
May 31 – June 2, Oslo Spektrum

10th anniversary

# Adventures in the Hybrid Cloud: Cybersecurity in the Twilight Zone

Andy Malone MVP, MCT

# Andy Malone MVP, MCT

- Microsoft  MVP (Security 15 Years)
- Microsoft Certified Trainer (24 years)
- Microsoft Internal Staff Instructor
- Founder: Cybercrime Security Forum!
- Worldwide event Speaker
- Published Author
- Subscribe to my YouTube Channel

nicX edition

# The Hybrid Cloud

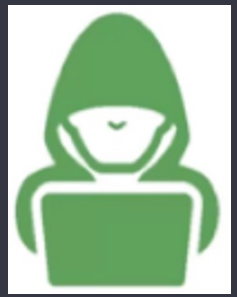
- Covid 19 has exposed Increased security risks from remote home working
- 2020-1 saw a massive increase in Social Engineering attacks (Phishing)
- Ransomware continues to be a potent weapon in extorting money from corporates & smaller organizations alike.
- Hybrid cloud solutions becoming a major focal point for hackers
- With focus on cloud skill dominance. On premises infrastructure skills are lagging. Thus, exposing weaknesses & potential vulnerabilities.
- Delayed cyber-attack detection and response
- Gaps in physical and information security

**Not since the heights of the mainframe era has the world witnessed computing systems of such complexity used by so many but designed and created by so few.**

12 Aug 2021

# IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach

# Cybercrime in 2022: The Threat Actors

| | HACKTIVISM | CRIME | INSIDER | ESPIONAGE |
|---|---|---|---|---|
| THREATS |  |  |  |  |
| MOTIVATIION | Hacktivists use computer network exploitations to gain and resources to advance their political or social cause. | Individuals and sophisticated criminal enterprises which act information and extort victims for financial gain. | Trusted insiders seeking to steal for personal, financial and ideological reasons. | Nation-state actors conduct computer intrusions to steal secrets, and property information from private companies. |

# Cyberthreats are Evolving

Malware-Less Attacks

'File-less' Malware

Tailored/Targeted Malware

Mass Distribution Malware

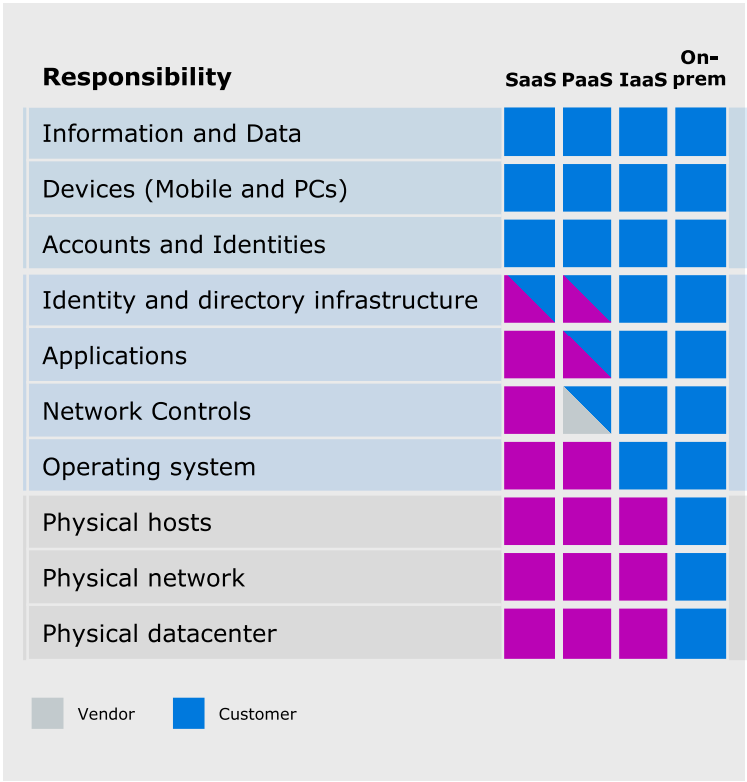
THREAT AGES

Malware and Infrastructure

Identity and Apps

# Designing a Secure Hybrid Cloud

# Building a resilient Hybrid cybersecurity program



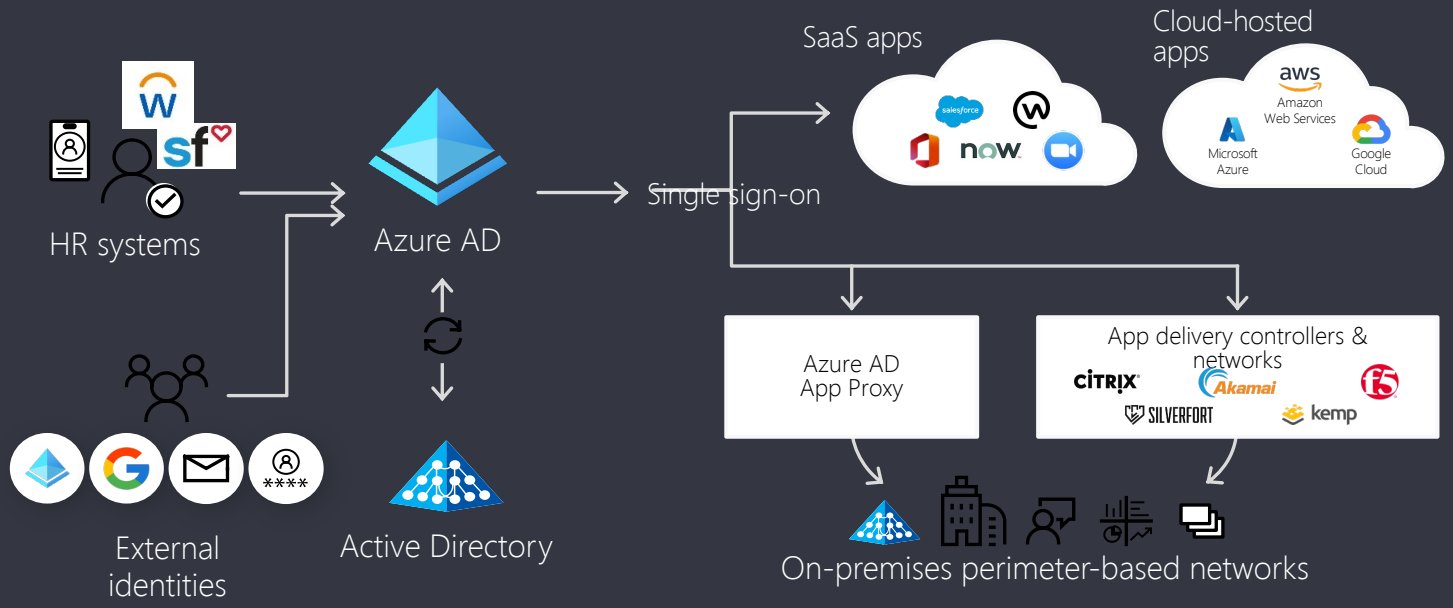

ESTABLISH A MODERN PERIMETER

MODERNIZE INFRASTRUCTURE SECURITY

"TRUST BUT VERIFY" EACH CLOUD PROVIDER

# Designing the Hybrid Cloud (Connectivity)

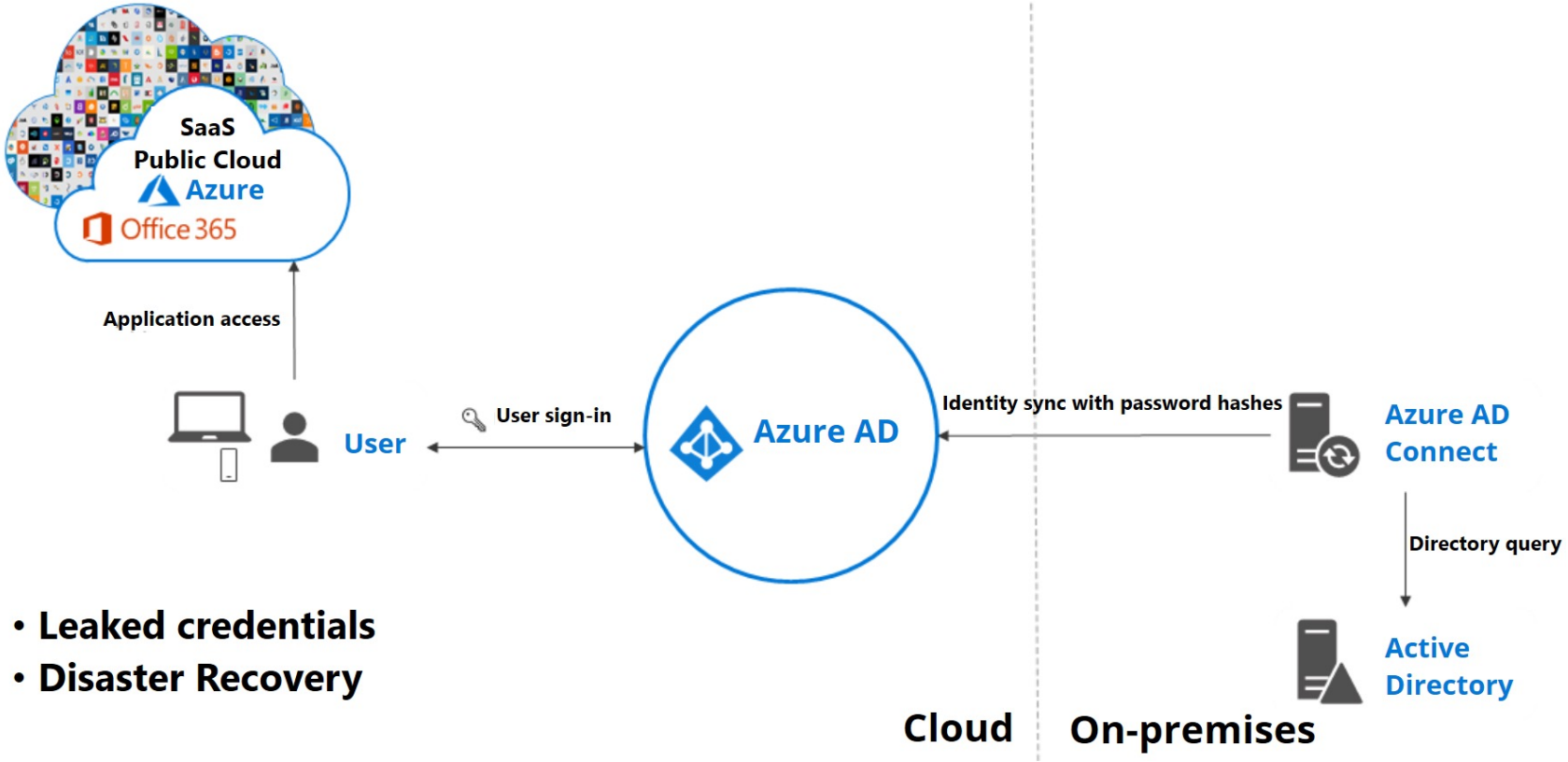
An IT architecture that incorporates some degree of workload portability, orchestration, and management across 2 or more environments.



# Hybrid Authentication  Methods

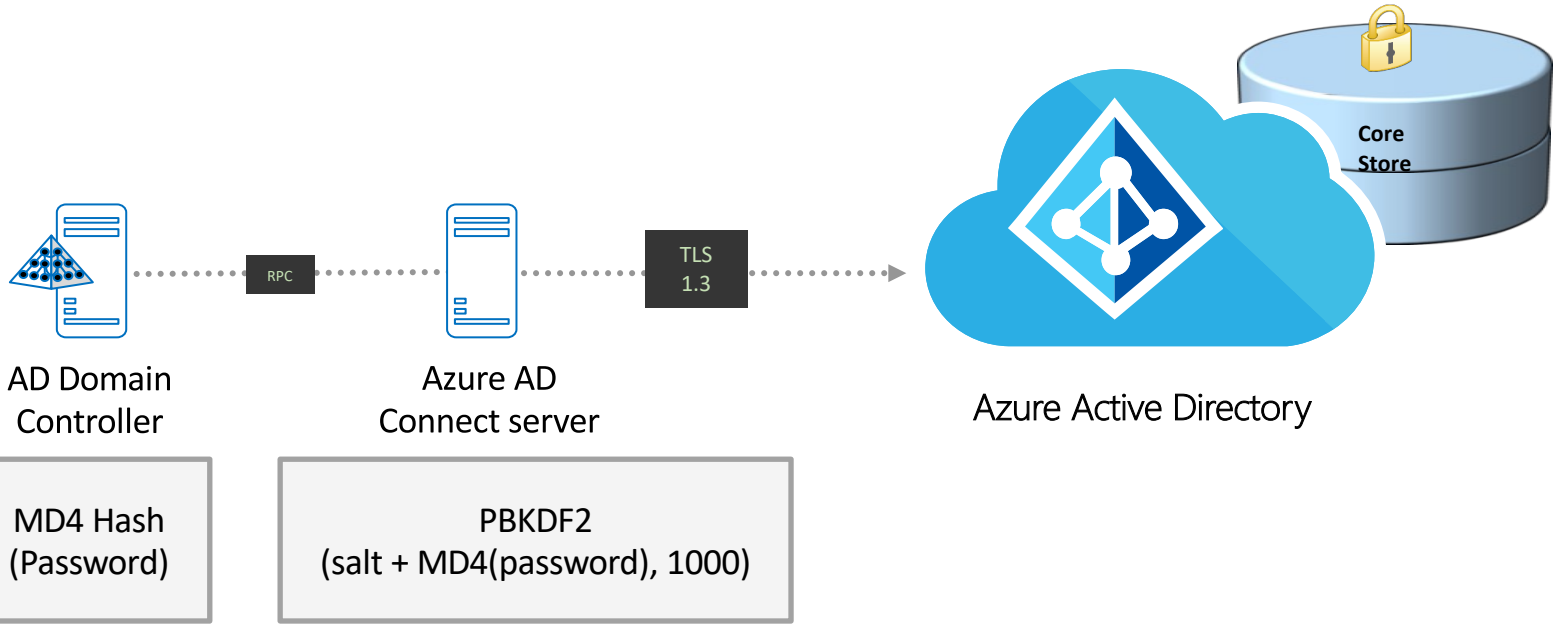
- Password hash sync
- Pass-through authentication
- Federated authentication
  - PTA, ADFS

# Password hash sync

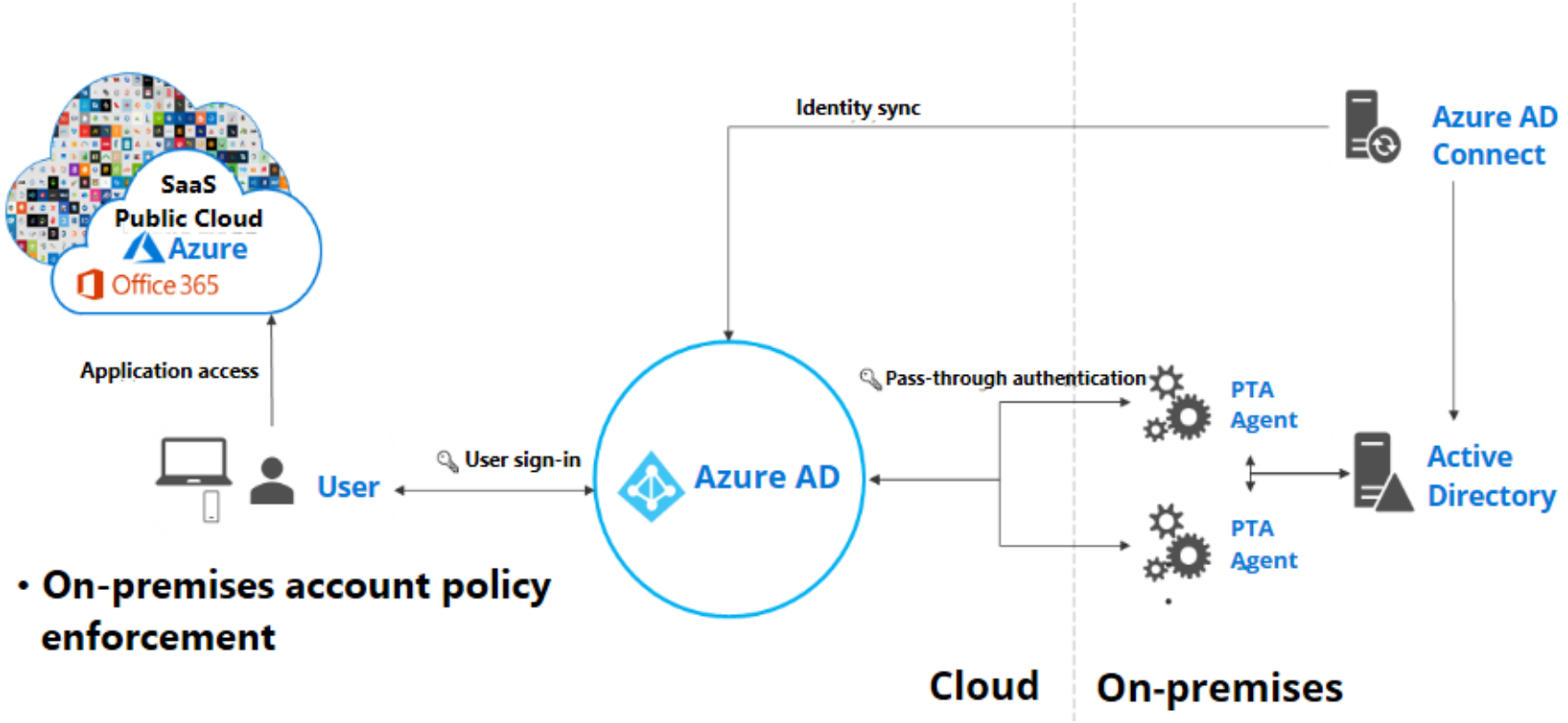



- **Leaked credentials**
- **Disaster Recovery**

# Password Hash Sync

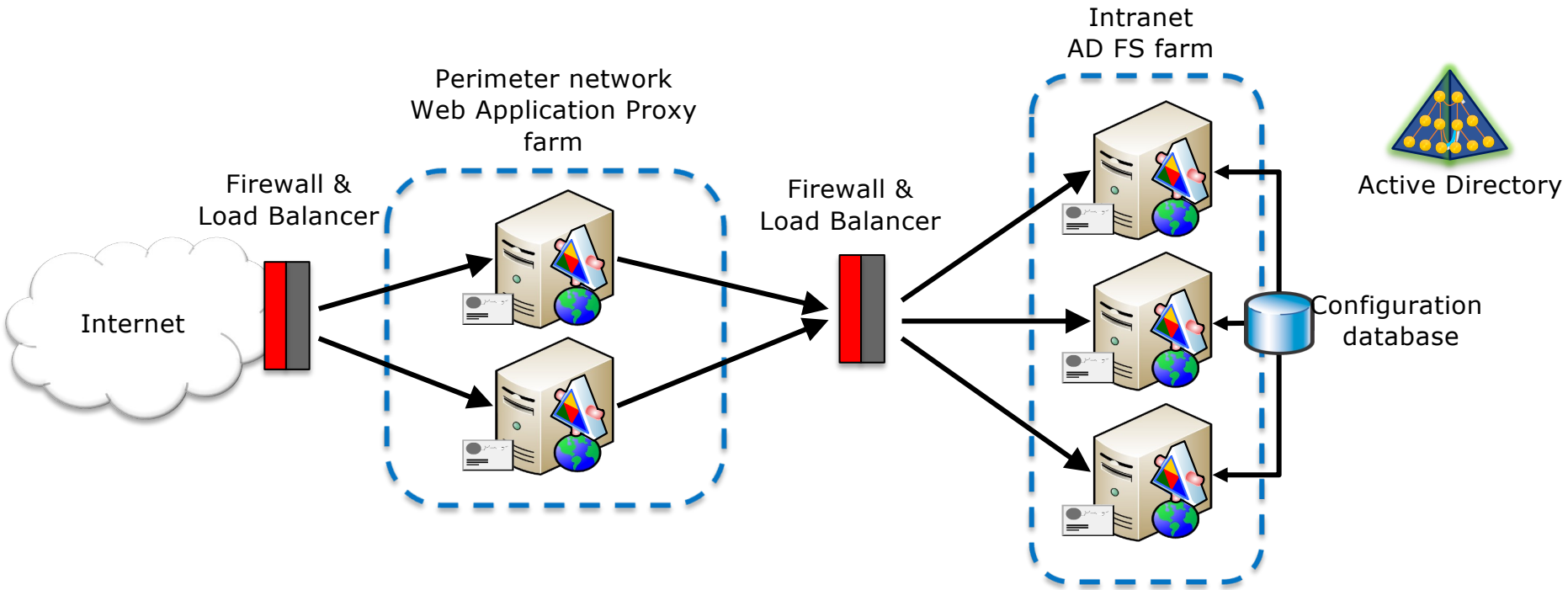


# Pass-through authentication (Oauth 2.0)




- **On-premises account policy enforcement**

# ADFS - Federation, but at at what cost?



# Federation, but at at what cost? The Solar Winds Hack

1. After establishing a foothold on the SW network, attackers targeted the identity provider used by CSP, to steal the means to issue IDs.
2. Once accomplished, they can use it to create IDs that enable the impersonate legitimate users, including accounts with administrative access.
3. Because these IDs are used to give access to data and services by cloud-based services, the attackers are able to access data and email just like legitimate users, including those with total access, and they do so.

# Hybrid Pitfalls, and how to avoid them

# Hybrid Connectivity - Pitfalls

Too many users with Admin permissions

ADDS & ADFS are Built on ageing Technologies & Protocols, NTLM, Kerberos, SAML

Too many active stale user accounts

Poor auditing practices

Badly implemented hybrid solutions are increasing organisations attack surface

# Hybrid Connectivity - Pitfalls

Pros

- Easy management of groups and user assignments
- Integration with web applications using Oauth 2.0
- Easily extends existing on premise AD

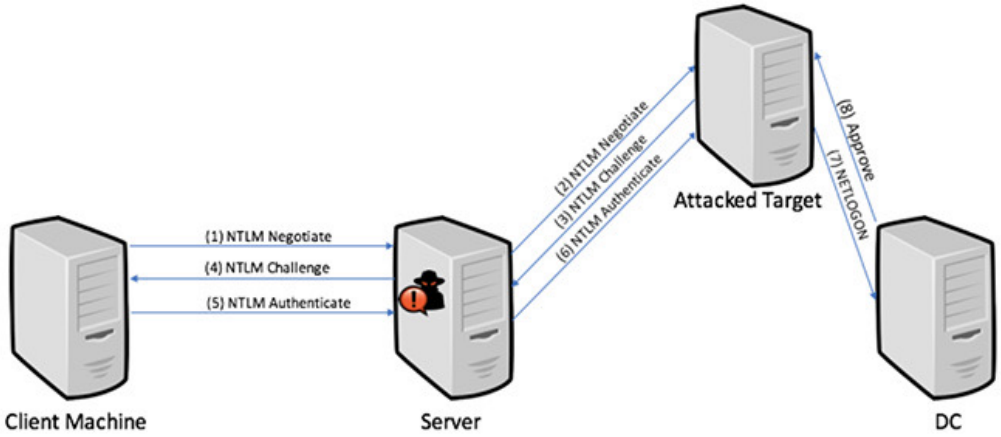
Cons

- The UI can be cumbersome to use
- Bulk edits for instance are better handled using PowerShell.
- Documentation can be hard to find when integrating AD into web apps
- Some settings in AD can be confusing with no obvious explanation
- Often a disconnection between Azure AD & other portals. Example Microsoft 365 Admin Centre

# Weakness begins on-prem with Active Directory

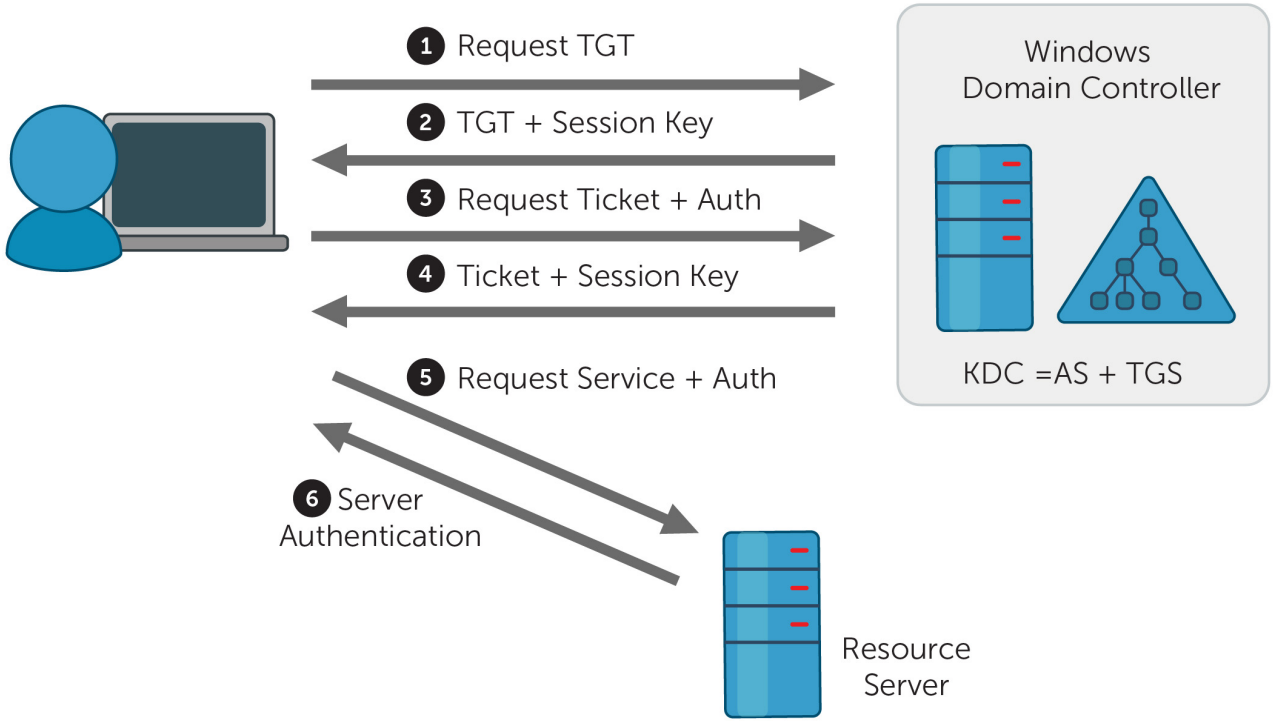
# Ageing Authentication Protocols - NTLM

- NTLM is **highly suspectable** to brute force attacks.
- Microsoft has upgraded its proprietary authentication scheme four times.
- Current authentication standards for NT clients and NT/Win2K servers is now NTLMv2. However, if you **haven't changed** the LMCompatabilityLevel variable under the following registry key on both NT/Win2K clients and servers, by default you're still using the LM scheme, which greatly decreases the security of your entire network:
  HKEY_Local_Machine\System\CurrentControlSet\control\LSA




*NTLM relay basic flow*

# Ageing Authentication Protocols Kerberos



# Kerberos Authentication Pro's & Cons

**Pro's**

1. Kerberos, Clients and services are mutually authenticated.
2. Various operating systems including Windows Server 2019 support it.
3. Kerberos Tickets have a limited period.
4. If the ticket gets stolen, it is hard to reuse the ticket because of strong authentication needs.
5. Passwords are never sent over the network unencrypted.
6. In Kerberos, secret keys are shared, which is more efficient than sharing public keys.

**Cons**

1. It is vulnerable to weak or repeated passwords.
2. It only provides authentication for services and clients.

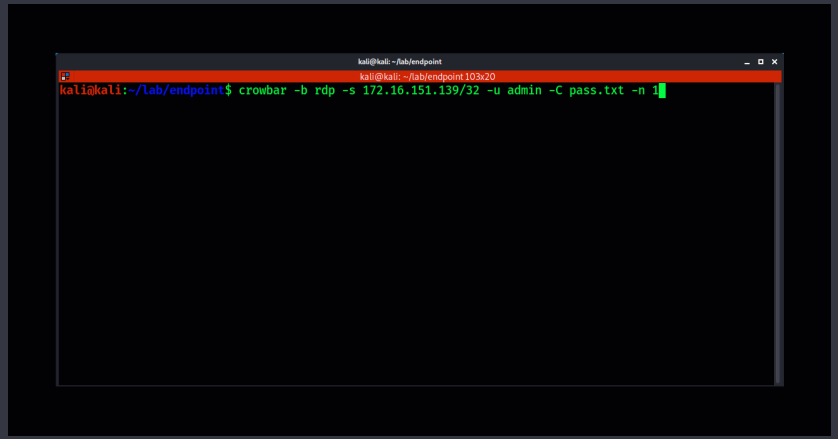
# Active Directory Attack Examples

# (1) Getting in the back door with Remote Desktop Attacks

Beware hackers who brute force the Remote Desktop Protocol

- Attackers consistently scan for endpoints with Remote Desktop Protocol Enabled. They use various scanning tools such as Massscan or Nmap to discover systems with port 3389 open.

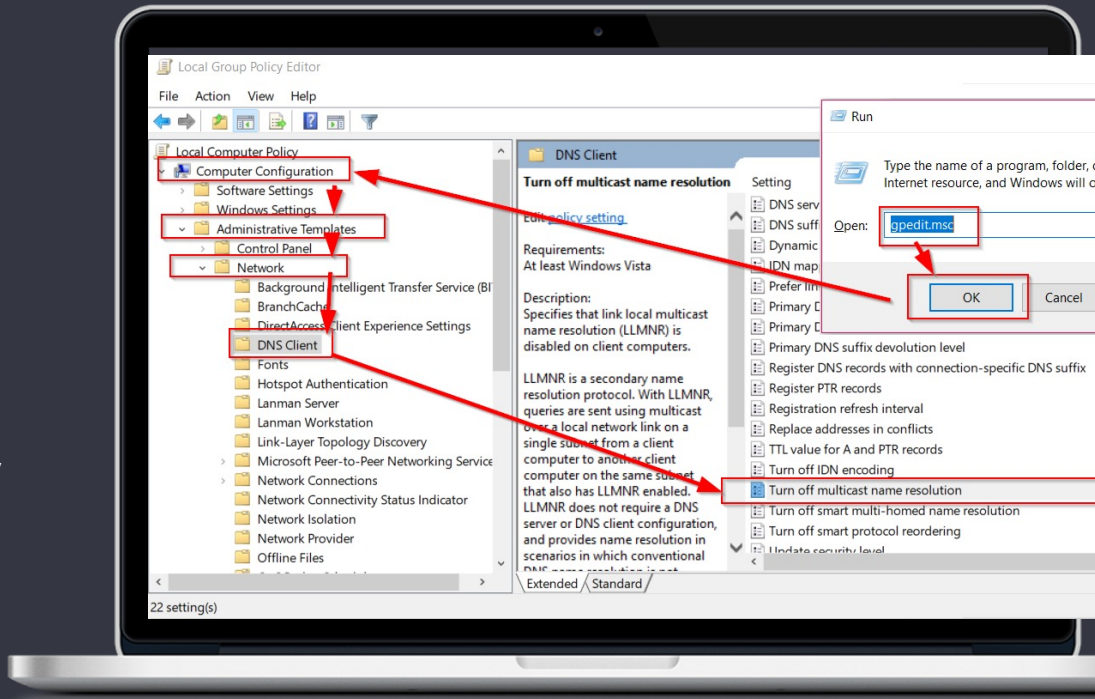
```
Nmap scan report for 172.16.151.139
Host is up (0.00043s latency).
Not shown: 65522 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: MATRIX)
1536/tcp open  msrpc         Microsoft Windows RPC
1537/tcp open  msrpc         Microsoft Windows RPC
1538/tcp open  msrpc         Microsoft Windows RPC
1539/tcp open  msrpc         Microsoft Windows RPC
1540/tcp open  msrpc         Microsoft Windows RPC
1541/tcp open  msrpc         Microsoft Windows RPC
1542/tcp open  msrpc         Microsoft Windows RPC
1543/tcp open  msrpc         Microsoft Windows RPC
1544/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: MATRIX
|   NetBIOS_Domain_Name: MATRIX
```




Never leave RDP directly exposed to the public internet without additional security controls

# (2) Disable Link-Local Multicast Name Resolution (LLMNR)

- Ageing Protocol LLMNR was a protocol that allowed name resolution without the requirement of a DNS server
- Uses port UDP 5355
- Few inbuilt protections to prevent unauthorized nodes from authoritatively claiming they were anyone
- Disable LLMNR with Active Directory GPO
- Computer Configuration -> Administrative Templates -> Network -> DNS ClientEnable Turn Off Multicast Name Resolution policy by changing its value to Enabled




Always MFA Solutions or an Access management solution to create strong passphrases so employees don't need to.

nicX edition

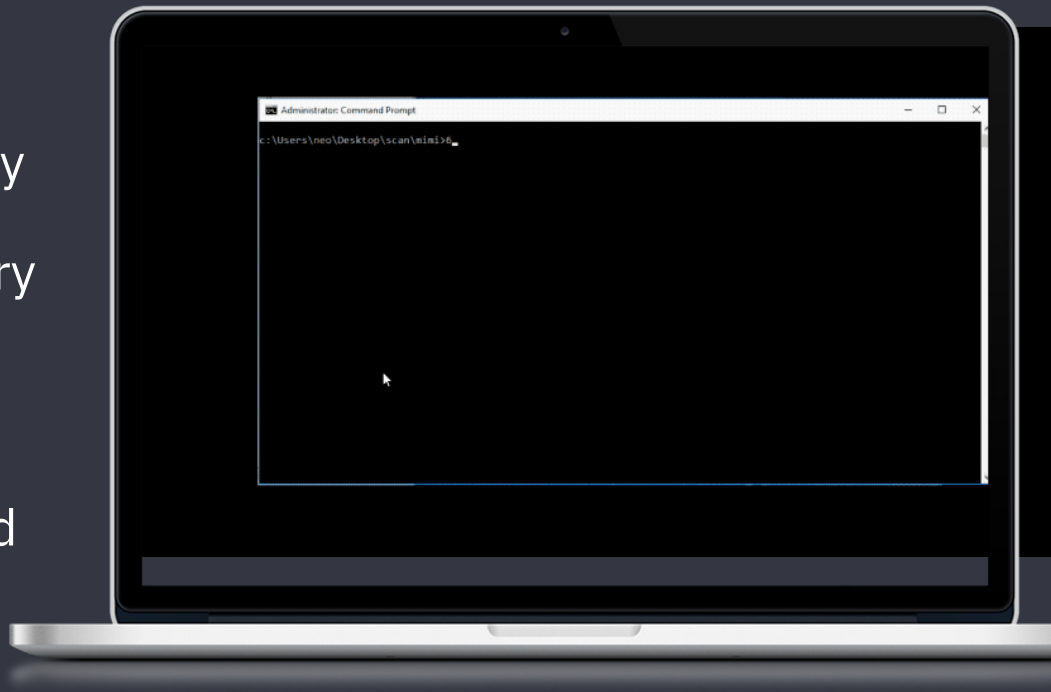
# (2) NetBIOS and LLMNR Name Poisoning using Responder

- Attackers continue to successfully use tools such as Responder, which can be executed via email, by listening over unauthorized network access, or even by plugging a USB into an unattended laptop.
- Responder will answer to network queries for SMB shares via LLMNR or NBT-NS.
- An unsuspecting victim's system will happily share its NTLM hash.
- Once the attacker has the hash, it's only a matter of time before they'll be able to crack it using tools like hashcat.


Always use either strong passwords or MFA Solutions or an Access management solution to create strong passphrases so employees don't need to.

# (3) Using Domain Admin Accounts for services

- Service accounts are great for running backups
- But poorly implemented or managed allow hackers to easily elevate privileges
- Attackers will modify the registry that will keep a cached credential in memory in cleartext.
- Windows 2012 disabled by default, however, can easily add the registry key to enable.




*[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest] "UseLogonCredential"=dword:00000001*

# (4) Beware Overprivileged and Unmanaged Service Accounts

- Hacker will target privileged accounts within your network
- Service accounts are top targets Service accounts with elevated domain privileges can access needed network resources
- This is a technique used when service accounts are configured to use the SPN (Service Principal Name) so when users or system needs access, a Kerberos ticket is issued signed with the NTLM hash of the account.

## KRBTGT account

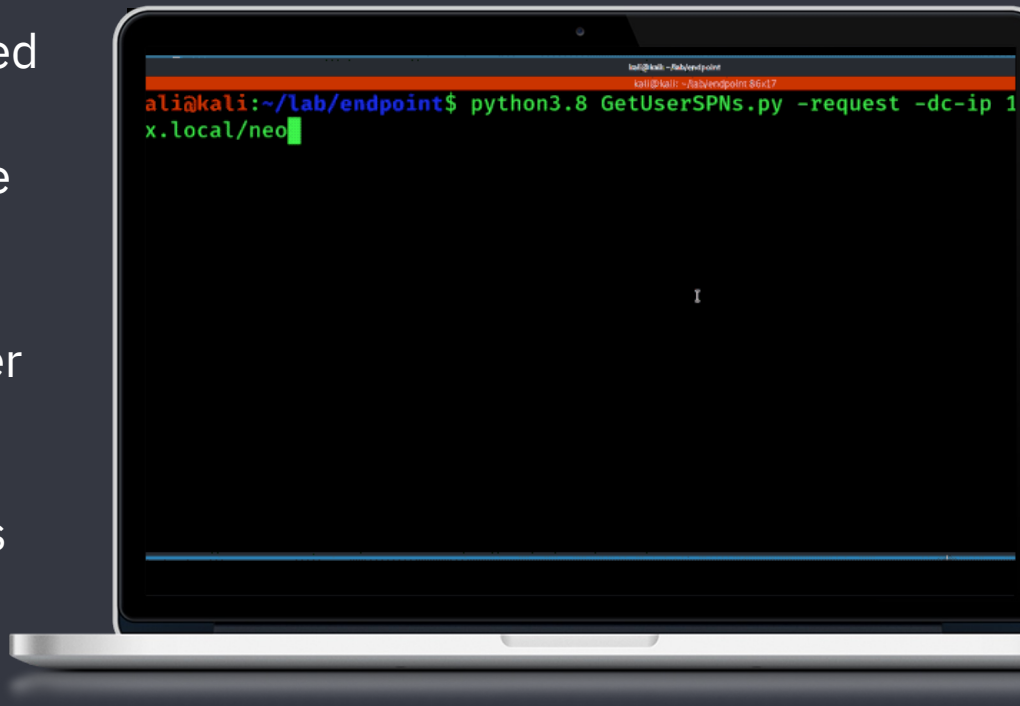
The KRBTGT account is a local default account that acts as a service account for the Key Distribution Center (KDC) service. This account cannot be deleted, and the account name cannot be changed. The KRBTGT account cannot be enabled in Active Directory.

KRBTGT is also the security principal name used by the KDC for a Windows Server domain, as specified by RFC 4120. The KRBTGT account is the entity for the KRBTGT security principal, and it is created automatically when a new domain is created.

Windows Server Kerberos authentication is achieved by the use of a special Kerberos ticket-granting ticket (TGT) enciphered with a symmetric key. This key is derived from the password of the server or service to which access is requested. The TGT password of the KRBTGT account is known only by the Kerberos service. In order to request a session ticket, the TGT must be presented to the KDC. The TGT is issued to the Kerberos client from the KDC.

# (5) Kerbroasting

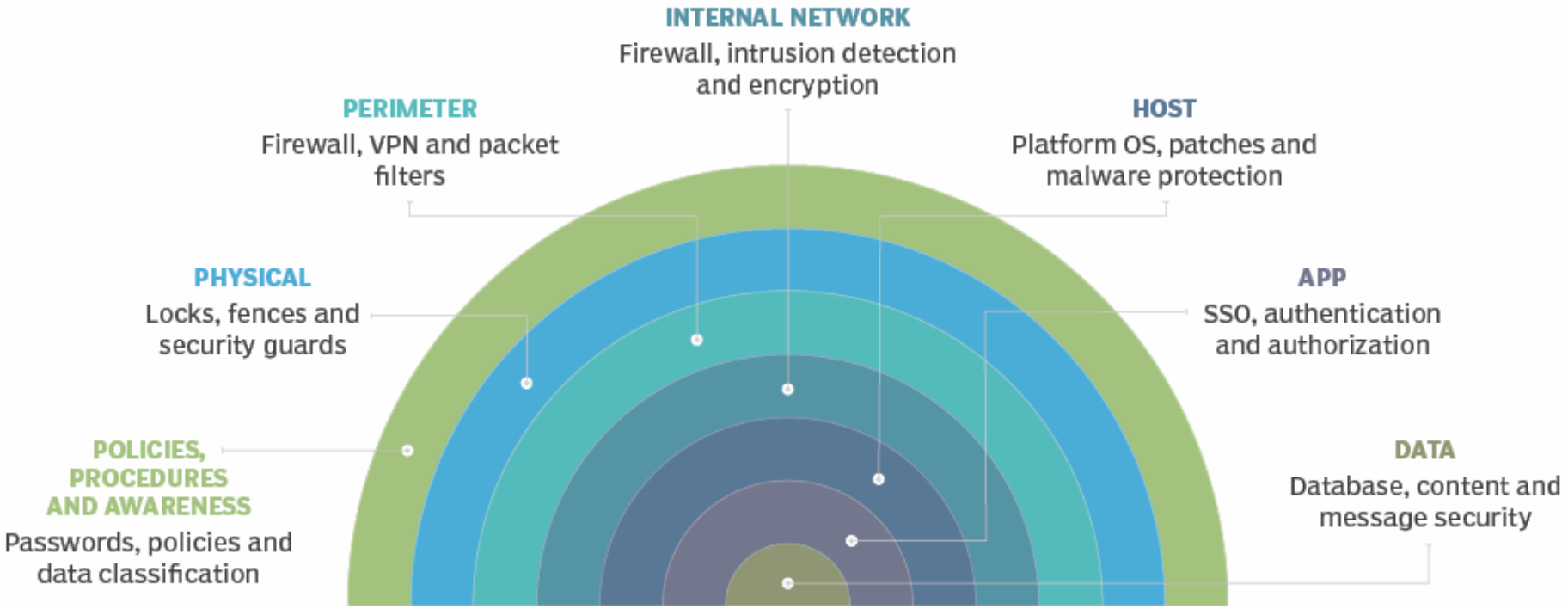
- A technique used by attackers to elevate privileges and gain privileged access to Active Directory.
- Successful due to common practice of using weak service account credentials
- Attacker uses standard domain user to request the SPN which is signed by the NTLM hash of the service account, and when poor passwords are used, cracking software can crack the hash revealing the plain text




GetUserSPN.py from Impacket

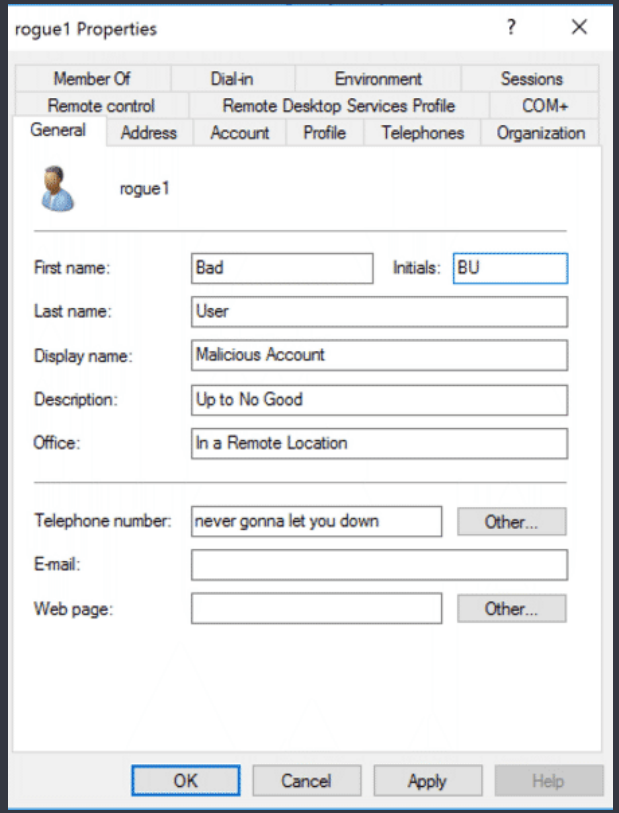
# Reducing your organisations hybrid attack surface
# On-Prem Solutions

# Adopt a Defence in Depth Strategy



# Harden Active Directory

1. Clean Up Stale Objects
2. Don’t Use Complex Passwords – Use Passphrases
3. Don’t Let Employees Have local Admin Accounts On Their Workstations
4. Lock Down Service Accounts
5. Eliminate Permanent Membership In Security Groups
6. Eliminate Admin-Like Permissions Where Possible
7. Stop reusing weak passwords / policies
8. Enable Multi Factor Authentication

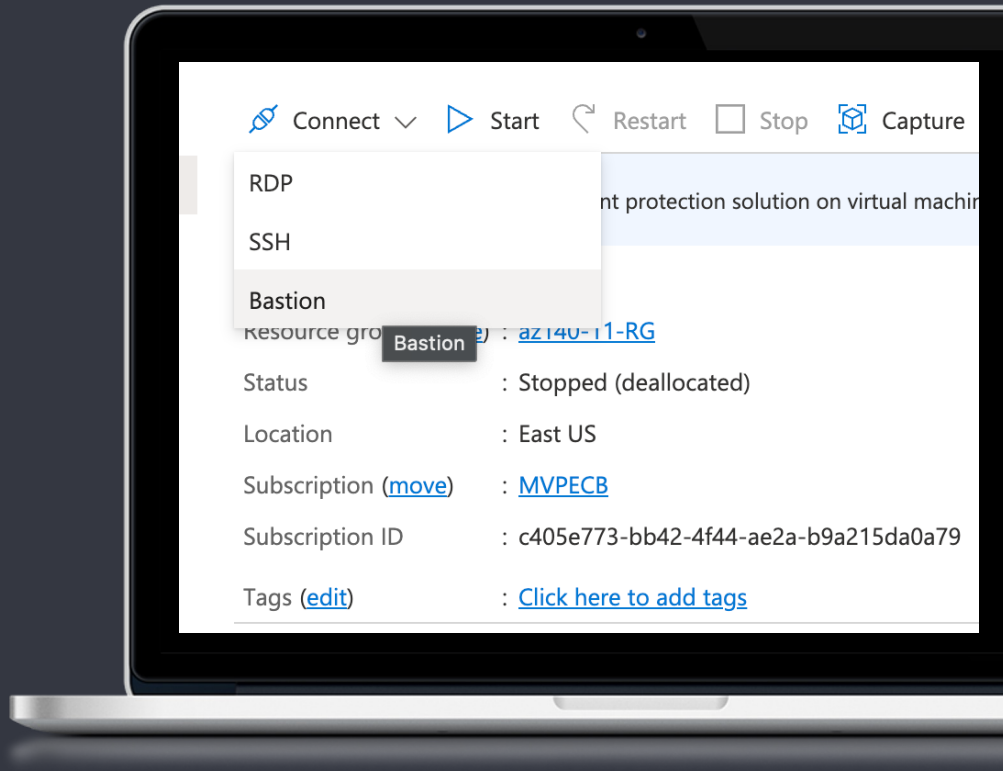


# Demo

ADDS – Clean me up Scotty!

# Consider Relocate your On-Prem DCs to the Cloud

- Critical Servers are protected by vendor
- Numerous redundancy solutions
- Replace venerable on-premise servers
- DCs can be protected by Azure Firewall solution
- Azure Bastion Service enables you to securely and seamlessly RDP & SSH to your VMs in your Azure virtual network, without exposing a public IP on the VM, directly from the Azure portal, without the need of any additional client/agent or any piece of software.
- Once in Hybrid. Remove the PODO TXT record from DNS to increase security.



# Client Hybrid AAD Join

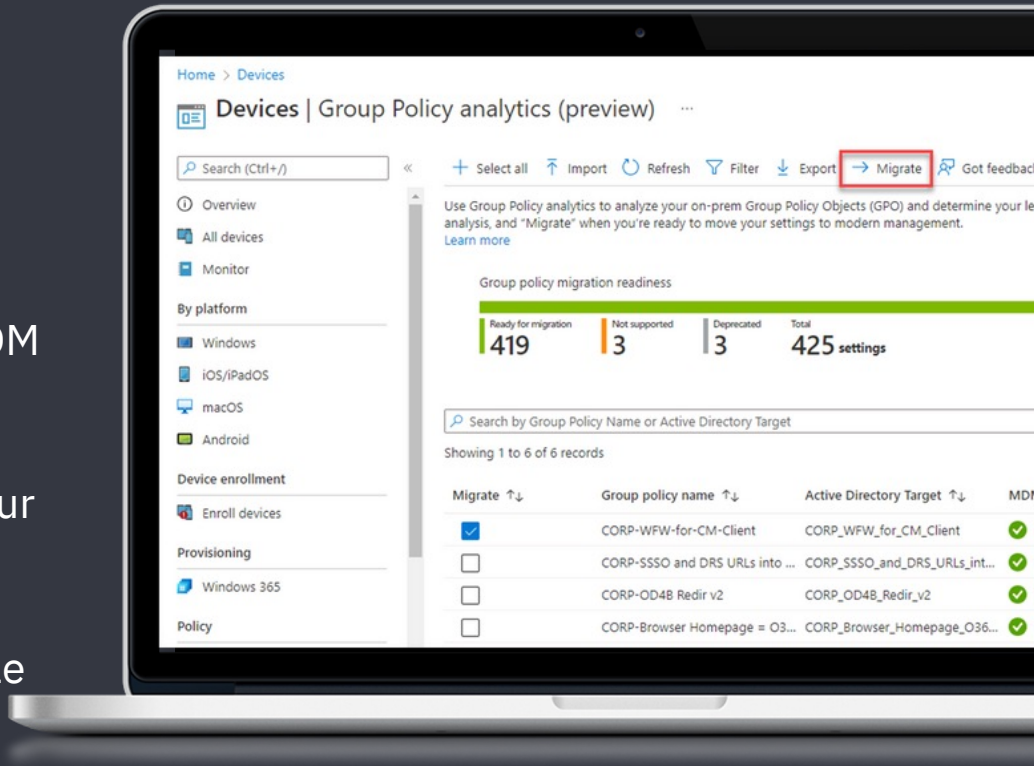
- Hybrid extends existing AD and registers AD joined PCs into AAD to allow for cloud capabilities such as device-based Conditional Access for Domain-Joined PCs
- However, can perpetuate a backwards-facing ‘on-premises centric’ model and reduce (or complicate) some key cloud benefits
- Typical user-based kerberos authentication, such as file-share access and printing, “just works” for sync'd AD users on an AADJ’d PC.
- Situations that require machine-based Kerberos authentication may not work because the AADJ PC doesn't have a computer account in the local AD
- Device Writeback from AAD doesn't create a true computer account in AD)

# Client Azure AD Join?

- AAD device join is forward-facing that brings benefits today & tomorrow, on- & off-prem.
- Allows users to natively join an approved device to your cloud from anywhere, without the need to contact the LAN/AD and establishes the device's foundation for zero trust
- Setup should require MFA as part of the join process
- Backward integration provides nearly 100% compatibility for on-prem resource access from an AADJ PC
- Typical user-based Kerberos authentication, such as file-share access and printing, "just works" for sync'd AD users on an AADJ'd PC.

# What about Group Policy?

- AADJ PCs won't connect to the SYSVOL share on a DC & process GPOs.
- However, MEM supports 1000s of GPO settings directly in the cloud.
- Most settings are now supported to AADJ'd PCs via the Windows built-in MDM channel
- Group Policy Analytics in MEM allows admins to upload a backup/export of your GPOs into MEM, which then evaluates those settings for MDM parity
- The tool can even generate a comparable MDM policy.

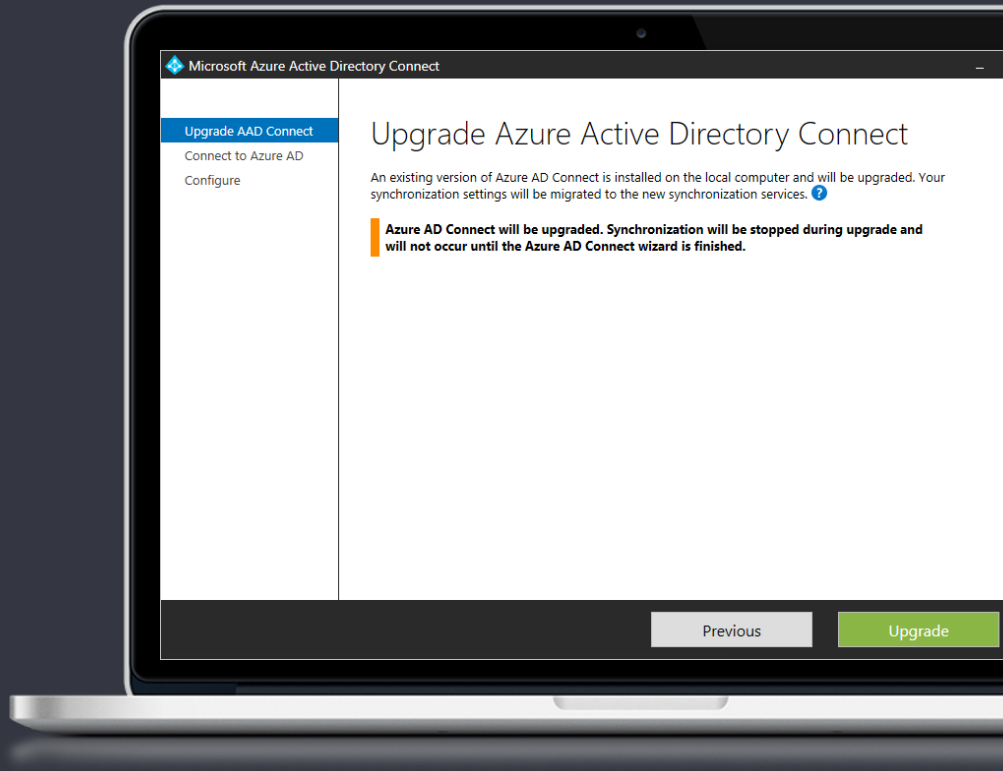


# Harden ADDS - Upgrade Azure AD Connect

- V1.0 was released several years ago.
- Since then, several components have been scheduled for deprecation and updated to newer versions

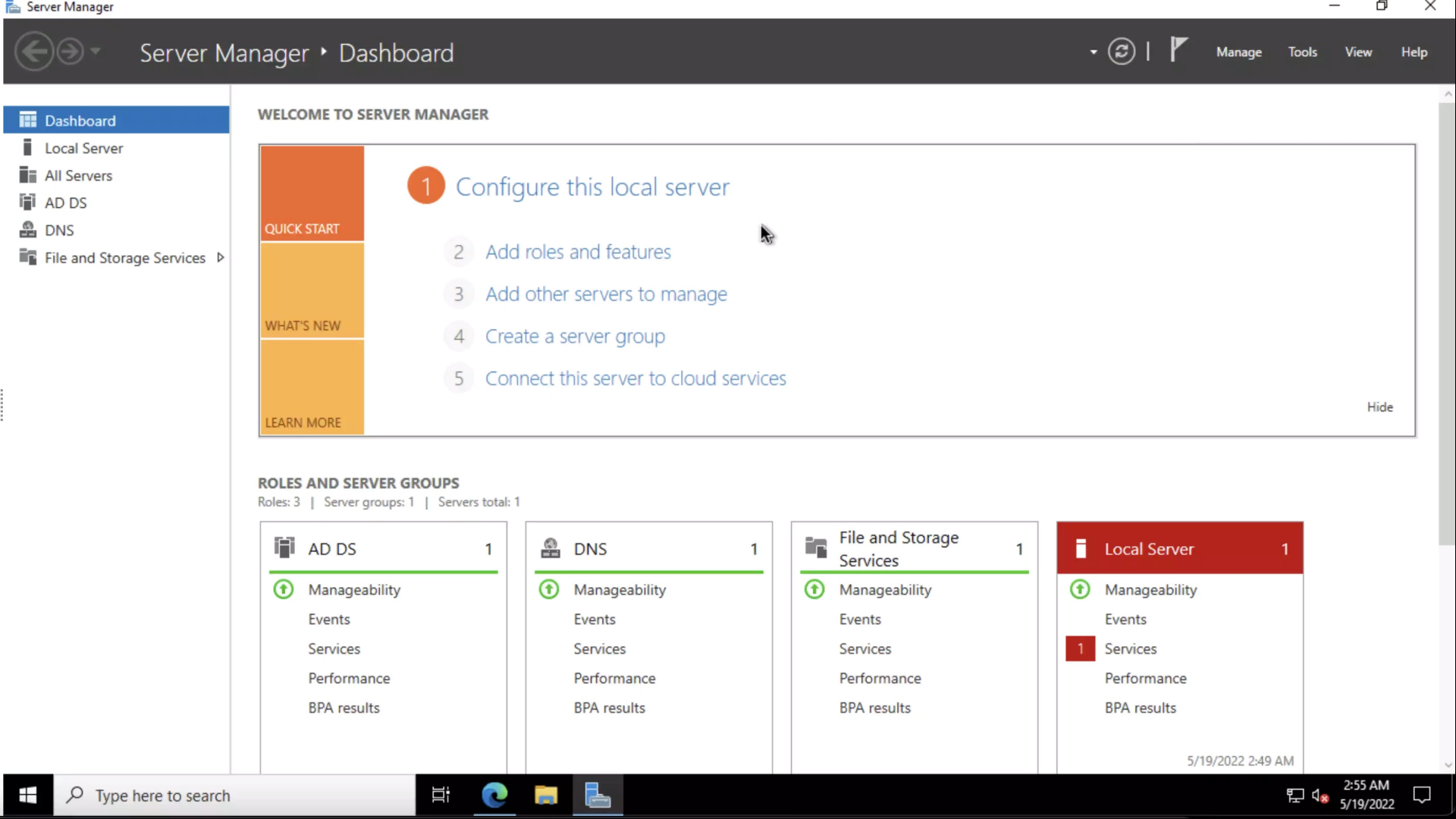
Now Includes

- SQL Server 2019 LocalDB
- MSAL authentication library
- Visual C++ Redist 14
- TLS V1.2
- All binaries signed with SHA2
- Windows Server 2012 and Windows Server 2012 R2 are no longer supported
- PowerShell 5.0 Support



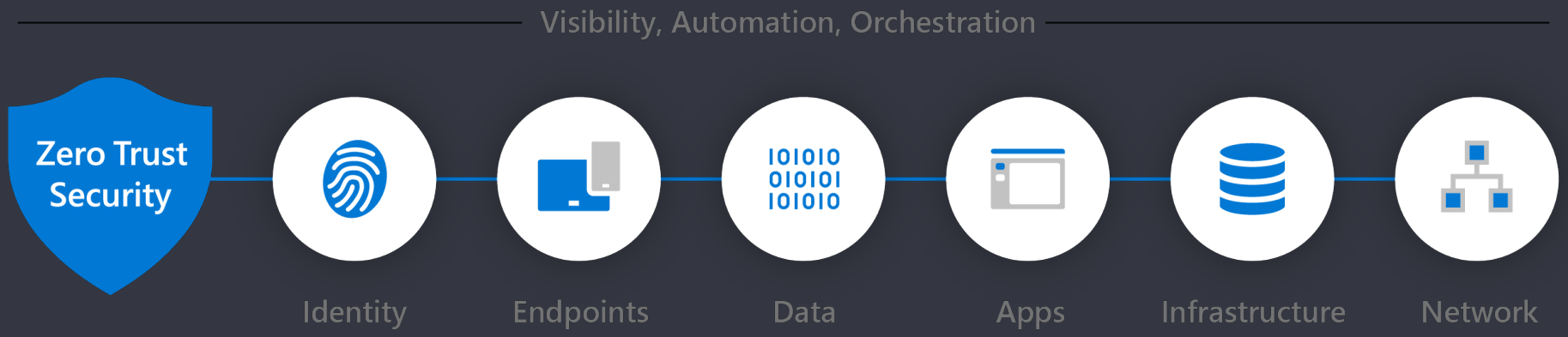
# Demo

Time to think alternate: Azure AD CloudSync

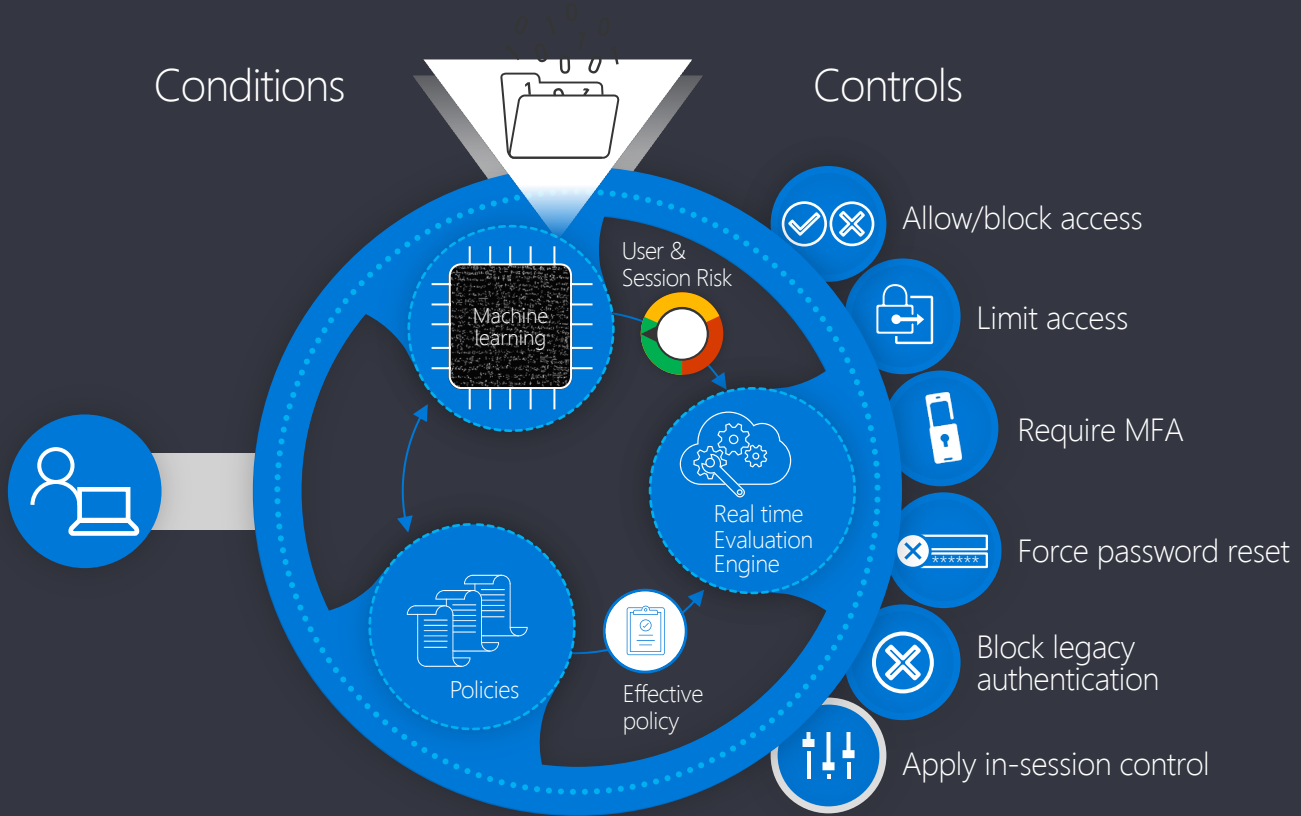

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DNS 1
Manageability
Events
Services
Performance
BPA results
File and Storage Services 1
Manageability
Events
Services
Performance
BPA results
Local Server 1
Manageability
Events
1 Services
Performance
BPA results
5/19/2022 2:49 AM
Type here to search
2:55 AM
5/19/2022

# Reducing your organisations hybrid attack surface
# Cloud Solutions

# Adopt a Zero Trust Posture



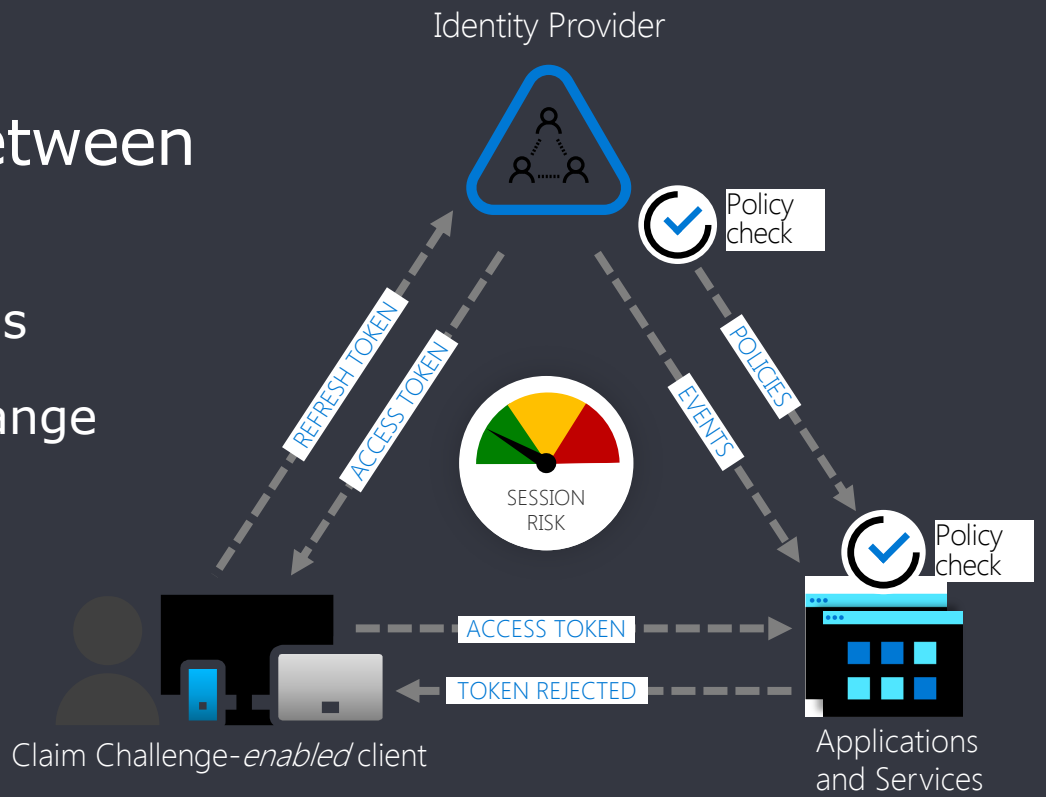
# Azure AD Conditional Access



# Continuous Access Evaluation Protocol (CAEP)

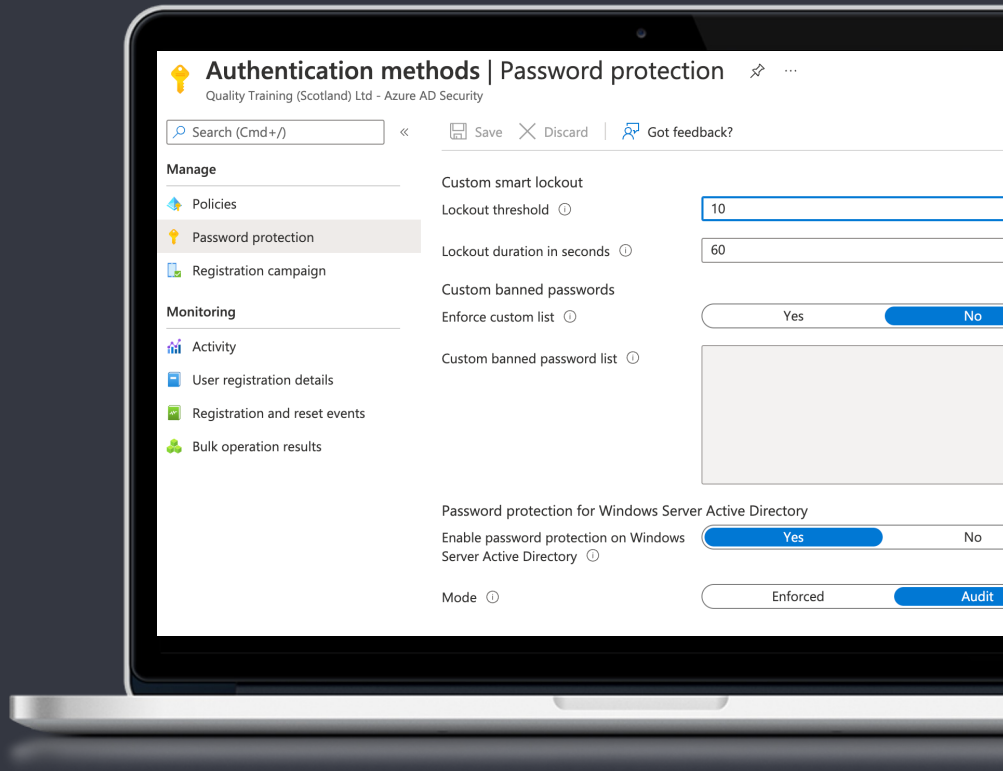
## Risk conversations between IdPs and applications

- IdPs can interrupt sessions
- Apps can alert IdPs to change



# Hardening ADDS – Enable Password Protection

- Azure Active Directory (Azure AD) Password Protection provides a global and custom banned password list.
- A password change request fails if there's a match in these banned password list
- To protect on-prem AD DS environments, install and configure Azure AD Password Protection to work with your on-prem DC.
- Simply register the Azure AD Password Protection proxy service & Password Protection DC agent in your on-prem environment and you’re good to go



# Make you Hybrid Data Immutable

- Archived data is fixed, unchangeable, and cannot be modified, encrypted or deleted.
- Immutable backups are a critical component of your organisation's business strategy and data recovery plan.
- This type of archived data cannot be altered or changed, and it is impervious to malicious deletion or ransomware encryption.
- Keeping immutable backups on air-gapped server media adds an additional layer of security to ensure you have a recent copy of your 'kidnapped' encrypted data.

# Make you Data Immutable

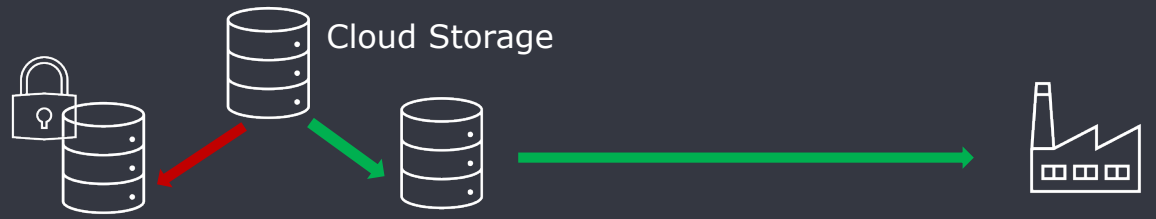
Label & Classify your important data with Rights Management technologies, such as Information Protection & Encryption

Establish Data Loss Prevention Policies (DLP) to prevent data leaks of your most sensitive data

Adopt solid Data Retention Policies as part of your overall Disaster Recovery / Business Continuity Plan.(DRP/BCP)

# Make you Data Immutable

- AAA Security Controls
- Hardening
- Native Immutability
- Data Management
- Data Analytics
- Deduplication
- Encryption




+

- Immutability
- Off Site Backup
- Elastic
- Multi Tier Solution

# Review

Slides and demos from the conference will be available at

**https://github.com/nordicinfrastructureconference/2022**