



10 Ways to Improve Entra ID Security Quickly



Sean Metcalf
@PyroTek3

Slides:

[PyroTek.io/BSNoVa2025](https://pyrotek.io/BSNoVa2025)

TRUSTEDSEC

About

- Identity Security Architect @ TrustedSec
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, Blue Team Con, multiple BSides, DEFCON, DerbyCon, RSA, TEC, Troopers, etc.
- Former Microsoft MVP
- Security Consultant / Researcher
- Own & Operate ADSecurity.org (Microsoft identity security info)

PyroTek.io/About

Sean Metcalf | @PyroTek3 | sean.metcalf@trustedsec.com





Agenda

1. User Defaults
2. Guest User Defaults
3. Application Consent Defaults
4. Entra ID Roles (Level 0 & 1)
5. Privileged Role Membership (admin accounts, MFA, etc.)
6. Role Assignable Groups
7. Highly Privileged Applications
8. Conditional Access
9. Partner Access
10. Secure Entra Connect
11. Bonus Content

Attackers Target Cloud



Suttons Law:

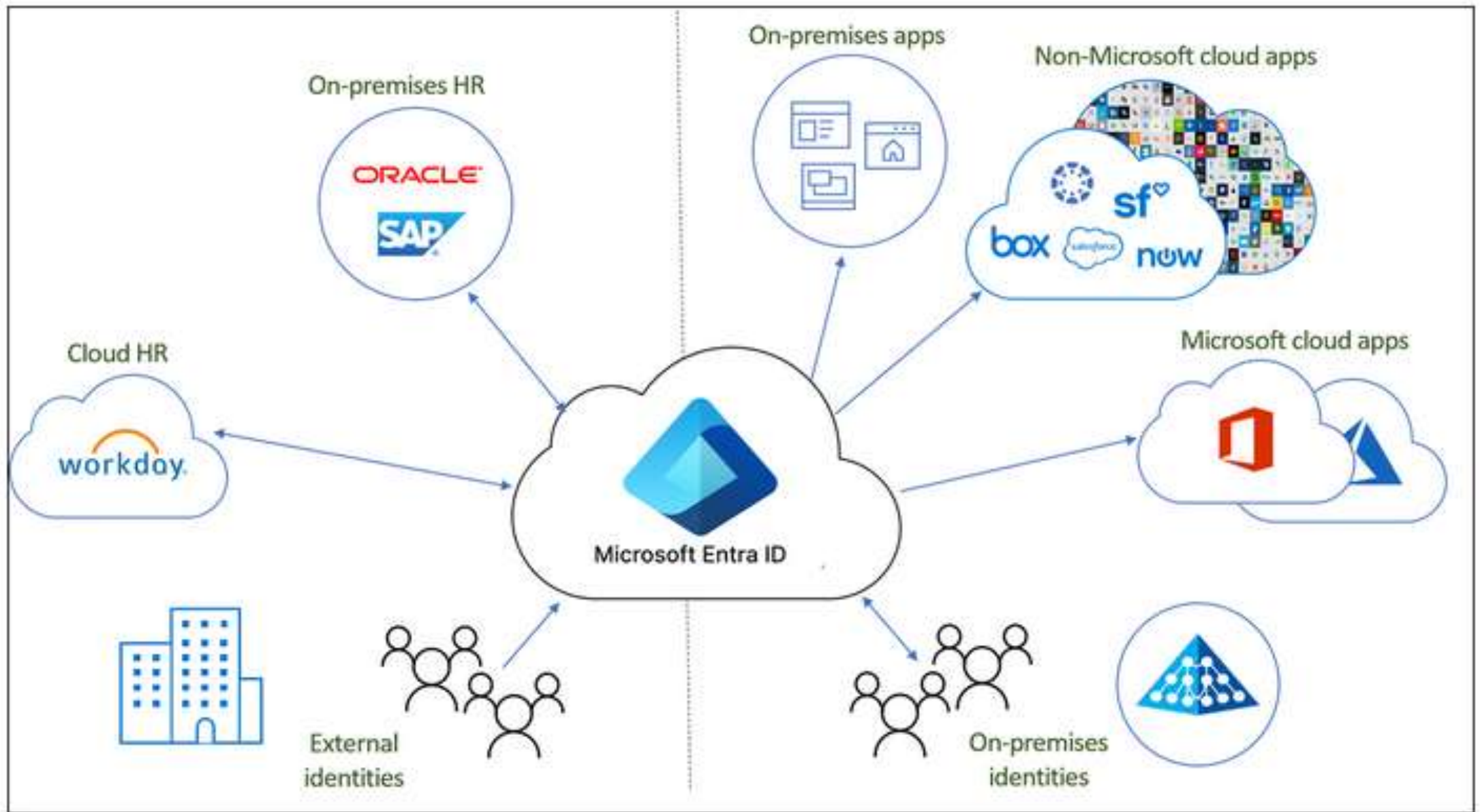
When diagnosing, one should first consider the obvious.

See also Occam's Razor ("entities should not be multiplied without necessity")



What does this mean?

Cloud security often misunderstood
Cloud is where the data is



<https://learn.microsoft.com/en-us/entra/identity/hybrid/what-is-provisioning>



#1 & #2 Secure Entra ID User & Guest Defaults

Unfortunate Defaults



Users:

- Can register applications
- Can consent to applications
- Can create new tenants
- Can join/hybrid join devices to the tenant & no MFA is required





Guests/External Accounts



- Guests have the same view rights as users
- Guests can invite other guests



Defaults

Default user role permissions

[Learn more](#) 


Users can register applications   Yes

Restrict non-admin users from creating tenants   No

Users can create security groups   Yes

Guest user access

[Learn more](#) 

- Guest user access restrictions 
- ☒ 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)

https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings

Default user role permissions

[Learn more](#) 

Recommended Settings


Users can register applications  ☐ No

Restrict non-admin users from creating tenants  ☒ Yes

Users can create security groups  ☐ No

Guest user access

[Learn more](#) 

Guest user access restrictions  ☐ 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)

https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings

Defaults

Users may join devices to Microsoft Entra ⓘ

All Selected None

Selected

No member selected


Users may register their devices with Microsoft Entra ⓘ

All None

 [Learn more on how this setting works](#)

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

Yes No

 We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using [Conditional Access](#). Set this device setting to No if you require Multifactor Authentication using Conditional Access.

Maximum number of devices per user ⓘ

50

https://portal.azure.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/_DeviceSettings/menuId~/null

Recommended

Users may join devices to Microsoft Entra ⓘ

All

Selected

None

Selected

1 member selected

Users may register their devices with Microsoft Entra ⓘ

All

None

[i Learn more on how this setting works](#)

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

Yes

No



We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using [Conditional Access](#). Set this device setting to No if you require Multifactor Authentication using Conditional Access.

https://portal.azure.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/_/DeviceSettings/menuId~/null

Defaults

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- ☒ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ☐ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ☐ Only users assigned to specific admin roles can invite guest users
- ☐ No one in the organization can invite guest users including admins (most restrictive)

Collaboration restrictions

⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. [Learn more.](#)

- ☒ 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)

https://portal.azure.com/#view/Microsoft_AAD_IAM/AllowlistPolicyBlade

Recommended Settings

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- ☐ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ☐ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ☒ Only users assigned to specific admin roles can invite guest users
- ☐ No one in the organization can invite guest users including admins (most restrictive)

Collaboration restrictions

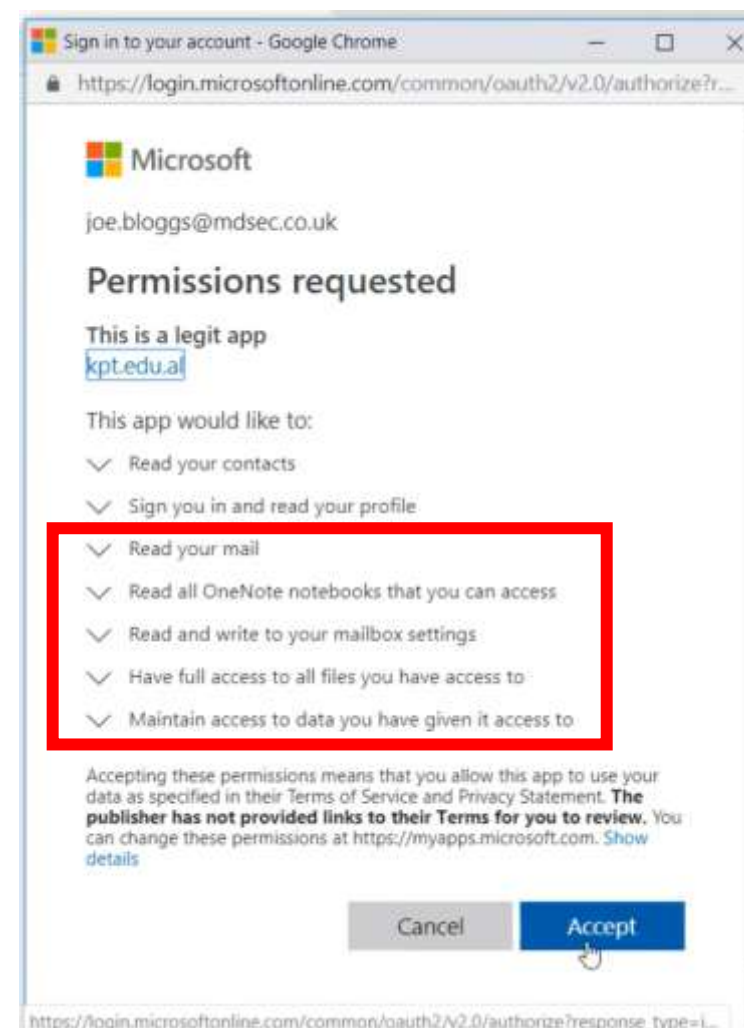
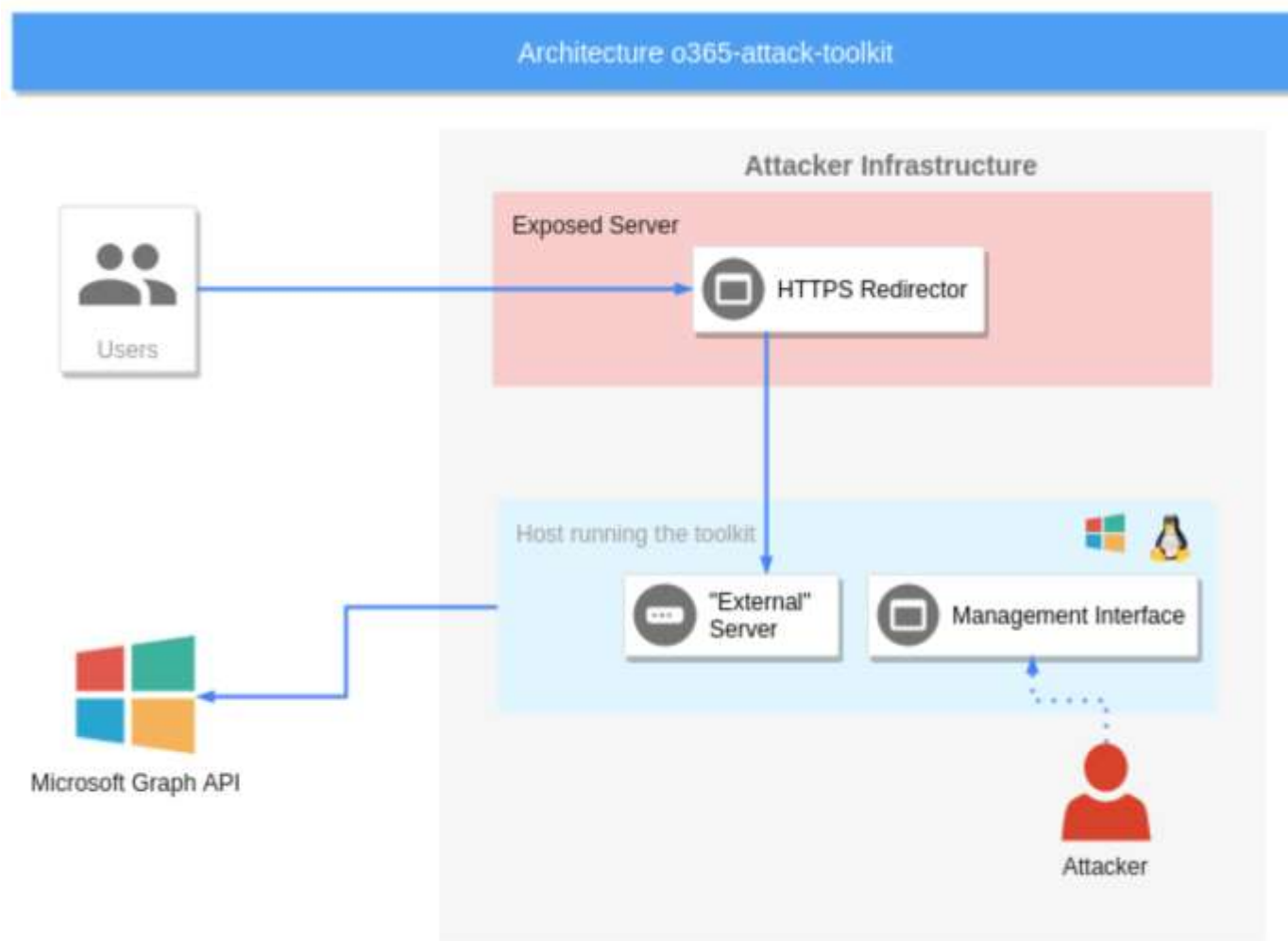
⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. [Learn more.](#)

- ☐ 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)

https://portal.azure.com/#view/Microsoft_AAD_IAM/AllowlistPolicyBlade

#3 Secure Entra ID Application Consent Defaults

Illicit Consent Grant Attack: MDsec O365 Attack Toolkit



<https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/>

Sean Metcalf | @PyroTek3 | sean.metcalf@trustedsec.com

Once Upon a Time...

Consent and permissions | User consent settings ...

Manage

 User consent settings

 Permission classifications



Save



Discard



Got feedback?

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data.

[Learn more about consent and permissions](#)

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)



Do not allow user consent

An administrator will be required for all apps.



Allow user consent for apps from verified publishers, for selected permissions (Recommended)

All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.



Allow user consent for apps

All users can consent for any app to access the organization's data.

Defaults

Consent and permissions | User consent settings ...

✕ ‹‹  Save  Discard |  Got feedback?

▼ Manage

User consent settings


Admin consent settings

Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.


User consent for applications






Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- ☐ Do not allow user consent
An administrator will be required for all apps.
- ☒ Allow user consent for apps from verified publishers, for selected permissions
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
 [3 permissions classified as low impact](#)
- ☐ Let Microsoft manage your consent settings (Recommended)
Automatically update your organization to Microsoft's current user consent guidelines. [Learn more](#)


https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/_/UserSettings


Recommended Settings


 **Consent and permissions | User consent settings** ...

   Save  Discard |  Got feedback?

Manage

 **User consent settings**

 Admin consent settings

 Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

☐ Do not allow user consent
An administrator will be required for all apps.

☐ Allow user consent for apps from verified publishers, for selected permissions
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

☒ **Let Microsoft manage your consent settings (Recommended)**
Automatically update your organization to Microsoft's current user consent guidelines. [Learn more](#)

https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/_/UserSettings

#4 Secure Entra ID Roles



There are
>100
Entra ID
Roles!

Sean Metcalf | @PyroTek3 | sean.metcalf@trustedsec.com

[illegible]

Microsoft's Privileged Azure AD Roles List (28) [PRIVILEGED]

- Application Administrator
- Application Developer
- Attribute Provisioning Administrator
- Attribute Provisioning Reader
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- Cloud Application Administrator
- Cloud Device Administrator
- Conditional Access Administrator
- Directory Writers
- Domain Name Administrator
- External Identity Provider Administrator
- Global Administrator
- Global Reader
- Helpdesk Administrator
- Hybrid Identity Administrator
- Intune Administrator
- Lifecycle Workflows Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

Microsoft's Privileged Azure AD Roles List (28) [PRIVILEGED]

- **Application Administrator**
- Application Developer
- Attribute Provisioning Administrator
- Attribute Provisioning Reader
- Authentication Administrator
- Authentication Extensibility Administrator
- B2C IEF Keyset Administrator
- **Cloud Application Administrator**
- Cloud Device Administrator
- Conditional Access Administrator
- **Directory Writers**
- Domain Name Administrator
- External Identity Provider Administrator
- **Global Administrator**
- Global Reader
- Helpdesk Administrator
- **Hybrid Identity Administrator**
- **Intune Administrator**
- Lifecycle Workflows Administrator
- Partner Tier1 Support
- **Partner Tier2 Support**
- Password Administrator
- **Privileged Authentication Administrator**
- **Privileged Role Administrator**
- Security Administrator
- Security Operator
- Security Reader
- User Administrator

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

Level 0 Entra ID Roles (5)

Effective Full Admin Rights or Capability to Gain Full Admin to Entra ID

- **Global Administrator**

- Full admin rights to the Entra ID, Microsoft 365, and 1-click full control of all Azure subscriptions
[From Azure AD to Active Directory \(via Azure\) – An Unanticipated Attack Path \(2020\)](#)

- **Hybrid Identity Administrator**

- “Can create, manage and deploy provisioning configuration setup from Active Directory to Microsoft Entra ID using Cloud Provisioning as well as manage Microsoft Entra Connect, Pass-through Authentication (PTA), Password hash synchronization (PHS), Seamless Single Sign-On (Seamless SSO), and **federation settings**.”
<https://medium.com/tenable-techblog/roles-allowing-to-abuse-entra-id-federation-for-persistence-and-privilege-escalation-df9ca6e58360>

- **Partner Tier2 Support**

- “The Partner Tier2 Support role can reset passwords and invalidate refresh tokens for all non-administrators and administrators (including Global Administrators).”

“not quite as powerful as Global Admin, but the role does allow a principal with the role to promote themselves or any other principal to Global Admin.”

[The Most Dangerous Entra Role You’ve \(Probably\) Never Heard Of](#)

- **Privileged Authentication Administrator**

- Microsoft: “do not use.”
“Set or reset any authentication method (including passwords) for any user, including Global Administrators. ... Force users to re-register against existing non-password credential (such as MFA or FIDO) and revoke remember MFA on the device, prompting for MFA on the next sign-in of all users.”

- **Privileged Role Administrator**

- “Users with this role can manage role assignments in Microsoft Entra ID, as well as within Microsoft Entra Privileged Identity Management. ... This role grants the ability to manage assignments for all Microsoft Entra roles including the Global Administrator role.”

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

Level 1 Entra ID Roles (1 of 2)

Highly Privileged Rights that have Privilege Escalation Potential Depending on Tenant Configuration or ability to reconfigure the security posture of the tenant

Role	Microsoft Description
Application Administrator	This is a privileged role. Users in this role can create and manage all aspects of enterprise applications, application registrations, and application proxy settings.
Authentication Administrator	This is a privileged role. Set or reset any authentication method (including passwords) for non-administrators and some roles. Require users who are non-administrators or assigned to some roles to re-register against existing non-password credentials (for example, MFA or FIDO), and can also revoke remember MFA on the device, which prompts for MFA on the next sign-in. Perform sensitive actions for some users.
Domain Name Administrator	This is a privileged role. Users with this role can manage (read, add, verify, update, and delete) domain names. Can be used in federation attacks.
Microsoft Entra Joined Device Local Administrator	During Microsoft Entra join, this group is added to the local Administrators group on the device.
Cloud Application Administrator	This is a privileged role. Users in this role have the same permissions as the Application Administrator role, excluding the ability to manage application proxy. This role grants the ability to create and manage all aspects of enterprise applications and application registrations.
Conditional Access Administrator	This is a privileged role. Users with this role have the ability to manage Microsoft Entra Conditional Access settings.
Directory Synchronization Accounts	This is a privileged role. Do not use. This role is automatically assigned to the Microsoft Entra Connect service, and is not intended or supported for any other use. Privileged rights: Update application credentials, Manage hybrid authentication policy in Microsoft Entra ID, Update basic properties on policies, & Update credentials of service principals
Directory Writers	This is a privileged role. Users in this role can read and update basic information of users, groups, and service principals. Privileged rights: Create & update OAuth 2.0 permission grants, add/disable/enable users, Force sign-out by invalidating user refresh tokens, & Update User Principal Name of users.

Level 1 Entra ID Roles (2 of 2)

Highly Privileged Rights that have Privilege Escalation Potential Depending on Tenant Configuration or ability to reconfigure the security posture of the tenant

Role	Microsoft Description
Exchange Administrator	Users with this role have global permissions within Microsoft Exchange Online. Trimarc flags this role since it is a role that threat actors target.
External Identity Provider Administrator	This is a privileged role. This administrator manages federation between Microsoft Entra organizations and external identity providers. With this role, users can add new identity providers and configure all available settings (e.g. authentication path, service ID, assigned key containers). This user can enable the Microsoft Entra organization to trust authentications from external identity providers.
Helpdesk Administrator	This is a privileged role. Users with this role can change passwords, & invalidate refresh tokens, Invalidating a refresh token forces the user to sign in again.
Intune Administrator	This is a privileged role. Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups. Privileged rights: Read Bitlocker metadata and key on devices
Password Administrator	This is a privileged role. Users with this role have limited ability to manage passwords.
Partner Tier1 Support	This is a privileged role. Do not use. The Partner Tier1 Support role can reset passwords and invalidate refresh tokens for only non-administrators. Privileged rights: Update application credentials, Create and delete OAuth 2.0 permission grants, & read and update all properties
Security Administrator	This is a privileged role. Users with this role have permissions to manage security-related features in the Microsoft 365 Defender portal, Microsoft Entra ID Protection, Microsoft Entra Authentication, Azure Information Protection, and Microsoft Purview compliance portal.
User Administrator	This is a privileged role. Can reset passwords for users.

Azure Privilege Escalation via Service Principal Abuse



Andy Robbins · Follow

Published in Posts By SpecterOps Team Members · 10 min read · Oct 12, 2021

Can a User with Role in Column A reset a password for a user with a Role in Row 2?


	(No Role)	Global Administrator	Privileged Authentication Administrator	Helpdesk Administrator	Authentication Administrator	User Administrator	Password Administrator	Directory Readers	Guest Inviter	Message Center Reader	Privileged Role Administrator	Reports Reader	Groups Administrator	(Any Other Role)
Global Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Privileged Authentication Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Helpdesk Administrator	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	No	No
Authentication Administrator	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	No	No
User Administrator	Yes	No	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	No
Password Administrator	Yes	No	No	No	No	No	Yes	Yes	Yes	No	No	No	No	No

<https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5>



#5 Secure Privileged Role Membership

Highly Privileged User Accounts

 **Global Administrator** | Assignments ...
Privileged Identity Management | Azure AD roles

[Add assignments](#) [Settings](#) [Refresh](#) [Export](#) [Got feedback?](#)

Manage


- Assignments
- Description
- Role settings

[Eligible assignments](#) **[Active assignments](#)** [Expired assignments](#)

Name	Principal name	Type	Scope	Membership	State	St...	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/...	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent




Showing 1 - 9 of 9 results. Sean Metcalf | @PyroTek3 | sean.metcalf@trustedsec.com

PIM Members are Permanent, Not Eligible

 **Global Administrator** | Assignments ...
Privileged Identity Management | Azure AD roles

« + Add assignments ⚙ Settings ↻ Refresh ↓ Export | 👤 Got feedback?

Manage

-  Assignments
-  Description
-  Role settings

Eligible assignments **Active assignments** Expired assignments

🔍 Search by member name or principal name

Name	Principal name	Type	Scope	Membership	State	St...	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/...	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/...	Permanent

Showing 1 - 9 of 9 results. Sean Metcalf | @PyroTek3 | sean.metcalf@trustedsec.com

Admin Accounts without MFA

The Following ☐ Global Admin Account(s) have MFA Successfully Configured:

UserDisplayName	UserPrincipalName	IsMfaCapable	IsMfaRegistered	IsPasswordlessCapable	MethodsRegistered
Sean Metcalf	sean@bigmegacorp.com	True	True	True	{microsoftAuthenticatorPasswordless,

The Following 7 Global Admin Account(s) don't have MFA Configured:

Cadence.Sparks@BigMegaCorp.onmicrosoft.com

Kenya.Bryan@BigMegaCorp.com

Janeya.Craig@BigMegaCorp.com

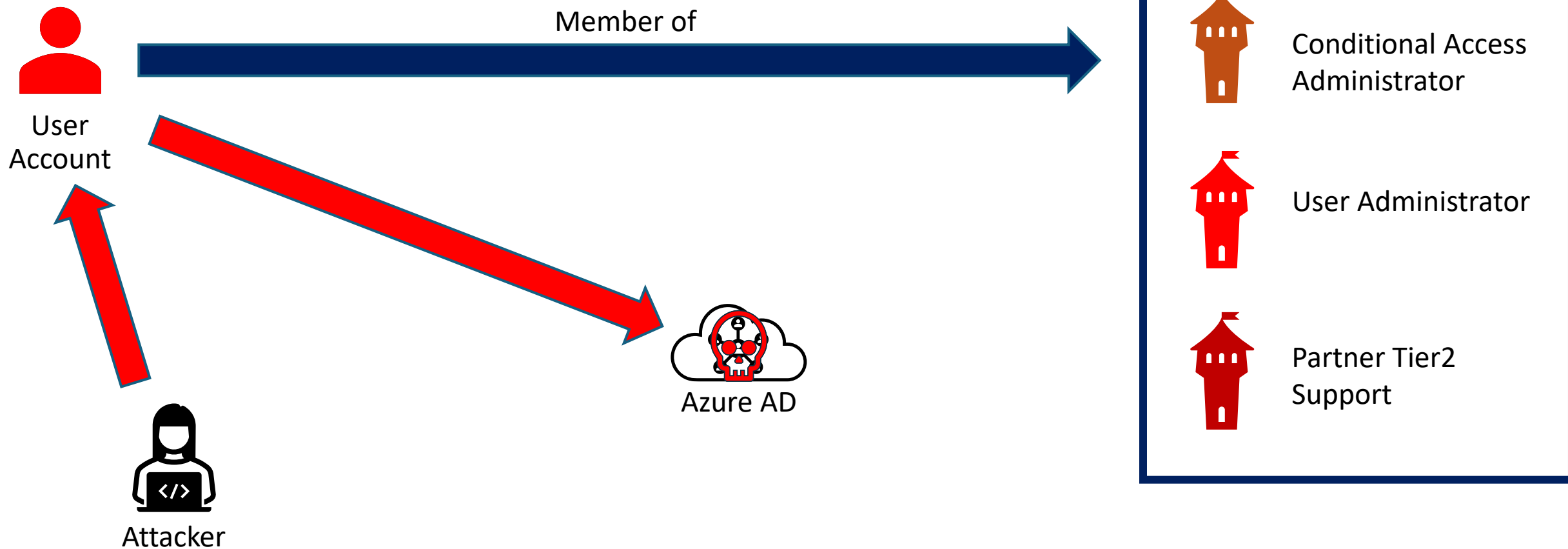
Annalina.Herman@BigMegaCorp.com

Seana.Brennan@BigMegaCorp.com

Chrissa.Bradley@BigMegaCorp.com

Shayla.Young@BigMegaCorp.com

Overprivileged User



#6 Secure Role Assignable Groups




Role Assignable Groups (RAGs)

- Role Assignable Groups are Security or Microsoft 365 group with the `isAssignableToRole` property set to true and cannot be dynamic.
- Created to solve the potential issue where groups are added to an Entra ID role and a group admin could modify membership.
- Only Global Administrators or Privileged Role Administrators can create Role Assignable Groups and manage them (membership).
- Role Assignable Group owners can manage them.
- There is an application permission (`Graph:RoleManagement.ReadWrite.Directory`) that provides management rights as well.
- 500 role-assignable groups maximum in an Entra ID tenant (creation maximum).

NOTE:




Only a Privileged Authentication Administrator or a Global Administrator can change the credentials or reset MFA or modify sensitive attributes for members & owners of a role-assignable group.

Privileged Roles with Group Nesting

 **Global Administrator** | Assignments ...
Privileged Identity Management | Azure AD roles

« + Add assignments ⚙ Settings ↻ Refresh ↓ Export | 🗨 Got feedback?

Manage

-  Assignments
-  Description
-  Role settings

Eligible assignments **Active assignments** Expired assignments

🔍 Search by member name or principal name

Name	Principal name	Type	Scope	Membership	State	Start time	End time
Global Administrator							
Shayla Young	Shayla.Young@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Seana Brennan	Seana.Brennan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Janeya Craig	Janeya.Craig@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
BigMegaCorp Global Admins	-	Group	Directory	Direct	Assigned	-	Permanent
Annalina Herman	Annalina.Herman@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Cadence Sparks	Cadence.Sparks@BigMegaCorp.onmicrosoft.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Sean Metcalf	sean@bigmegacorp.com	User	Directory	Direct	Assigned	-	Permanent
Chrissa Bradley	Chrissa.Bradley@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Kenya Bryan	Kenya.Bryan@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent
Aafiyah Rodgers	Aafiyah.Rodgers@BigMegaCorp.com	User	Directory	Direct	Assigned	9/11/202...	Permanent

Showing 1 - 10 of 10 results.

Sean Metcalf | @PyroTek3 | sean.metcalf@trustedsec.com

Group Nesting – Have to Open Groups

Home > BigMegaCorp Global Admins

BigMegaCorp Global Admins Members

Group

Overview
Diagnose and solve problems

Manage

Properties
Members
Owners
Roles and administrators
Administrative units
Group memberships
Assigned roles
Applications

+ Add members X Remove Refresh Bulk operations Columns Got feedback?

Direct members All members

Search by name Add filters

	Name	Type	Email	User type
<input type="checkbox"/>	Aadit White	User	Aadit.White@BigMegaCorp.com	Member
<input type="checkbox"/>	Cadence Mclean	User	Cadence.Mclean@BigMegaCorp.com	Member
<input type="checkbox"/>	Dane Pineda	User	Dane.Pineda@BigMegaCorp.com	Member
<input type="checkbox"/>	Dirk Lester	User	Dirk.Lester@BigMegaCorp.com	Member
<input type="checkbox"/>	Tyrek Miller	User	Tyrek.Miller@BigMegaCorp.com	Member
<input type="checkbox"/>	Wilson Merritt	User	Wilson.Merritt@BigMegaCorp.com	Member

Role Assignable Group Owners



Home > BigMegaCorp Global Admins

BigMegaCorp Global Admins | Owners

Group

« + Add owners ✕ Remove ↺ Refresh ≡ Columns 🗨 Got feedback?

🔍 Search by name + Add filters

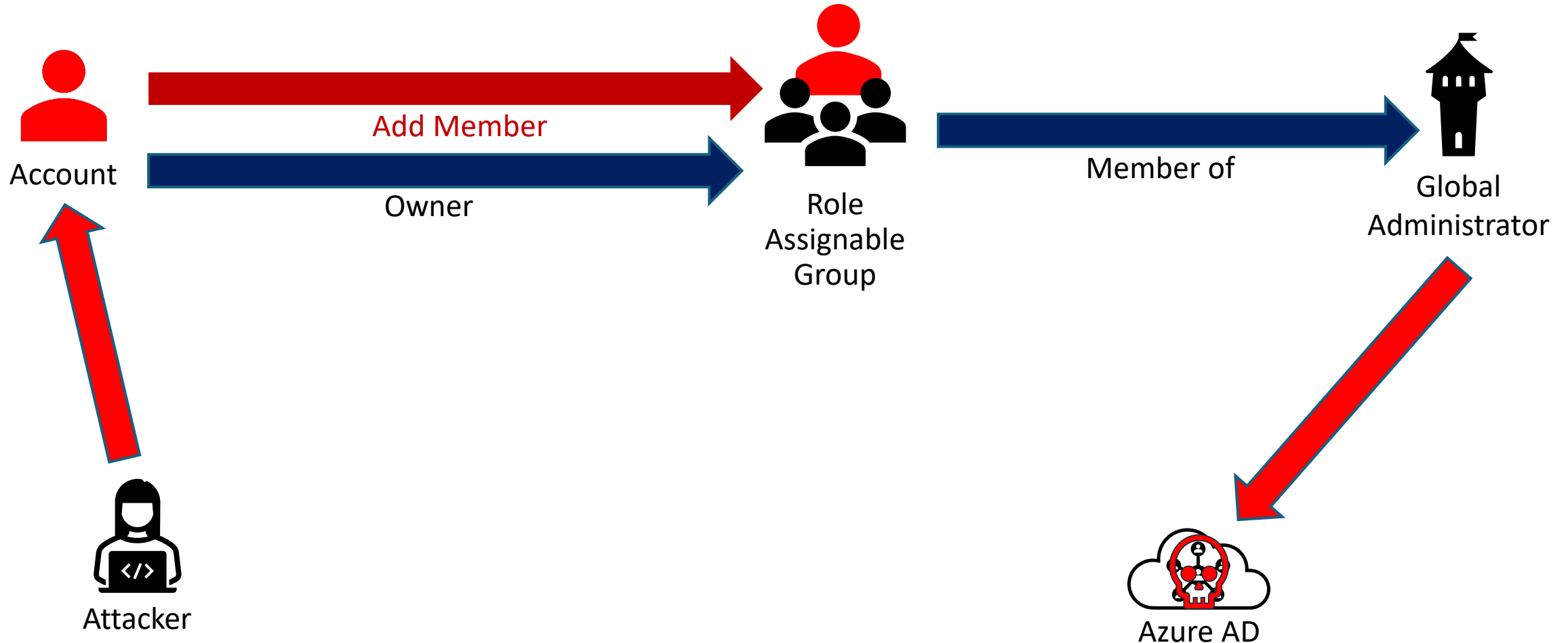
	Name	Type	Email	User type
<input type="checkbox"/>	 Kate Pena	User	Kate.Pena@BigMegaCorp.com	Member
<input type="checkbox"/>	 Robert Marquez	User	Robert.Marquez@BigMegaCorp.com	Member

Manage

- Overview
- Diagnose and solve problems
- Properties
- Members
- Owners**

Role Assignable Group Owners can manage group membership

Compromise Azure AD through Role Assignable Group Owner Rights





#7 Secure Highly Privileged Applications

Permissions Structure

OBJECT . ACCESS . CONSTRAINT

Examples:

Application.ReadWrite.All

Calendars.ReadWrite

Calendars.ReadWrite.All

Directory.ReadWrite.All

Mail.ReadWrite

Mail.Send

User.ReadWrite.All

Permissions Structure: Constraint

All	Shared	AppFolder	No constraint
grants permission for the app to perform the operations on all of the resources of the specified type in a directory.	grants permission for the app to perform the operations on resources that other users have shared with the signed-in user. This constraint is mainly used with Outlook resources like mail, calendars, and contacts.	grants permission for the app to read and write files in a dedicated folder in OneDrive. This constraint is only exposed on Files permissions and is only valid for Microsoft accounts.	the app is limited to performing the operations on the resources owned by the signed-in user.

Level 0 Applications

Effective Full Admin Rights or Capability to Gain Full Admin to Entra ID

Directory.ReadWrite.All

- “Directory.ReadWrite.All grants access that is broadly equivalent to a global tenant admin.” *

AppRoleAssignment.ReadWrite.All

- Allows the app to manage permission grants for application permissions to any API & application assignments for any app, on behalf of the signed-in user. **This also allows an application to grant additional privileges to itself, other applications, or any user.**

RoleManagement.ReadWrite.Directory

- Allows the app to read & manage the role-based access control (RBAC) settings for the tenant, without a signed-in user. This includes instantiating directory roles & **managing directory role membership**, and reading directory role templates, directory roles and memberships.

Application.ReadWrite.All

- Allows the calling app to create, & manage (read, update, update application secrets and delete) applications & service principals without a signed-in user. This also allows an application to act as other entities & use the privileges they were granted.

Reviewing Azure AD Permissions with PowerShell

```
PS C:\> Get-AzureADPSPermissions -ApplicationPermissions | Select ClientDisplayName,ResourceDisplayName,Permission
```

ClientDisplayName	ResourceDisplayName	Permission
Trimarc RD TestApp	Windows Azure Active Directory	Device.ReadWrite.All
Trimarc RD TestApp	Windows Azure Active Directory	Member.Read.Hidden
Trimarc RD TestApp	Windows Azure Active Directory	Directory.ReadWrite.All
Trimarc RD TestApp	Windows Azure Active Directory	Domain.ReadWrite.All
Trimarc RD TestApp	Windows Azure Active Directory	Application.ReadWrite.OwnedBy
Trimarc RD TestApp	Windows Azure Active Directory	Application.ReadWrite.All
Trimarc RD TestApp	Office 365 Exchange Online	User.Read.All
Trimarc RD TestApp	Office 365 Exchange Online	Mail.ReadWrite
Trimarc RD TestApp	Office 365 Exchange Online	MailboxSettings.ReadWrite
Trimarc RD TestApp	Office 365 Exchange Online	Contacts.ReadWrite
Trimarc RD TestApp	Office 365 Exchange Online	Mailbox.Migration
Trimarc RD TestApp	Office 365 Exchange Online	Calendars.ReadWrite.All
Trimarc RD TestApp	Office 365 Exchange Online	Mail.Send
Office 365 ASI App	Office 365 Management APIs	ServiceHealth.Read
Office 365 ASI App	Office 365 Management APIs	ActivityFeed.Read

<https://gist.github.com/psignoret/9d73b00b377002456b24fcb808265c23>

Who are the Application Owners for TestApp?

```
PS C:\> Get-AzureADApplication -Objectid $appid | select displayname,Objectid,appid
```

DisplayName	Objectid	AppId
-----	-----	-----
Trimarc RD TestApp	c8e9b6fe-cc98-4e90-8b7b-15fba500d49c	2f337e5f-8414-45a4-b48f-e0ec2014a1d4

```
PS C:\> Get-AzureADApplicationOwner -objectId $AppId
```

Objectid	DisplayName	UserPrincipalName	UserType
-----	-----	-----	-----
71575fad-39b2-475a-b519-314dde65e7cf	Sean Metcalf	sean@trimarcrd.com	Member
13cf788e-baf0-4b1e-b9fa-46128a6468d0	Joe User	JoeUser@TrimarcRD.com	Member
f4d30f9e-0837-4e3f-974e-ef282a2fcef	Darth Vader	DarthVader@TrimarcRD.com	Member
f2a0fb99-bdaf-49ce-9192-9488ea5d3dae	Boba Fett	BobaFett@TrimarcRD.com	Member

Application Escalation



```
PS C:\Data\_MCSA> get-azureadpspermissions -ApplicationPermissions|select ClientObjectID,ClientDisplayName,ResourceDisplayName,Permission
```

ClientObjectID	ClientDisplayName	ResourceDisplayName	Permission
9211cb77-c065-4fd9-a80b-bb3a3015caee	Lots 'o Privs!	Microsoft Graph	DelegatedPermissionGrant.ReadWrite.All
9211cb77-c065-4fd9-a80b-bb3a3015caee	Lots 'o Privs!	Microsoft Graph	Directory.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa	Overpermissioned App	Microsoft Graph	Application.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa	Overpermissioned App	Microsoft Graph	AppRoleAssignment.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa	Overpermissioned App	Microsoft Graph	DelegatedPermissionGrant.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa	Overpermissioned App	Microsoft Graph	Directory.ReadWrite.All
01438f2c-8d6d-4f11-9f76-f179fd3246fa	Overpermissioned App	Microsoft Graph	RoleManagement.ReadWrite.Directory



Attacker

<https://gist.github.com/psignoret/9d73b00b377002456b24fcb808265c23>

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Application Escalation: Find the App Owner

```
PS C:\Data\_MCSA> Get-AzureADApplication -SearchString 'overpermissioned'
```

ObjectId	AppId	DisplayName
-----	-----	-----
fbe4ea6c-0ae4-46b2-a6f0-5f96e3f4858f	5e356a56-f302-4987-923a-0e282ea31d39	Overpermissioned App

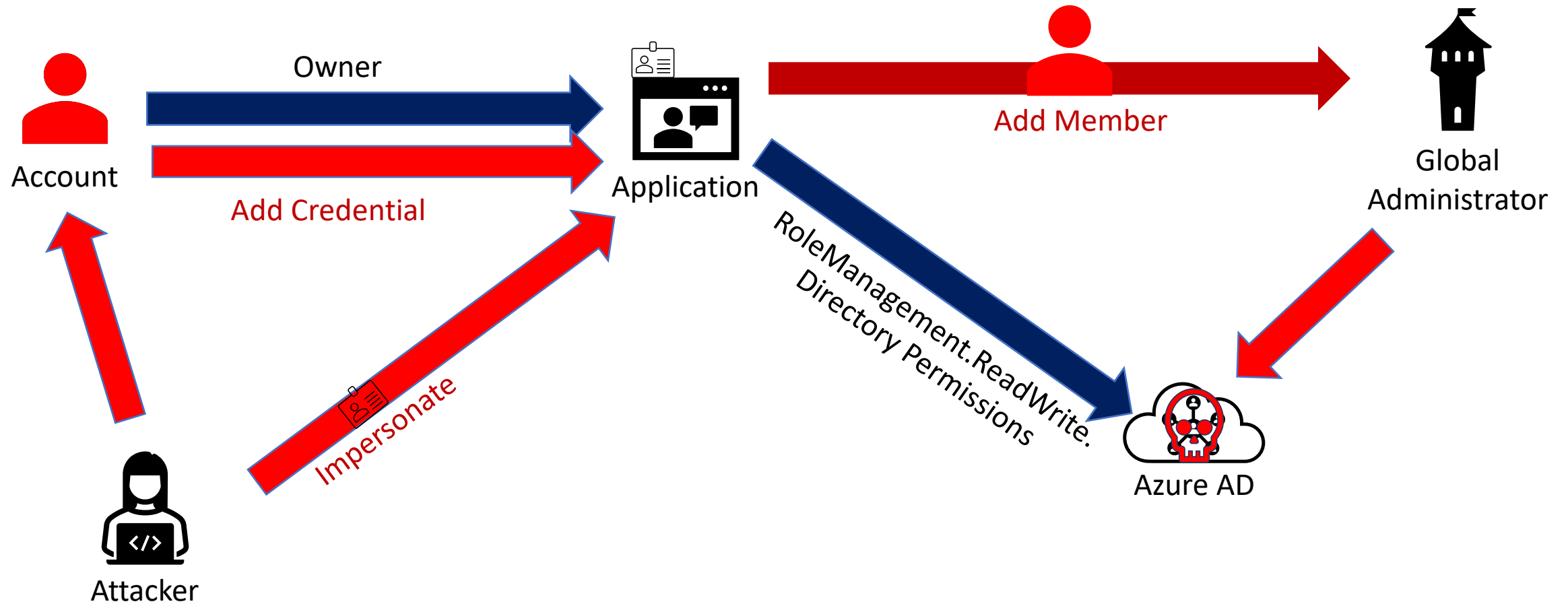
```
PS C:\Data\_MCSA> get-azureadapplicationowner -ObjectId 'fbe4ea6c-0ae4-46b2-a6f0-5f96e3f4858f'
```

ObjectId	DisplayName	UserPrincipalName	UserType
-----	-----	-----	-----
ab2365a7-24a1-4ac0-9cd0-2d529d759323	Kenyatta Yoder	Kenvatta.Yoder@BigMegaCorp.onmicrosoft.com	Member
70d9a5f5-7190-4452-a743-4f2bede82c06	Shayla Santana	Shayla.Santana@BigMegaCorp.com	Member
7d8afa78-d799-4bdc-8e33-3dff42fbbac3	Cadence Mclean	Cadence.Mclean@BigMegaCorp.com	Member

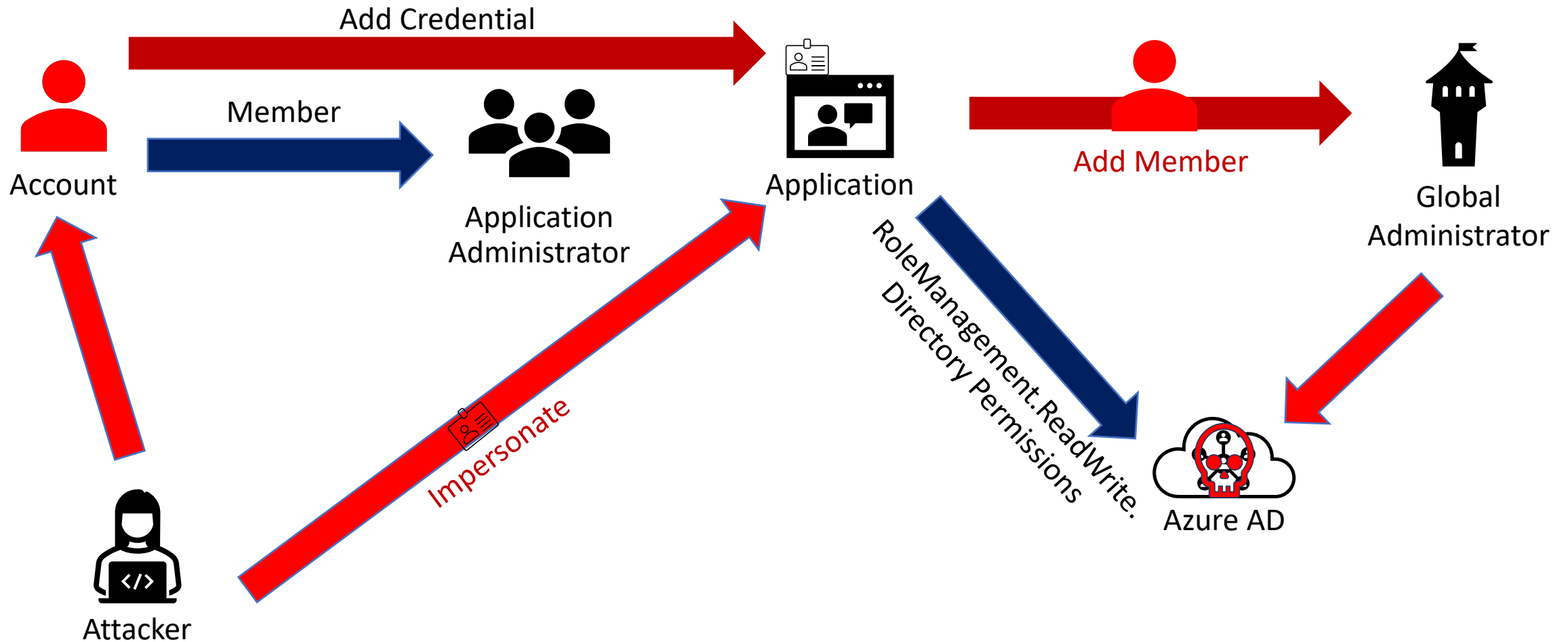


Attacker

Compromise Azure AD through Application Permissions



Compromise Azure AD through Application Permissions



#8 Secure Entra ID with Conditional Access Policies



Conditional Access Policies

Policies apply after (first-factor) authentication

Requires P1 licensing

Rules based on:

- Who is connecting?
- Where are they connecting (from)?
- What app and/or device is connecting?
- When does this apply?



Signal



Decision



Enforcement

◊ << + New policy + New policy from template ↑ Upload policy file 👤 What if ↺ Refresh ⚙️ Preview features 🗨️ Got feedback?

📘 Overview

☰ Policies

💡 Insights and reporting

🔧 Diagnose and solve problems

▼ Manage

↔️ Named locations

🖨️ Custom controls (Preview)

📄 Terms of use

⚙️ VPN connectivity

👤 Authentication contexts

🛡️ Authentication strengths

☰ Classic policies

> Monitoring

> Troubleshooting + Support

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#) 📄

All policies

8

Total

Microsoft-managed policies

🏆 0

out of 8

🔍 Search

🔍 Add filter

8 out of 8 policies found

Policy name	State	Creation date	Modified date
CA001: Require multi-factor authentication for admins	Report-only	5/29/2022, 11:10:03 PM	5/29/2022, 11:19:17 PM
CA003: Block legacy authentication	Report-only	5/29/2022, 11:10:15 PM	
CA005: Require multi-factor authentication for guest access	Report-only	5/29/2022, 11:10:28 PM	
CA007: Require multi-factor authentication for risky sign-ins	Report-only	5/29/2022, 11:10:39 PM	
Require compliant or hybrid Azure AD joined device or multifactor authentic...	Report-only	1/19/2024, 3:13:25 PM	
Require multifactor authentication for Azure management	Report-only	1/19/2024, 3:13:13 PM	
Require multifactor authentication for all users	Report-only	1/19/2024, 3:12:52 PM	
Securing security info registration	Report-only	1/19/2024, 3:12:31 PM	

Common Conditional Access Policies



Require users to use MFA when connecting outside of the corporate network



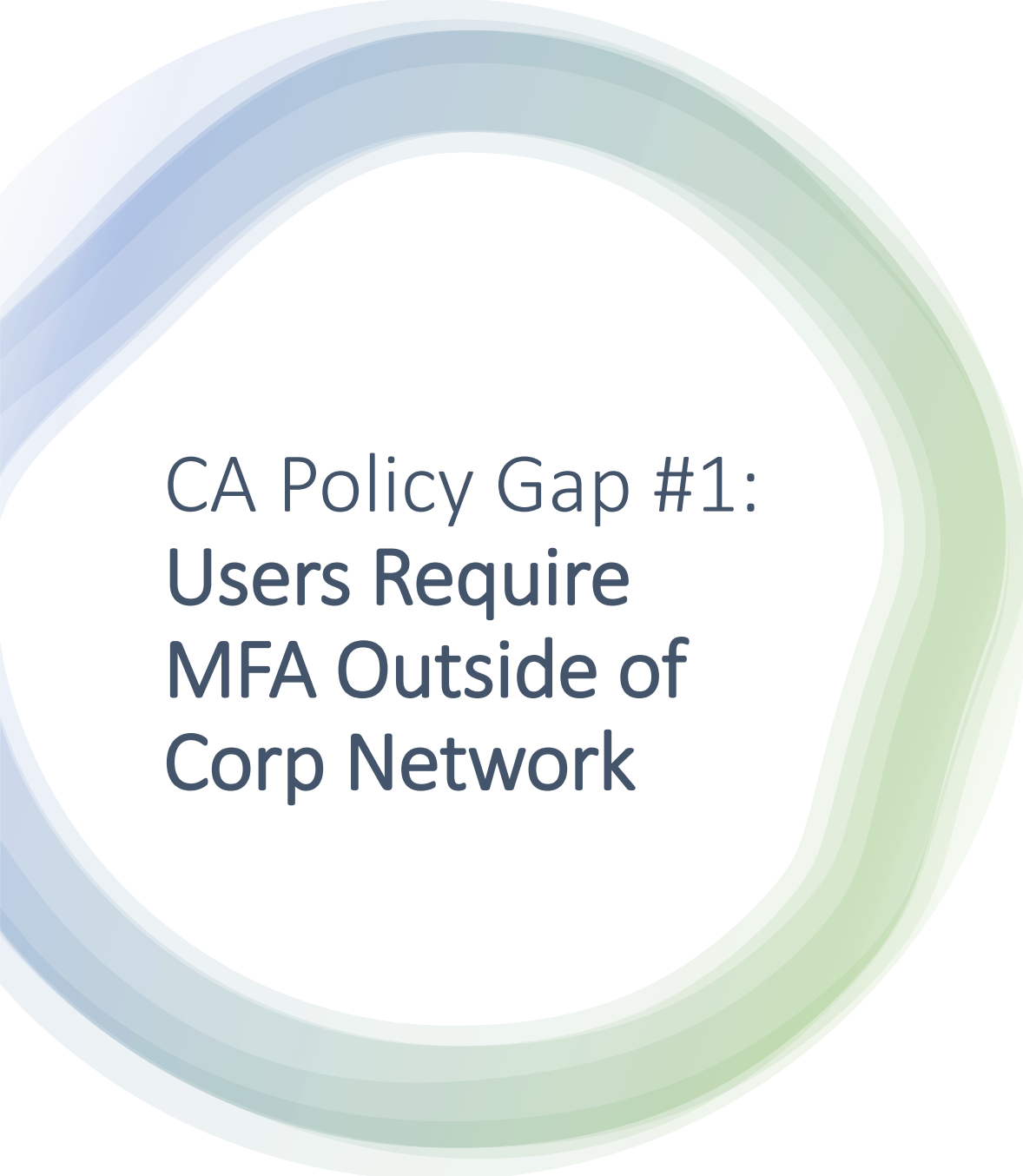
Require MFA for users with certain administrative roles



Block legacy authentication (username & password auth)



Block/Grant access from specific locations



CA Policy Gap #1: Users Require MFA Outside of Corp Network

CAP requires users to MFA when they are working remotely (not on the corporate network or connected via VPN)

Assumes no attacker would be on the corporate network

Attacker can use username/password without having to MFA

Fun Fact: Attackers love SSO!

CA Policy Gap #2:

Admins don't require MFA

MFA is required for certain users to access specific applications

However, there is no CAP that requires MFA for Admins

Or... CAP only requires members of a few roles use MFA

Attacker can use username/password without having to MFA

- Fun Fact: Attackers love SSO!

CA Policy Gap #3:

Exclusions

- CAP includes several security controls
 - MFA required
 - AAD Joined & Compliant device
 - Location based access
- However, there are exclusions:
 - Admins
 - VIPs
 - Executives
 - HR
 - Etc
- This creates a significant gap in security posture
- Attackers love being excluded from security controls!

Microsoft Provided Conditional Access Policies



Baseline Policies



Conditional Access Templates



Microsoft Managed Policies

Microsoft Managed Policies (MMP)

- Deployed automatically in reporting mode
- Modification is limited:
 - Exclude users
 - Turn on or set to Report-only mode
 - Can't rename or delete any Microsoft-managed policies
 - Can duplicate the policy to make custom versions
- Microsoft might update these policies in the future
- MMPs turn on (set to enabled) 90 days after introduced to the tenant
- Currently focuses on 3 areas:
 - MFA for admins accessing Microsoft Admin Portals
 - MFA for per-user MFA configured on users
 - MFA and reauthentication for risky sign-ins

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/managed-policies>

Key Conditional Access Policies

Require	Require MFA for accounts with administrative roles (preferably FIDO2)
Block	Block legacy authentication (username & password authentication)
Block	Block location by geography
Block	Block device code flow*
Enforce	Enforce device compliance on all devices
Restrict	Restrict access to apps by location
Require	Require MFA for guest users



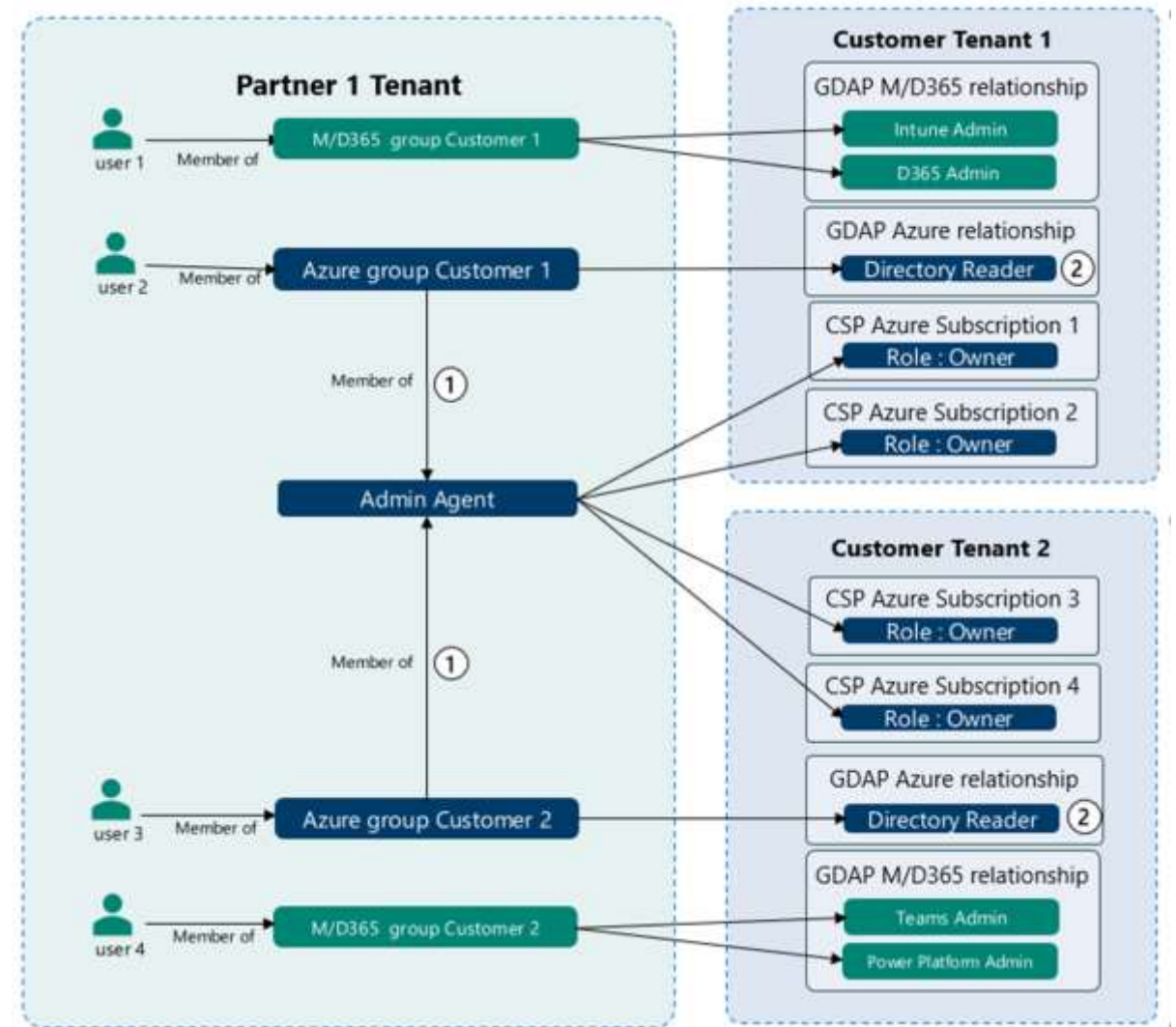
#9 Secure Partner Access

Partner Relationships – aka Delegated Administration

- A configured partner can have admin rights to a customer tenant (“delegated administration”).
- This is provided when the partner requests access to the customer environment.
- When the customer accepts this request:
 - “Admin agent” role in partner tenant is provided effective “Global Administrator” rights to customer tenant.
 - “Helpdesk Agent” role in partner tenant is provided effective “Helpdesk Administrator” (Password Administrator) rights to customer tenant.
 - These are the only options.
 - They **apply to all customer environments** – there is no granular configuration.
- A partner with dozens of customers will result in all partner accounts in these groups having elevated rights in all customer environments.

Shift to granular delegated admin privileges (GDAP) ASAP!

Move to Granular Delegated Admin Privileges (GDAP)



<https://learn.microsoft.com/en-us/partner-center/gdap-introduction>



Trimarc RD - BIG MEGA CORP | Delegated admin partners ...

×

«

Got feedback?

▼ Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Delegated admin partners

ⓘ

Delegated admin partners are Microsoft partners that you have authorized to administer Microsoft services in your tenant using delegated administration privileges.

Partner Name	Relationship type	Roles
No partner relationships		

Check Partner Configuration for your tenant here:

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/PartnerRelationships



#10 Secure Entra Connect

Compromising Entra Connect (on-prem)



Compromise Active Directory



Get admin rights on
Entra Connect server
(or SQL db)

OU admin rights
Local admin rights
GPO modify rights
Get local admin password on
other systems (when not
unique)



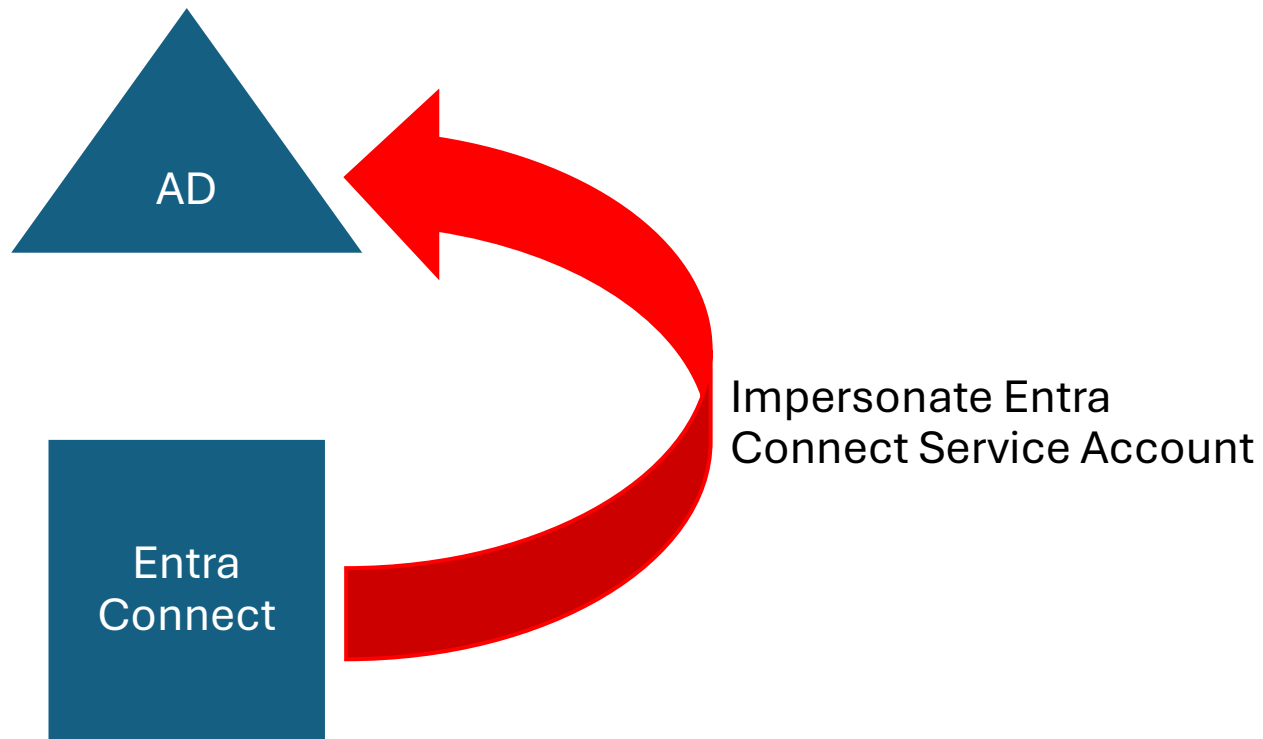
Gain control of
management system

Microsoft SCCM (or similar)
Vulnerability scanner

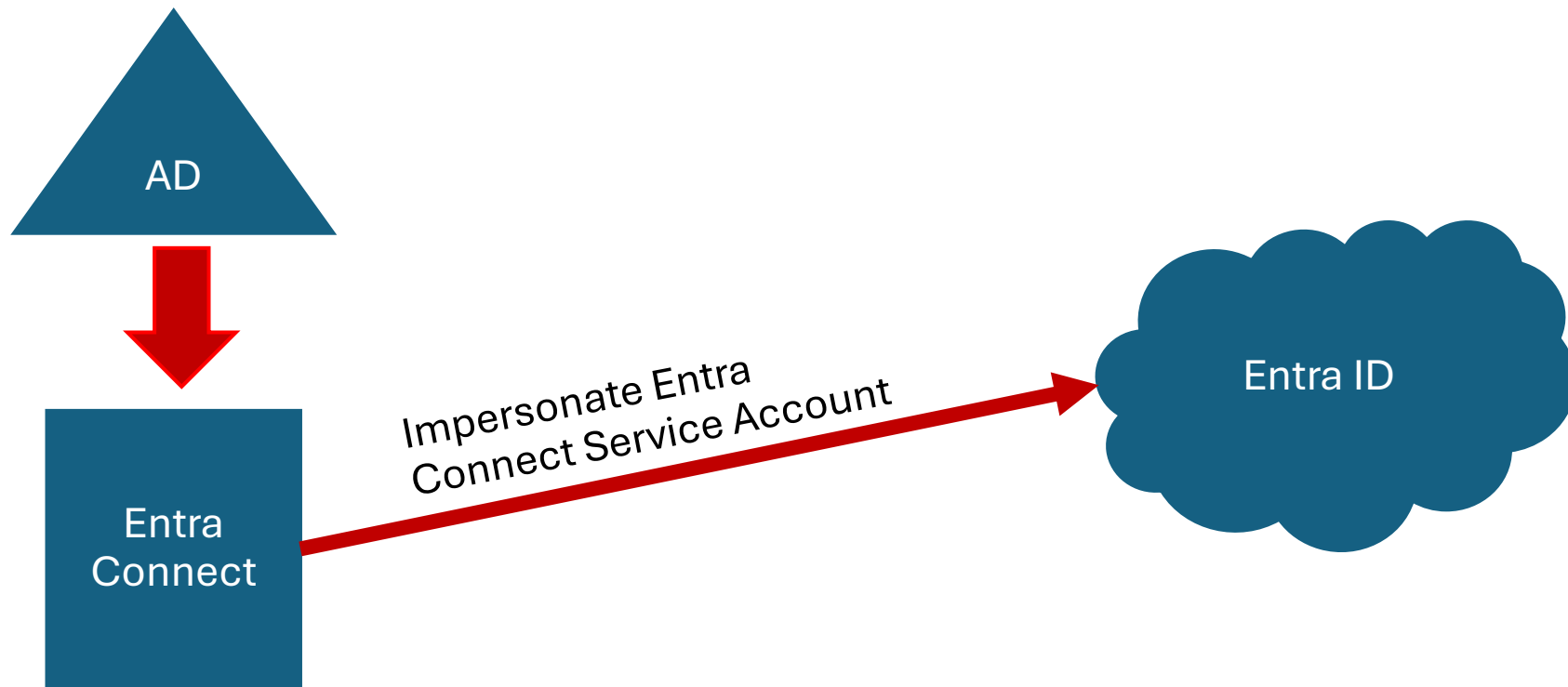


Compromise VMware (or other virtual
platform)

From Entra Connect to Active Directory



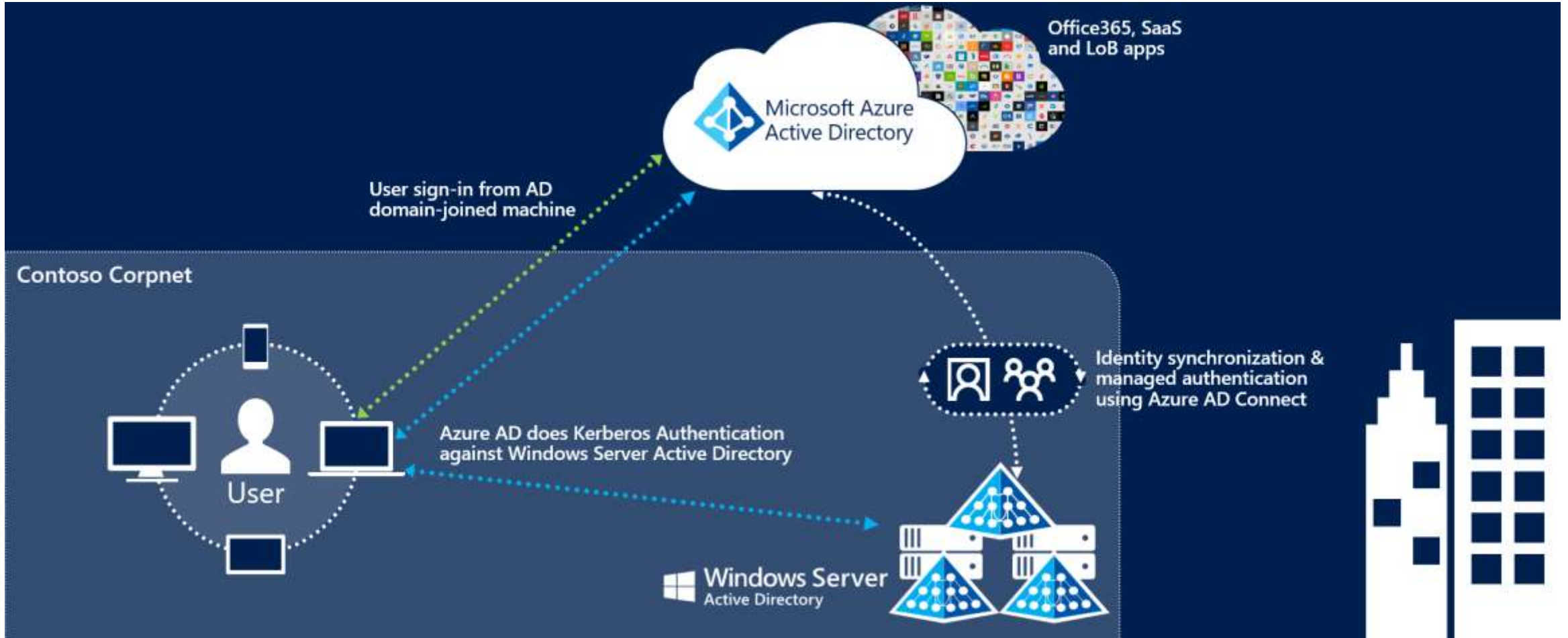
From Entra Connect to Entra ID



Defending Azure AD Connect

Treat	Treat the Azure AD Connect server, SQL server/database, & service account as Tier 0 (like Domain Controllers).
Ensure	Ensure that the Azure AD Connect server & SQL server/database is in a top-level admin OU.
Limit	Limit the group policies that apply to Azure AD Connect related systems.
Restrict	Restrict local admin rights on Azure AD Connect related systems.

Securing Seamless Single Sign-On (SSSO)



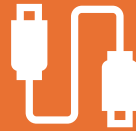
Attacking Azure AD Seamless Single Sign-On

- Managed by Azure AD Connect
- “Azure AD exposes a publicly available endpoint that accepts Kerberos tickets and translates them into SAML and JWT tokens”
- Compromise the Azure AD Seamless SSO Computer Account password hash (“AZUREADSSOACC “)
- Generate a Silver Ticket for the user you want to impersonate and the service ‘aadg.windows.net.nsatc.net ‘
- Inject this ticket into the local Kerberos cache
- Azure AD Seamless SSO computer account password doesn’t change

<https://www.dsinternals.com/en/impersonating-office-365-users-mimikatz/>

Sean Metcalf | @PyroTek3 | sean.metcalf@trustedsec.com

Securing Seamless Single Sign-On (SSSO)



For Windows 10, Windows Server 2016, and later versions, it's recommended to use SSO via primary refresh token (PRT).

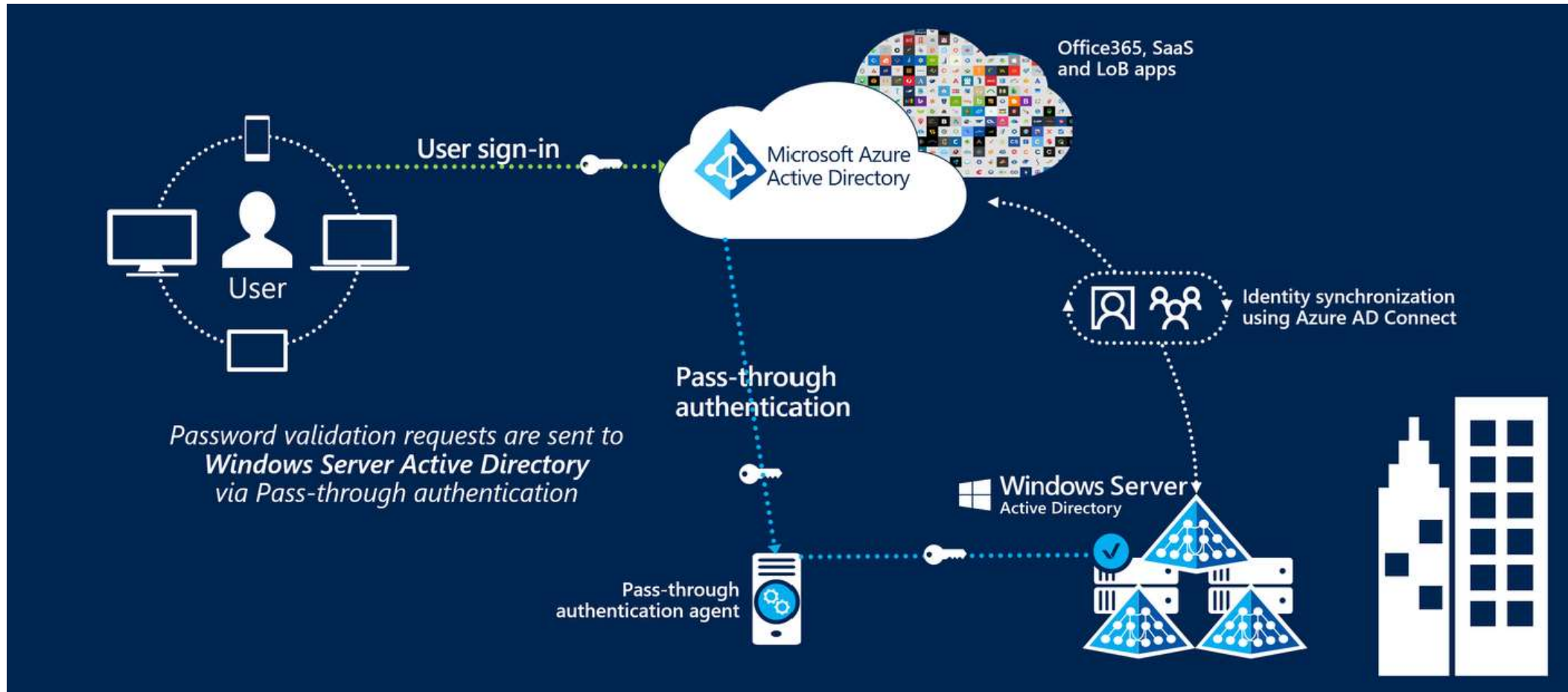


For Windows 7 and Windows 8.1, it's recommended to use Seamless SSO



Ensure the Azure AD Seamless Single Sign-On key (password) changes several times a year.

Microsoft Pass-Through Authentication (PTA)



<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

Attacking Microsoft PTA



Managed by Azure AD Connect



Compromise server hosting PTA (typically Azure AD Connect server)



Azure AD sends the clear-text password (not hashed!) to authenticate the user.



Inject DLL to compromise credentials used for PTA

<https://blog.xpnsec.com/azuread-connect-for-redteam/>

Sean Metcalf | @PyroTek3 | sean.metcalf@trustedsec.com

Securing Pass Through Authentication (PTA)

- Treat Azure AD Connect as a Tier 0 asset (like a Domain Controller)



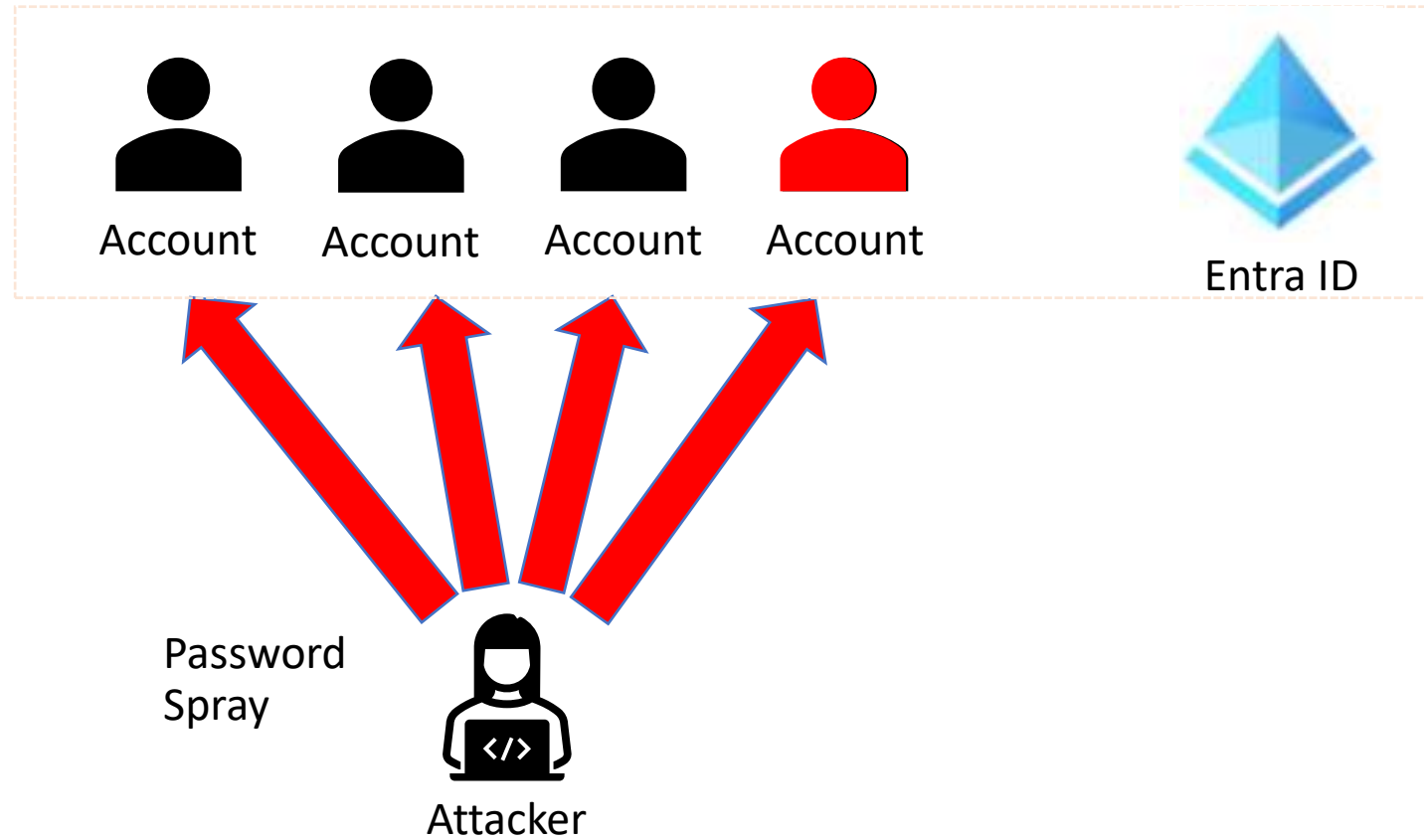


Entra ID Attacks

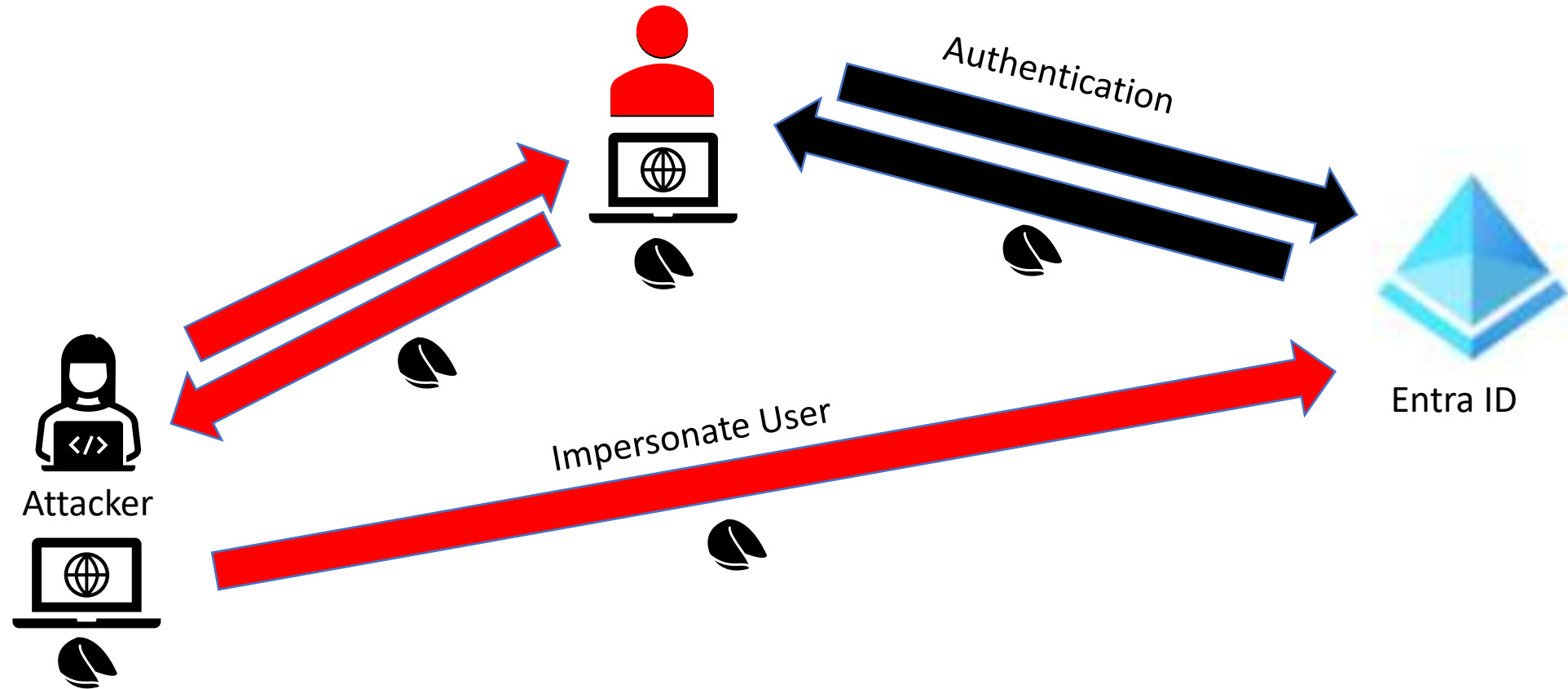
Attack Tools

- [AADInternals](#)
- [Evilginx2](#)
- [GraphRunner](#)
- [GraphSpy](#)
- [Microburst](#)
- [MFASweep](#)
- [MSOLSpray](#)
- [O365Recon](#)
- [Onedrive_user_enum](#)
- [ROADTools](#)
- [Teamfiltration](#)
- [TokenTactics/TokenTactics2](#)

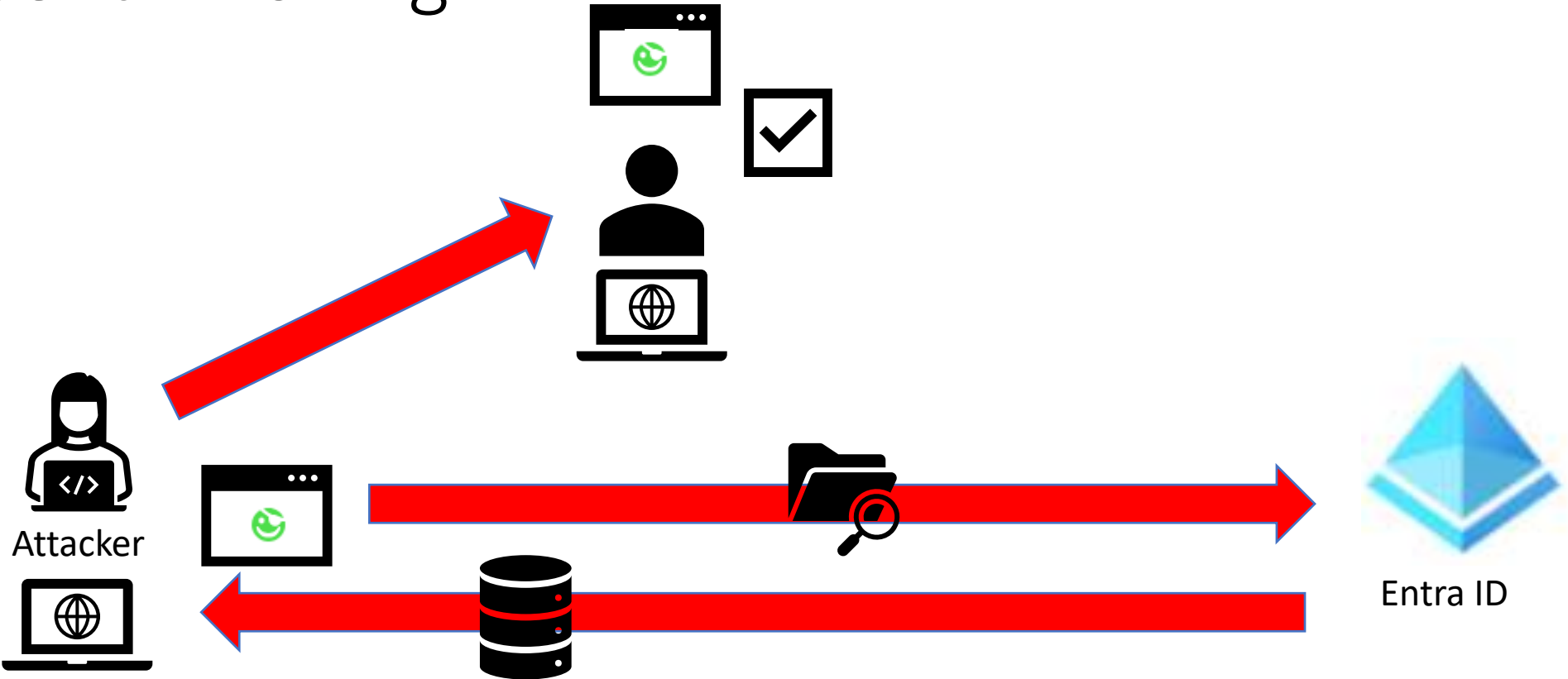
Password Spray Attack



Token Theft & Replay

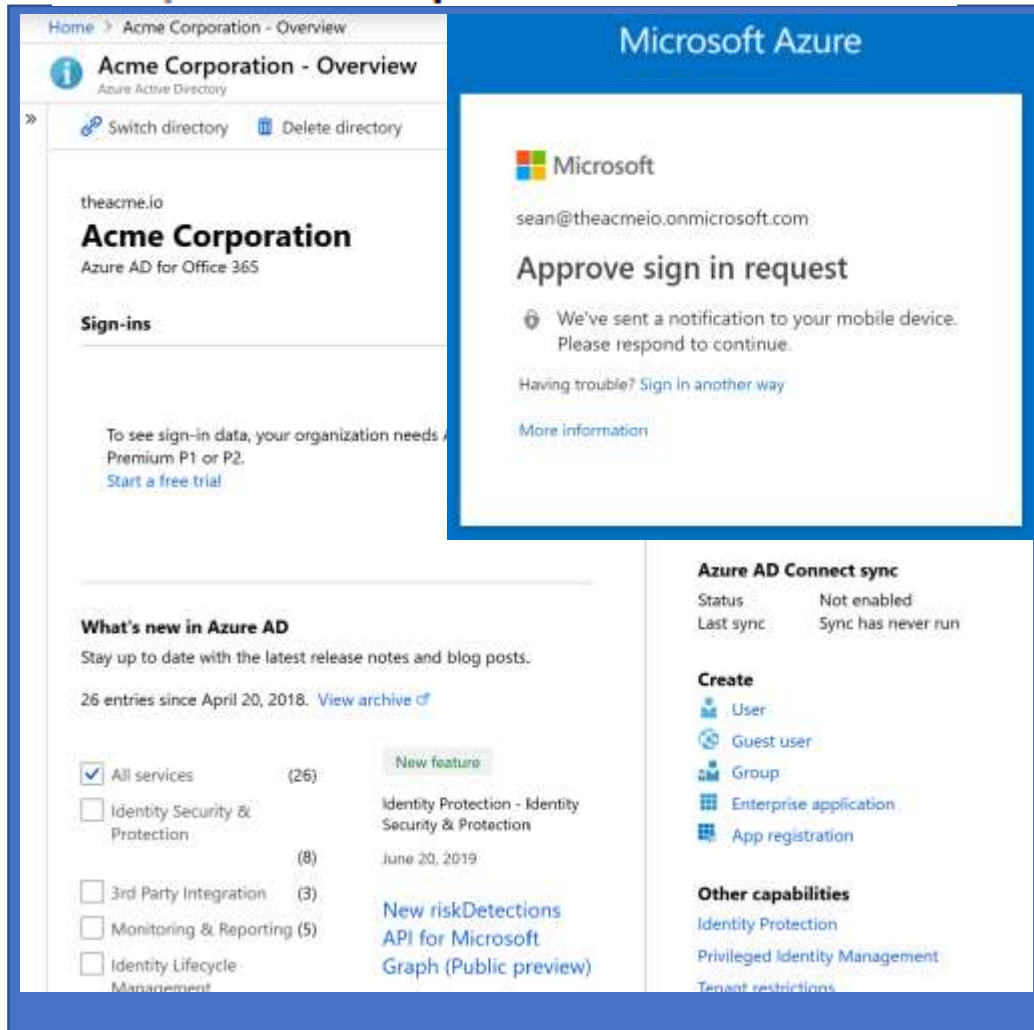


Consent Phishing

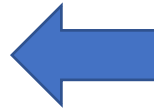


Token Theft with evilginx

<https://aad.portalazure.com/>



Auth



Token



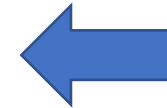
evilginx.

<https://github.com/kgretzky/evilginx2>

<https://aad.portal.azure.com/>

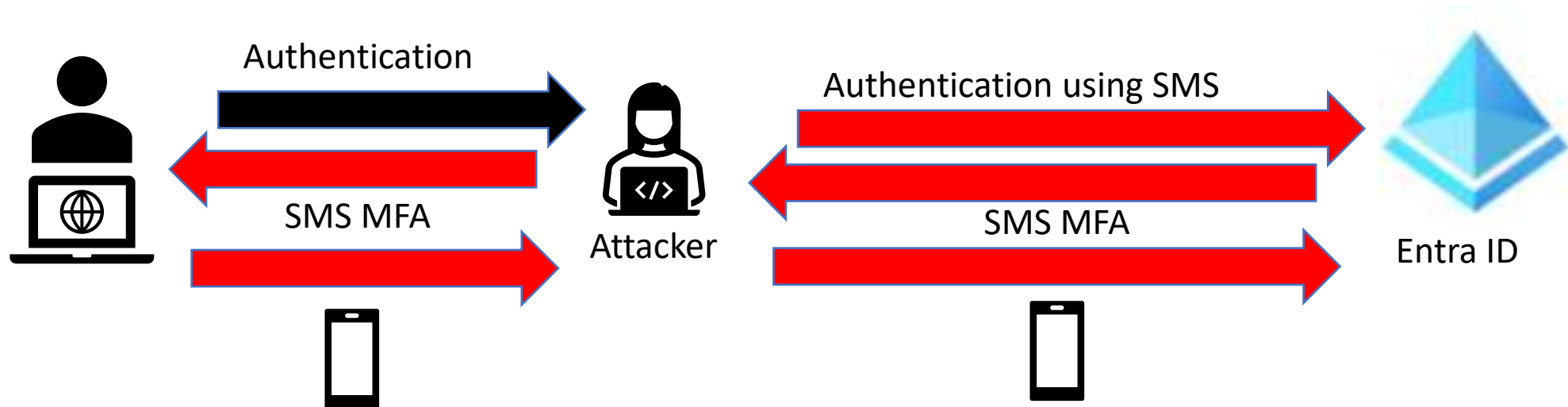


Auth

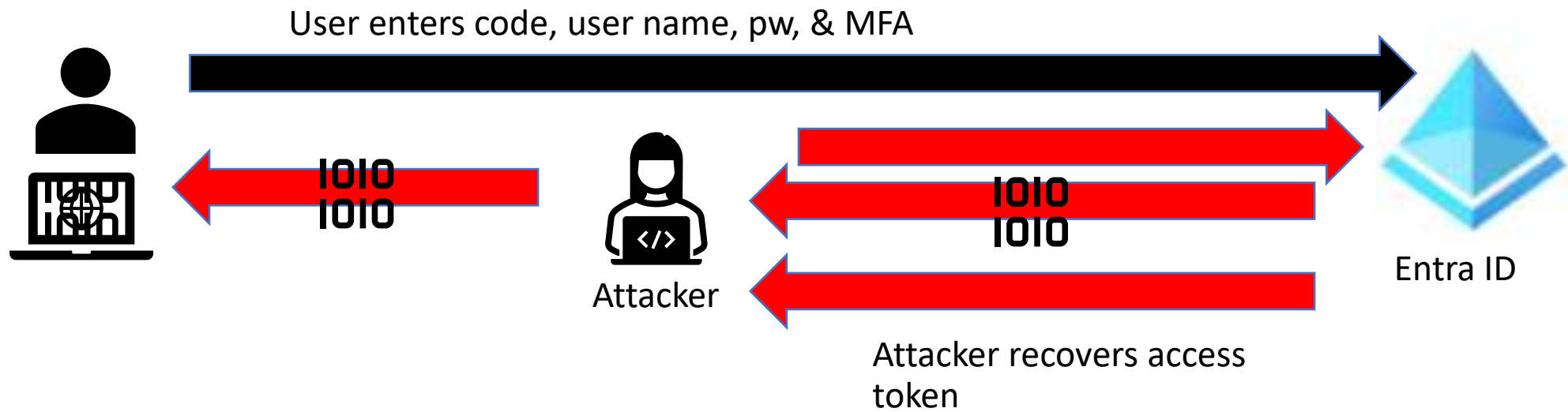


Token

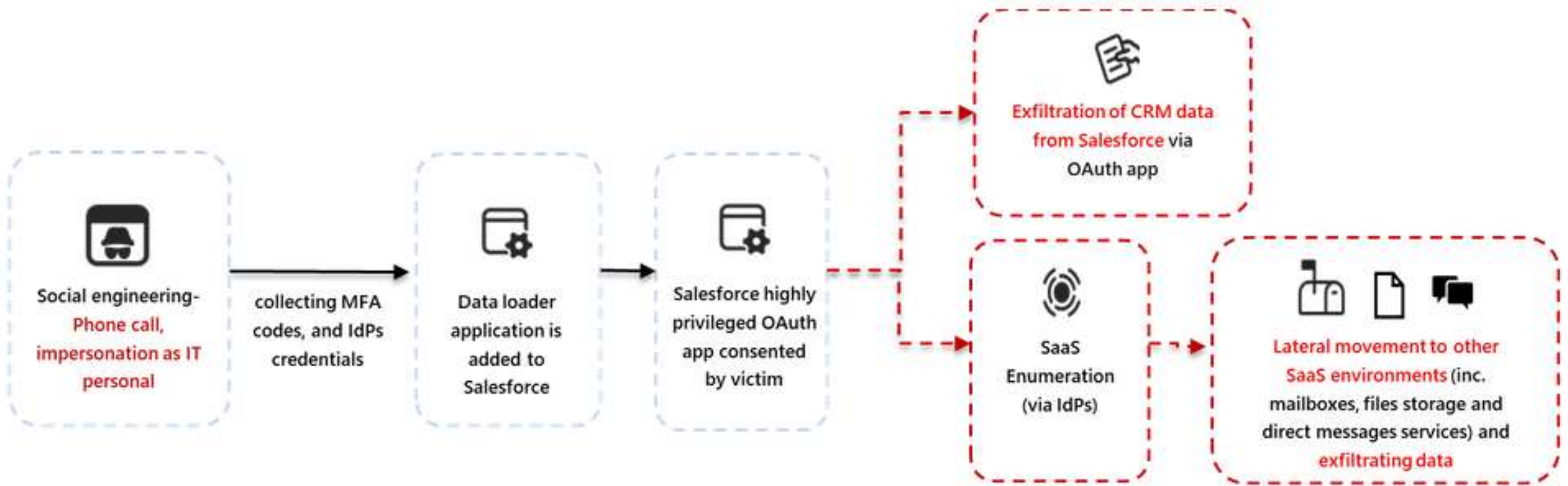
MFA Downgrade Attack



Device Code Flow Attack



Salesforce OAuth Attack



<https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/protect-against-oauth-attacks-in-salesforce-with-microsoft-defender/4450584>



Bonus: Securing Entra ID

Securing Entra ID - Microsoft Summary



Manage from Cloud controlled Devices

Use Azure AD Join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure, which can compromise device and security controls.



No on-prem account has Azure AD / Microsoft Office 365 privileges

Privileged on-premises software must not be capable of impacting Azure AD privileged accounts or roles.



Use Azure AD cloud authentication to eliminate on-prem credential dependencies.

Always use strong authentication, such as Windows Hello, FIDO, the Microsoft Authenticator, or Azure AD MFA.

On-Prem: Entra Password Protection

- Prevent users from selecting known bad passwords
- Start in audit mode to get an idea how bad it is

Custom smart lockout

Lockout threshold ⓘ

10

Lockout duration in seconds ⓘ

70

Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

seahawks
mariners
sounders
redmond
washington

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

<https://aka.ms/deploypasswordprotection>

Phishing Defensive Layers

Require Users to MFA, preferably FIDO2

- Microsoft Authenticator app recommended

Conditional Access Policy

- Enforce MFA
- For specific apps
- Location based grant/block rules

Risk Based Policy

- Only prompt the user to take action when risk is detected

People will fall to Phishing no matter what so we must monitor...

Key Cloud Administration Security Controls

- Use admin systems for cloud administration
- Enforce FIDO2 for Level 0 roles
- FIDO2 keys for Emergency “Break Glass” Accounts
- Leverage Conditional Access policies to enforce MFA for admins from all locations

What are the most resilient MFA methods?

Folks, the **Azure MFA** enforcement will soon start rolling out and there will be **NO EXCEPTIONS** for **emergency access** accounts!

Here's a quick guide to help you pick the most resilient MFA method for your emergency access accounts 📌

TLDR: Use FIDO2 security key for emergency accounts

Rank	Depends on	Method
1 (Gold)	Entra Auth Service	FIDO2 security key
2 (Silver)	Entra Auth Service + Azure MFA Service	Password + Hardware Tokens OTP
3 (Bronze)	Entra Auth Service + Azure MFA Service + Phone carrier / Mobile OS / Internet	Password + Microsoft Authenticator Passwordless

<https://x.com/merill/status/1821027962864726249/>

Common Persistence Method Checks

Review Illicit Consent Grants

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide>

Review Exchange Forms/Rules for potentially malicious settings.

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide>

Review Exchange Online mailbox permissions for unusual/unintended configuration (Get-ExoMailboxPermission)

<https://docs.microsoft.com/en-us/powershell/module/exchange/powershell-v2-module/get-exomailboxpermission?view=exchange-ps>

Key Mitigations

- Disable Device Code Flow
<https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows>
- Leverage the Microsoft Authenticator app for MFA
- Disable Text/SMS as an MFA option
- Ensure cloud admins use a different system from standard web browsing
 - Another browser (at a minimum)
 - Remote into a cloud admin server
 - Use a separate computer for admin actions
- Ensure all Windows computers have VBS backed by a TPM
- Remove local admin rights from standard users on AAD Joined devices
- Do not allow users to join their own devices
- Don't let users consent to application permissions (or at least use Microsoft recommended)

Secure Entra ID Quickly Checklist

1. Set “Users can register applications” to No
2. Set “Restrict non-admin users from creating tenants” to Yes
3. Set “Users can create security groups” to No
4. Set Guest user access restrictions to “*Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)*”
5. Restrict who can join devices to Microsoft Entra & require MFA
6. Set Guest invite settings to “*Only users assigned to specific admin roles can invite guest users*”
7. Set User consent settings to “*Let Microsoft manage your consent settings (Recommended)*”
8. Review Level 0 role membership and ensure members are admin accounts, are PIM Eligible, & are not synchronized from on-prem
9. If you’re using Role Assignable Groups, ensure Owners are not set on Level 0 & 1 roles
10. Scrutinize any applications with Level 0 Application permissions
11. Ensure that Conditional Access requires MFA for Level 0 & 1 role members for every authentication, preferably FIDO2/Microsoft Authenticator push (service accounts & service principles excepted).
12. Remove any standard Delegated Administration and shift to Granular Delegated Admin Privileges (GDAP)
13. Treat Entra Connect as a Tier 0 asset (like a Domain Controller)
14. Ensure Cloud Admins are using a separate browser for admin activities (minimum) or connecting to a dedicated cloud admin server (recommended)
15. Ensure there is at least 1 emergency access admin account configured with a FIDO2 key(s).



Stay Up to Date on Entra ID Security

- [@TechBrandon](#) - Brandon
- [@_dirkjan](#) – Dirk-Jan
- [@EricaZellic](#) – Erica Zellic
- [@inversecos](#) - Inversecos
- [@ITGuySoCal](#) - Joe Stocker
- [@Merill](#) – Merrill Fernando
- [@NathanMcNulty](#) – Nathan McNulty

Sean's Entra ID Security List:
[PyroTek.io/EntralDSecurityList](https://pyrotek.io/EntralDSecurityList)



Conclusion



Attacker cloud capability continues to evolve

Defender methods need to evolve as well

There are key mitigations that disrupt multiple attacks



Slides:

PyroTek.io/BSNoVa2025

Sean Metcalf

@PyroTek3

sean.metcalf@trustedsec.com

Security Articles, Slides, & Video:

ADSecurity.org



Questions?