matrix of complex issues for each service managed via AAD.

In fact, keeping track of the permissions of third-party apps is critical and is an area that is undermanaged in most AAD implementations. These permission requests will trigger a one-time-only pop-up that lists the permissions the app needs. These lists can be lengthy and should be reviewed carefully before acceptance, but rarely are.

Organizations also might face these two new scenarios related to permissions that need to be understood in a security context:

- **Third-party tools that pull data from Azure AD and store it in their own database.** For example, an application registered in Azure AD that allows for a CRM system to read user profiles or has other read permissions effectively has the ability to retrieve and store data for itself. Once the data is taken from Azure AD, it sits in an external database, leaving the organization to rely on the security framework of the third-party tool.

- **Third-party tools with write access that can make changes within their tool.** In this case, the required authentication to make changes in the tenant is moved from Azure AD to whatever controls the third-party tool has. A user might be able to log into the tool without multifactor authentication because it does not support single sign-on (SSO), operating instead with the application acting as the permission proxy that does the action on their behalf without some of the checks that would normally be required.

IT organizations should strongly consider restricting who can approve applications or, at the very least, have clear guidance on what permissions should be considered appropriate. Taking a hybrid identity approach requires dealing with a much broader permission model. To do so effectively, organizations must establish strong governance of what apps are going to be turned on and what access rights they will get.

Understand the risk of hybrid identity management

Whether authentication is handled in the cloud, on-premises, or both, putting security first is always a must. While managing identity in a hybrid environment might seem as simple as joining a Windows device to AAD, failing to account for changes to the risk landscape opens the door to issues that can cause headaches in the future. Knowledge is always your first line of defense, but the amount of documentation needed to fully understand security in AAD is daunting. Native or third-party tools that automate that understanding and reduce the complexity of security will help lower security risk during and after the rollout of your hybrid environment.

The 3 Core Security Configurations You Need to Know in Azure Active Directory

To effectively secure a hybrid Active Directory environment, IT and security teams need a good understanding of Azure Active Directory (AAD) roles, applications, and multifactor authentication (MFA). After mastering these concepts, you can dig deeper into the complex task of securing a hybrid environment knowing that the core is in good shape.

Each piece of the security configuration triad represents a critical point of focus for security. But while these subjects are frequently discussed independently, they are interconnected. When effectively managed and working seamlessly together, these three configurations form the foundation of a solid hybrid AD security strategy.

What are Azure AD roles?

Azure AD is managed by two types of roles: built-in roles and custom roles. Azure AD has about 60 built-in roles, each with their own permissions. These roles are broken into three categories:

- Service-specific roles (e.g., CRM Service Administrator)
- Azure AD-specific roles (such as Application Administrator or Groups Administrator)
- Cross-service roles (such as Service Support Administrator)

Azure AD also supports the creation of custom roles that can be set with whatever permissions the administrator wants. These custom roles can then be assigned to a user by creating a role assignment that grants the user the permissions in a role definition according to its defined scope. Getting your permission model all tied up in roles can lead to security confusion, and administrators should proceed with caution.

Knowing the privileges associated with all these roles and what roles are tied to particular users is critical for security. We advocate for companies to regularly assess their on-premises AD environment for orphaned accounts, accounts with excessive privileges, and other red flags. This same diligence must be applied to the cloud environments as well. Once threat actors have breached an environment, one of their key tactics is to elevate their privileges. Monitoring role creations and modifications can alert the organization to a possible attack. Most of these changes, when investigated, will likely turn out to be legitimate. However, any unauthorized alteration of roles or privileges will be caught as well.

MFA prevents an estimated 99% of account compromises. Unfortunately, MFA is often not fully implemented.

MFA provides a strong defense

In a certain light, MFA can be seen as an early warning system. Suppose an attacker steals a user's credentials and attempts to log into their account. In that case, the second factor effectively stops threat actors in their tracks and alerts the organization to the attack. MFA prevents an estimated 99% of account compromises. Unfortunately, MFA is often not fully implemented. It is not uncommon for privileged accounts to be protected via MFA while others are not.

In other situations, all privileged accounts might have MFA except for one, which is given a Temporary Access Pass. This type of fragmented approach to MFA opens potential security holes for attackers to exploit by making it easier for threat actors armed with stolen or compromised credentials to slip by undetected.

Microsoft partially enables MFA automatically through Security Defaults. These defaults are:

- Requiring all users to register for Azure AD Multi-Factor Authentication
- Requiring administrators to perform MFA
- Blocking legacy authentication protocols
- Requiring users to perform MFA when necessary
- Protecting privileged activities like access to the Azure portal

Security Defaults can be turned on in the Azure portal. If your tenant was created on or after Oct. 22, 2019, Security Defaults might already be enabled. The goal of the defaults is to help organizations that are just beginning to understand their security needs. It's important to remember, however, that the default security settings will only force the following nine Azure AD administrator roles to perform additional authentication every time they log in:

- Global administrator
- SharePoint administrator
- Exchange administrator
- Conditional Access administrator
- Security administrator
- Helpdesk administrator
- Billing administrator
- User administrator
- Authentication administrator

Other users will only be prompted to authenticate with an additional method under certain circumstances, such as using a new device or performing certain tasks. The Security Defaults also block legacy authentication methods, which account for many of the compromised login attempts organizations face. Since older protocols might bypass MFA, shutting them down as an attack vector is a vital part of securing Azure AD.

Any indication that MFA has been circumvented—such as users being unregistered—should trigger an investigation.

Securing applications in Azure Active Directory

A new concept for Active Directory administrators is the importance of registering applications within Azure AD, which is a new level of access for users both within and outside of the AAD perimeter. Applications are common to extend your Azure Active Directory to other services, especially SaaS services. Security Defaults will also require users to authenticate via MFA when they log in via these new applications. However, MFA is not a cure-all for security.

While MFA can limit the effectiveness of stolen credentials, controlling the risk posed by third-party applications is not just about password protection.

Consider this scenario: an attacker targeting an organization's Azure AD tenant decides that instead of tricking a victim into giving up their password, they will instead attempt to trick them into installing malicious applications. If they are successful, the user will grant the threat actor the keys to the kingdom—giving them access and control over the user's account. If the user is moving quickly, they might not fully consider the rights the application is being provided. Application Registrations need to be reviewed and Self-Service Application assignment should be considered only if you feel fully comfortable with your end users recommending applications for use. In most cases there should be a formal process for application requests.

Many organizations might not think about applications as an attack vector, and this tactic is more difficult to detect because there is no malicious code executing on the user's endpoint. It simply relies on social engineering and abuses trust. With the ever-growing number of cloud applications in use in today's enterprises, you can close the door on these types of attacks by reviewing the list of applications. (Click the "Enterprise Applications" option under the "Manage" section in the Azure portal.) You can also monitor the consent events in Azure AD to see if unauthorized applications have been granted rights they should not have.

Take a holistic view of hybrid AD security

When thinking about security in the cloud, IT leaders should take a step back and view it holistically. One layer of protection should reinforce every other layer. Effective role assignment limits the damage attackers can do if they trick a user into enabling a malicious application. Having the ability to enforce MFA can prevent a third party from using the application to circumvent access controls. If the fabric of your organization's approach to security is woven together carefully, you can substantially reduce your risk exposure.

"Many **organizations might not think about applications as an attack vector**, and this tactic is more difficult to detect because there is no malicious code executing on the user's endpoint. It simply relies on social engineering and abuses trust."

Time to Leave ADFS Behind for Authenticating in Hybrid AD Environments?

One of the biggest challenges of adopting cloud services is extending identity policies from the on-premises environment into the cloud. In an Active Directory (AD) environment, it might be tempting to turn to Active Directory Federation Services (ADFS), which has long been the answer for providing single sign-on capabilities to allow users to authenticate and access applications that otherwise would not be available to them using only Active Directory, such as Azure and Microsoft 365.

> "As was demonstrated in the SolarWinds supply chain attack, a vulnerability in the on-premises environment can **ultimately lead to the compromise of the Azure AD tenant**."

However, as threat actors continue to target cloud environments, it is fair to examine whether ADFS is the best solution for organizations embracing hybrid environments. While ADFS is not inherently unsecure, the complexity of implementing it properly leaves it susceptible to attackers. As was demonstrated in the SolarWinds supply chain attack, a vulnerability in the on-premises environment can ultimately lead to the compromise of the Azure AD tenant. In addition to being another set of physical servers to manage, ADFS servers also expand the attack surface businesses need to protect.

Even Microsoft has recommended organizations consider migrating away from ADFS, noting in a January 2021 blog post: "If you want to extend MFA and Conditional Access to legacy on-premises apps, including header-based apps, use Azure AD Application Proxy or an integrated solution from one of our secure hybrid access partners. With our migration tools, you can modernize authentication of all apps and retire your ADFS implementation. This will help prevent attacks that are particularly difficult to detect in on-premises identity systems."

A world without ADFS

To help organizations connect all their apps to Azure AD, Microsoft introduced Password Hash Synchronization (PHS) and Pass-through Authentication (PTA). Using Password Hash Synchronization, Active Directory administrators can synchronize a hash of a user's on-premises AD password hash to Azure AD. In effect, this allows users to leverage services like Microsoft 365 using the same password they would for their on-premises AD account.

The second method of managed authentication for Azure AD is Pass-through Authentication, which validates users' passwords against the organization's on-premises Active Directory. It uses authentication agents in the on-premises environment. These agents listen for password validation requests sent from Azure AD and do not require any inbound ports to be exposed to the internet to function. Passwords do not have to be present in Azure AD in any form, eliminating a potential attack vector. In addition, on-premises policies such as account expiration or log-on hour restrictions can be applied to accounts. As a pre-requisite for Pass-through Authentication to work, users need to be provisioned into Azure AD from on-premises Active Directory using Azure AD Connect.

While there are still use cases where it might make sense to maintain an ADFS deployment—such as using ADFS for user certificate authentication—for many organizations, the case to move away from ADFS is strong. By using PHS and PTA, organizations can reduce the number of passwords users have to remember. However, that is only one of the benefits that can come from migration. ADFS is complex to deploy and requires physical hardware that must be maintained. If an ADFS server is not kept current with the latest patches, it is vulnerable to attacks. PHS, on the other hand, is maintained by Microsoft, and using it decreases the infrastructure organizations need to protect.

If you are at the beginning of your hybrid journey, ADFS should not be your first option for linking the authentication between the on-premises and online workloads. However, if you have deployed ADFS, you're looking at a migration, which still provides enhanced security over ADFS.

Changing authentication methods, however, is no trivial task and requires significant planning and testing. Any migration away from ADFS should occur in stages to allow for sufficient testing and potential downtime. At a minimum, organizations should be running Azure AD Connect 1.1.819.0 to successfully perform the steps to migrate to password hash synchronization. The method for switching to PHS depends on how ADFS was originally configured. If ADFS was configured via Azure AD Connect, then the Azure AD Connect wizard must be used. In this situation, Azure AD Connect automatically runs the Set-MsolDomainAuthentication cmdlet and automatically unfederates all the verified federated domains in the Azure AD tenant.

If an organization did not originally configure ADFS by using Azure AD Connect, it can use Azure AD Connect with PowerShell to migrate to PHS. However, the AD administrator must still change the user sign-in method via the Azure AD Connect wizard. The AD Connect wizard will not automatically run the Set-MsolDomainAuthentication cmdlet, leaving the administrator with full control over what domains are converted and in what order.

Decreasing the Azure AD attack surface

For businesses with hybrid environments, connecting all applications to Azure AD reduces complexity and offers an opportunity to decrease the attack surface. As a side benefit, it also has the potential to improve the user experience by implementing single-sign-on as well as stringent account security controls. As organizations adopt hybrid identity approaches to support their cloud initiatives, they should take the time to examine whether ADFS best suits their needs.

For businesses with hybrid environments, connecting all applications to Azure AD reduces complexity and offers an opportunity to ***decrease the attack surface***.

— Doug Davis, Senior Product Manager at *Semperis*

ABOUT THE AUTHOR

Doug Davis, Senior Product Manager at Semperis, has been immersed in the Microsoft ecosystem for more than 20 years working on delivering migration, management, and analytics products that help customers understand, secure, and enhance their investment in Server, Office, and related products.

semperis

semperis.com