PASS THE WHAT NOW?

UNDERSTANDING CREDENTIAL ATTACKS IN A WINDOWS 11 WORLD

OVERVIEW

- Authentication and authorization
- Legacy Windows protocols
- Attacks against legacy protocols
- “Modern authentication” protocols
- How the new stuff relates to the old
- Attacks against the new stuff
- What we can do to protect our networks

AUTHENTICATION VS AUTHORIZATION

- Authentication is the process of proving your identity

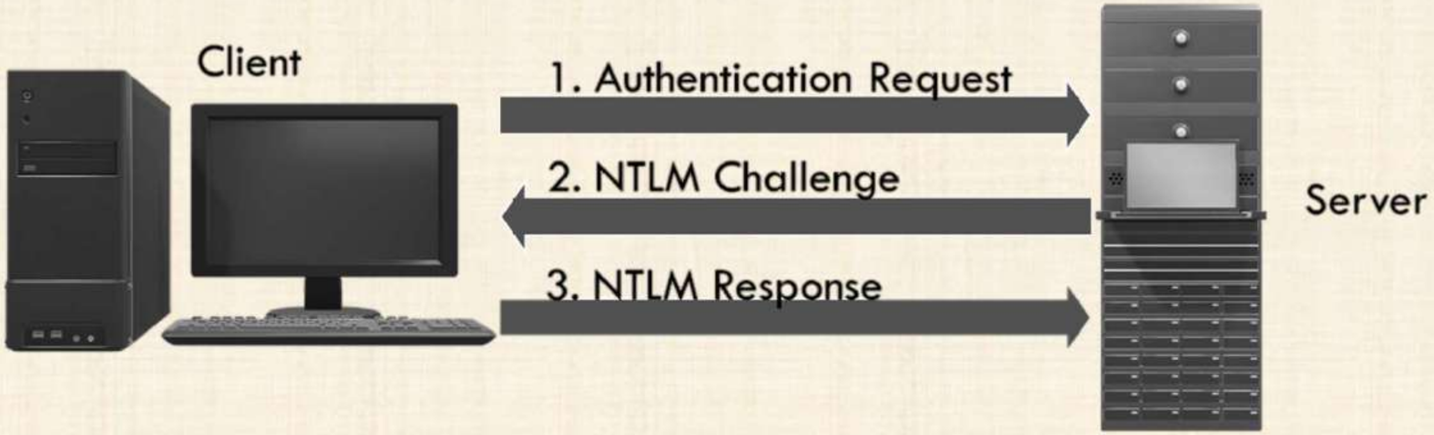
AUTHENTICATION VS AUTHORIZATION

- Authorization is being granted access to a resource

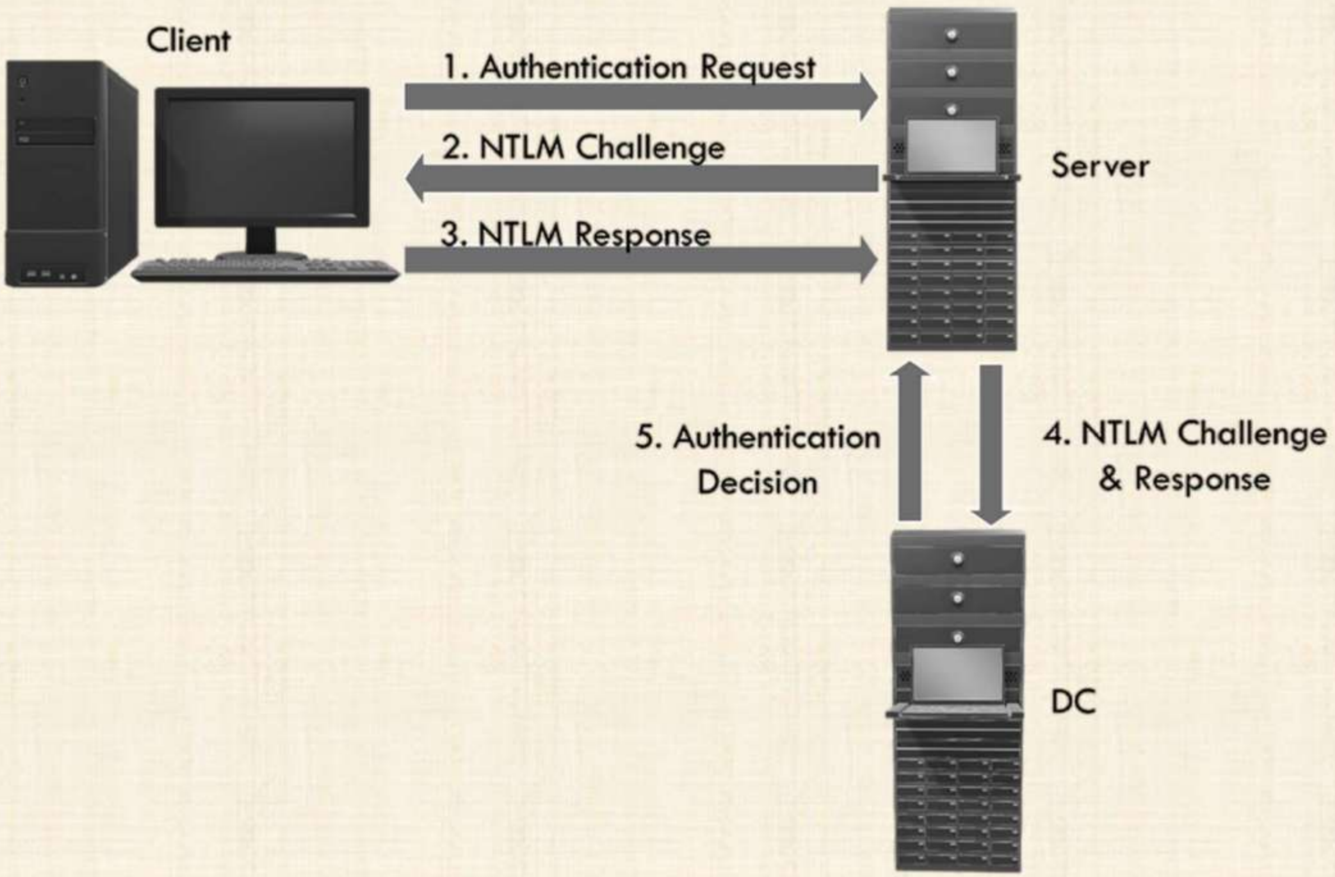
PASSWORD HASHES

- Username and password/passphrase are used to prove identity
- Passwords are not stored in plain text, but as a hashed representation of the password
- Local accounts stored in Security and Accounts Manager registry hive
- Domain accounts stored in NTDS.dit on Domain Controller
- Stored in Local Security Authority Subsystem Service (LSASS) process memory during interactive logon

NTLMV2 CHALLENGE RESPONSE AUTHENTICATION PROTOCOL



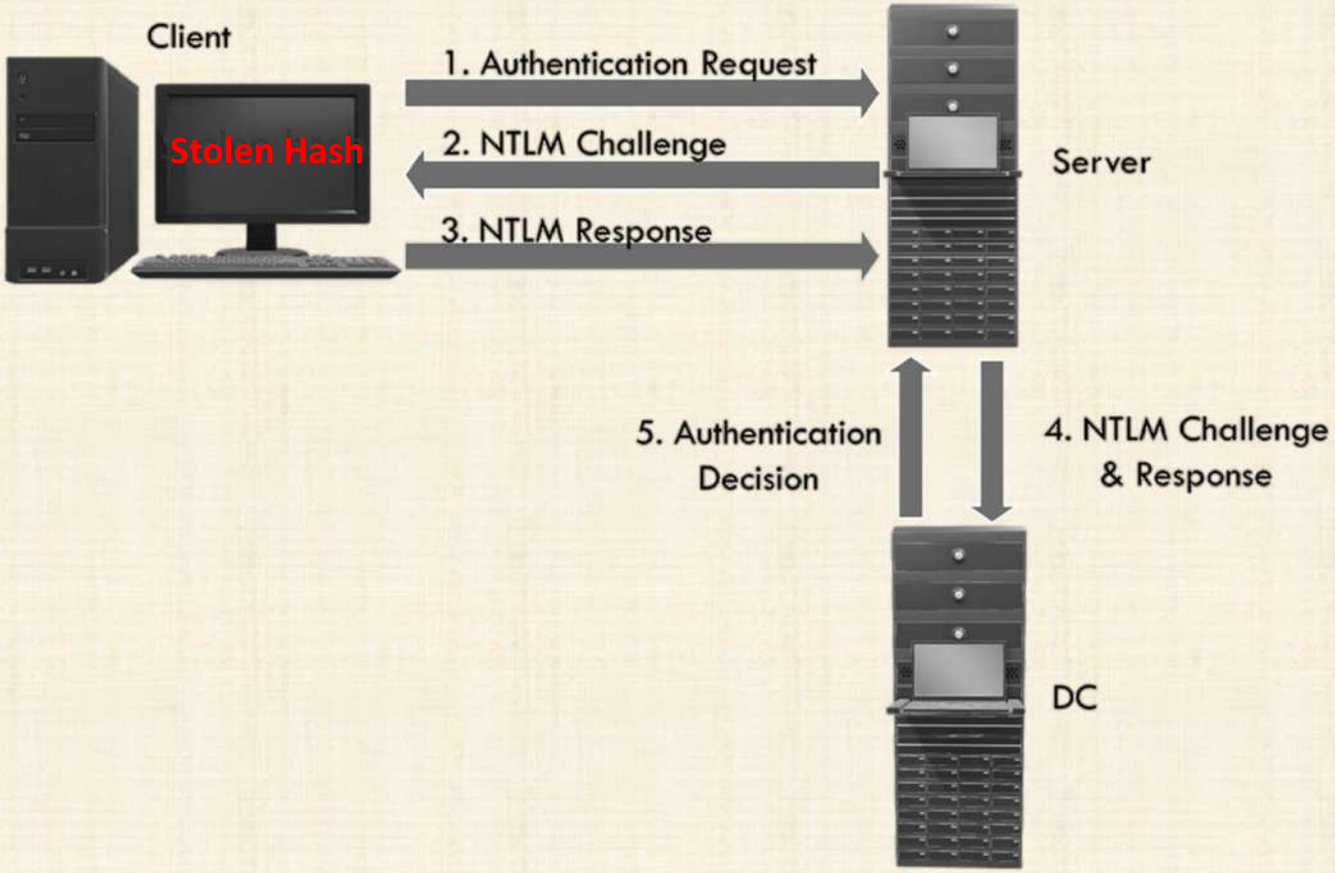
NTLMV2 (DOMAIN)


Client
1. Authentication Request
2. NTLM Challenge
3. NTLM Response
Server
5. Authentication Decision
4. NTLM Challenge & Response
DC

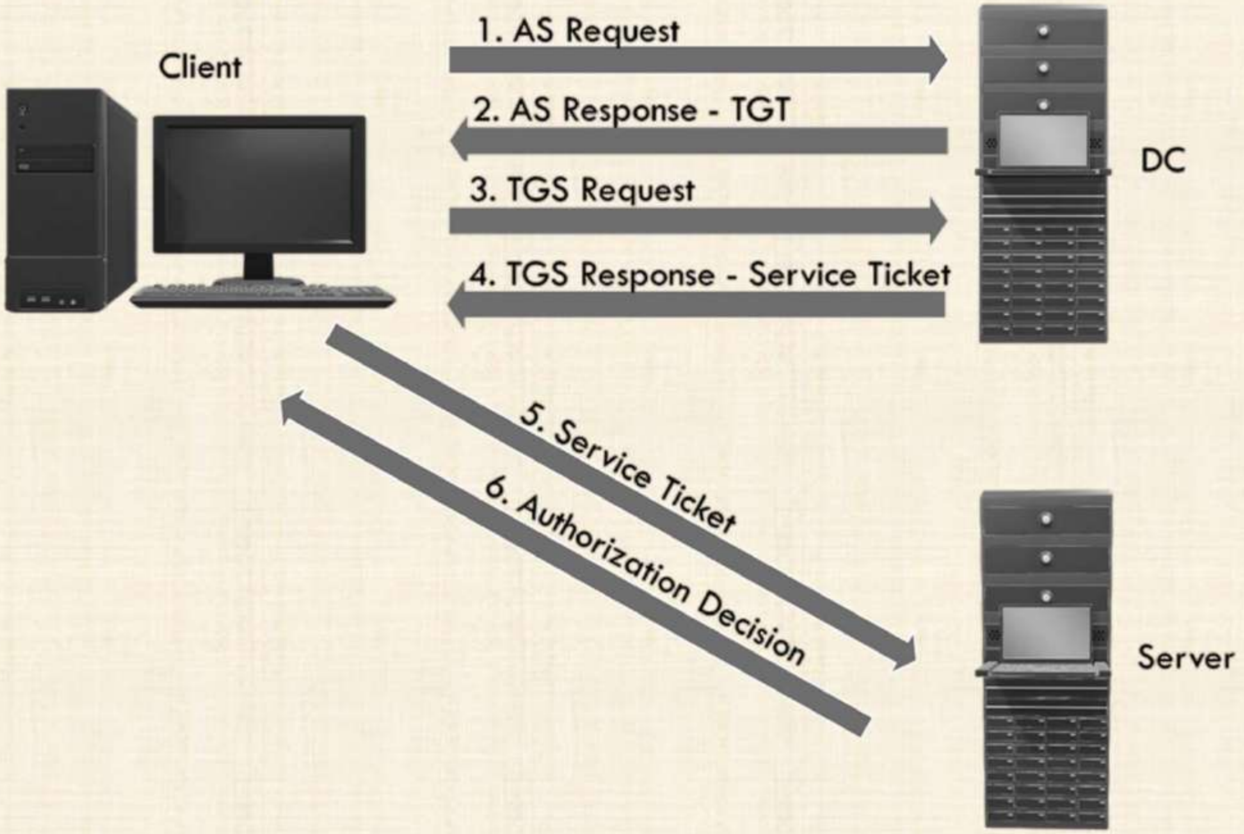
PASS THE HASH

But if an attacker can steal the hash…

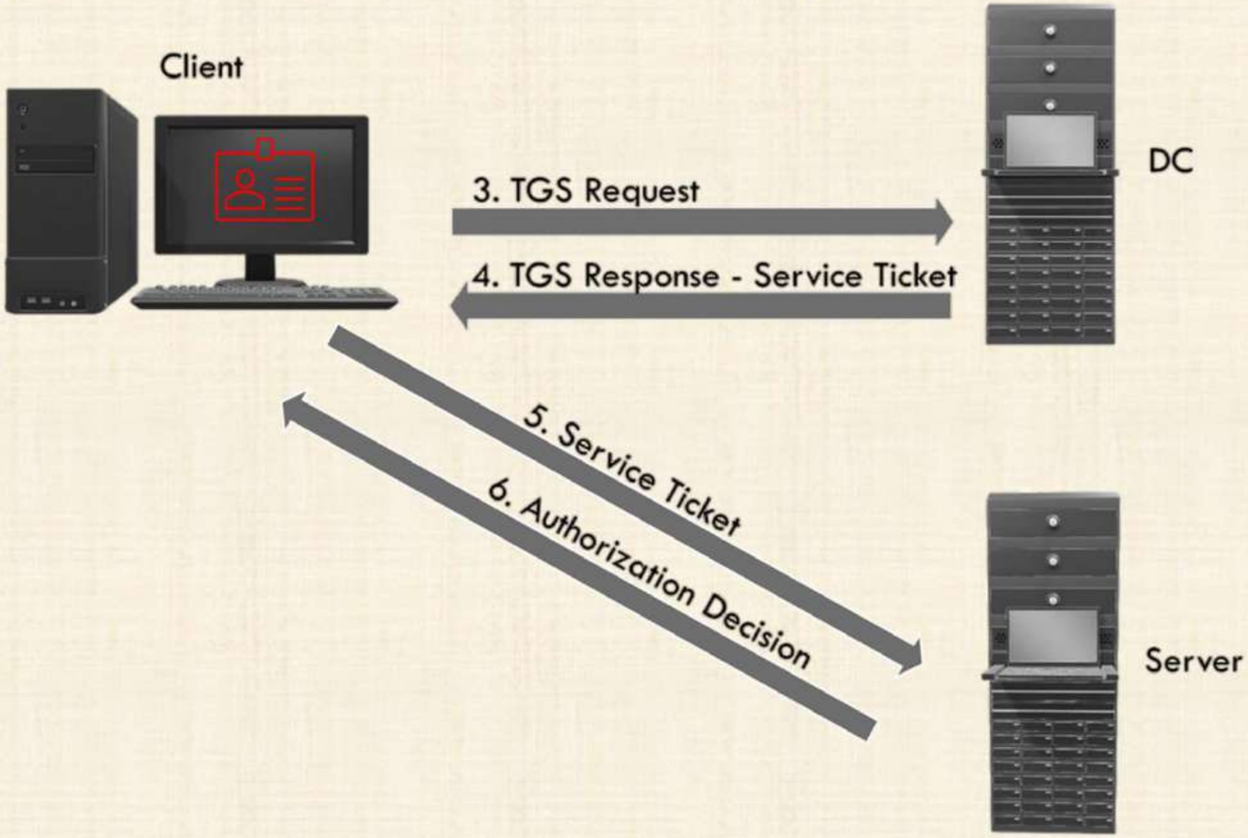
PASS THE HASH (DOMAIN)


Client
Stolen Hash
1. Authentication Request
2. NTLM Challenge
3. NTLM Response
Server
5. Authentication Decision
4. NTLM Challenge & Response
DC

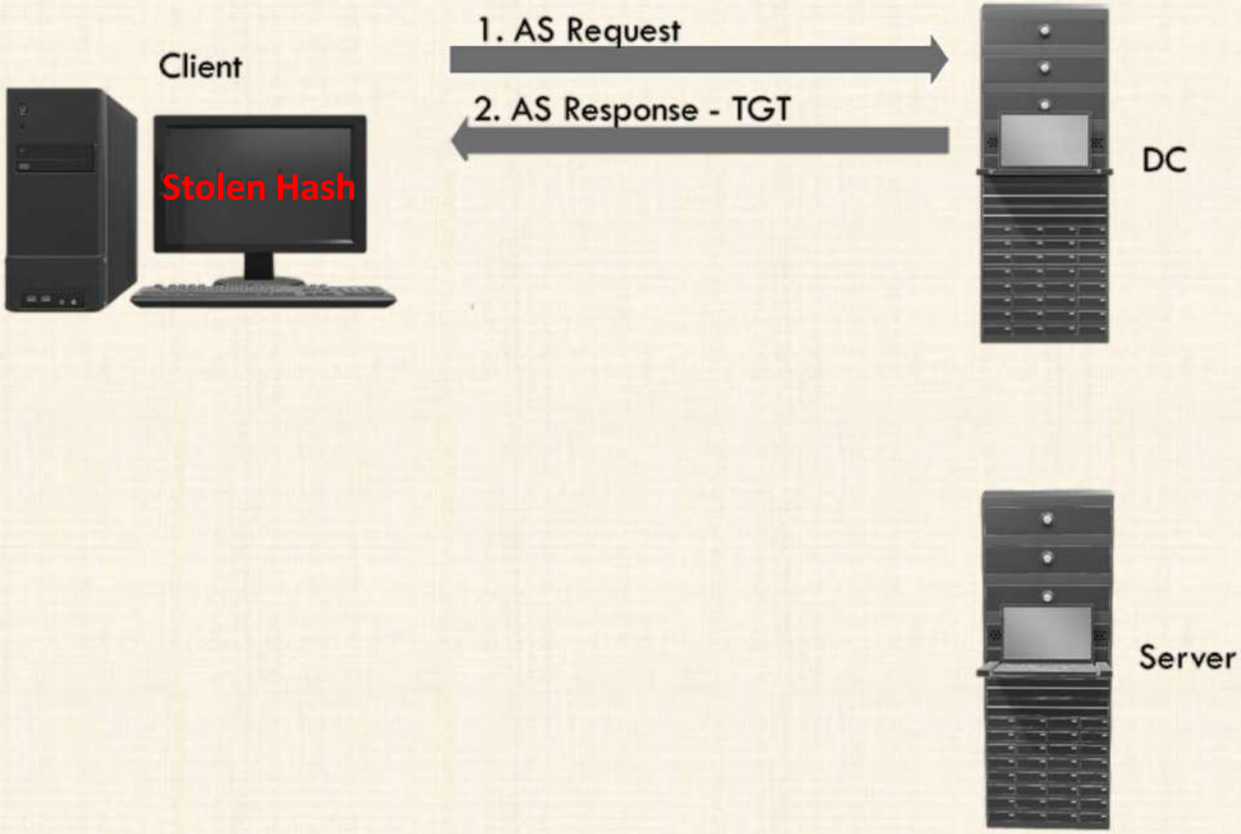
KERBEROS: AUTHORIZATION TO RESOURCE



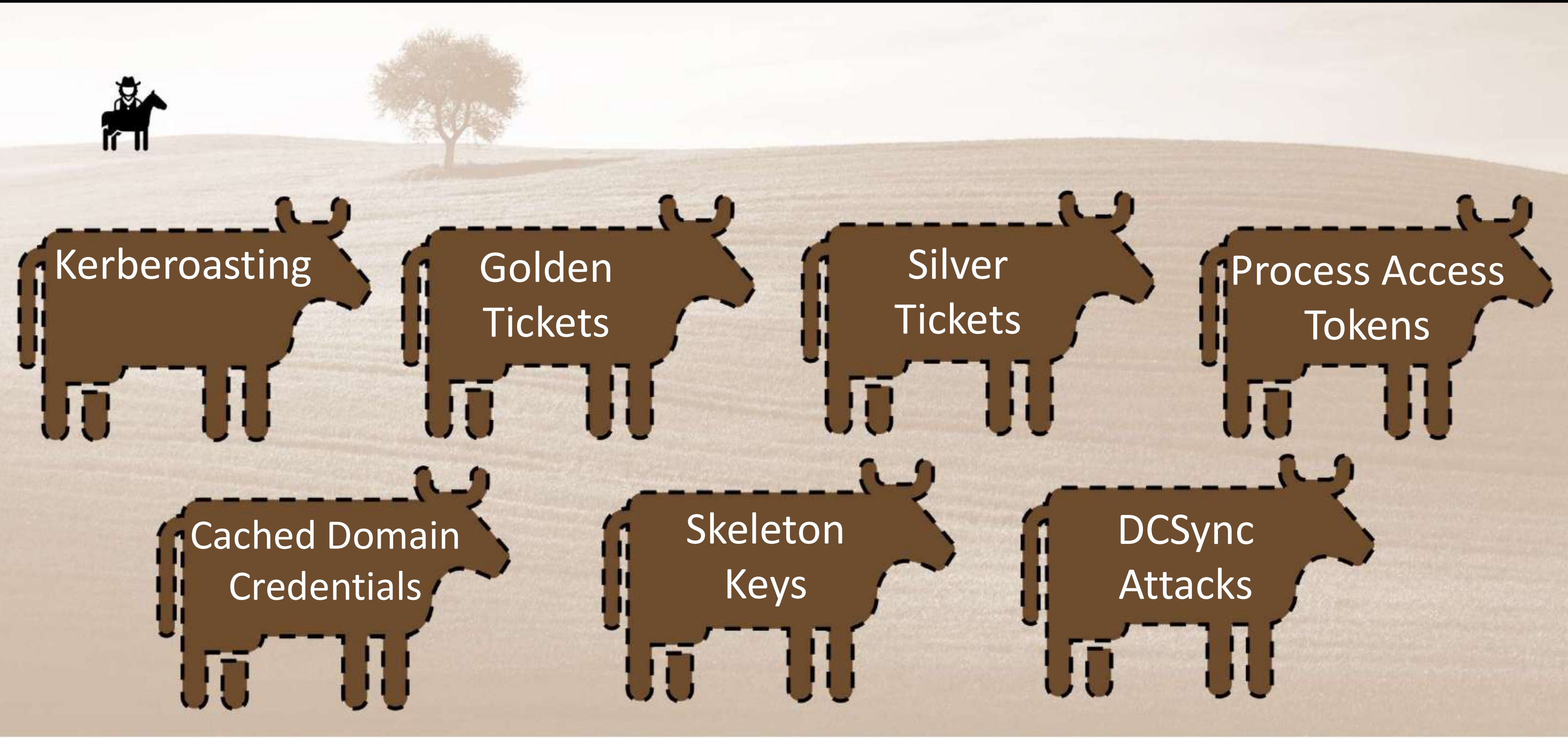
PASS-THE-TICKET



OVERPASS-THE-HASH



BUT WAIT, THERE'S MOOOORE!



Kerberoasting

Golden Tickets

Silver Tickets

Process Access Tokens

Cached Domain Credentials

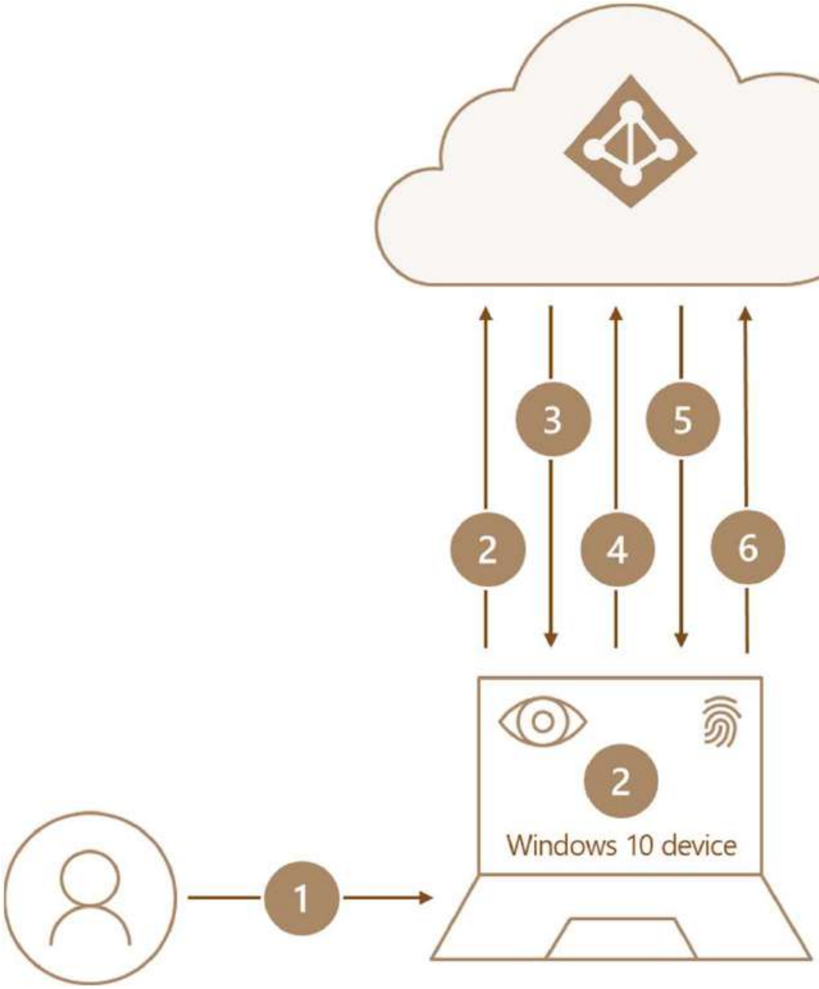
Skeleton Keys

DCSync Attacks

MODERN AUTHENTICATION

- Entra ID (formerly Azure Active Directory)
- Robust Authentication through CloudAP
- Uses access tokens, refresh tokens, and cookies for authorization
- These tokens/cookies give you access to cloud resources

MODERN AUTHENTICATION

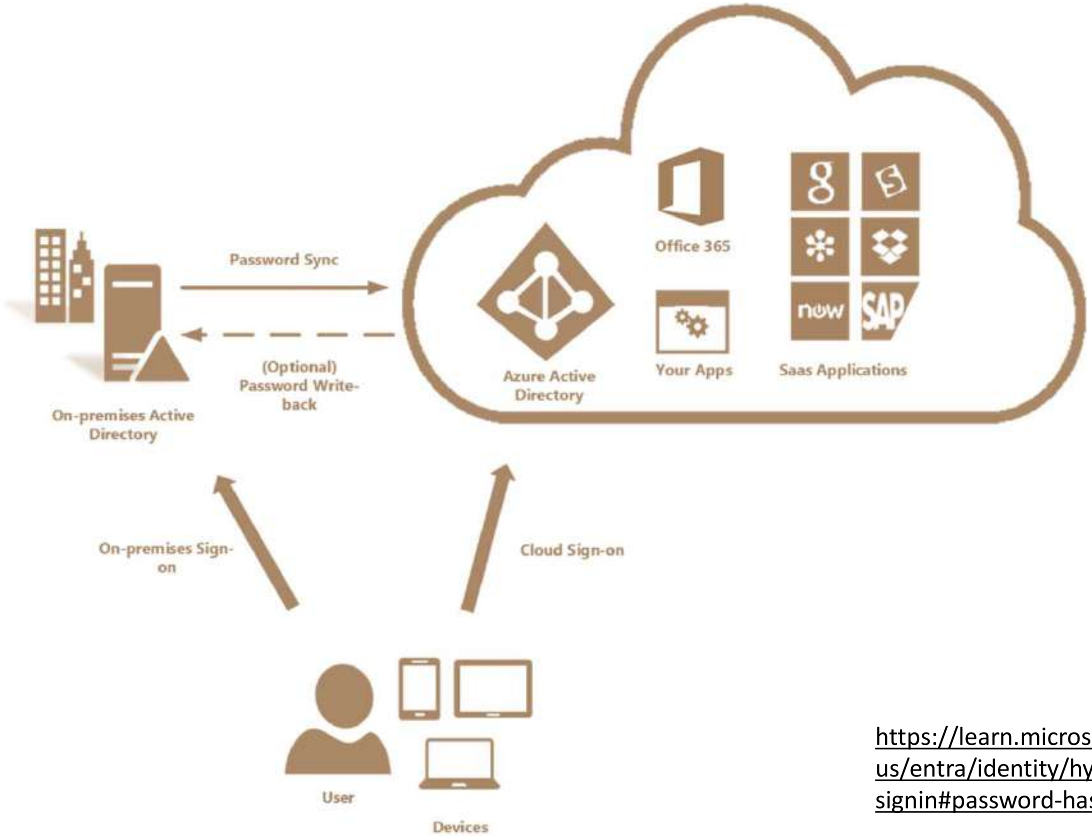


https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless

BUT WE STILL USE ACTIVE DIRECTORY

HYBRID JOIN OPTIONS

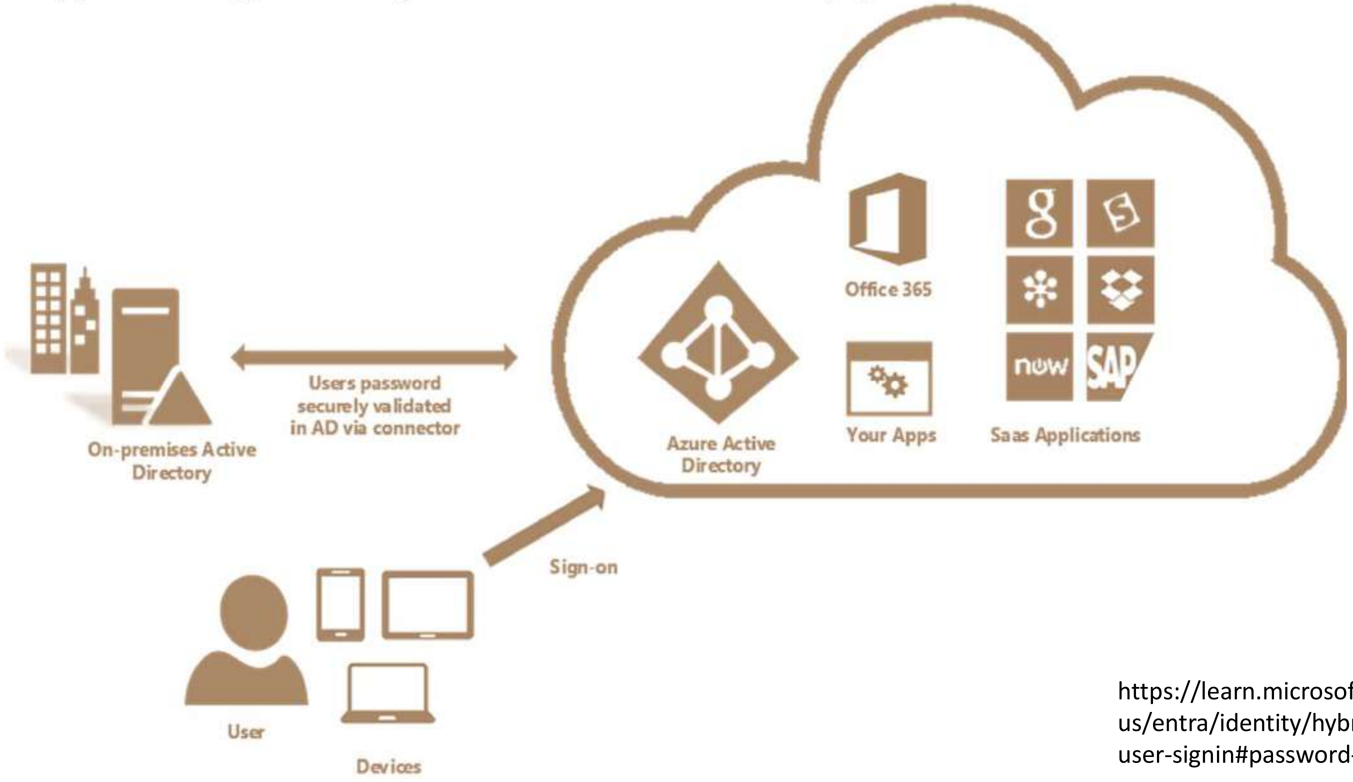
- Password hash Synch: Synch AD usernames and hashes to Entra



https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-user-signin#password-hash-synchronization

HYBRID JOIN OPTIONS

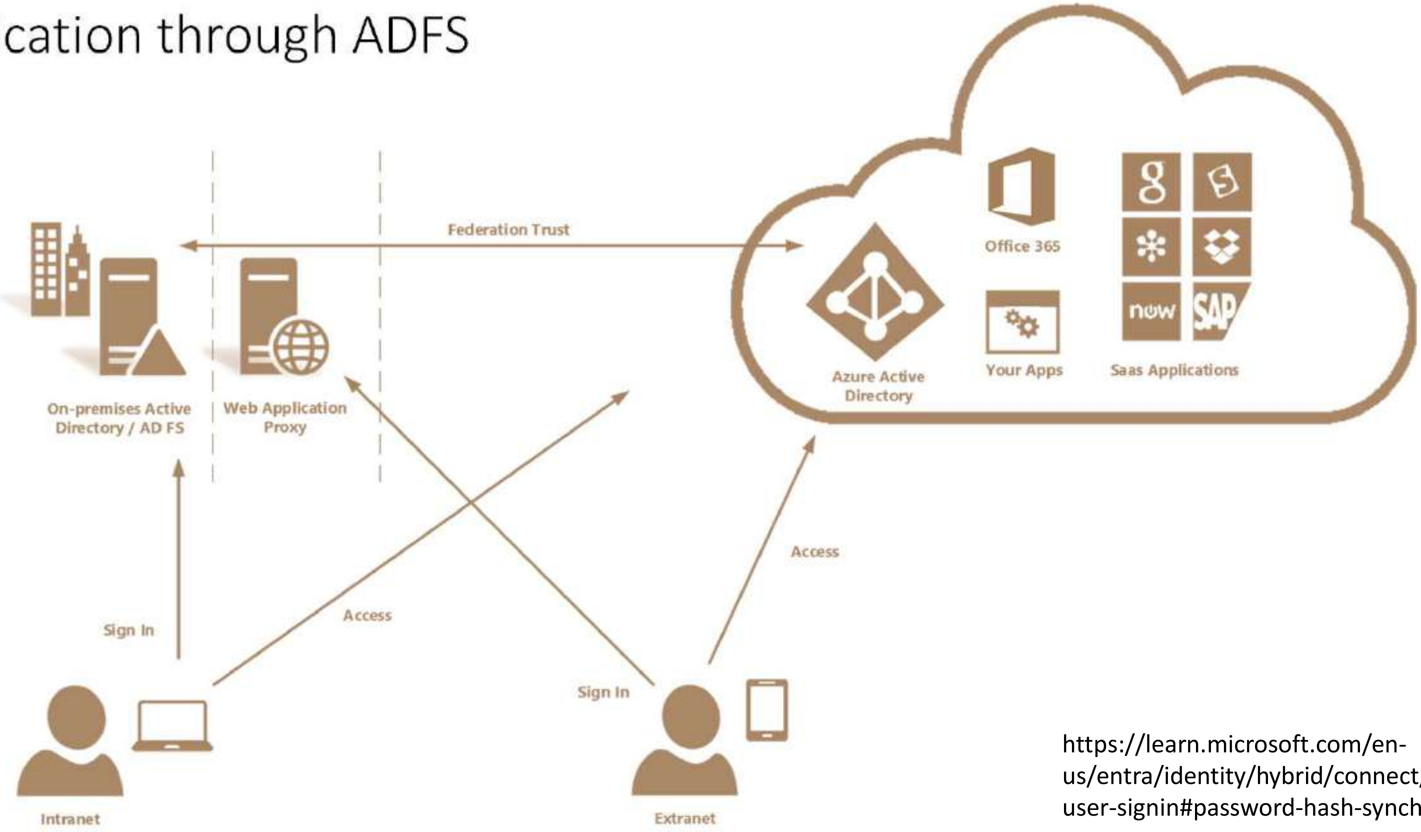
- Passthrough authentication: Synch just the AD usernames to Entra and send encrypted logon request to ADDS for approval



https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-user-signin#password-hash-synchronization

HYBRID JOIN OPTIONS

- Use Federated authentication: Entra trusts ADDS to do the authentication through ADFS



https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-user-signin#password-hash-synchronization

MICROSOFT ENTRA JOINED DEVICES WITH PASSWORD

- Microsoft Entra Connect syncs identity and password hash information
- Password works for both cloud and on-prem
- CloudAP, NTLM, and Kerberos used depending on resource requested
- Not a great solution, with many pitfalls. Hybrid join usually better

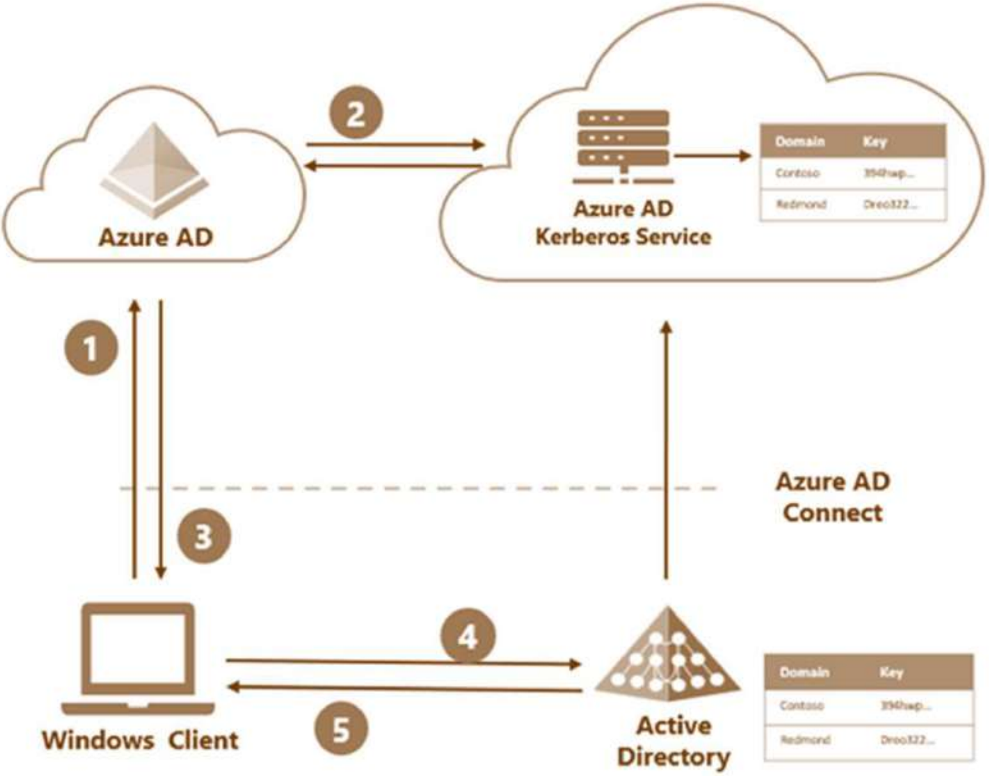
MICROSOFT ENTRA JOINED DEVICES WITH WINDOWS HELLO FOR BUSINESS

- Passwordless Authentication based on asymmetric cryptographic keys

- Microsoft Entra Kerberos

MICROSOFT ENTRA JOINED DEVICES WITH WINDOWS HELLO FOR BUSINESS

- Microsoft Entra Kerberos
- Partial TGT with just the SID issued
- Passed back to Client with PRT
- Used to get full TGT from on-prem DC



Domain	Key
Contoso	394hwp...
Redmond	Dreo322...

Domain	Key
Contoso	394hwp...
Redmond	Dreo322...

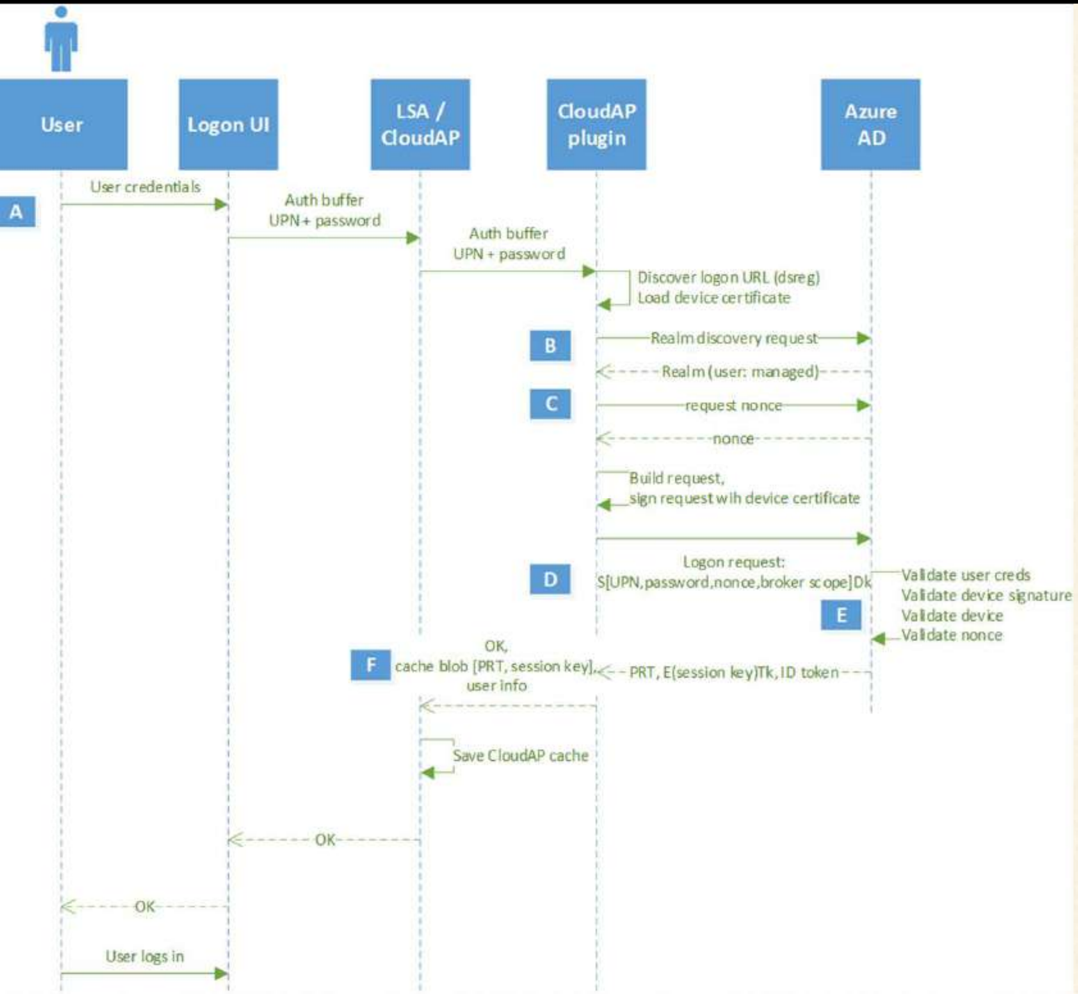
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-hello-for-business-hybrid-cloud-kerberos-trust-is-now/ba-p/3651049

WINDOWS HELLO FOR BUSINESS ON-PREM ONLY

- Uses Asymmetric cryptography through certificates
- Can support MFA if desired
- Private key stored in TPM
- Public key available to the DC
- PIN or biometrics access private key and complete authentication
- But…DC issues a TGT
- And we are back to PTT

WHAT ABOUT MODERN AUTHENTICATION SECURITY?

CLOSER LOOK AT THE PRT: AUTHENTICATION



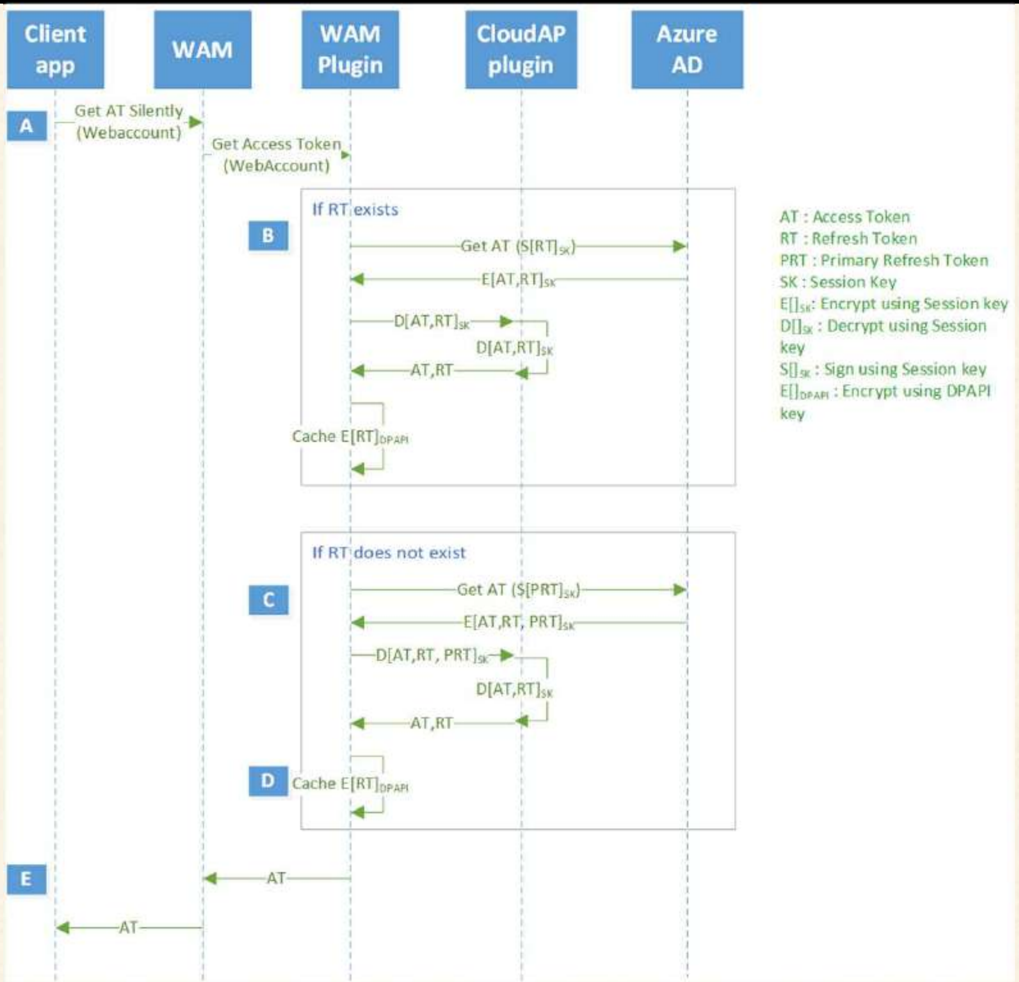
- Device gets a public/private key pair at registration
- Private key stored in TPM, accessed with PIN or biometrics
- Login Prompt -> CloudAP -> Logon request signed with device key -> EntraID
- PRT, Session Key <- EntraID
- A key in TPM is used to encrypt the session key and then encrypted session key and PRT stored in lsass

https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token#prt-issuance-during-first-sign-in

CLOSER LOOK AT THE PRT: AUTHORIZATION

- PRT is used to prove identity (like a TGT) and is valid for 14 days by default
- Renews automatically during use
- Access Tokens (AT) are used to access a resource (like a Service Ticket)
- Refresh Token (RT) is a shorter-lived proof of identity

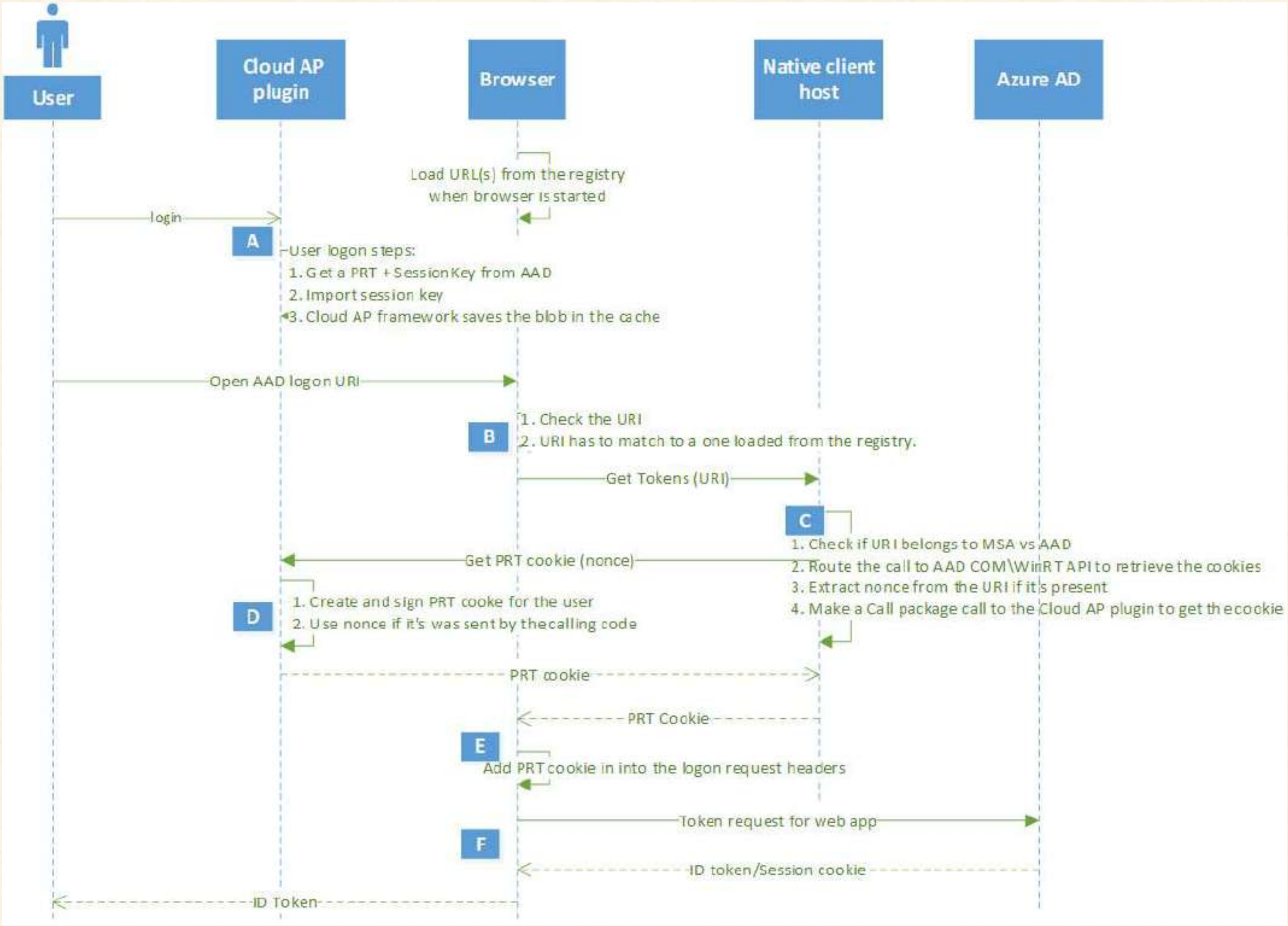
CLOSER LOOK AT THE PRT: APPLICATION AUTHORIZATION EXCHANGE



AT : Access Token
RT : Refresh Token
PRT : Primary Refresh Token
SK : Session Key
$E[]_{SK}$: Encrypt using Session key
$D[]_{SK}$: Decrypt using Session key
$S[]_{SK}$: Sign using Session key
$E[]_{DPAPI}$: Encrypt using DPAPI key

https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token#prt-usage-during-app-token-requests

CLOSER LOOK AT THE PRT: BROWSER AUTHORIZATION EXCHANGE



User
Cloud AP plugin
Browser
Native client host
Azure AD
Load URL(s) from the registry when browser is started
login
A
User logon steps:
1. Get a PRT + SessionKey from AAD
2. Import session key
3. Cloud AP framework saves the blob in the cache
Open AAD logon URI
B
1. Check the URI
2. URI has to match to a one loaded from the registry.
Get Tokens (URI)
C
1. Check if URI belongs to MSA vs AAD
2. Route the call to AAD COM\WinRT API to retrieve the cookies
3. Extract nonce from the URI if it's present
4. Make a Call package call to the Cloud AP plugin to get the cookie
Get PRT cookie (nonce)
D
1. Create and sign PRT cooke for the user
2. Use nonce if it's was sent by the calling code
PRT cookie
PRT Cookie
E
Add PRT cookie in into the logon request headers
Token request for web app
F
ID token/Session cookie
ID Token

https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token#browser-sso-using-prt

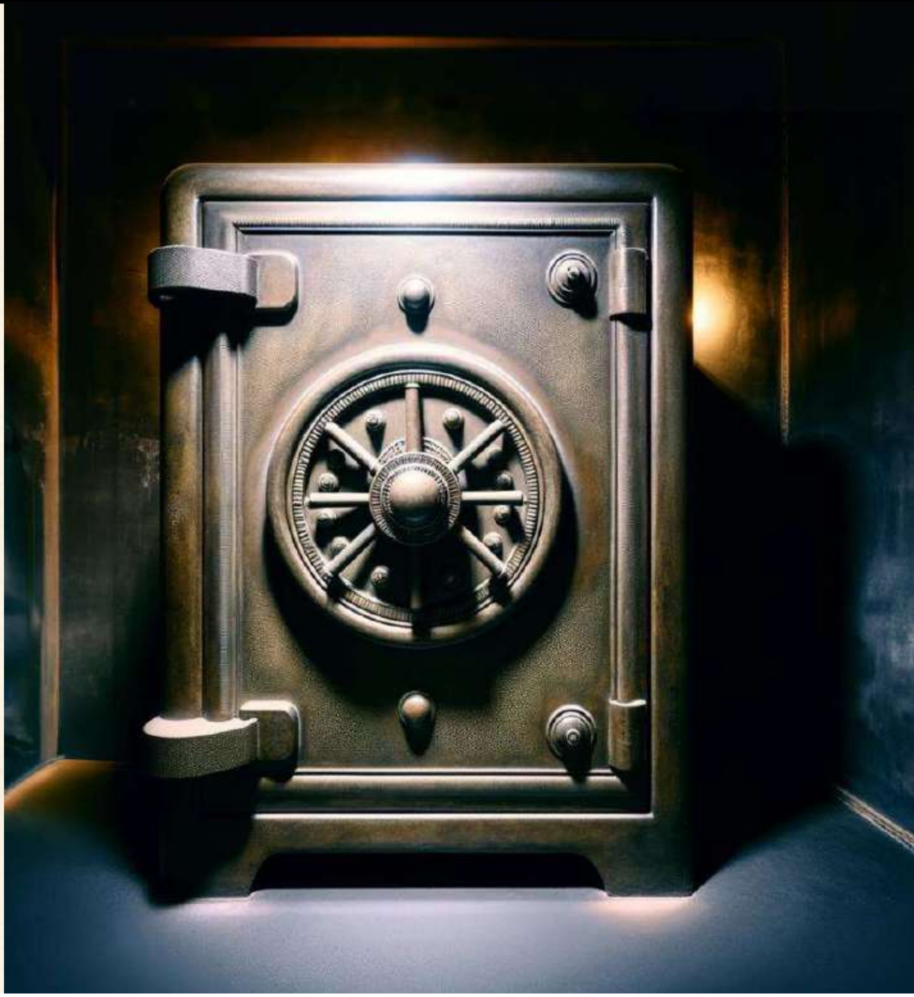
PASS THE PRT

- Browser is the new endpoint
- ROADTools follows same process as a browser to request a PRT cookie
- Transmit the PRT cookie in the browser
- Access the web service
- Claims in the PRT cookie persist, like device ID, MFA status, etc.
- Works with the local user’s permissions

WHAT WILL KEEP US SAFE?

TRUSTED PLATFORM MODULES (TPM)

- Windows 11 designed to use TPM 2.0
- Do not bypass this requirement
- Securely stores critical key information
- Without TPM, these keys exposed in memory



VIRTUALIZATION BASED SECURITY

- Credential Guard
- Uses Hyper-V isolation to protect NTLM and Kerberos credentials
- Does not protect Entra ID credentials

ENDPOINT DETECTION AND RESPONSE

- Many of these attack vectors can be detected or blocked
- A useful, but not perfect, control

DISABLE LM, NTLMV1 AND NTLMV2

- Can cause some issues with legacy programs

- New options in Windows 11 Insider Preview (25992 – Canary) allow for blocking outbound SMB use or selectively blocking if not on an allow list

- Also disable or monitor for use of RC4 with Kerberos (Overpass-the-hash and Kerberoasting attacks)

STRENGTHEN SMB

- Disable SMBv1
- Require SMB signing to block relay attacks
- Enable SMB failed logon rate throttling:

Set-SmbServerConfiguration -InvalidAuthenticationDelayTimeInMs 2000

CAREFUL USE OF CREDENTIALS

- Use Remote Credential Guard for RDP
- Domain Protected Users Security Group
- Use PowerShell Remoting

PRIVILEGED ACCESS WORKSTATIONS

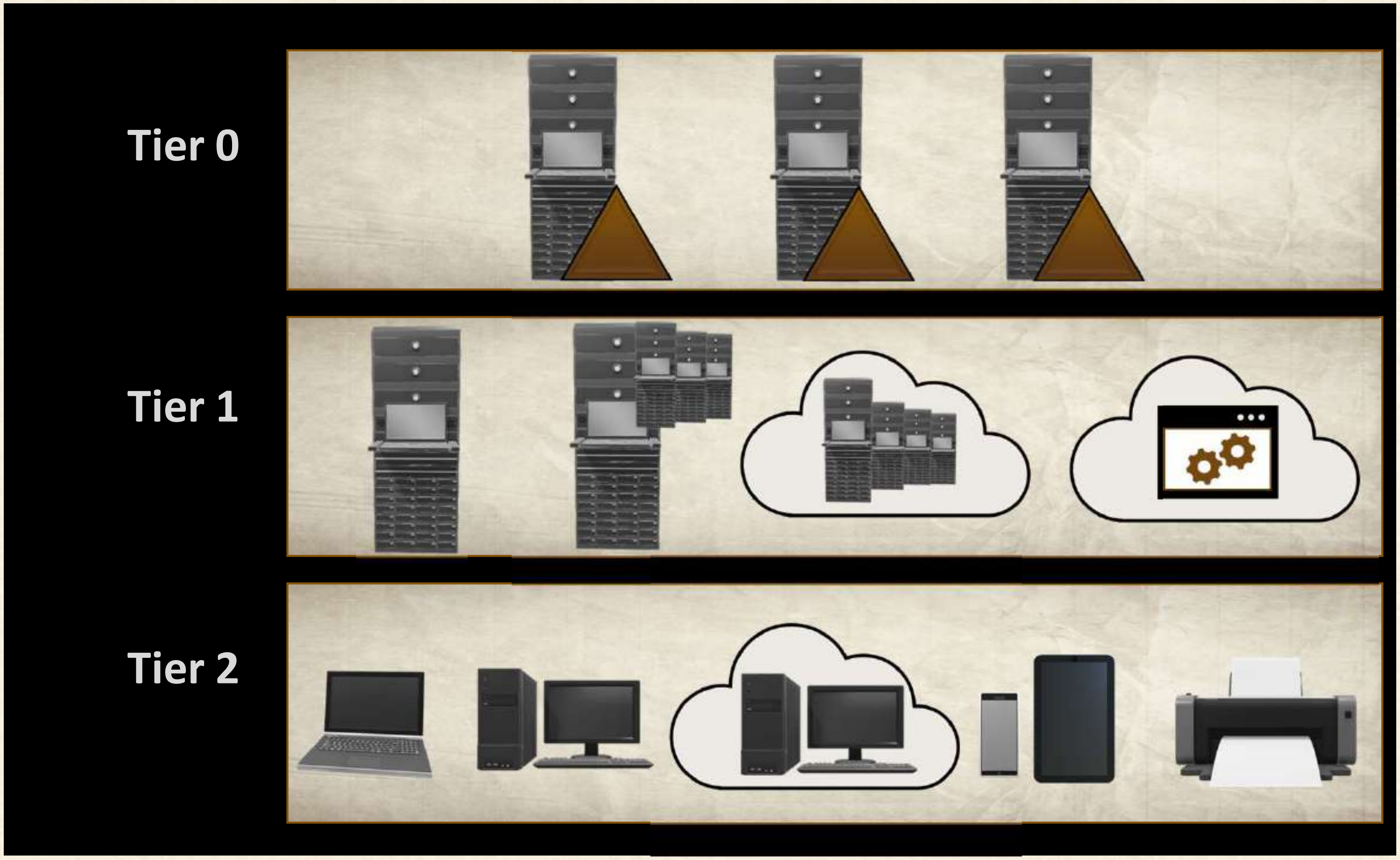
- Your credentials are most exposed where you logon

- Separate systems for admin and regular use

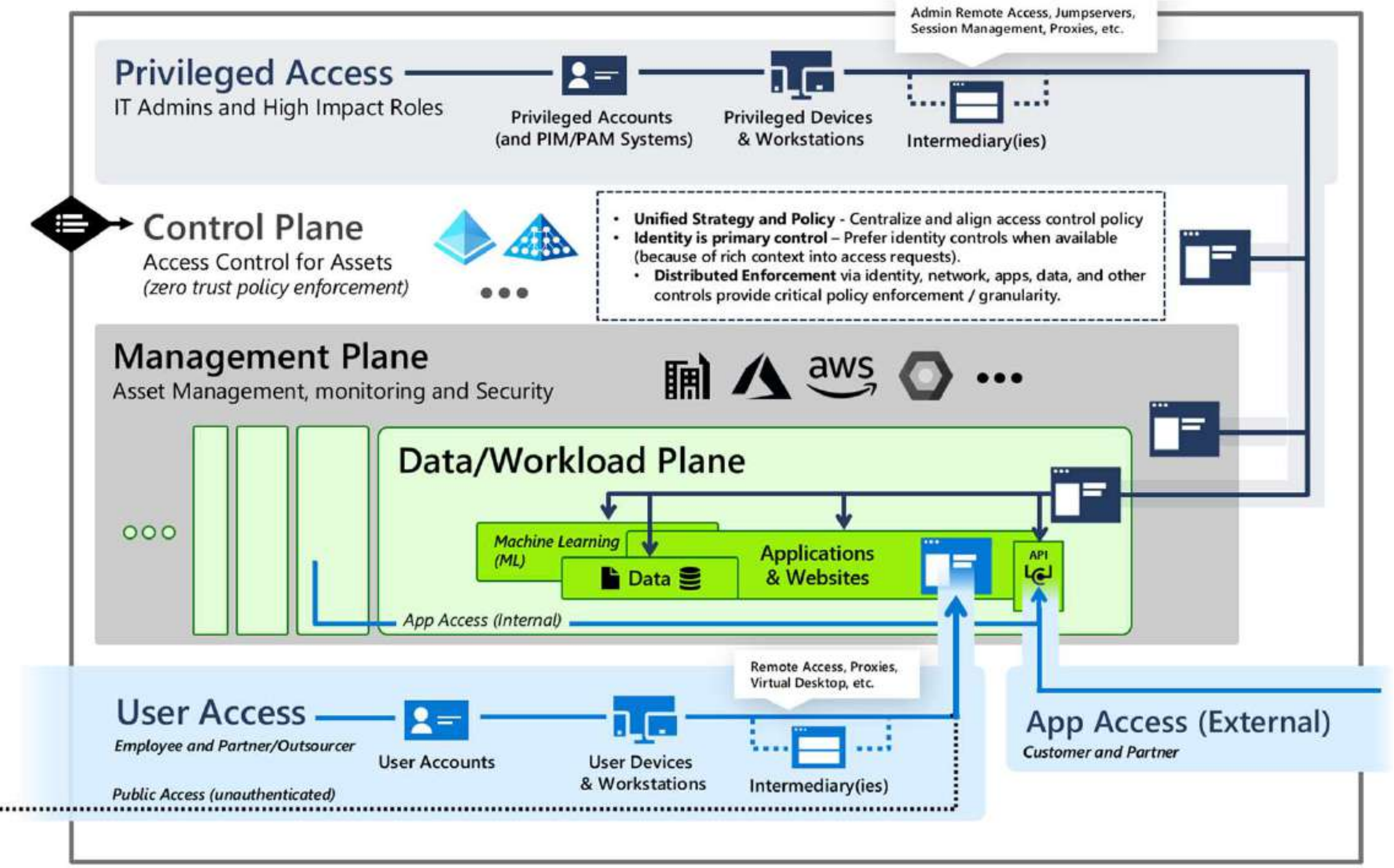
SEGMENTATION AND ZERO TRUST

- Don’t allow connections without a business need
- Host based firewalls, Zero Trust products, physical or virtual subnetting with firewalled access

ENTERPRISE ACCESS MODEL ON PREM



ENTERPRISE ACCESS MODEL EXTENDS TO CLOUD


Admin Remote Access, Jumpservers, Session Management, Proxies, etc.
Privileged Access
IT Admins and High Impact Roles
Privileged Accounts (and PIM/PAM Systems)
Privileged Devices & Workstations
Intermediary(ies)
Control Plane
Access Control for Assets
(zero trust policy enforcement)
• Unified Strategy and Policy - Centralize and align access control policy
• Identity is primary control – Prefer identity controls when available (because of rich context into access requests).
• Distributed Enforcement via identity, network, apps, data, and other controls provide critical policy enforcement / granularity.
Management Plane
Asset Management, monitoring and Security
aws
Data/Workload Plane
Machine Learning (ML)
Data
Applications & Websites
API
App Access (Internal)
Remote Access, Proxies, Virtual Desktop, etc.
User Access
Employee and Partner/Outsourcer
User Accounts
User Devices & Workstations
Intermediary(ies)
Public Access (unauthenticated)
App Access (External)
Customer and Partner

Privileged Access

Enables IT administrators and other high impact roles to access to sensitive systems and data. *Stronger security for higher impact accounts*

Control and Management Planes

Provide unified access and management for workloads and assets *(and provide attackers shortcut for illicit objectives)*

Data/Workloads

Create and store business value in

- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

User and App Access

How employees, partners, and customers access these resources

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model#evolution-from-the-legacy-ad-tier-model

USER ACCOUNT MONITORING

- Monitor accounts for abnormal use
- UEBA solutions
- Especially critical for privileged accounts
- Don’t forget Entra ID

SUMMARY

- Authorization credentials continue to be the weak point in credential security
- Hashes, TGTs, PRTs can all be stolen and used to impersonate a user
- Don’t assume that the latest and greatest tech is safe
- You need to use defense-in-depth approach
- And engage in active cyber defense of your network…on prem and in the cloud

ADDITIONAL RESOURCES

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-user-signin

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-pta

https://learn.microsoft.com/en-us/entra/identity/devices/concept-primary-refresh-token

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-hello-for-business-hybrid-cloud-kerberos-trust-is-now/ba-p/3651049

https://trustedsec.com/blog/azure-ad-kerberos-tickets-pivoting-to-the-cloud

THANK YOU!