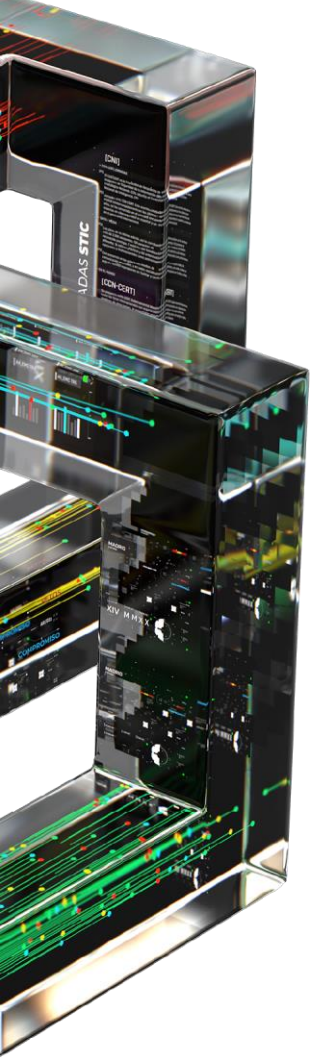
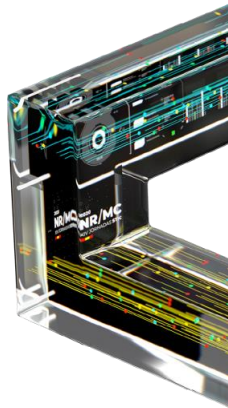


#XIVJORNADASCCNCERT

Bypassing Office 365 Security Controls



ccn-cert
centro criptológico nacional

- Juan Garrido
- nccgroup
- Juan.garrido@nccgroup.trust

Filtración de datos

Fuga de información sensible

- Información comprometedora
- Información secreta
- Información de clientes

Impacto negativo en la empresa

Si hay fuga, hay daño (Aunque no se venda)

Canales encubiertos

Ampliamente utilizados desde hace siglos

Los datos se ocultan utilizando un medio aparentemente inocuo

Metodología muy variada

- Depende mucho de los conocimientos y “picardía” del que lo realiza
- Desde el punto de vista del atacante, el medio siempre será inseguro

To the Members of the California State Assembly:

I am returning Assembly Bill 1176 without my signature.

For some time now I have lamented the fact that major issues are overlooked while many unnecessary bills come to me for consideration. Water reform, prison reform, and health care are major issues my Administration has brought to the table, but the Legislature just kicks the can down the alley.

Yet another legislative year has come and gone without the major reforms Californians overwhelmingly deserve. In light of this, and after careful consideration, I believe it is unnecessary to sign this measure at this time.

Sincerely,

Arnold Schwarzenegger

Madrid en 60 segundos

EL PERSONAJE DEL DÍA

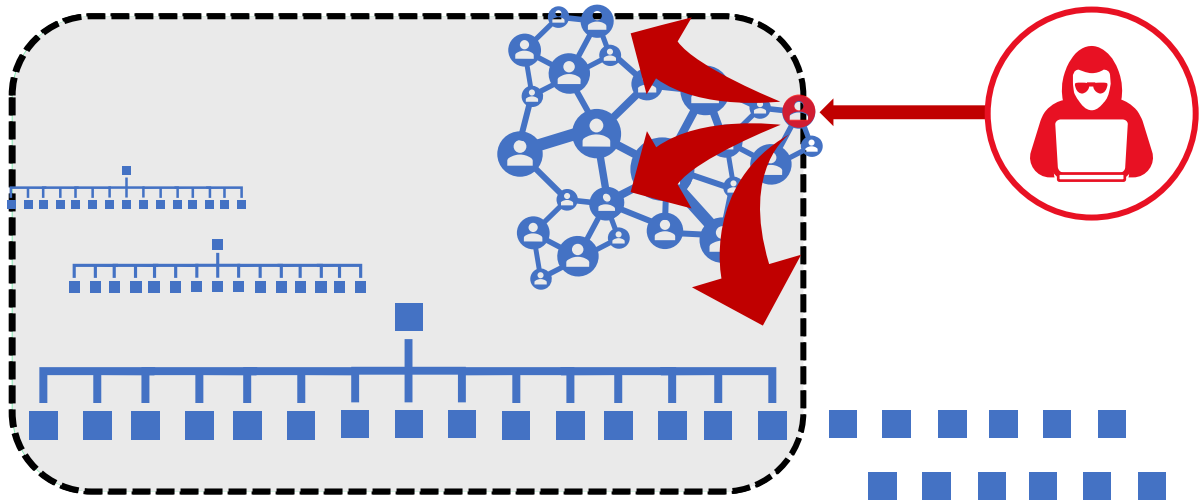
Julio Iglesias

Cantante

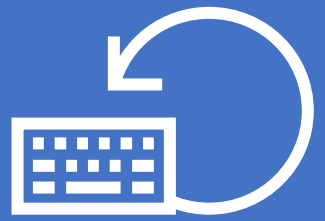
Julio Iglesias ha entrado en una polémica sin quererlo por la decisión de Ana Botella de investirle como hijo predilecto. O, por lo menos, la oposición es la que ha criticado este reconocimiento porque, dicen, es una decisión que ha llegado sin el acuerdo de los grupos. Estas propuestas, aseguran, las tienen que alcanzar los partidos en consenso, pues son unos «honores que la ciudad tiene que entregar y no otorgarlos sólo el Gobierno». Al margen de esto, se prevé que marzo sea el mes en que Madrid otorgue el premio al cantante.

¿Por qué es necesaria una iniciativa Zero Trust?

Control de acceso: Mantener los **recursos** lejos de **atacantes**



1. **La seguridad IT es compleja**
   - Muchos dispositivos, usuarios, conexiones, etc..
2. **Estrategia de "Red confiable y segura"**
   - Riesgo bajo de ataque dentro de la red
3. **Acceso desde cualquier sitio**
   - BYOD, WFH, Mobile, and SaaS
4. **Ataque a la identidad**
   - Phishing y robo de identidad
   - Carga de trabajo alta para los equipos de seguridad



Ataque a la identidad para bypassear los controles de red

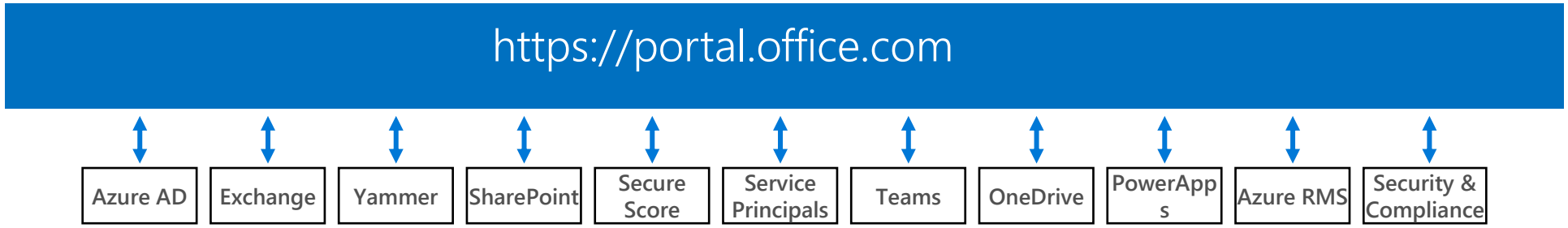
Una simple contraseña no es suficiente para proteger identidades

La identidad puede ser usada en múltiples aplicaciones

Puede ser usada incluso fuera de nuestra red

Un portal
Múltiples servicios
Toda la información

Azure AD
Exchange
Skype for Business
Teams
Yammer
SharePoint
Etc…



Zero Trust Principles

Verifica de manera explicita

Autentica basándote en todos los puntos de acceso disponibles, incluyendo localización, salud del dispositivo, identidad de usuario, anomalías, etc..

Principio del mínimo privilegio

Minimiza el acceso a los datos a sólo lo que el usuario necesite. Aplica reglas de DLP, Tags, derechos de acceso (RMS), etc..

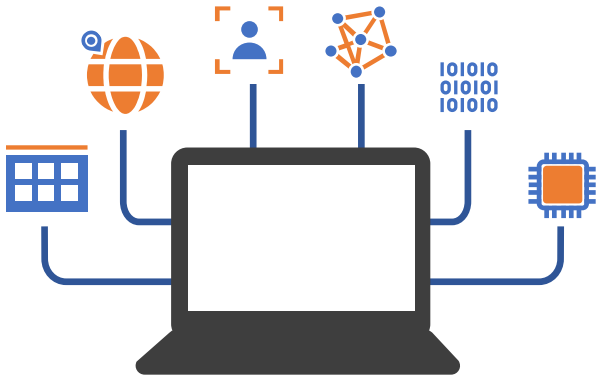
Asumir brecha de seguridad

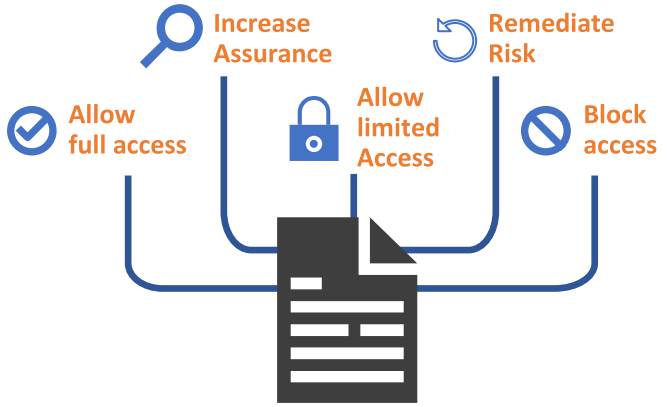
Minimiza el daño verificando todas las sesiones, desde todos los puntos de acceso

Bypass Location Policies

Zero Trust Principles

Nunca confíes y siempre verifica





Signal

Para informar al usuario

Dispositivo
- MDM
- Threat Detection
- Azure AD…

Usuario
- MFA
- Análisis de comportamiento
- Etc..

Decision

Basada en la política de la empresa

Aplica decisiones a todo intento de acceso

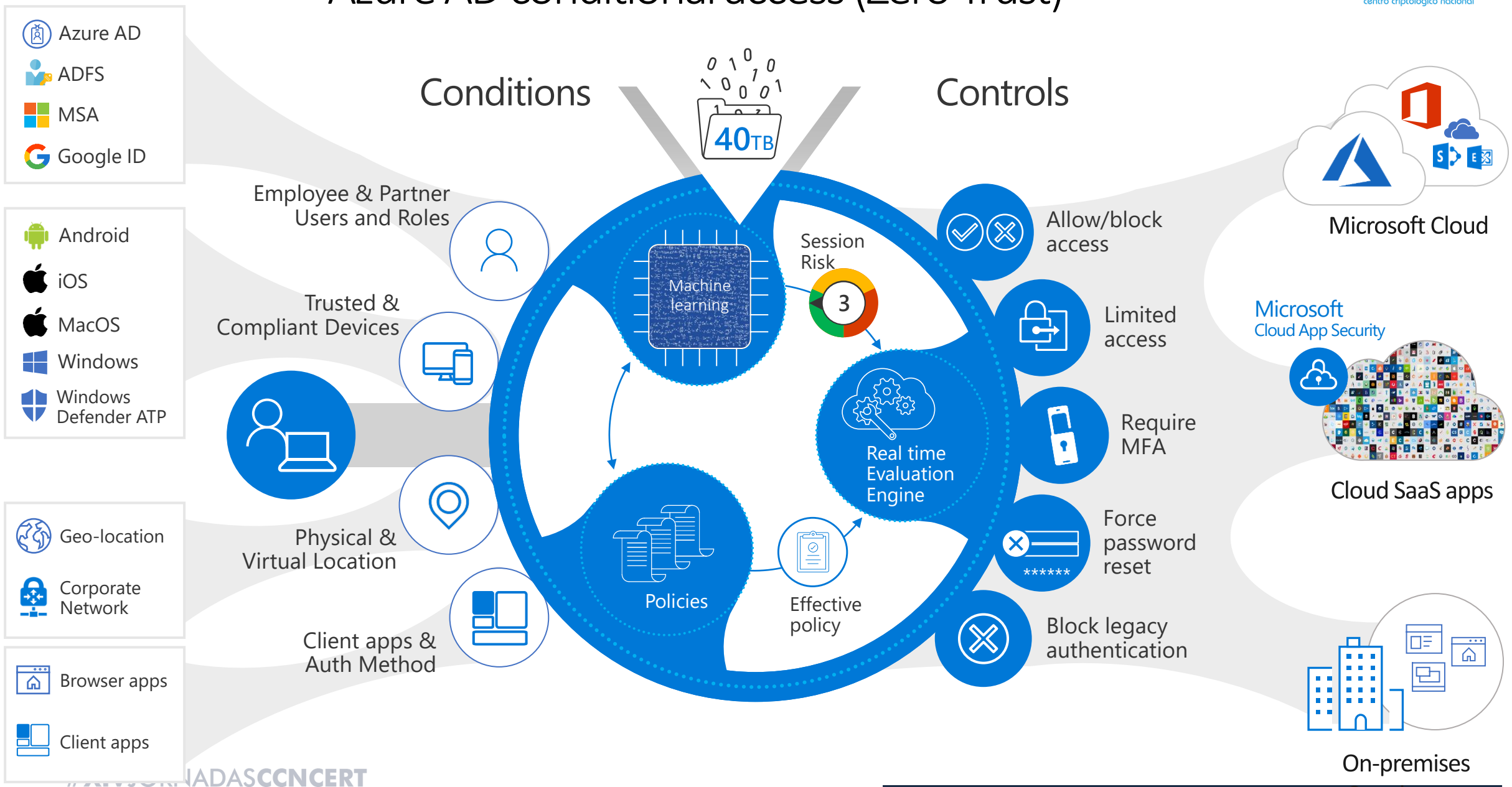
Re-Evalua las decisions durante la sesión

Refuerzo

Políticas aplicadas a los recursos

OAUth aplicaciones
Aplicaciones SaaS
Aplicaciones Legacy
Etc…

Azure AD conditional access (Zero Trust)



Conditional Access Ejemplo

User

- **Role**: Director
- **Group**: Spain Users
- **Device:** Windows
- **Config:** Corp
- **Location**: Spain
- **Last Sign-in**: 5 hrs ago

Device

- **Health**: Device compromised
- **Client**: Browser
- **Config**: Anonymous
- **Last seen**: EEUU

Conditional access risk

- High
- Medium
- Low

Bloquea Acceso

Fuerza acciones adicionales

Office Resources

Sensitivity: Medium

- Actividad maliciosa detectada en dispositivo
- IP anónima
- Localización desconocida

Abuso de APIs ocultas

- Cada uno de estos servicios tiene como mínimo una API asociada (O un Web Service) para ser consumida desde el portal de Office o por módulos de PowerShell
- Muchos servicios tienen múltiples APIs
- Estas APIs a su vez pueden tener un sistema de versiones. En función de la version utilizada, ésta mostrará mas o menos información
- Muchas de estas APIs exponen un fichero de metadatos en donde se indican los métodos existentes, así como los parámetros de entrada

Abuso de APIs ocultas

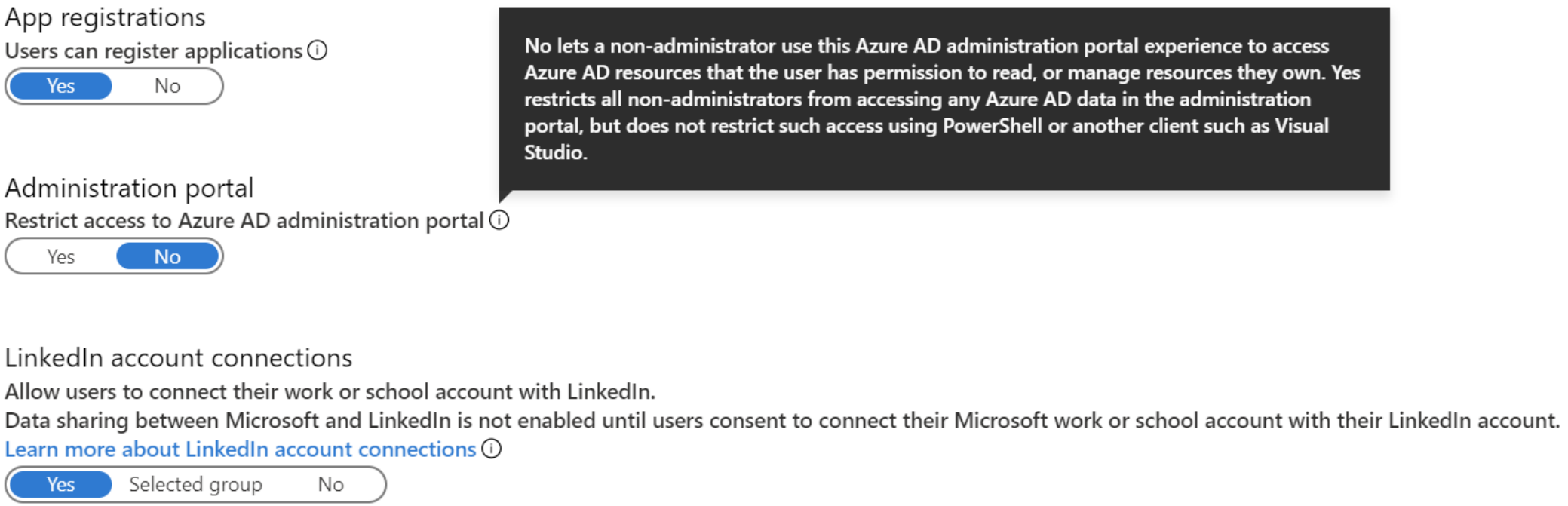
OneDrive & SharePoint Online

Endpoint	Tipo de Acceso	Versiones
https://graph.microsoft.com	Información básica de O365 y Azure Active Directory	V1.0 & beta
https://[dominio]-my.sharepoint.com/personal	Acceso OneDrive	
https://[dominio].sharepoint.com https://[site][dominio].sharepoint.com https://[dominio]-admin.sharepoint.com	Acceso SharePoint Online	
https://webshell.office.com	Acceso funcionalidades Office 365 desde el Portal	
https://[subdomain].sphomep.svc.ms	Datos estáticos, miniaturas de documentos, imágenes, etc..	
https://portal.office.com	API usada por el propio portal con información para bypassear location based policies	

Abuso de APIs ocultas

Azure Active Directory

- Un administrador podrá denegar el acceso al portal de Azure AD
- Pero no podrá denegar el acceso a ciertas APIs



Bypass Conditional Access

Abuso de APIs ocultas

OneDrive & SharePoint Online

Endpoint	Tipo de Acceso	Versiones
https://graph.microsoft.com	Información básica de O365 y Azure Active Directory	V1.0 & beta
https://[dominio]-my.sharepoint.com/personal	Acceso OneDrive	
https://[dominio].sharepoint.com https://[site][dominio].sharepoint.com https://[dominio]-admin.sharepoint.com	Acceso SharePoint Online	
https://webshell.office.com	Acceso funcionalidades Office 365 desde el Portal	
https://[subdomain].sphomep.svc.ms	Datos estáticos, miniaturas de documentos, imágenes, etc..	
https://portal.office.com	API usada por el propio portal con información para bypassear location based policies	
https://portal.azure.com	El portal de Azure tiene capacidades para pedir tokens de otras aplicaciones	

Bypass Conditional Access

Abuso de APIs ocultas

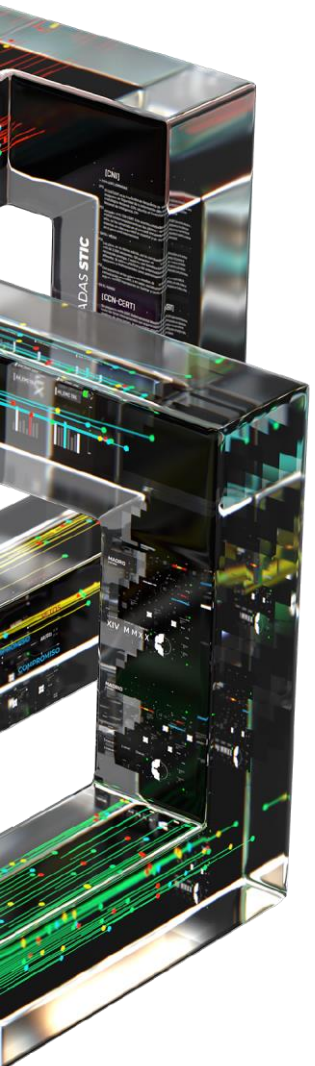
OneDrive & SharePoint Online

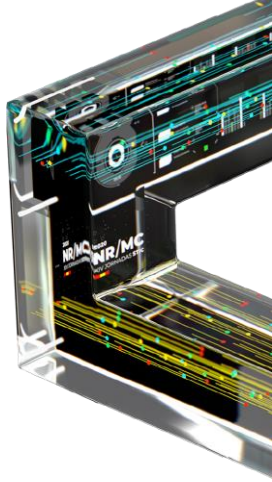
Endpoint	Tipo de Acceso	Versiones
https://graph.microsoft.com	Información básica de O365 y Azure Active Directory	V1.0 & beta
https://[dominio]-my.sharepoint.com/personal	Acceso OneDrive	
https://[dominio].sharepoint.com https://[site][dominio].sharepoint.com https://[dominio]-admin.sharepoint.com	Acceso SharePoint Online	
https://webshell.office.com	Acceso funcionalidades Office 365 desde el Portal	
https://[subdomain].sphomep.svc.ms	Datos estáticos, miniaturas de documentos, imágenes, etc..	
https://portal.office.com	API usada por el propio portal con información para bypassear location based policies	
https://portal.azure.com	El portal de Azure tiene capacidades para pedir tokens de otras aplicaciones	
https://msgraph.yammer.com	API no documentada de Yammer	
https://www.yammer.com/api	API Yammer	

Bypass Conditional Access

Conclusiones

- Configura y habilita las auditorías en el portal de Security & Compliance Manager
- Revisa los privilegios de los usuarios y revoca el acceso a servicios que no vayan a usar
- Configura el acceso a recursos basados en Conditional Policies
  - Crea políticas para toda aplicación
  - Evita generar políticas que afecten a todas las aplicaciones
  - Crea cuentas de tipo break-glass
- Deshabilita la autenticación básica en todos los servicios de Office 365
- Revoca privilegios que no sean necesarios:
  - Acceso a Exchange desde PowerShell
  - Acceso a la aplicación de Graph Explorer





MUCHAS GRACIAS

#XIVJORNADASCCNCERT