Microsoft Security

The Ultimate Guide for Protecting Hybrid Identities in Entra ID

Dr Nestori Syynimaa (@DrAzureAD)

Microsoft Threat Intelligence

Contents

Hybrid Identity

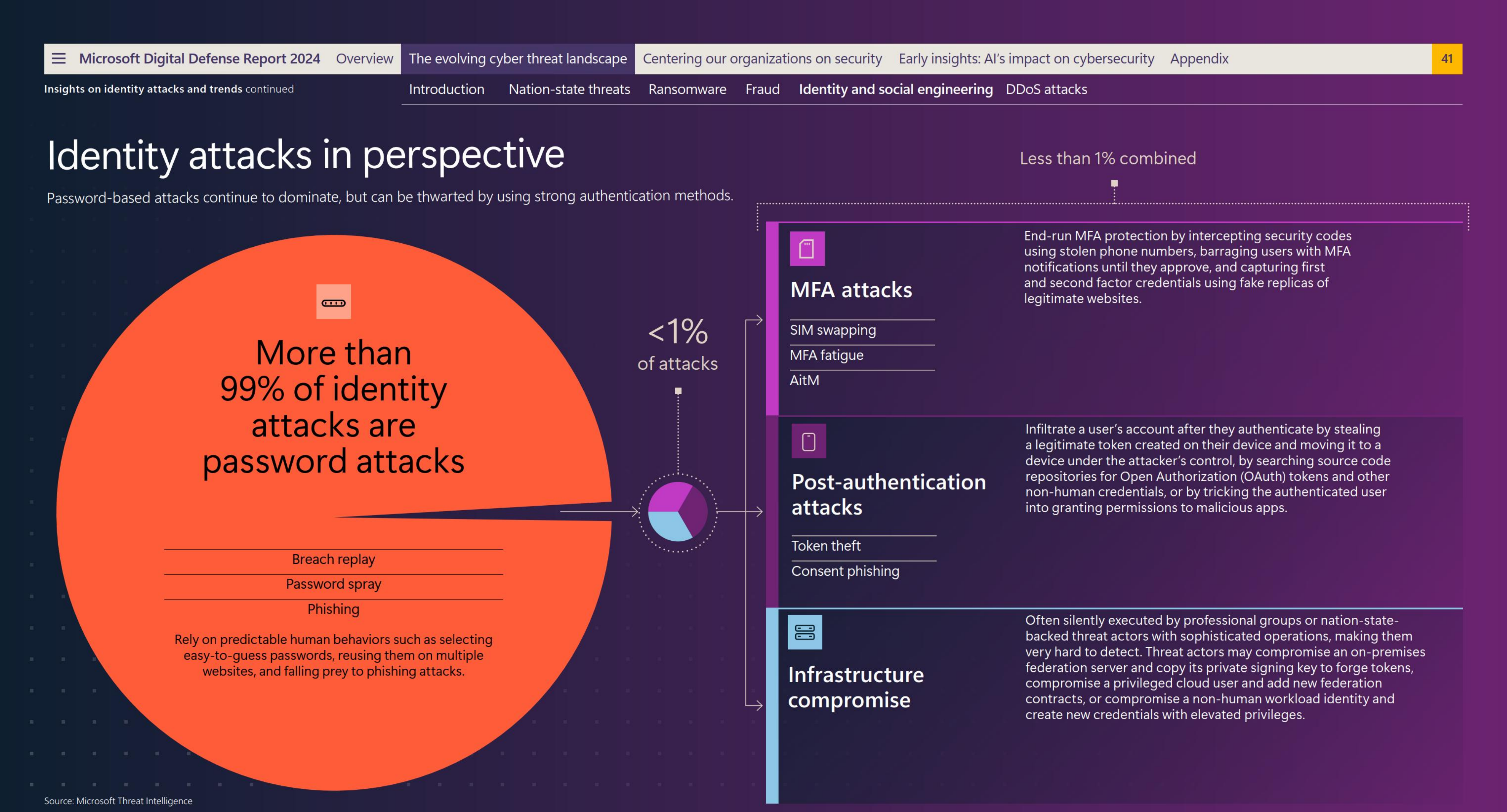
Entra Connect Sync

Entra Cloud Sync

Pass-Through Authentication (PTA)

Identity Federation (+ AD FS)

> **Hackers don’t break in, they log in**
>
> Corey Nachreiner
> CSO, WatchGuard



Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

More than 99% of identity attacks are password attacks

- Breach replay
- Password spray
- Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1% of attacks

Less than 1% combined

MFA attacks

- SIM swapping
- MFA fatigue
- AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.

Post-authentication attacks

- Token theft
- Consent phishing

Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.

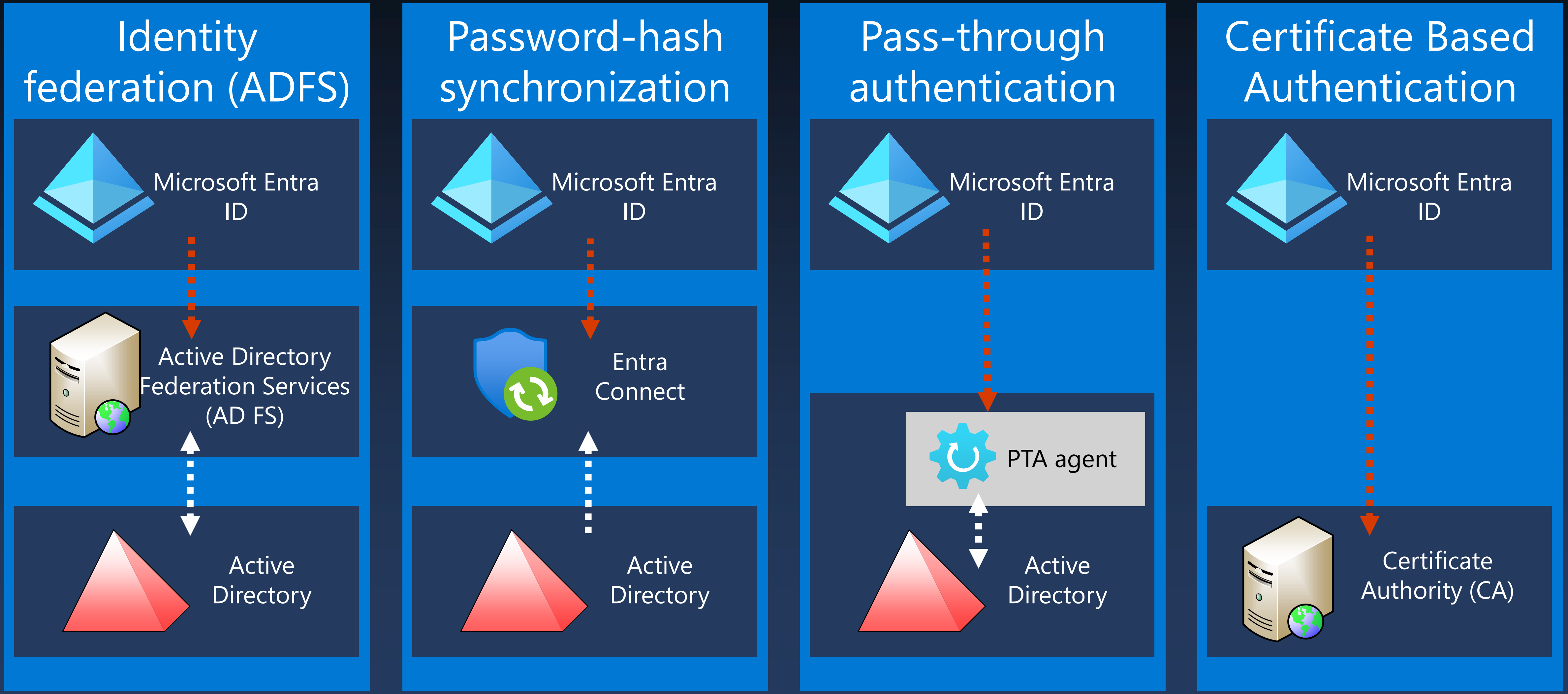
Infrastructure compromise

Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Source: Microsoft Threat Intelligence

https://www.microsoft.com/en-gb/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

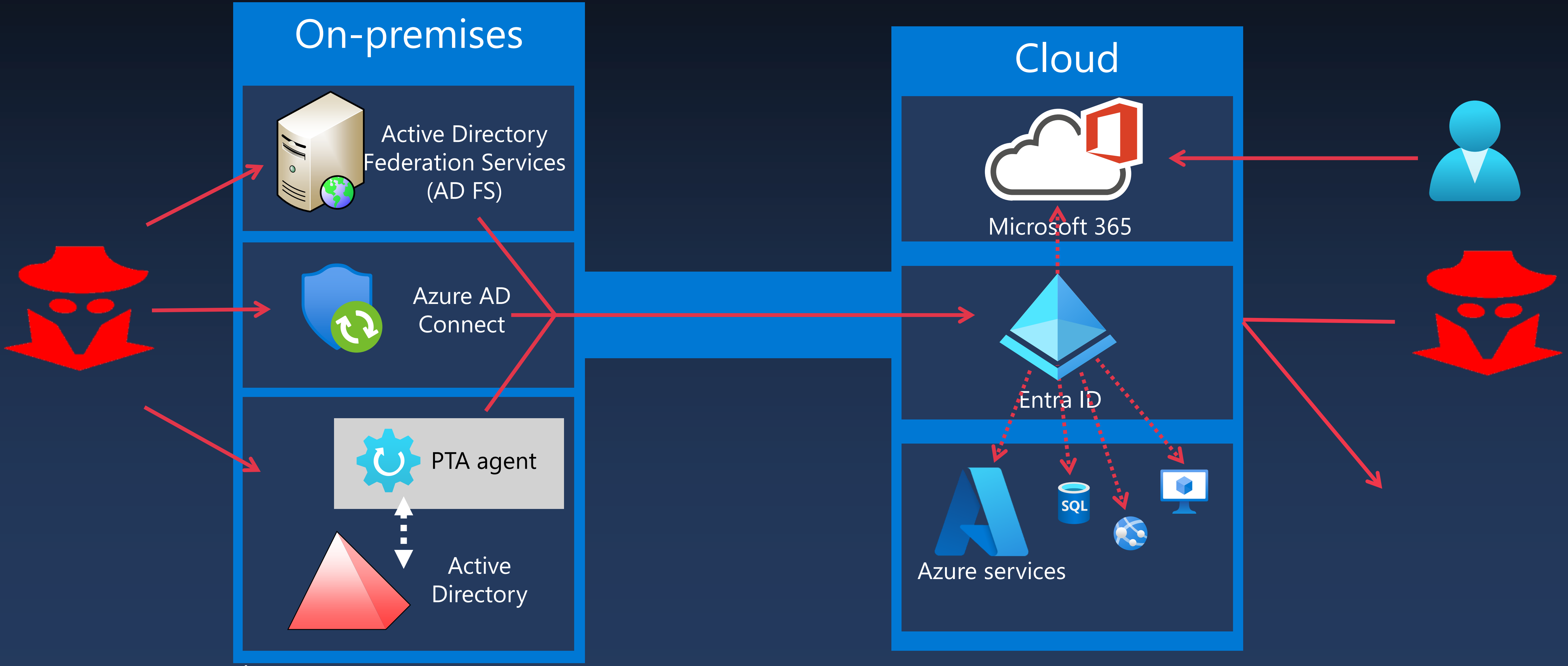
Hybrid Authentication Options


Identity federation (ADFS)
Microsoft Entra ID
Active Directory Federation Services (AD FS)
Active Directory
Password-hash synchronization
Microsoft Entra ID
Entra Connect
Active Directory
Pass-through authentication
Microsoft Entra ID
PTA agent
Active Directory
Certificate Based Authentication
Microsoft Entra ID
Certificate Authority (CA)

Source: Secureworks

* Supports seamless single sign-on

(Hybrid) Cloud Security



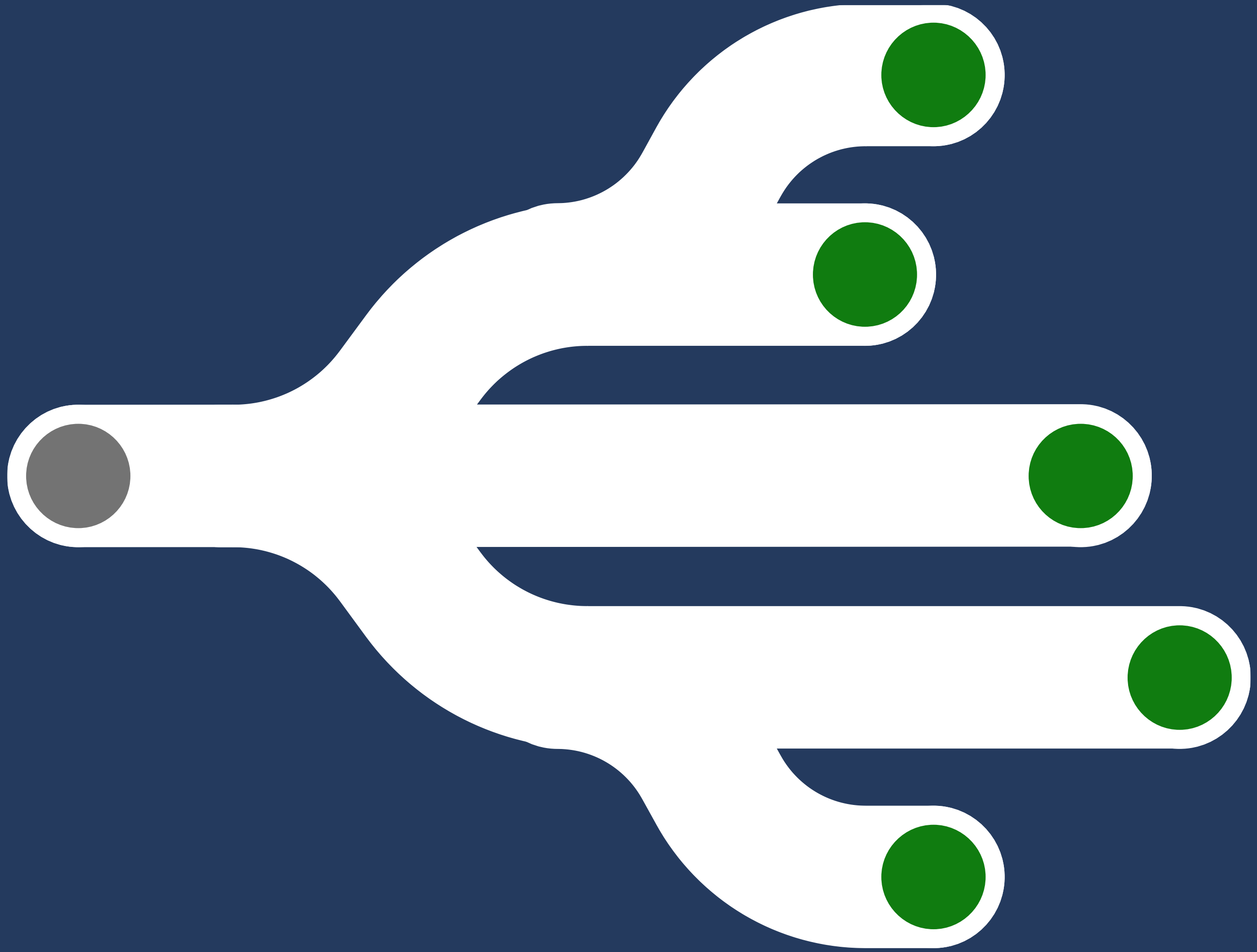
Source: Secureworks

> Biggest problem with network defense is that defenders think in lists. Attackers think in graphs.
>
> As long as this is true, attackers win.

John Lambert

Corporate Vice President, Security Fellow, Microsoft

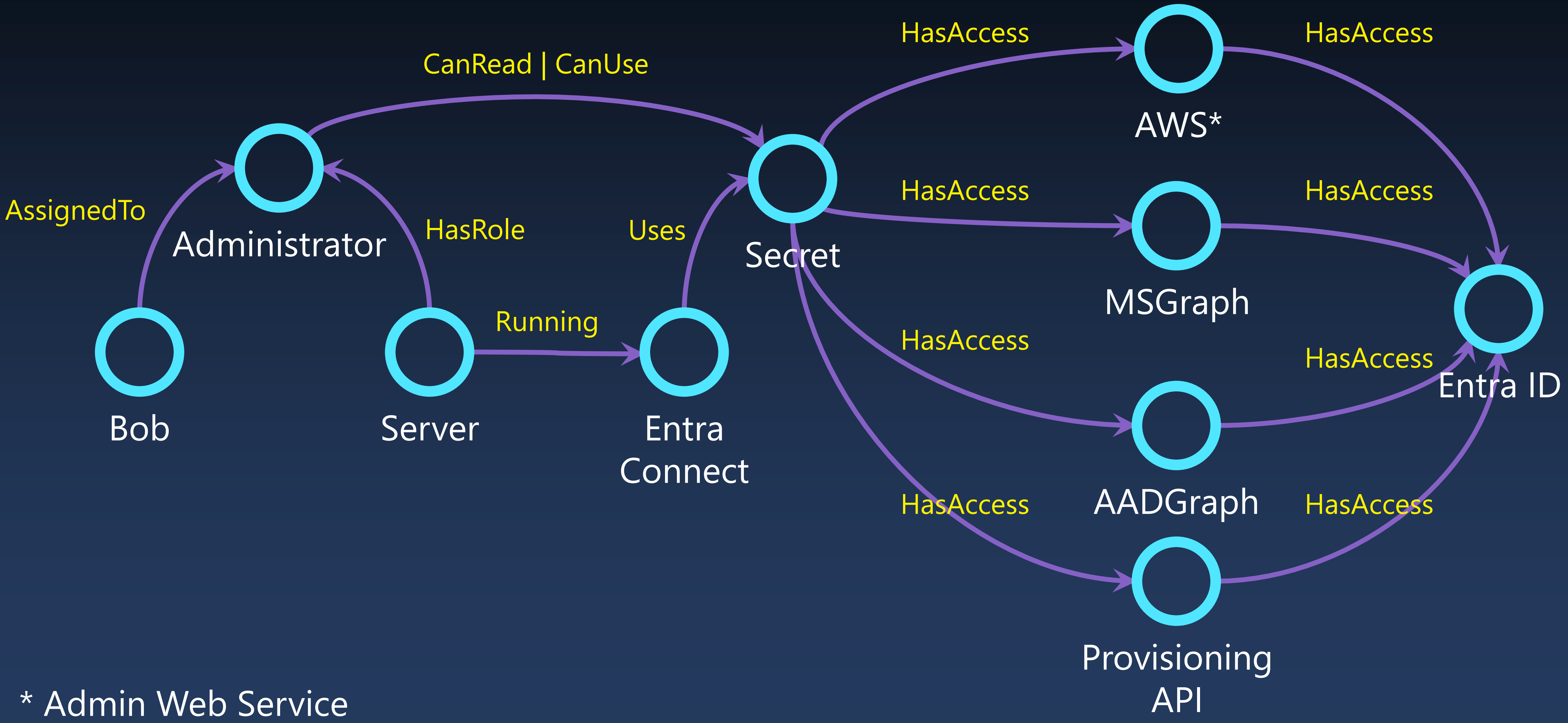
Entra Connect Sync



Entra Cloud Connect

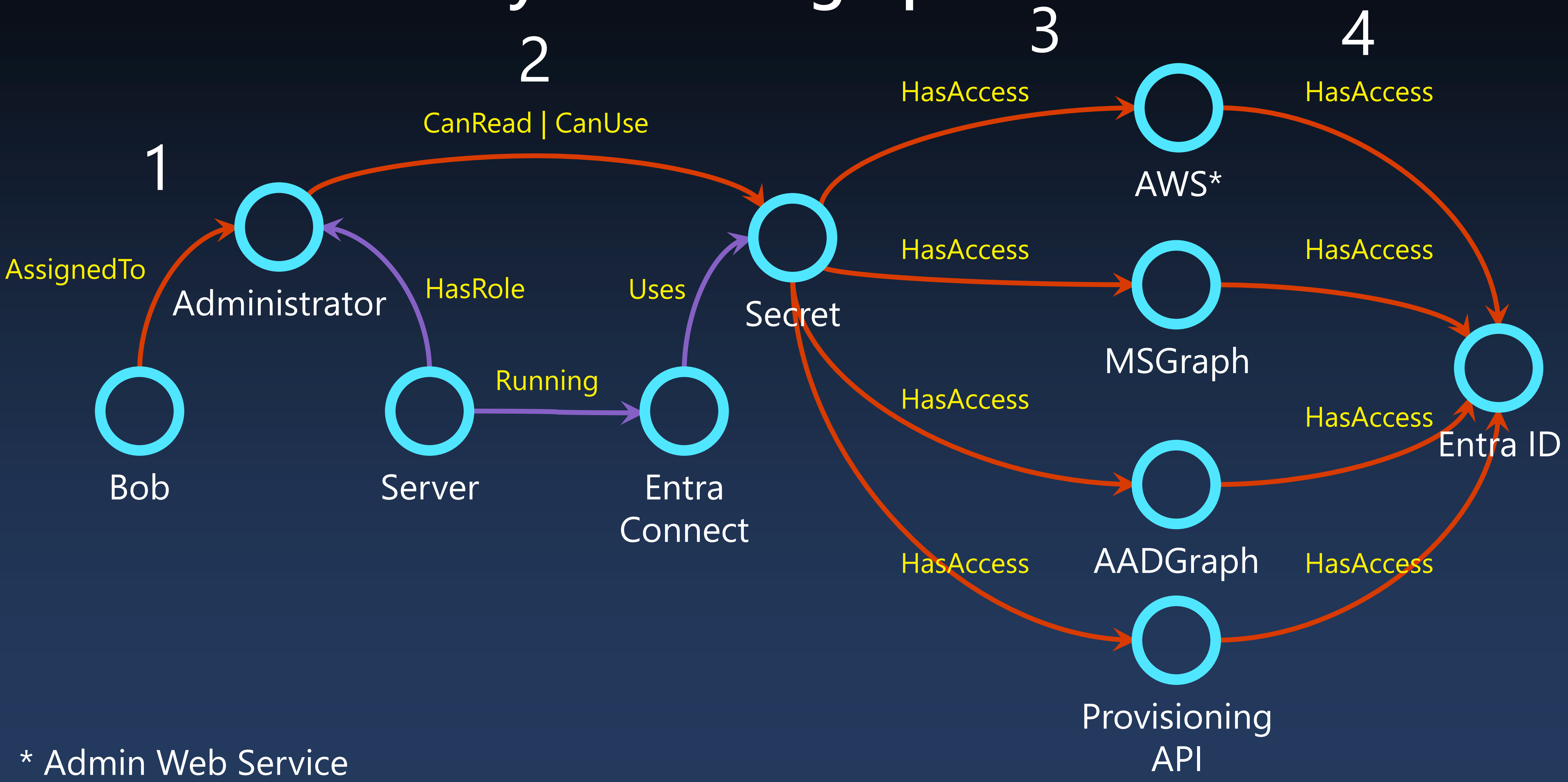
- Synchronises objects between Entra ID and on-premises AD
- Uses Entra ID *user* or *application* identity

Entra Connect Sync attack graph



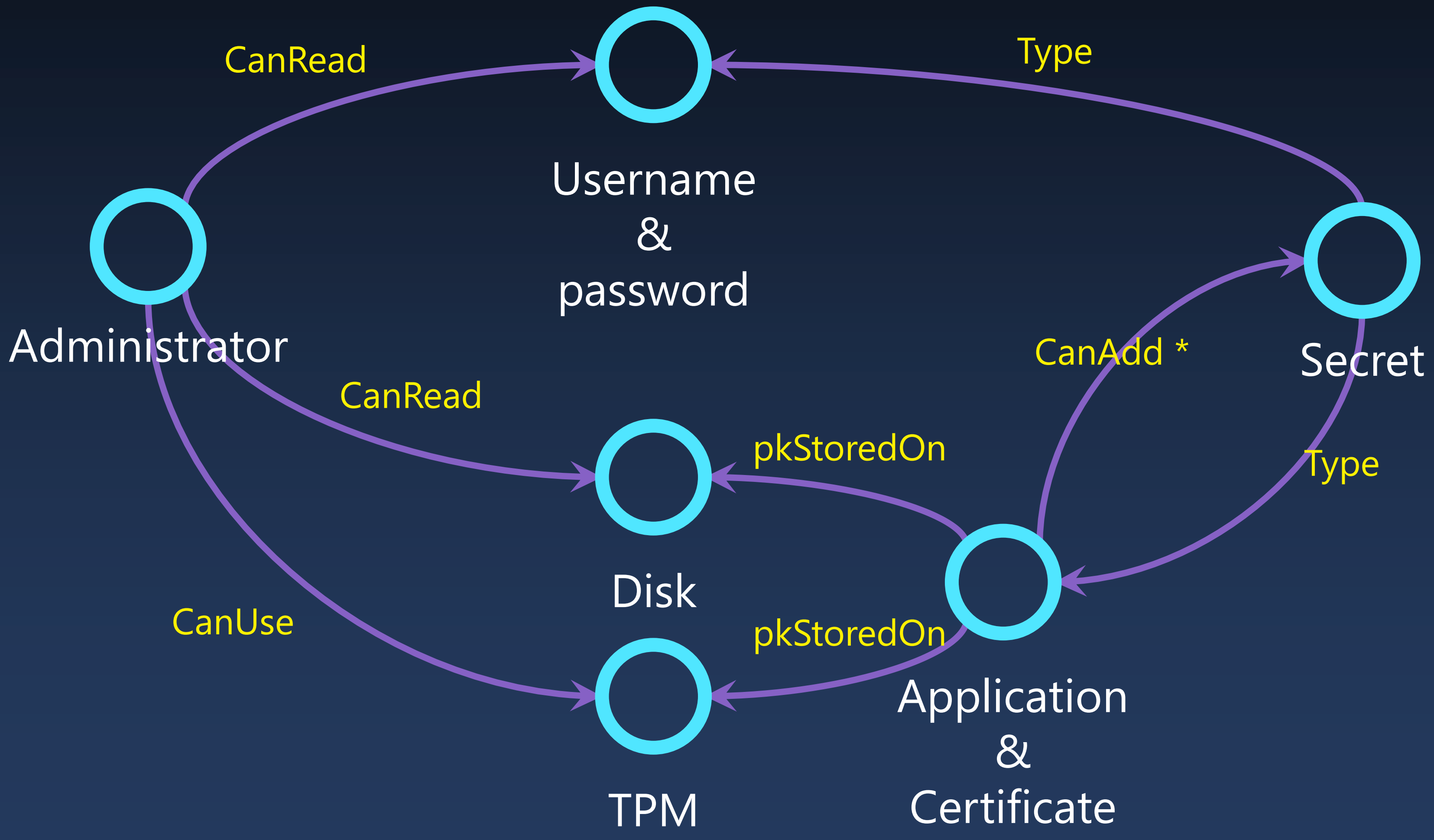
* Admin Web Service

Entra Connect Sync attack graph



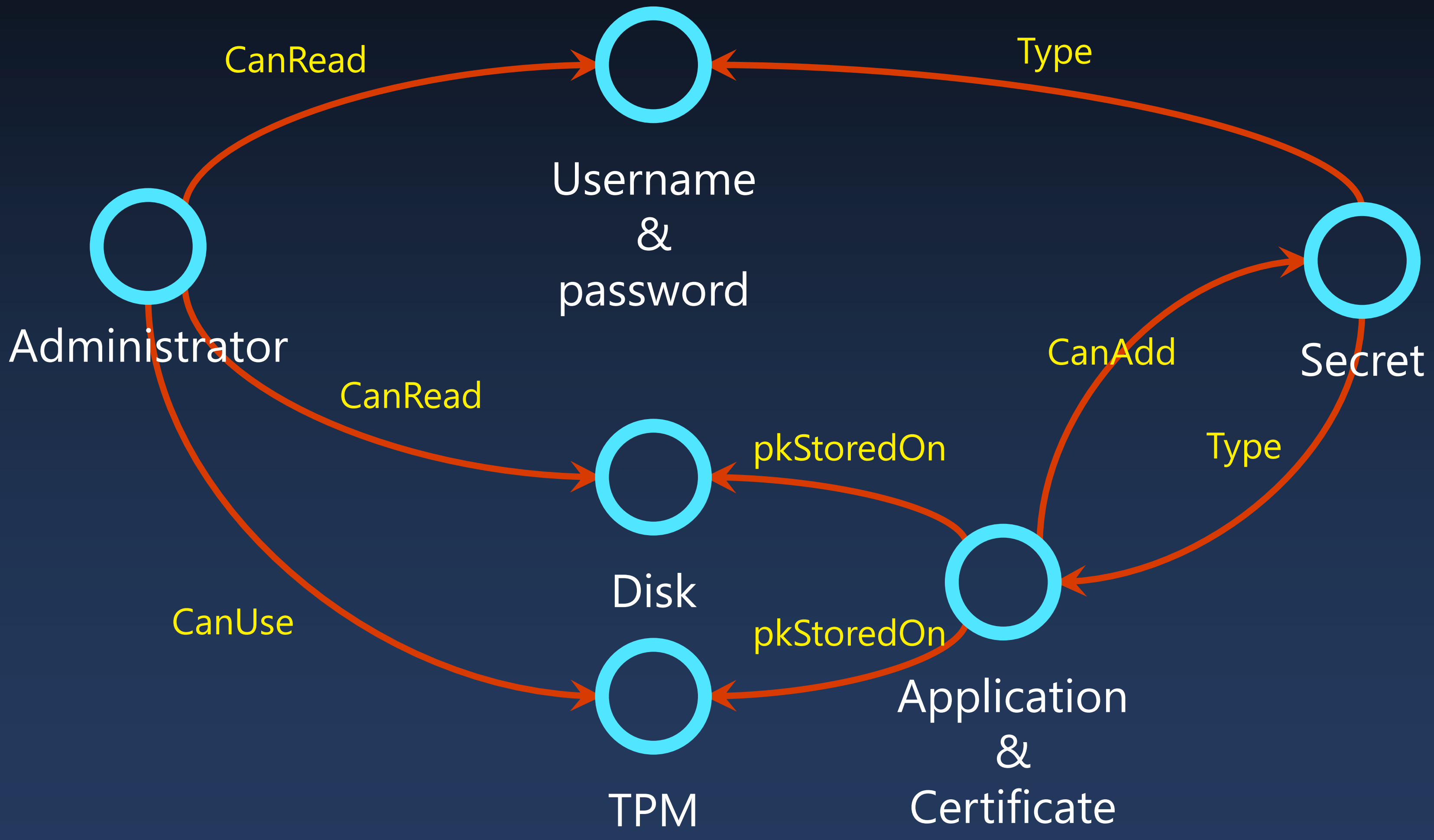
* Admin Web Service

2. Access to secret

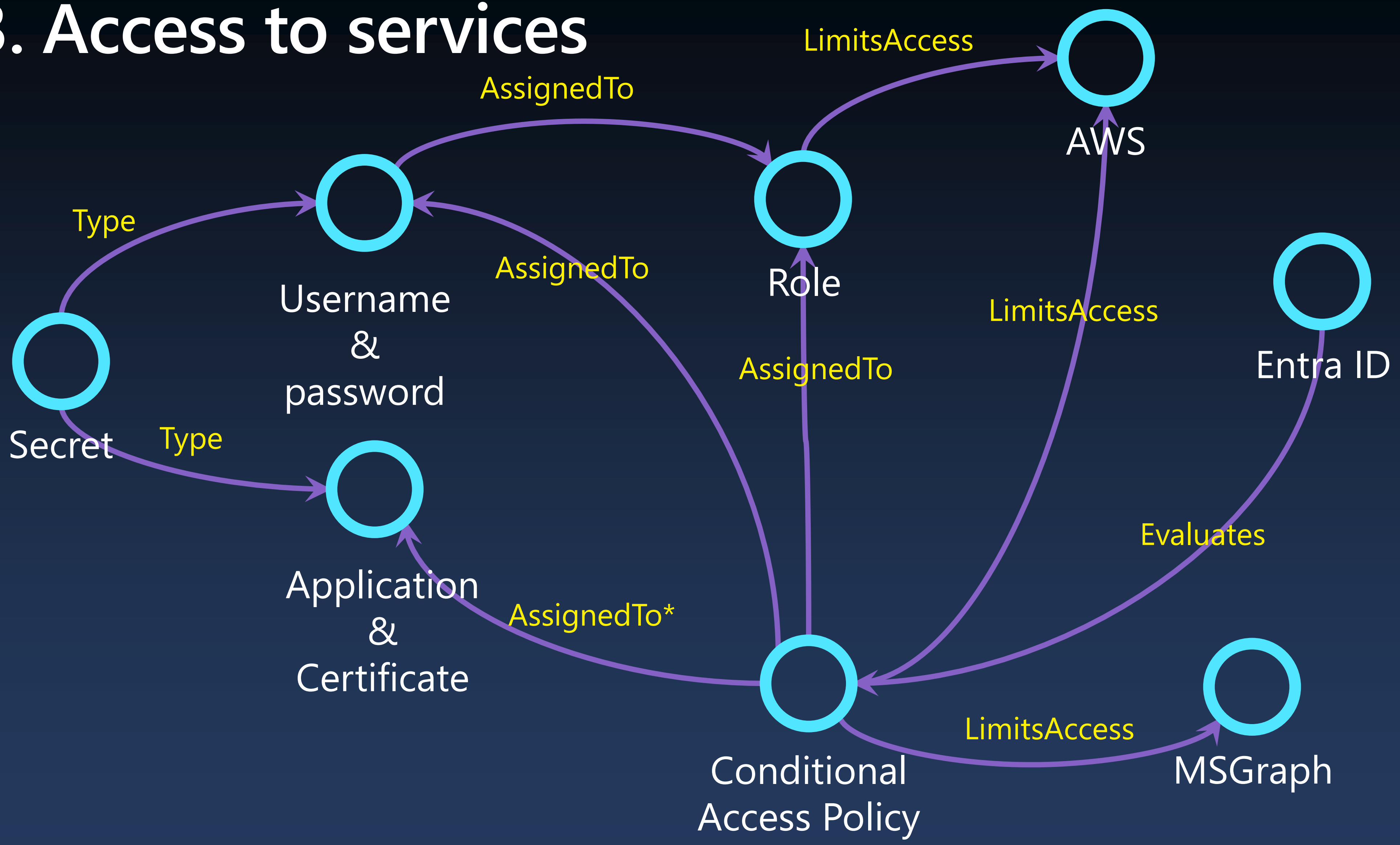


* https://specterops.io/blog/2025/06/09/update-dumping-entra-connect-sync-credentials/

2. Access to secret

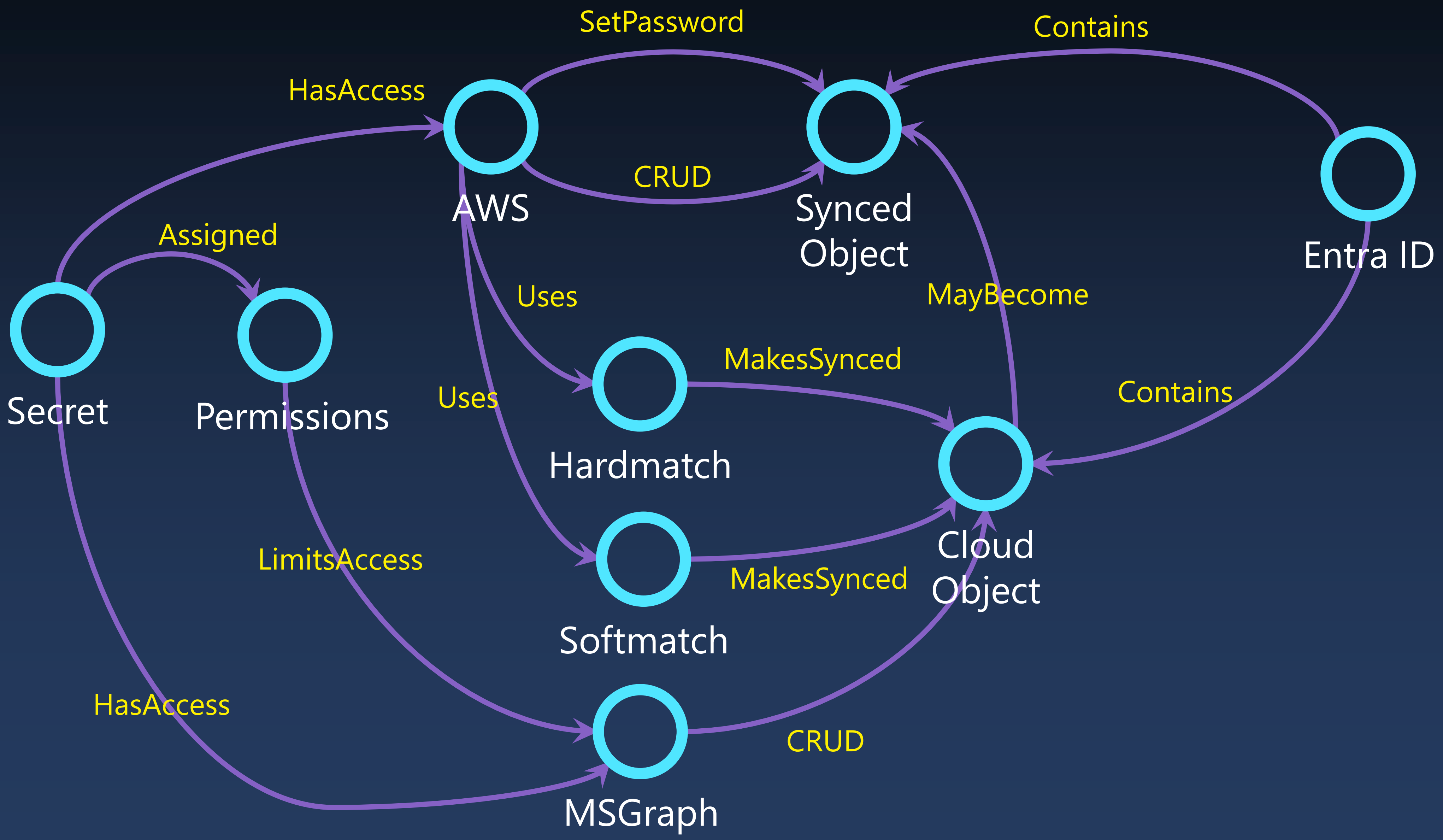


3. Access to services



* Workload identities https://learn.microsoft.com/en-us/entra/workload-id/workload-identities-overview

4. Access to Entra ID

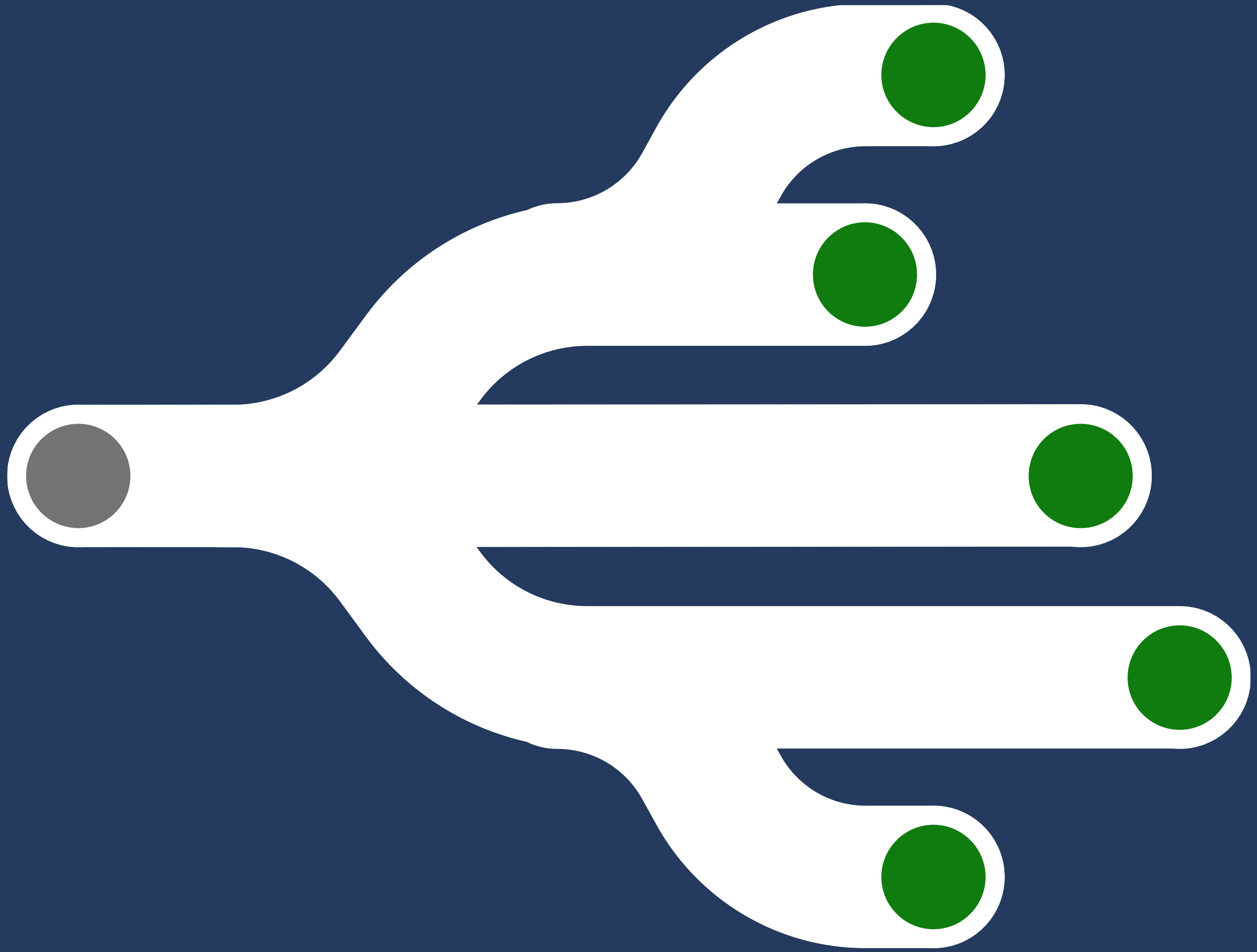


Protecting Entra ID Connect Sync

Area	Action
Limit access to server	Limit number of local administrators, POLP[1]
Limit access to secret	Use application identity with TPM[2]
Limit access to services	Use Conditional Access Policy to limit access, requires Workload Identities for application identity[3]
Limit access to Entra ID	Block all soft and hard match[4] features, POLP

1. Principle Of Least Privilege
2. https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/authenticate-application-id
3. https://learn.microsoft.com/en-us/entra/workload-id/workload-identities-overview
4. https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-syncservice-features

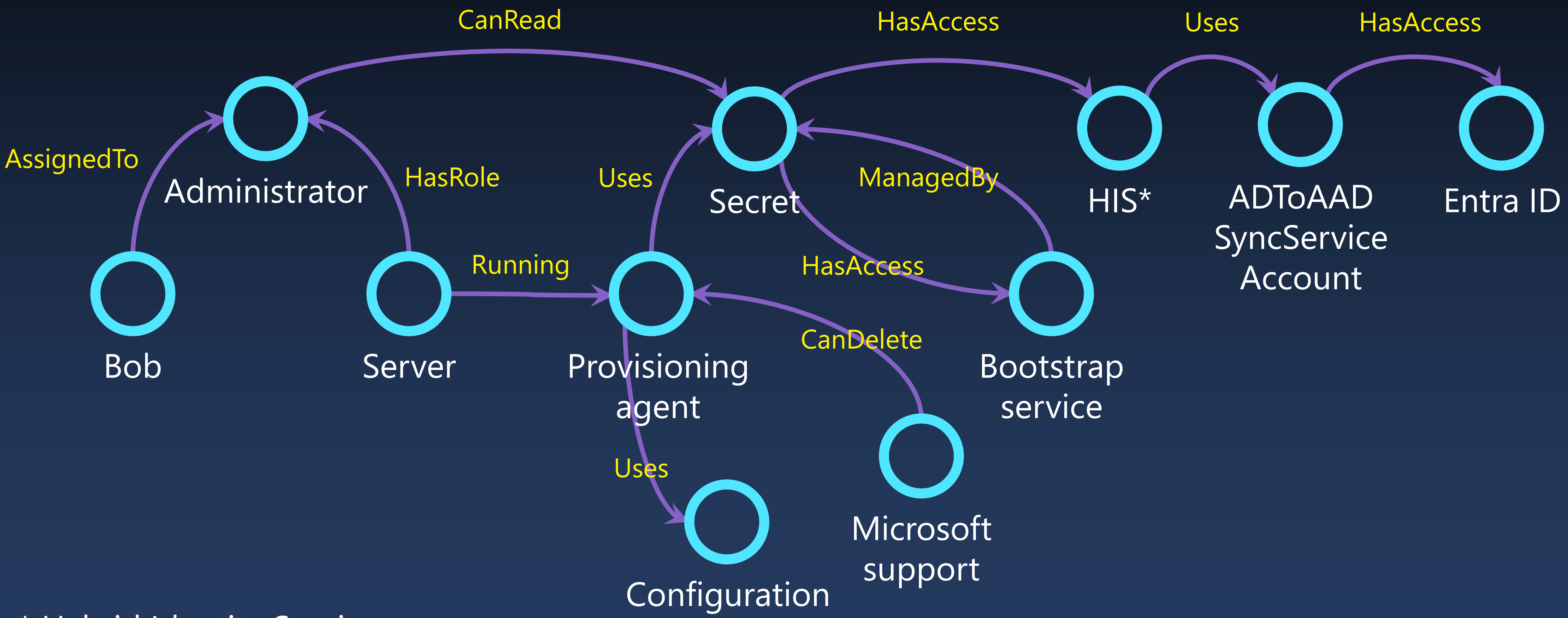
Entra Cloud Sync



Entra Cloud Sync

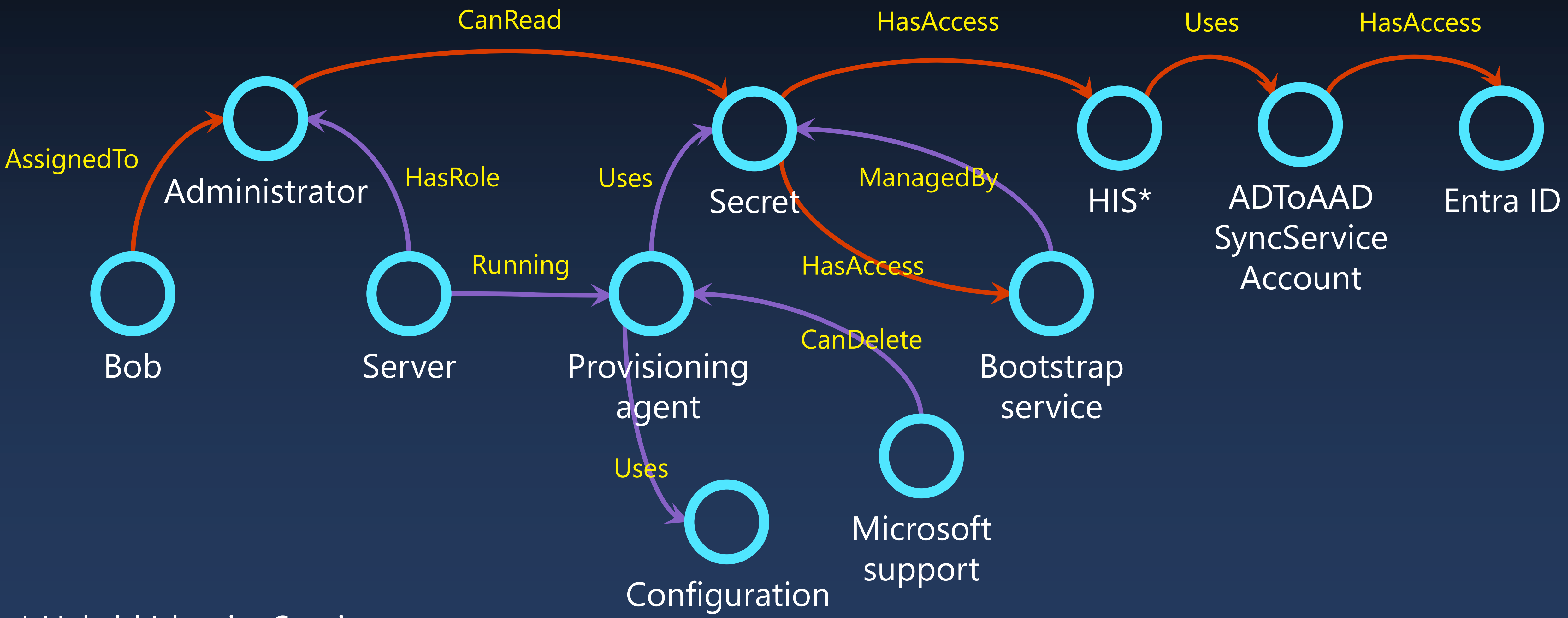
- Synchronises objects between Entra ID and on-premises AD
- Uses certificate based authentication (CBA)

Entra Cloud Sync attack graph (overview)



* Hybrid Identity Service

Entra Cloud Sync attack graph (overview)



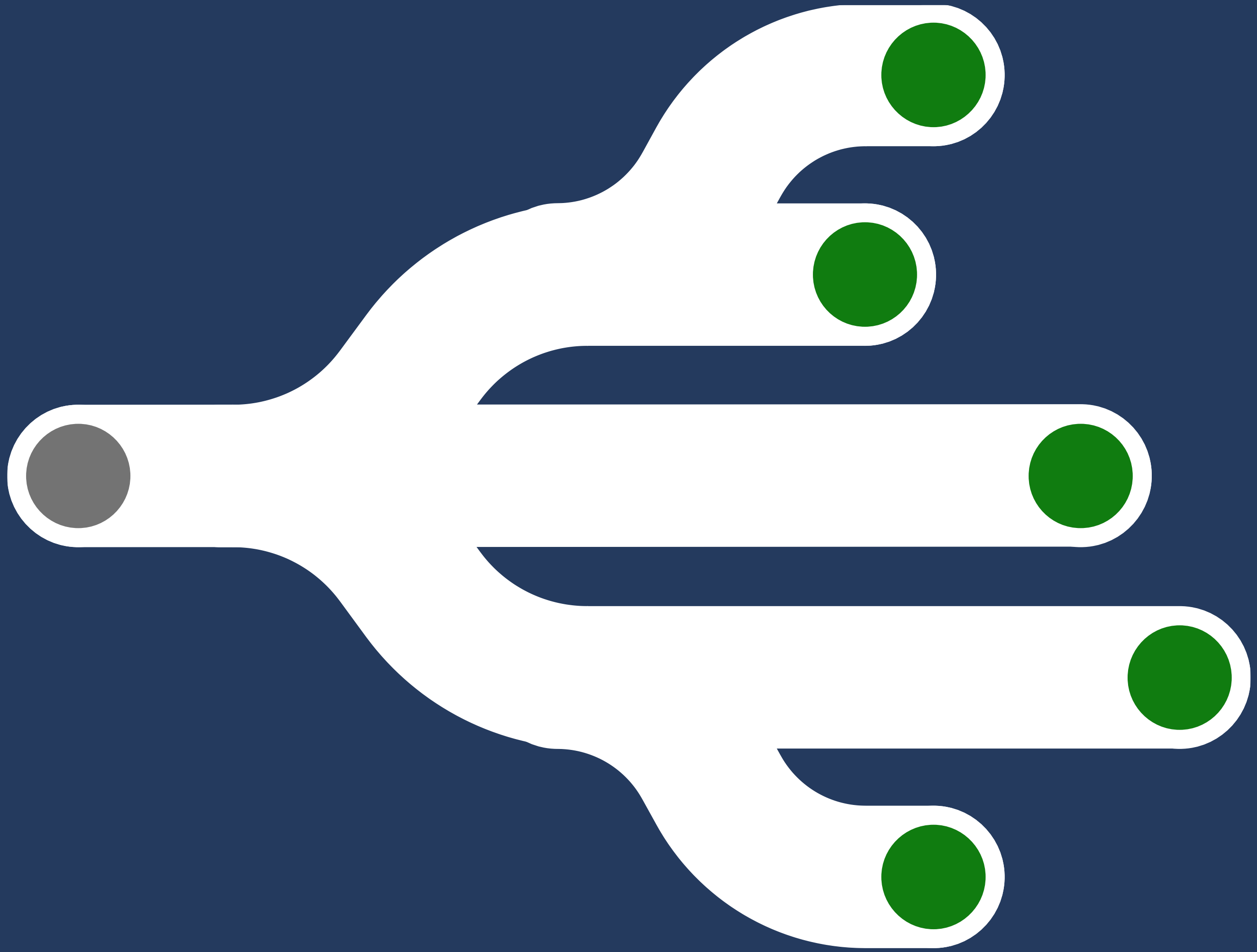
* Hybrid Identity Service

Protecting & mitigating Entra Cloud Sync

Area	Action
Limit access to server	Limit number of local administrators, POLP[1]
Prevent access to services	Delete configuration[2] Contact Microsoft support to delete compromised agent(s)
Prevent access to Entra ID	Disable or remove *ADToAADSyncServiceAccount*

1. Principle Of Least Privilege
2. https://portal.azure.com/#view/Microsoft_AAD_Connect_Provisioning/CloudSyncMenuBlade/~/CloudSyncConfigurations

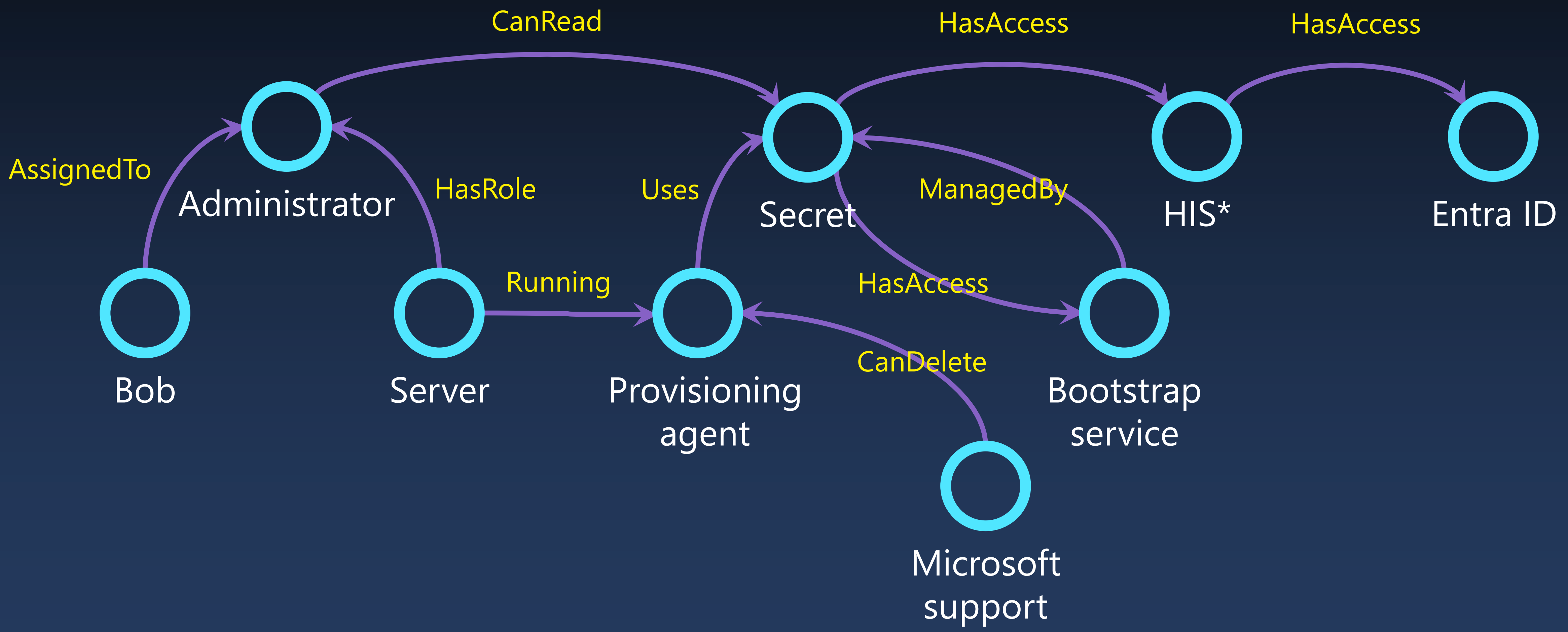
Pass-Through Authentication



Pass-Through Authentication (PTA)

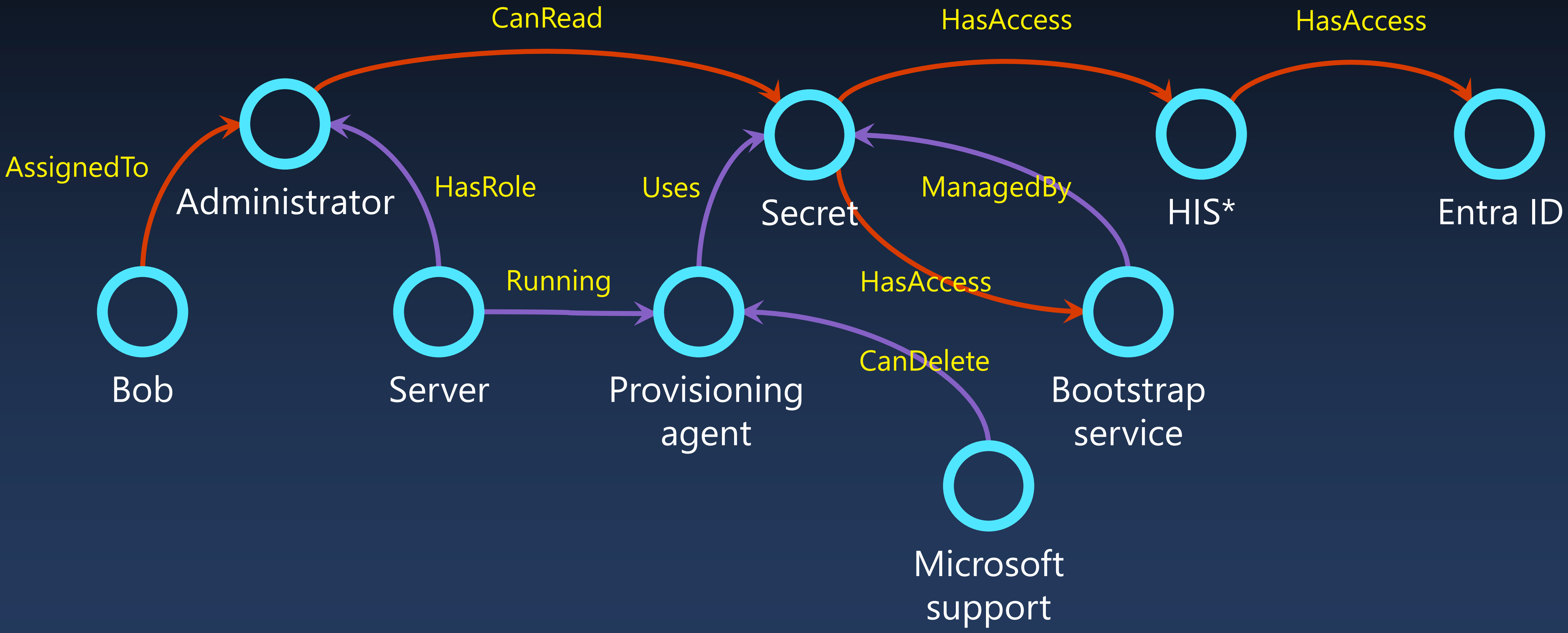
- Verifies credentials against on-premises AD
- Uses certificate based authentication (CBA)

PTA attack graph



* Hybrid Identity Service

PTA attack graph



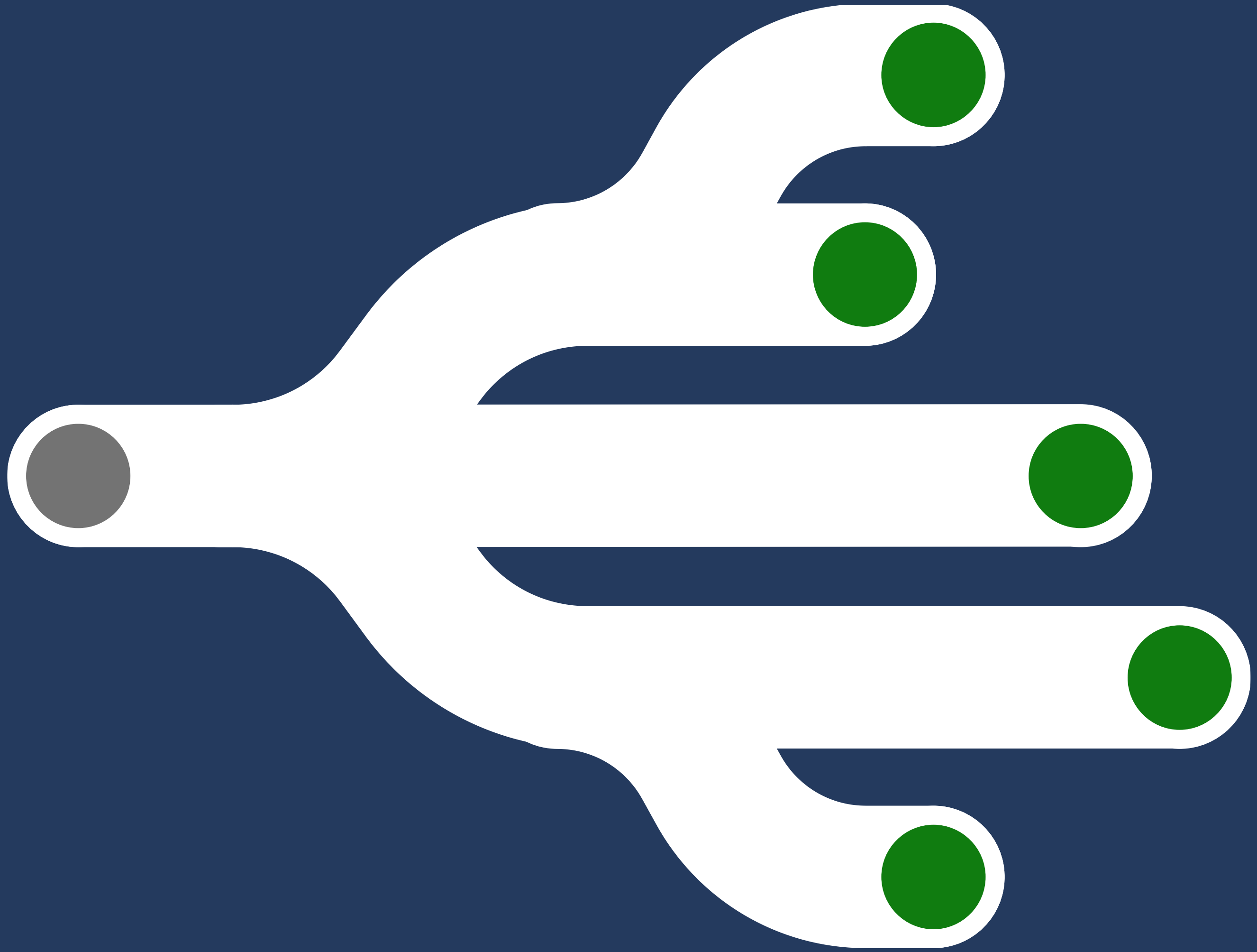
* Hybrid Identity Service

Protecting & mitigating PTA attacks

Area	Action
Limit access to server	Limit number of local administrators, POLP[1]
Prevent access to services	Disable PTA Contact Microsoft support to delete compromised agent(s)

[1] Principle Of Least Privilege

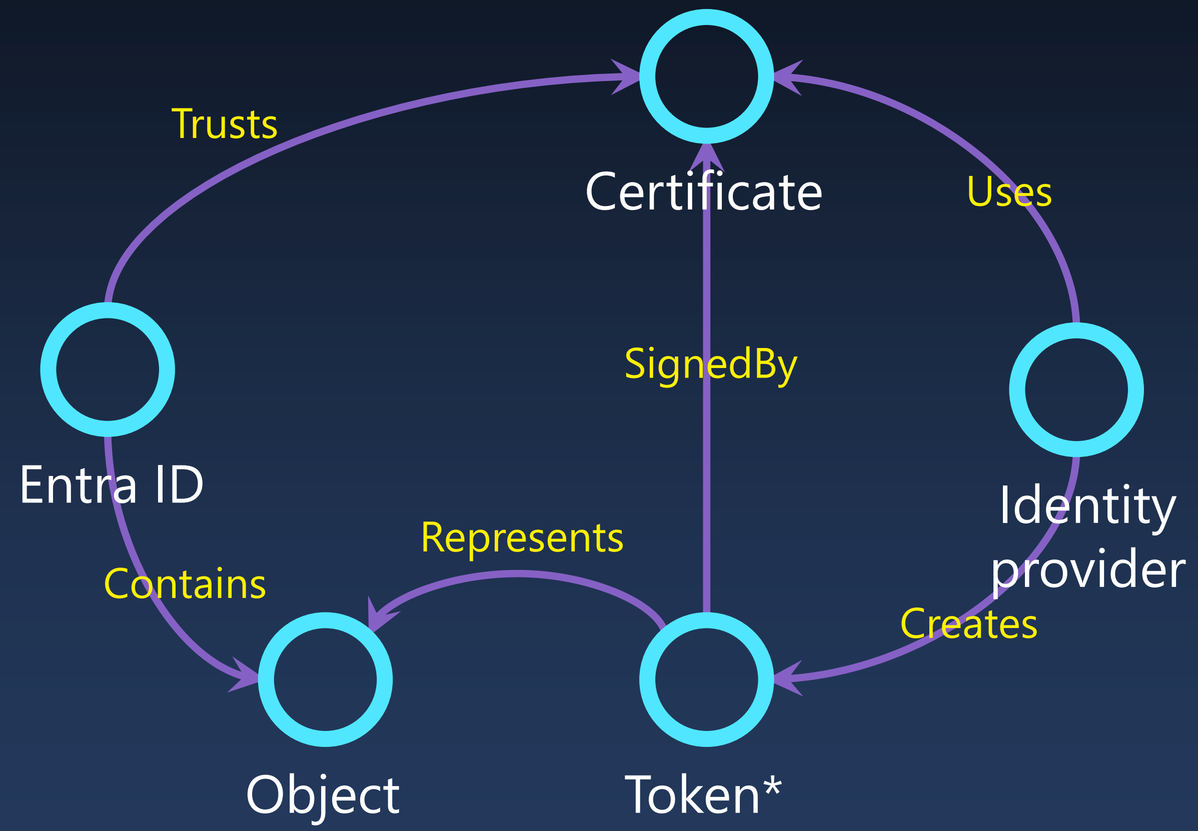
Federated Identity



Federated Identity

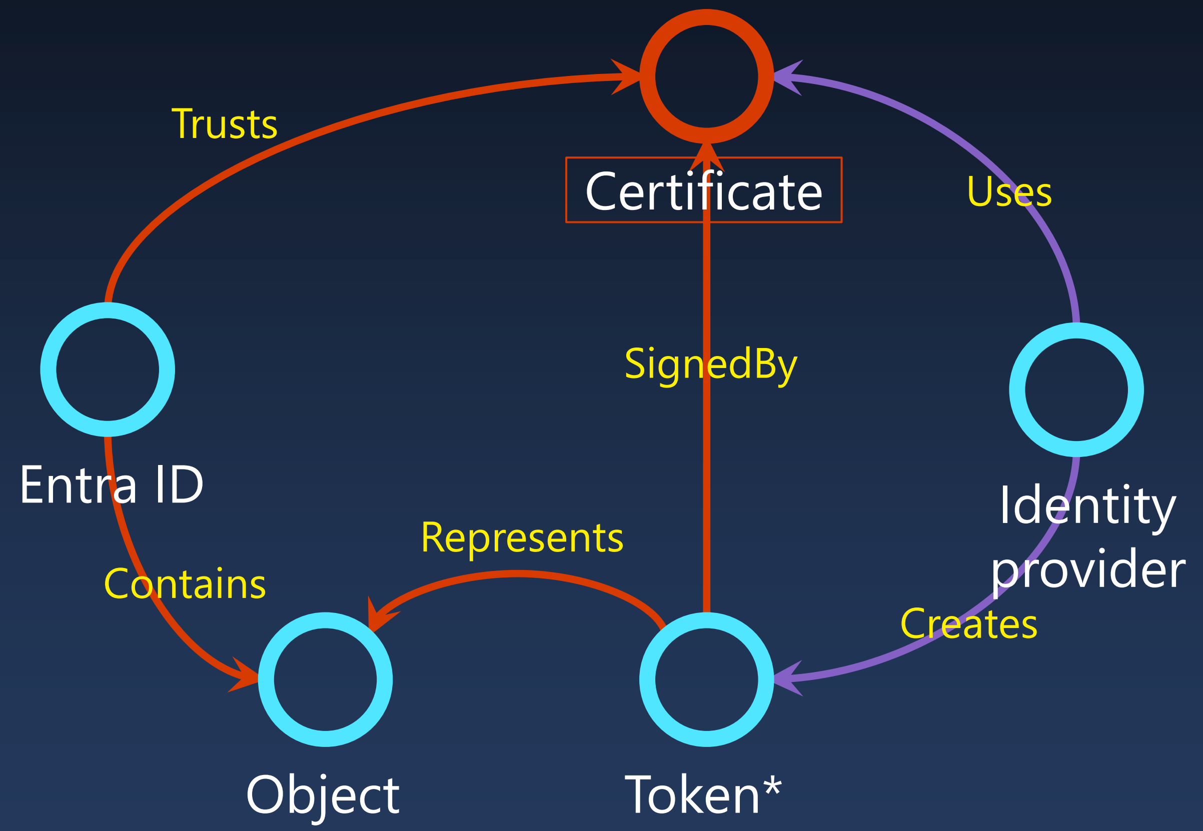
- Verifies credentials against external Identity Provider (IdP)
- Entra ID accepts tokens signed with IdP’s private key

Federated Identity attack graph



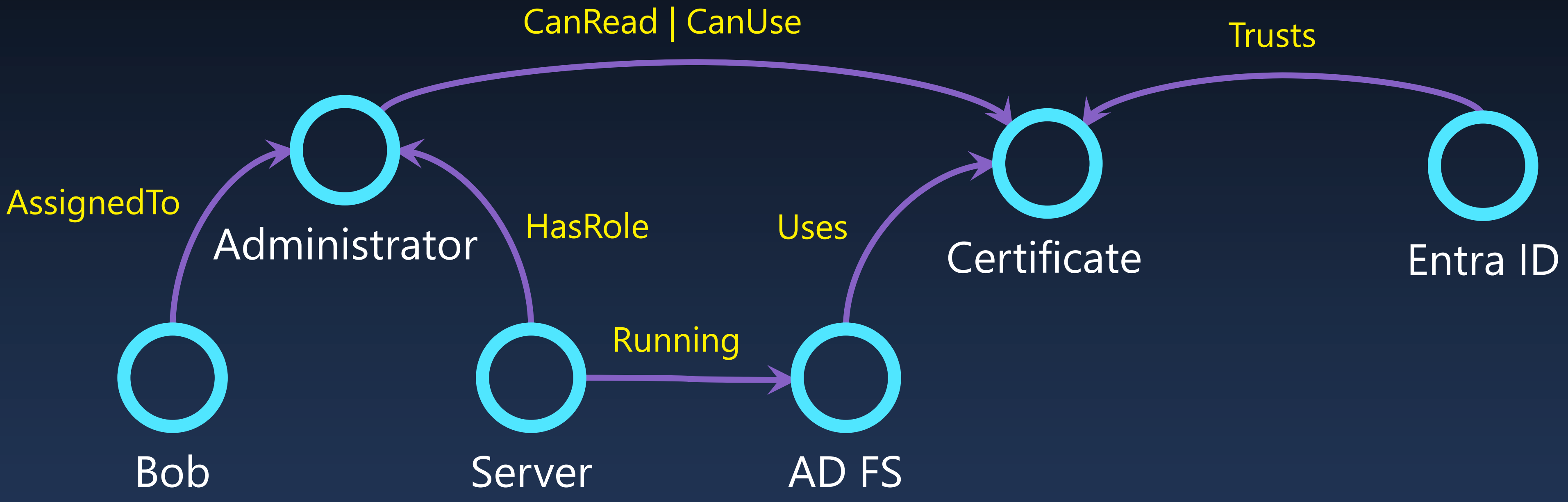
* OAuth, SAML, WS-FED, etc.

Federated Identity attack graph

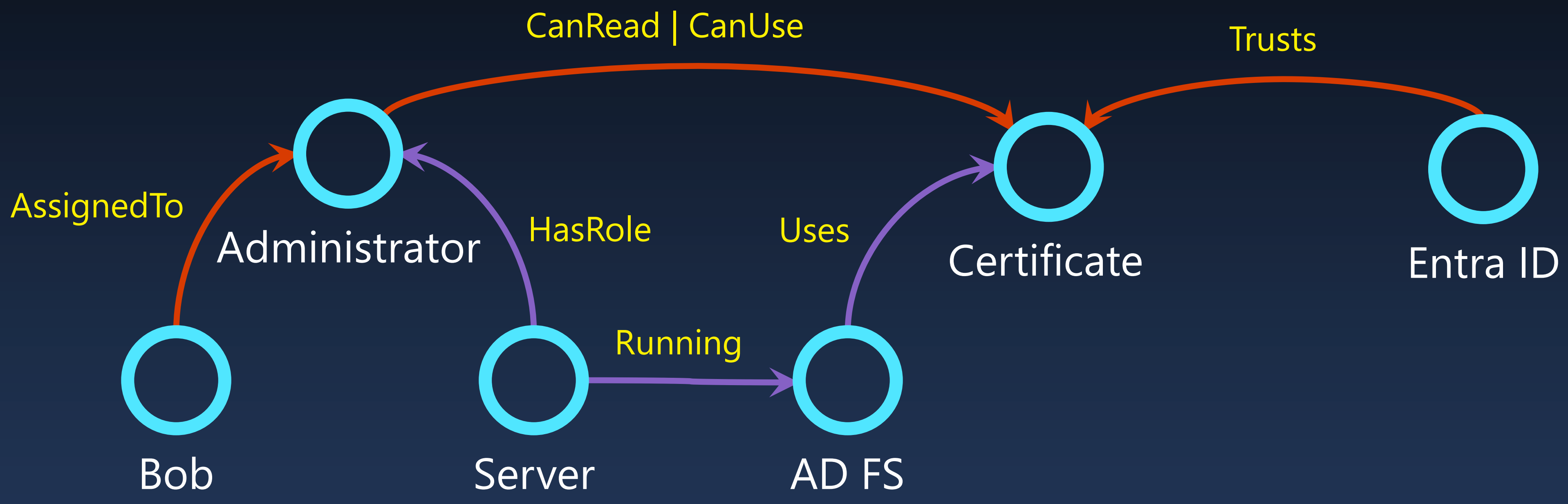


* OAuth, SAML, WS-FED, etc.

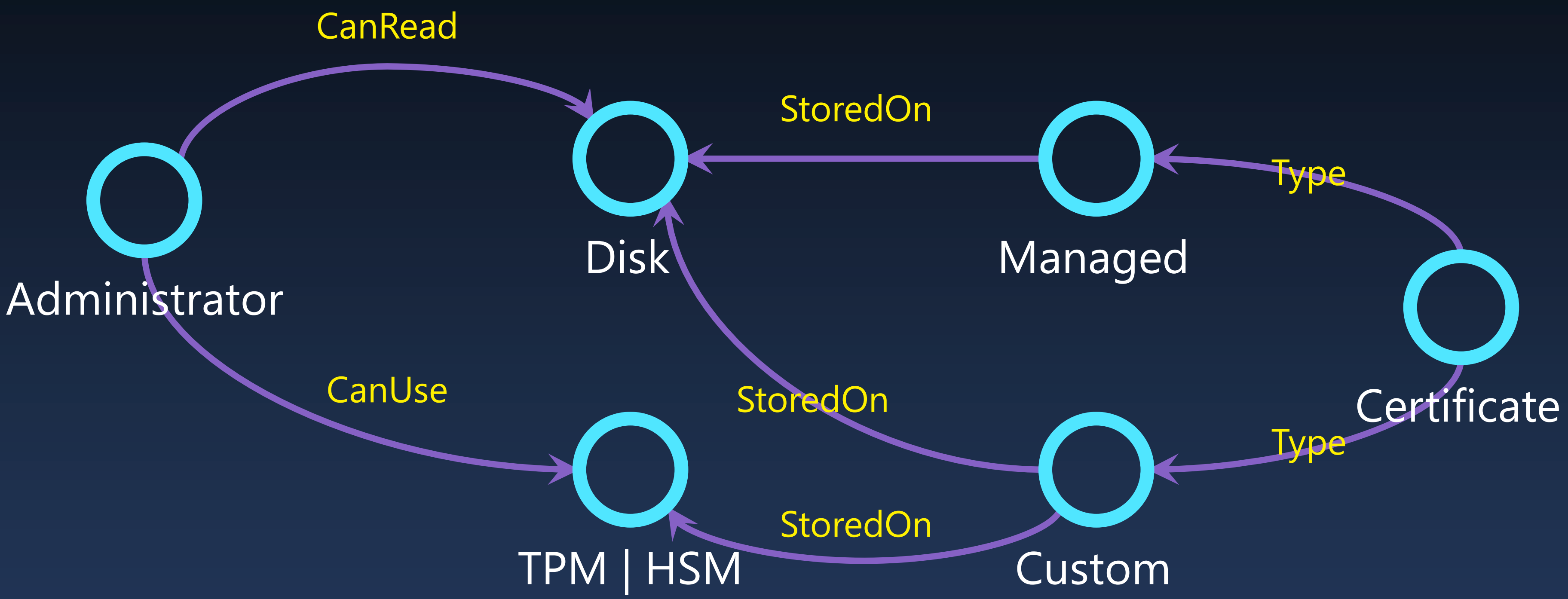
AD FS attack graph



AD FS attack graph

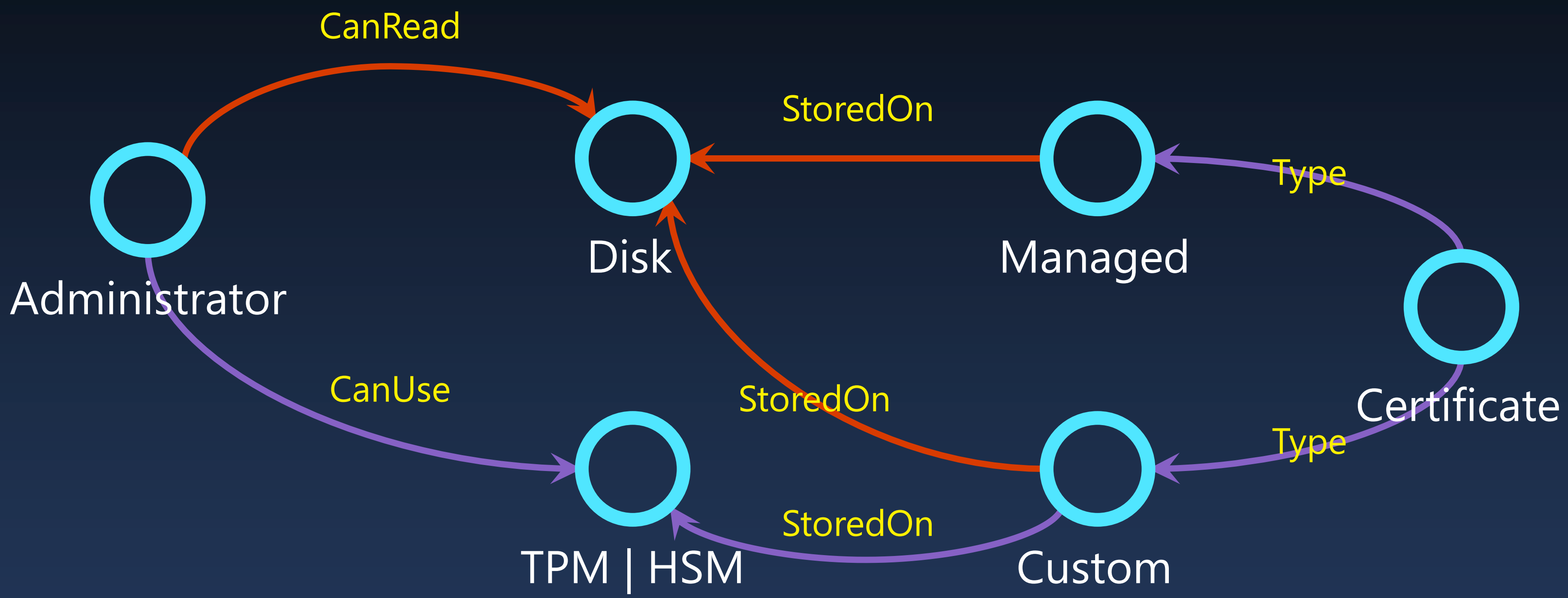


Accessing AD FS token signing certificate

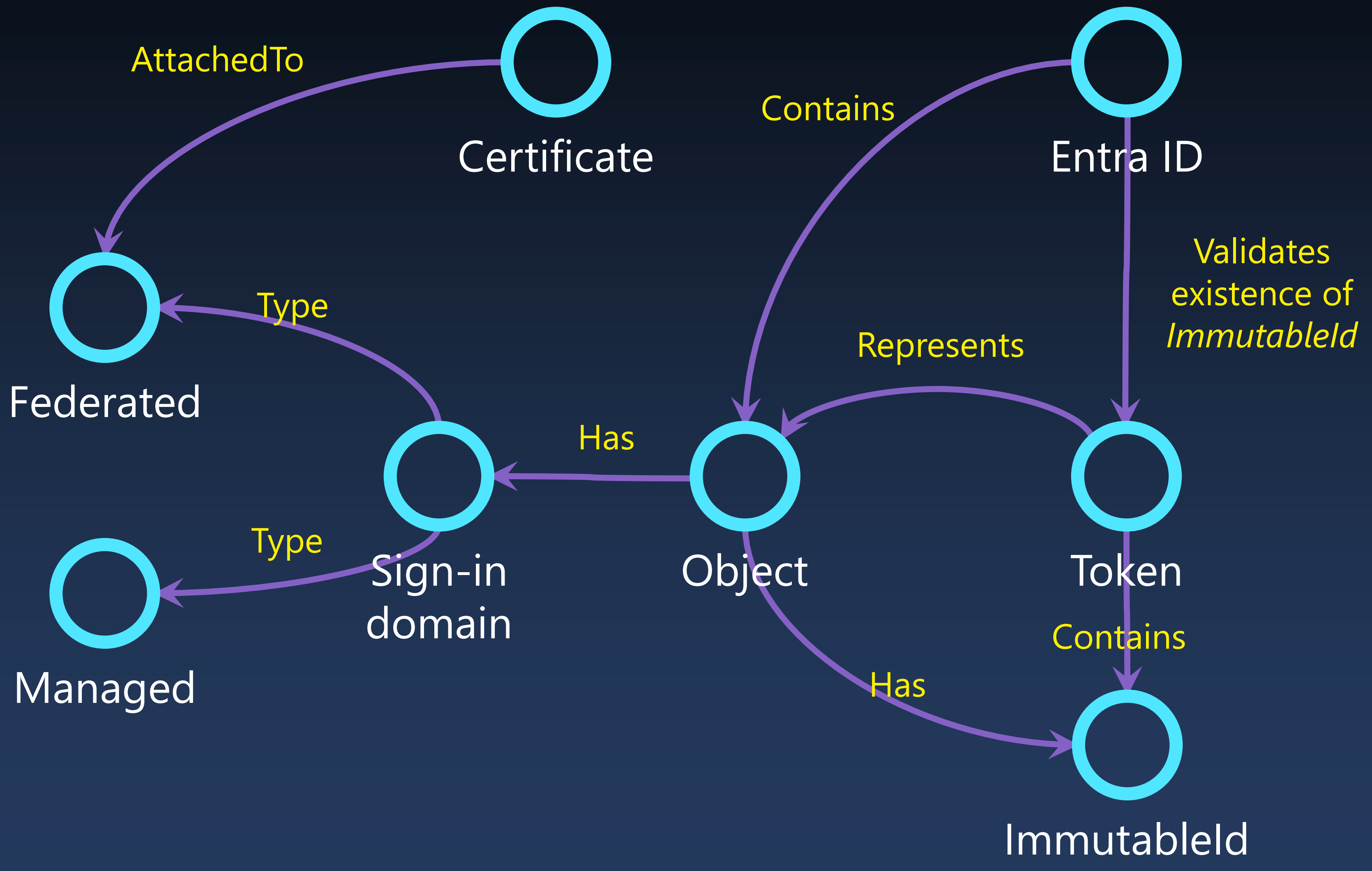


TPM: Trusted Platform Module
HSM: Hardware Security Module

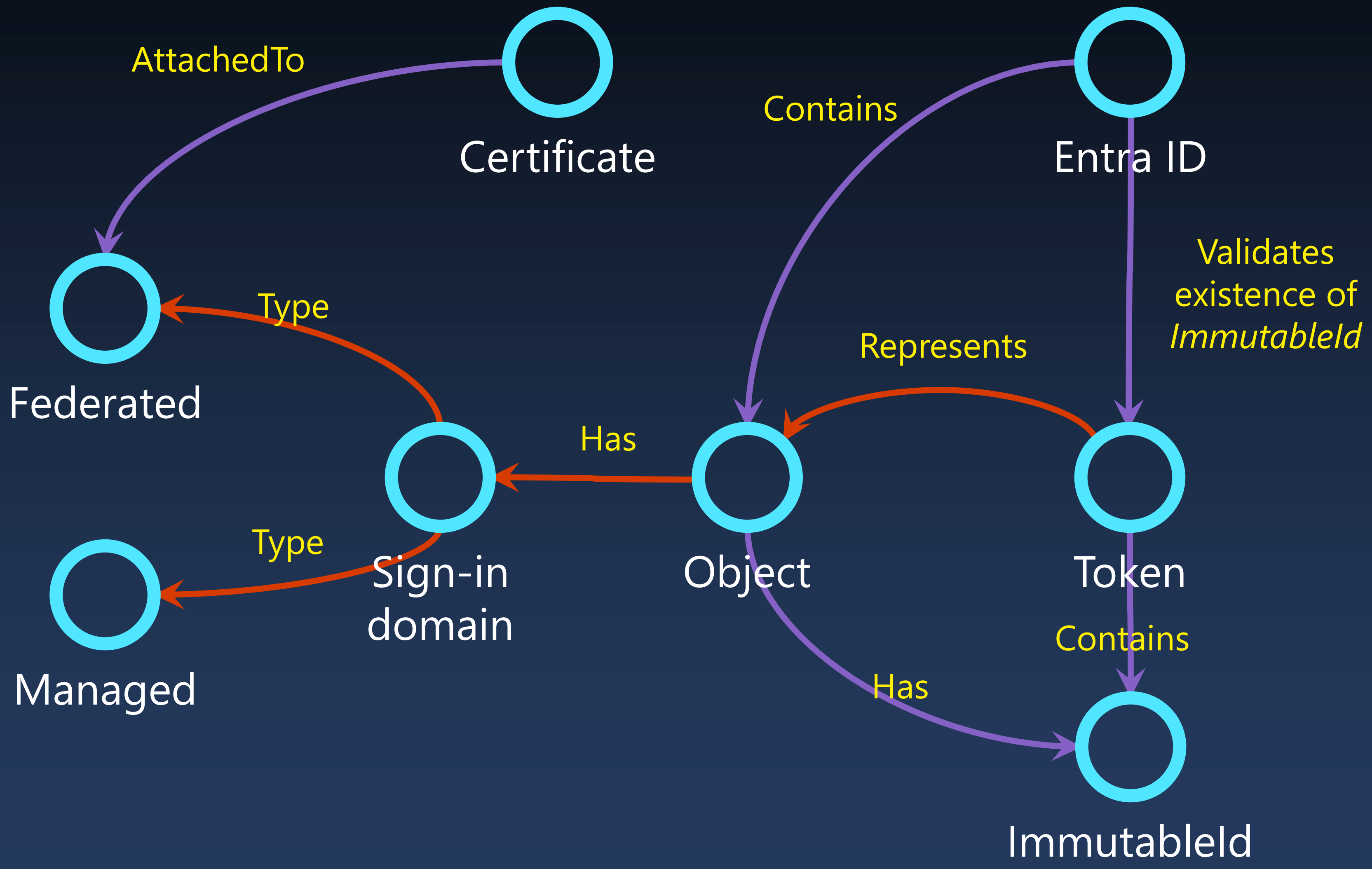
Accessing AD FS token signing certificate



Exploiting trust



Exploiting trust



Protecting Identity Federation

Area	Action
Limit access to server	Limit number of local administrators, POLP[1]
Limit access to AD FS certificate	Use custom certificates Store certificate on TPM or HSM
Limit trust	Set **federatedIdpMfaBehavior** to **rejectMfaByFederatedIdp**[2] Set **federatedTokenValidationPolicy**'s **validatingDomains** to **all**[3]

1. Principle Of Least Privilege
2. https://learn.microsoft.com/en-us/graph/api/resources/internaldomainfederation
3. https://learn.microsoft.com/en-us/graph/api/resources/federatedtokenvalidationpolicy