Whitepaper

Mobile Workforce and Modern Authentications: Challenges and Considerations

by **Subhra Shankar Banerjee**

LTIMindtree

Contents

Abstract

In the world of Windows Active Directory (AD), thousands of users use laptops and desktops to access their applications, with their password being the primary guardian of their data. Kerberos has been a core engine in this world, providing a distributed authentication service that allows a device run by a user to prove its identity to a server, without sending data across the network that might allow an attacker to intercept the traffic. Kerberos authentication has been used by applications around the world for almost two decades now, and it continues to dominate even today. Kerberos authentication is based on a triangular relationship between users, computers, and resources where a security chain is formed. Users would typically connect their system to the LAN cable and operate from the office with application servers in the direct vicinity of the domain controllers. In such a scenario the Kerberos authentication is easy to achieve. Also, timestamps play a crucial role in Kerberos authentication, where the machines need to be in a time skew window of resources to make it happen.

However, there are several challenges involved in terms of usability across different platforms and different devices. In today's digital world, there is a rising demand for ubiquitous access to organizational data from multiple devices that could be located anywhere, but without compromising integrity. In this scenario, Kerberos authentication is hard to achieve as applications/data need to be accessed from devices that are not even connected to enterprise network. That's where Modern Authentication technology plays a vital role.

Re-inventing Legacy Authentication

Modern authentication has been designed to address challenges that held back traditional authentication from performing optimally and delivering a good user experience. It allows documents and information to be shared or accessed across any device, without the device being part of the AD domain, while maintaining the integrity of the document. We can use Multifactor Authentication (MFA), which is becoming the default authentication method today, with a Compound Annual Growth Rate (CAGR) of 15.52%, to provide security, flexibility, and ease of access. Modern authentication is a decided step away from a world where we depended on what we know, i.e., passwords, to a world with what we have (MFA with a device which user owns etc.)

In modern authentication, there is no restriction that the computers and users need to be a part of the same domain. The authentication is not tied to a computer from where it is accessed but to the user identity, which means that the system can be a member of any domain or workgroup, with the following conditions:

- **Reliable internet connections.**
- **Web URL to access the application(s).**
- **Password to access the application(s).**
- **Device for second factor if enabled.**
- **Optional VPN connections.**

Application access is not affected by the source device from where a user is logging in, opening a plethora of options for application access. The user can work from anywhere while maintaining compliance. Recently, conditional access policies have also stormed the market, providing IT admins the ability to control data access based on the user's location.

One important thing to consider is whether all applications need to be accessed remotely from outside the corporate network or not. This decision is generally driven by business demand and ease of doing transactions on a day-to-day basis. There are certain applications that need very high security and control and should only be accessible from the machine which is connected to corporate LAN. Even the authentication is local to a specific resource domain and does not follow user domain. Also, certain applications have their own identity databases, which are purely internal. These applications are not fit for modern authentication unless there is a change in corporate policy or application coding.

Azure AD as Modern Authentication

Microsoft revolutionized the Windows server market with Active Directory in Windows 2000. History is in the making again with Azure AD, which is one of the backend infrastructures for modern authentication. Many major vendors are now supporting their products with Azure AD, and several organizations have already begun moving their AD to Azure. It does not work on Kerberos and only relies on user accounts and MFA for authentications. If the application is integrated with Azure AD, users can access the applications from anywhere using Azure AD credentials, as it is purely Internet-based and is backed by Microsoft Azure's high-security datacenter. It can co-exist with the on-premise AD and can perform at par with AD authentication. A VPN connection (optional) is not required for connecting to applications which are integrated with Azure AD. With features like conditional access, identity/password protection, self-service password reset option, MFA, enterprise-grade reporting, and tracking/logging backed by an SLA of 99.9%, Azure AD has become the authentication method of choice.

However, this transformation to Azure AD as a mainstream authentication platform is not very easy to achieve and involves several considerations and coordination across the enterprise application and infrastructure team.

Let's look at the key factors that help an enterprise in its transformation journey:

Password Hash Sync or Federated

Azure AD provides the option of syncing on-premise AD password (double-hashed password, not the actual password) to Azure AD. As per MSFT, this is the recommended approach, as it helps organizations keep their passwords more secure. This option also provides a significant advantage by granting access to Microsoft-released reports such as leaked credential reports, password expiration policies etc. If you are still concerned about password security in a public cloud, such as if you are working in BFSI domain, it is better to go with a federated domain or passthrough authentications. There is an excellent article from MSFT, which explains this in detail.

Hybrid Azure AD Join, or Only Azure AD Joined Device

Azure AD joined devices are those which are joined to only Azure and not the on-premise AD. Thus, it becomes a company-owned mobile device. Hybrid Azure AD joined devices are those that are joined to Azure AD as well as the on-premise AD.

To make it simple, let us consider the following scenarios for an organization:

- A major chunk of users rarely come to office or do not have access to standard corporate network.
- There are many field workers who work mostly remotely and do not prefer to come to office.
- Most applications in the enterprise are SaaS applications, which is dependent on SAML token.
- There are no specific or very less dependencies on a traditional server, like file server integration with specific applications.
- Security tools in the enterprise are well equipped to support mobile devices.

If your answer is yes to most or all of these scenarios, then Azure AD joined machines are the best option for your organization.

However, **machines that are joined to Azure AD only are all workgroup machines from AD standpoint**, hence:

- The logic of Kerberos authentication does not hold true anymore. We need an alternative solution or compatible solution with all applications.
- Applications that are tightly integrated with on-premise AD and dependent on Kerberos authentications will need to find an alternative mechanism to authenticate, for example, certificate-based authentication.
- If the application is web-based and not a thick client, we can leverage Azure AD Application proxy for integrating the on-premise applications with Azure AD authentications.

Now consider the following scenarios:

- Users are present occasionally in the office in a round turn (WFH + WFO).
- There is an on-premise file server on which critical applications are dependent.
- There are restrictions on certain applications, which need to be accessible only from the office network.
- You can leverage AADCONNECT with no other sync tool in place.

If most or all of the above points hold true for you, it is best to go with a Hybrid Azure AD join device, where we have the advantage that all devices will be AD domain-joined, and we can enjoy the benefits of both worlds.

Modern Authentication Adoption Considerations

This section details the adoption considerations of Azure AD based authentication from on-premise AD authentications.

Device management: SCCM + Intune or Only Intune

We need to find a mechanism to manage the devices that are Azure AD and Hybrid Azure AD joined. Intune is the answer. It is already being used worldwide to manage mobile devices with the latest functionalities and can be used to manage the laptop/desktops in the enterprise even if they are domain-joined. With features like Autopilot, i.e. a collection of technologies used to set up and pre-configure new devices and prepare them for use in a shorter span of time, device management has been simplified. It comes packaged with Out Of Box Experience (OOBE) and requires no IT support personnel to provision the device before handing over to the end-user. White gloves support (where branch office IT support personnel prepare the device before shipping it to the end user with OOBE in user absence) enhances the user experience because they get new devices loaded with all applications. Intune provides all the functionalities of device tracking and actions like remote wipe, in case of lost devices, along with application packaging.

However, Intune lacks certain features, like software metering and server management. If the existing SCCM infrastructure is using these features, we need to go with a solution that combines SCCM and Intune to provide an additional advantage because we can use SCCM for managing devices that are entirely on-premise, like desktop/servers etc., and Intune to manage mobile devices.

Identity Sync Mechanism: On-premise to Cloud

AADCONNECT has become a default tool nowadays to sync on-premise AD to Azure AD. Syncing of computer accounts like laptops and desktops to Azure AD from on-premise AD is a must for a hybrid Azure AD joined environment. Tools like OKTA have the capability of syncing users and groups from on-premise to Azure AD but lack the features of device sync, which is done by Azure AD connect. Now, there is a hard restriction on Azure AD that two sync engines like OKTA and AAD CONNECT cannot work together for the same tenant of Azure AD. Hence, it is best recommended to use AADCONNECT for synching users, devices, and computer accounts to Azure AD. Also, we need to consider that migration of sync engine from tools like OKTA to AADCONNECT is a big-bang cutover migration where sync needs to be stopped for all users in OKTA and enabled for all users in AADCONNECT.

VPN and NAC Authentications

We need to clearly articulate the authentication mechanism of VPN and NAC devices, especially when deciding whether we are going to have both device and user authentications, or user authentications alone. This is important in an Azure AD joined device scenario, as the machine account does not exist in on-premise AD. Hence, Kerberos authentication is impossible to achieve. Certificate-based authentication can be an alternate mechanism to this problem, but we need to have CSR generated for devices and users individually. We have an alternate solution of using Microsoft PKI with Network Device Enrollment Service (NDES) for issuing certificate to end machines. But this is a complex process and needs much more planning for deployment. If we want to go with Hybrid Azure AD joined devices, then user and device authentication is easily achieved as we have the benefit of both Kerberos authentications and Azure AD authentication.

Migration Across Forest

Enterprises go through multiple changes, sometimes internal like a re-organization, or external like a merger and de-merger. AD migration is very common in this scenario. When there is a need to move resources from one AD forest to another, SID history in migration has been a problem solver for many scenarios during the migration co-existence phase. Now, one part of this process is user profile data re-permission. For Azure AD joined devices, user data is mostly stored in OneDrive. Also, email and file server data is stored in SharePoint. Thus, tenant-to-tenant migration of user data is critical here. There are tools like Bit Titan, Quest, and Binary Tree which can be used for this migration. For Hybrid Azure AD joined devices, re-permission is the same process as traditional domain-joined machines. We can leverage the same set of tools as mentioned above for this re-permission of profiles and file servers.

Time Sync

We know that erstwhile Windows systems would obtain the time from domain controllers that in turn obtain it from the standard time server of the organization. But in Azure AD joined machines, there is no domain controller to sync time. We can re-target all the machines to time.windows.com and let the domain controllers sync time from another time source. But there can be a delay of some seconds between the devices and application servers, and this delay cannot be accurately accounted for. If the internal time server is reachable from outside, we can point all the laptops to those time servers as well.

However, this becomes a critical point when we integrate all the logs from different sources with any log's analytics tools. The more the time difference between different devices, the more challenging it will be for various tools to determine and forecast any threats. Hence, proper planning of a time server is critical in this scenario.

Local Admin Group Membership

By default, on domain-joined machines, domain admins are added to local admin groups in client machines, and any other groups can be added to local admin using GPO to client machines. In the world of Azure AD joined machines, the Azure AD global administrator roles and the Azure AD device administrator roles are added to local admin when managed through Intune. However, we don't have the privilege of adding any custom group to the local admin group. Hence, departmental/ location-based grouping of machines and adding specific local IT support group is not supported as of now. In situations where a local IT support is critical to run the business, Hybrid Azure AD joined devices is a better option.

Group Policy Processing and Control

In the world of AD joined machines, Group Policy Processing (GPP) has always played a crucial role in terms of maintaining security and providing control. In large enterprises, it is very easy to find hundreds of GPO settings getting processed for machines that are joined to domain. This not only provides control but also helps in pushing many registries, files, etc. to devices, and facilitates the application installations and provides a working environment for those applications. This does not change in the world of Hybrid Azure AD joined devices because GPO gets processed easily as machines are joined to domains.

Now, we enter the world of Azure AD joined machines that are in a work group where there is no GPO processing for end devices. The closest alternative is to push maximum settings through Intune policies. However, there are limitations to it. Through ADMX and CSP, we can push machine settings to mobile devices. However, it is yet to mature and come to a point where the Configuration Service Provider (CSP) becomes a complete replacement of GPO.

Microsoft has come up with a new tool for GPO assessment to decide which GPO can be completely migrated to Intune and which cannot be replaced with Intune. If nothing works out, we ultimately fall back on PowerShell script for accomplishing our task. There are third-party tools in the market like PolicyPak that can be considered in this regard.

File server

File Server has always been a critical part of enterprise architecture. Technologies have evolved around it with Distributed File System (DFS), DFS Replications (DFS-R) and, storage technologies like Network Attached Storage (NAS), Storage Area Network (SAN) and other third-party replication software like Doubletake taking its share in the market. Also, we have technologies that sync data to cloud with data tiering like Azure Files, Panzura, etc. However, files and folder shares are still used by many enterprises today irrespective of the backend technologies mentioned above.

In traditional scenarios where machines are joined to the AD or Hybrid joined Azure AD devices, these shares are mapped using SMB/script (pushed through GPO/GPPs) related technologies with near perfect working conditions. In case of Azure AD joined devices, we can still leverage SMB shares and script after connecting to the corporate VPN. However, we need to understand that the DFS namespace that has been used since ages cannot be used from Azure AD joined machines as they are in a workgroup.

Understanding this challenge and to reduce the data maintenance cost of enterprise, many organizations have started migration of home folders to ODFB (One Drive for Business). File Server to SharePoint migration is another migration which needs to be seriously considered when moving to modern authentication and management as SharePoint suits the purpose of Hybrid Azure AD joined devices and Azure AD joined devices. However, the ODFB client tool has some limitations and does not support non-persistent VDI. But still, SharePoint + ODFB is a step into a new world of digitization, and there will be more improvements in the near future.

Authentication in Printing

In a domain-joined infrastructure, printers are mapped using GPO and script, which allows us to print without issues. In secure printing, a printing job is stored in the server and is processed only when an access card or authentication is entered on the printer/MFD. However, for devices where all devices are Azure AD joined, there is no GPO to map printers. For instance, if an employee from a different location wanted to print something in a branch office he's visiting, he will need to map the printer manually using the local IP. To prevent such hassles, cloud printing solutions and mobile printing solutions like SafeQ/PrinterLogic work best as they also support bring-your-own-device (BYOD) scenarios. In the recent development, Microsoft has released O365 cloud print solution in private preview intended to replace on-premise print servers.

Database Access for Applications

In three-tier applications, the user performs all the data entry using a front-end applications page which is connected to a middle tier, which is responsible for all operations in the database. However, there are still several critical applications which have never been updated for years and have old architecture where the front-end of the application directly interacts with the SQL database using ODBC drivers. These applications can make or break the entire migration. It's a technical limitation in MS SQL that users cannot perform integrated AD authentication for the SQL database, nor can they perform read/write operation from a device not joined to domain. This poses a significant challenge for Azure AD joined devices. In this scenario, there are three options:

- Change the applications to make them three-tier.
- Migrate the SQL database from on-premise SQL to Azure SQL.
- Access the application from WIN10 VDI solutions like Windows Virtual Desktop or Citrix.

Device Shipment and Provisioning

In the traditional world, user devices are formatted with a new OS image during an OS migration. The end user of a computer system needs to coordinate with local IT vendors to get their system re-imaged as per the standards of the new environment, because it is impossible to perform these tasks in remote access scenarios. However, with a growing number of users sourcing their computers directly from the factory, there is a rising demand for remote re-imaging. That's where the Intune cloud with AutoPilot Deployment comes into the picture. There are two types of devices, as explained below, when it comes to cloud connectivity:

- Azure AD joined devices are those which are joined to only Azure and not On-Premise AD. Thus, it became a company-owned mobile device.
- Hybrid Azure AD joined devices are those which are joined to Azure AD as well as on-premise AD.

Limitations: Hybrid Azure AD join devices need direct connectivity to domain controllers when it is provisioned. Hybrid Azure AD join is not supported over VPN as of now.

Hybrid Azure AD join devices are ideal for situations where users are primarily present on-premise and their devices can be managed by Intune or a combination of Intune and SCCM. However, there is a technology constraint to this. We cannot provision Hybrid Azure AD join devices from locations outside corporate network. Hence, for remote users, it is impossible to provide a Hybrid Azure AD joined device unless we cache the user password (which is a security risk) before shipping the device to the end user. The remote user will need to visit the office when he gets the new laptop. In this scenario, it is best to use an Azure AD joined laptop which is not joined to on-premise AD.

Are We Ready for Modern Authentication?

Security readiness

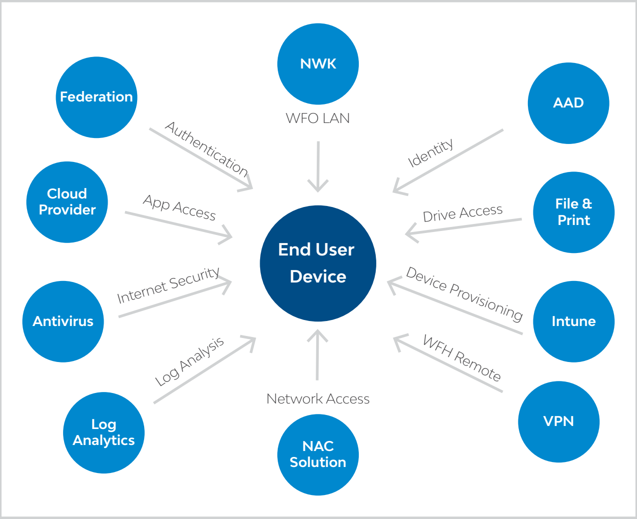
The existing security solution in the enterprise should be able to adapt to the changes that modern authentications bring. Tools like Cisco ISE have released integration with Intune, while most SIEM tools in the market are adaptive to cloud events and analytics. Application Security is another area where we need to focus, as insecure data storage and insufficient encryption methods make applications vulnerable.

Device readiness

End-user devices need to be ready for this new world of modern authentication. Autopilot is only supported for major vendors like Lenovo, HP, Dell, etc.. The vendor market and Microsoft need to work together to get themselves into autopilot. However, every hardware vendor could have a different way to handle Autopilot, which needs to be understood before devices are shipped.

Application readiness

If applications need to be prepared for modern authentication, additional time needs to be estimated for research and design, so that end coders and applications owners have enough time to adapt to the change. There could also be some applications that don't even have a source code. In such cases, the only option is to find a replacement for each such application.



System Context Diagram: Modern Device Management and Authentication

Conclusion

Modern authentication is gaining traction rapidly in several industries. Even large enterprises have started migrating their applications from think to a modern web-based application with a single identity source. Azure AD joined devices have become critical because they offer a lot of flexibility in terms of provisioning and usability for end users. However, we need to perform a total assessment of the application landscape of the enterprise before moving to Azure AD or modern authentications. It is recommended to upgrade the application to the newest version before migrating to modern authentication.

It is never easy to upgrade the application or the database. Sometimes, getting hold of the coders of the applications is difficult as well. Migration is a continuous process which happens over a time period. We also need to understand that any application which will be introduced in the environment will require flexibility and agility in order to move to modern authentication methods.

References

- https://www.ysoft.com/en/products/enterprise-workflow-platform/print-management/ysoft-safeq-print-management-suite
- https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises
- https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
- https://www.policypak.com/
- https://panzura.com/
- https://docs.microsoft.com/en-us/intune/enrollment/windows-enroll

Author

Subhra Shankar Banerjee

Digital Workplace Architect, LTIMindtree

With more than 13 years of overall IT experience in design, consulting, implementation, maintenance and management of IT infrastructure, Subhra works as a Solution Architect with LTIMindtree, providing consultancy and design solutions for Microsoft technologies. Specialized in Active Directory, Subhra is responsible to drive RFP/RFQ/RFI to build comprehensive Modern Workplace solution response.