Hybrid Active Directory Attacks: Anatomy and Defenses

identiverse

#identiverse

Derek Melber

VP of Product Engagement and Outreach

QOMPLX

derek.melber@qomplx.com

Goals for today

- Identity is the new security boundary
- Hybrid AD for most organizations
- Attacker tactics
- Securing on-prem AD
- Securing Azure AD

Azure Active Directory

Identity is the new security boundary

Azure Active Directory

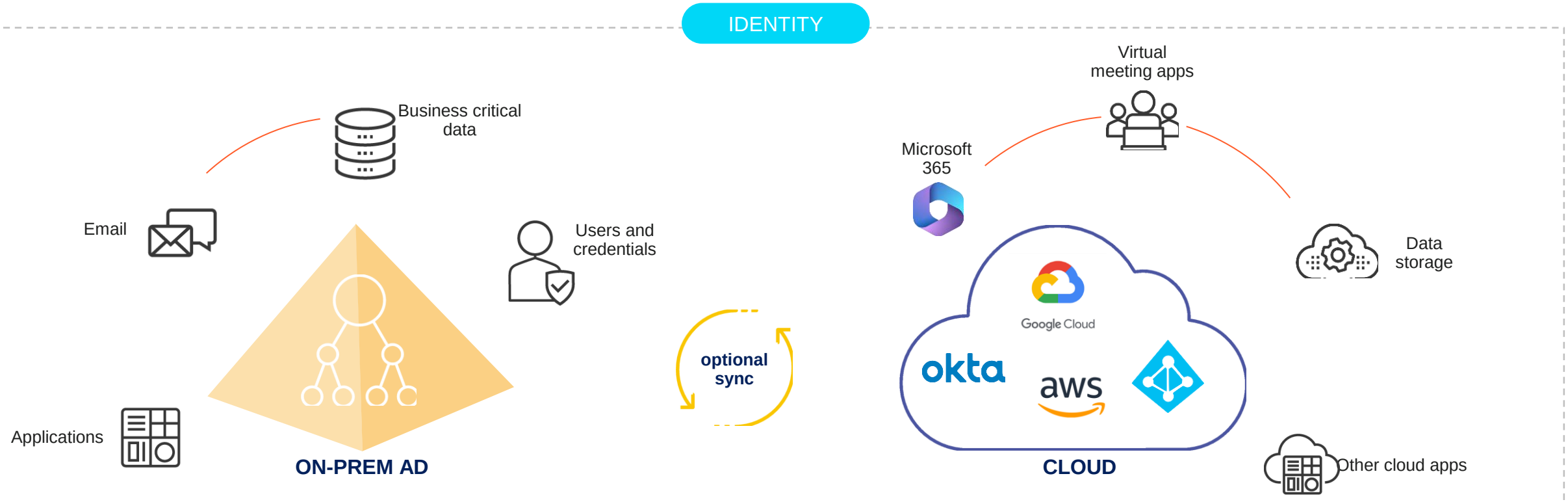
- Cloud identity as target
  - 94% - Enterprises using cloud
  - 88% - Cloud breaches due to human error
  - 75% - Enterprises focusing on cloud security

ON-PREM AD

- AD identity as target
  - 90% - Est attacks involve AD in some form
  - 50% - Orgs experiencing AD attack in last 2 years
  - 40% - Attacks successful due to bad AD hygiene

Hybrid AD for most organizations

Identity – the heart of every organization



AD vs AAD

- Not the same (but you know that)
- Most organizations are hybrid (but you know that)
- Just because you care more about AAD, doesn't make it more important
  (bet you never considered that)
- AAD is just as messed up as AD (but you never considered that)
- AAD has just as many avenues for attackers as AD (bet you did not think that was the case)

Attacker Tactics

Typical Attack Tactics

0. Target recognition
1. Phishing and exploits on selected targets
2. Initial entry point compromise
3. Local privilege escalation
4. Company's infrastructure cartography
5. Lateral movement
6. Credentials replay on privileged accounts
7. Privileges escalation on AD
8. Post exploitation (persistence, backdooring)

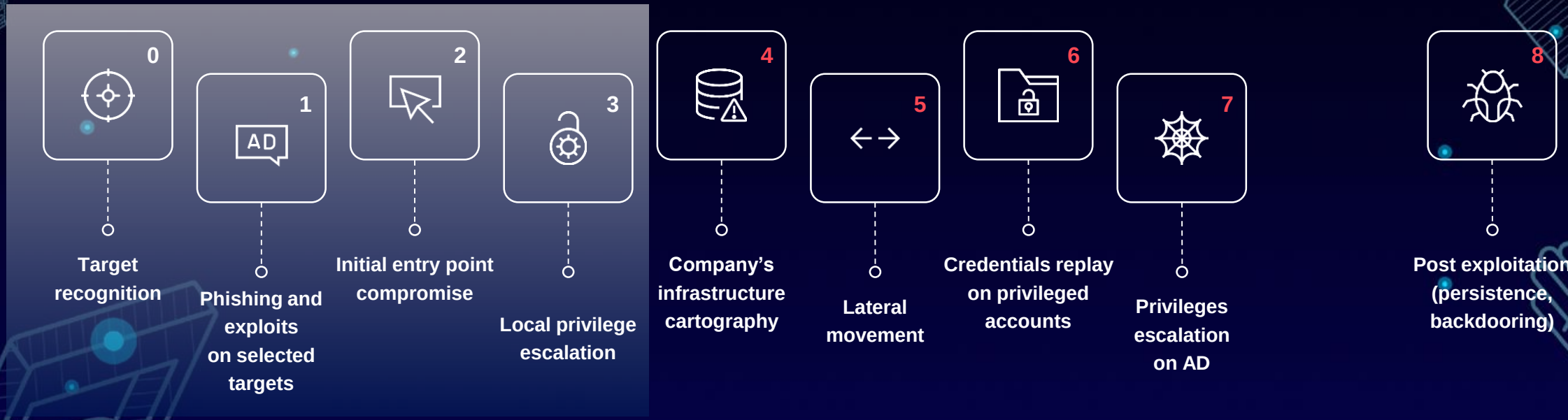
Attacker Tactics:

- Exploit vulnerabilities and misconfigurations
- Mine credentials
- Install enumeration tools

Current identity solutions

SECURITY TECHNOLOGIES:

PAM / MFA / IGA / AM / CIEM



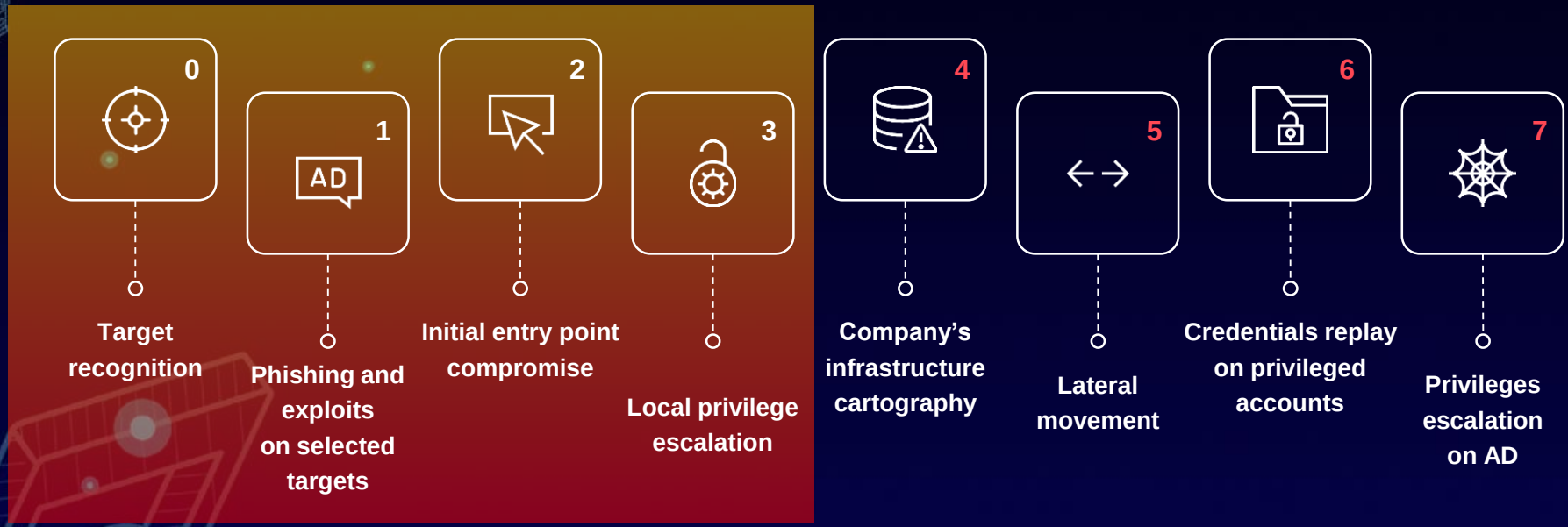
Attacker Tactics:

- Exploit vulnerabilities and misconfigurations
- Mine credentials
- Install enumeration tools

Current identity solutions

SECURITY TECHNOLOGIES:

PAM / MFA / IGA / AM / CIEM



Identities not secured

Securing On-prem AD

Ensure exploitable configurations are correct

- Privileged users with SPNs
- Unconstrained Kerberos Delegations
- Privileged Primary group ID
- Privileged SIDHistory
- Incorrect adminSDHolder entries
- Shadow Admins
- …

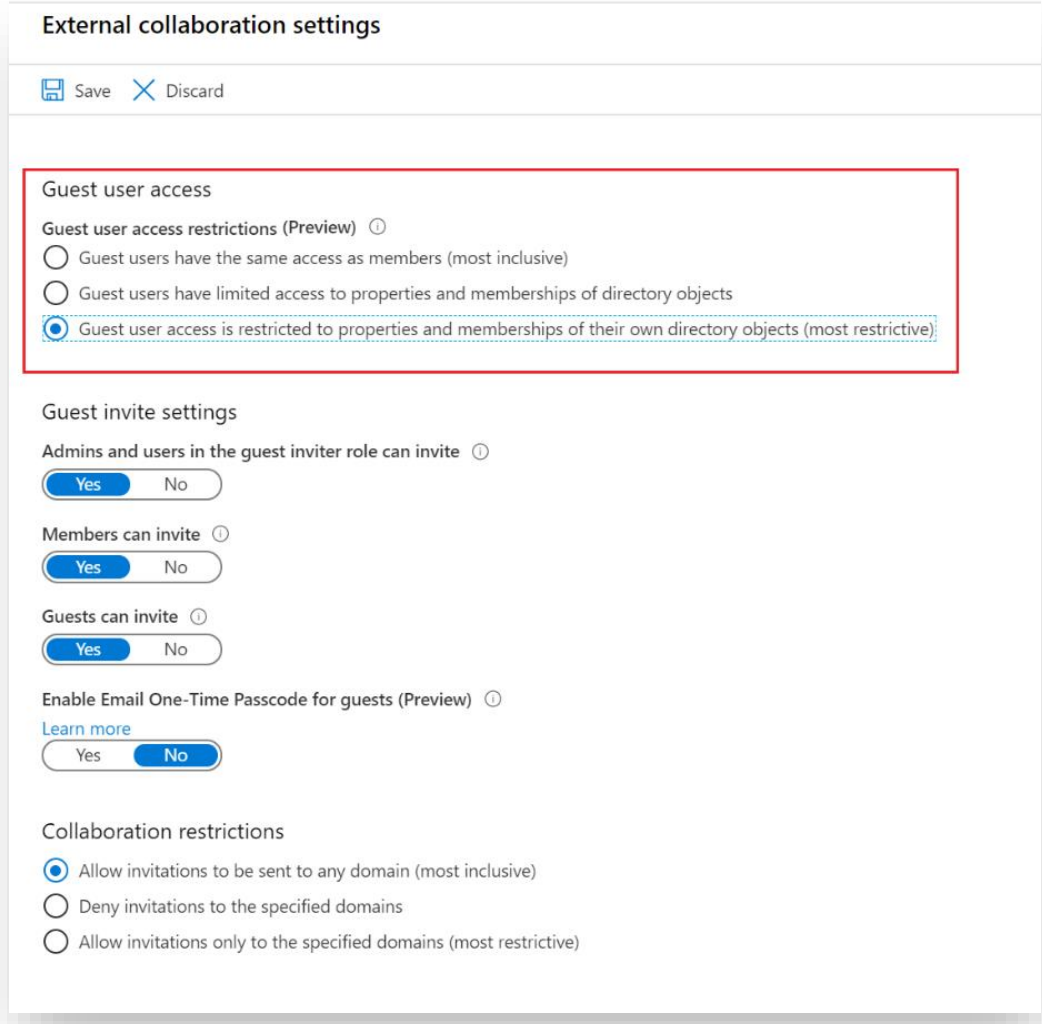
Securing Azure AD

Controlling AAD guests

- “Guest users have the same access as members”
- “Guest users have limited access to properties and memberships of directory objects”
- “Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)”

What can I get from AAD with guest?

- “Guest users have limited access to properties and memberships of directory objects”
  - Guest users can’t list objects
  - Guest users can read object properties
    - Users and contacts
    - Groups
    - Applications
    - Devices
    - Organization
    - Roles and scopes
    - Subscriptions
    - Policies


External collaboration settings
Save
Discard
Guest user access
Guest user access restrictions (Preview)
Guest users have the same access as members (most inclusive)
Guest users have limited access to properties and memberships of directory objects
Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)
Guest invite settings
Admins and users in the guest inviter role can invite
Yes
No
Members can invite
Yes
No
Guests can invite
Yes
No
Enable Email One-Time Passcode for guests (Preview)
Learn more
Yes
No
Collaboration restrictions
Allow invitations to be sent to any domain (most inclusive)
Deny invitations to the specified domains
Allow invitations only to the specified domains (most restrictive)

Azure AD Connect

- Utility installed on-premise
  - Has a high-privilege account in AD
  - Has also a high-privilege account in Azure AD
  - High value target!

```
PS C:\Users\baasbob> Get-ADUser -LDAPFilter "(samAccountName=MSOL_*)" -properties name,description | select name,descrip
tion | fl


name        : MSOL_206b1a1ede1f
description : Account created by Microsoft Azure Active Directory Connect with installation identifier
              206b1a1ede1f490e9c5caa0debc0523a running on computer o365-app-server configured to synchronize to tenant
              frozenliquids.onmicrosoft.com. This account must have directory replication permissions in the local
              Active Directory and write permission on certain attributes to enable Hybrid Deployment.
```

PowerShell Copy

```
Get-ADSyncADConnectorAccount
```

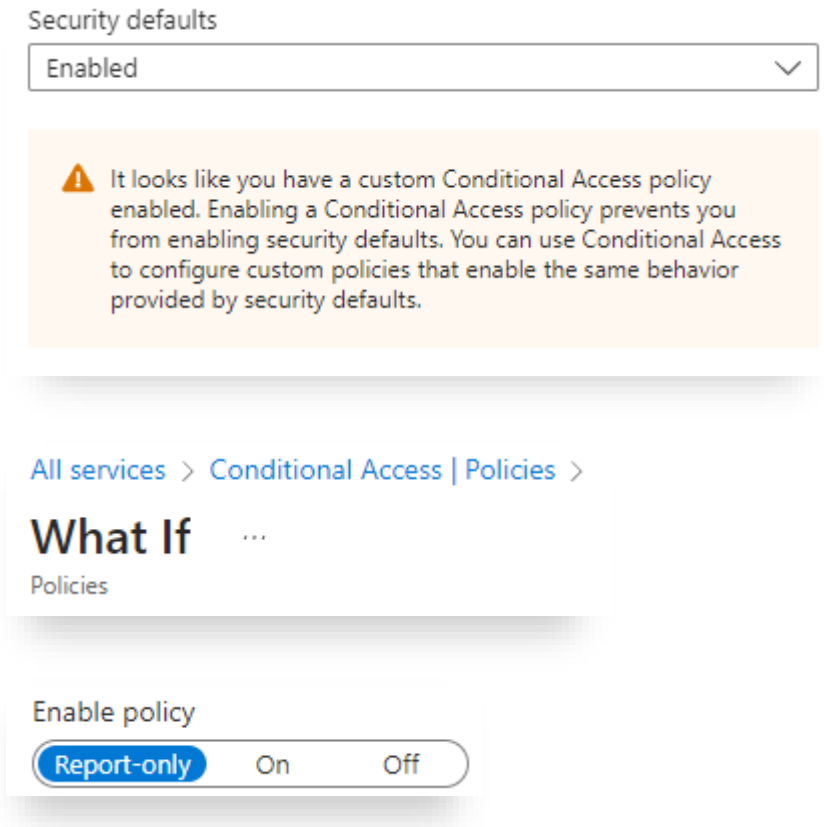
(Part of ADSyncConfig Module)

What can Sync account do?

- Dump all on-premise password hashes (if PHS is enabled)
- Log in on the Azure portal (since it’s a user)
- Bypass conditional access policies for admin accounts
- Add credentials to service principals
- Modify service principals properties
- Modify/backdoor/remove conditional access policies
- Perform a DCSync with AD!

Conditional Access Policies

- Default
  - Properties – Manage Security Defaults
- Creation of a new one
  - Default is trumped
- Difficult to know what is actually in place!
  - Who has MFA?
  - When is MFA required?



Tier 0 Principals

One of the following AzureAD admin roles:

- Global Administrator
- Privileged Role Administrator
- Privileged Authentication Administrator
- Authentication Policy Administrator

One of the following MS Graph app roles:

- RoleManagement.ReadWrite.Directory
- AppRoleAssignment.ReadWrite.All
- Policy.ReadWrite.AuthenticationMethod
- Organization.ReadWrite.All

Protect Tier 0 principals:

- Recommendations:
- Ensure MFA is enabled and enforced for Tier 0 principals where feasible
- Make sure the apps are not asking to be over permissioned
- Treat Organization.ReadWrite.All as a highly privileged operation
- Don’t give out app-only Organization.ReadWrite.All to any app
- Don’t allow apps you don’t trust to have delegated Organization.ReadWrite.All
- Ensure Tier 0 principal activities are carefully monitored for any suspicious activity

THANK YOU!

Derek Melber

derek.melber@qomplx.com

identiverse

#identiverse