



Ingeniería
Tecnología
Seguridad

ENERO 2026
Que proponemos?

MICROSOFT **ENTRA**

Gestión de Acceso Seguro



Aumentando Capas de Seguridad - Acceso a Recursos Locales, Mas que una VPN -
Sincronizando AD - Extendiendo Directiva Local - AuthN y AuthZ; MFA - SSO - ZTNA - Tenants



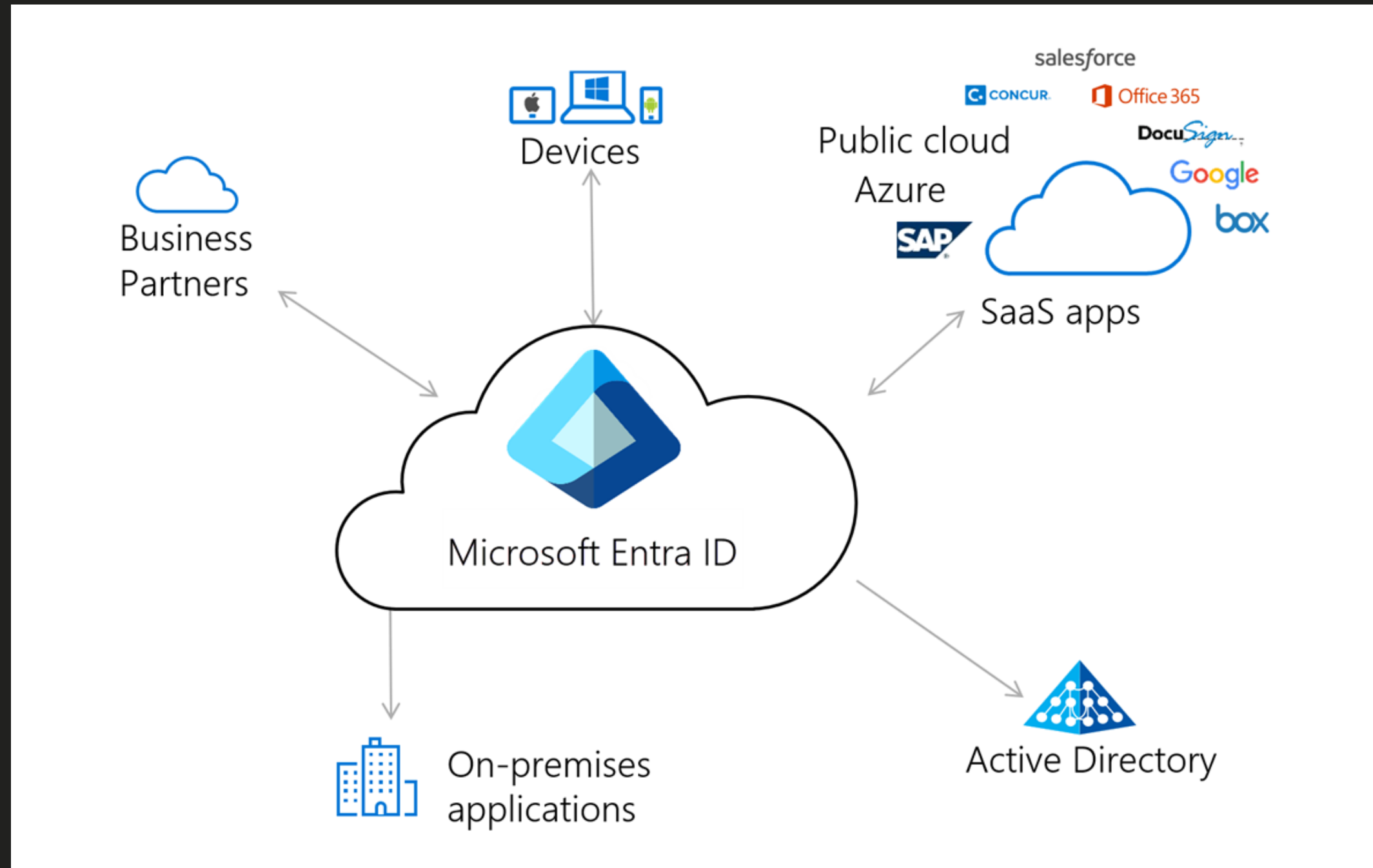
Microsoft Entra Suite

for Unified Identity & Network Security!



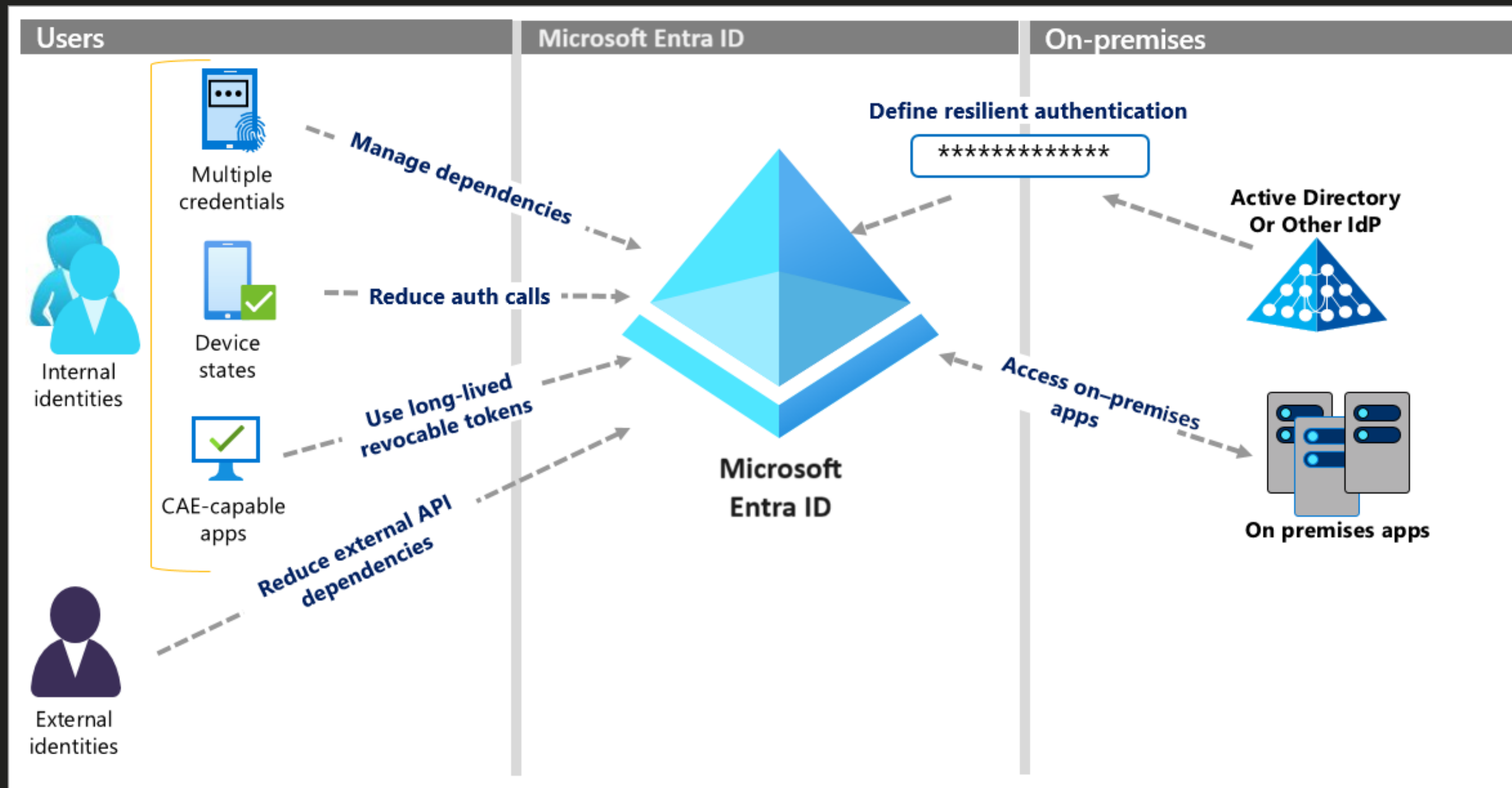


MICROSOFT **ENTRA ID**





MICROSOFT ENTRA ID





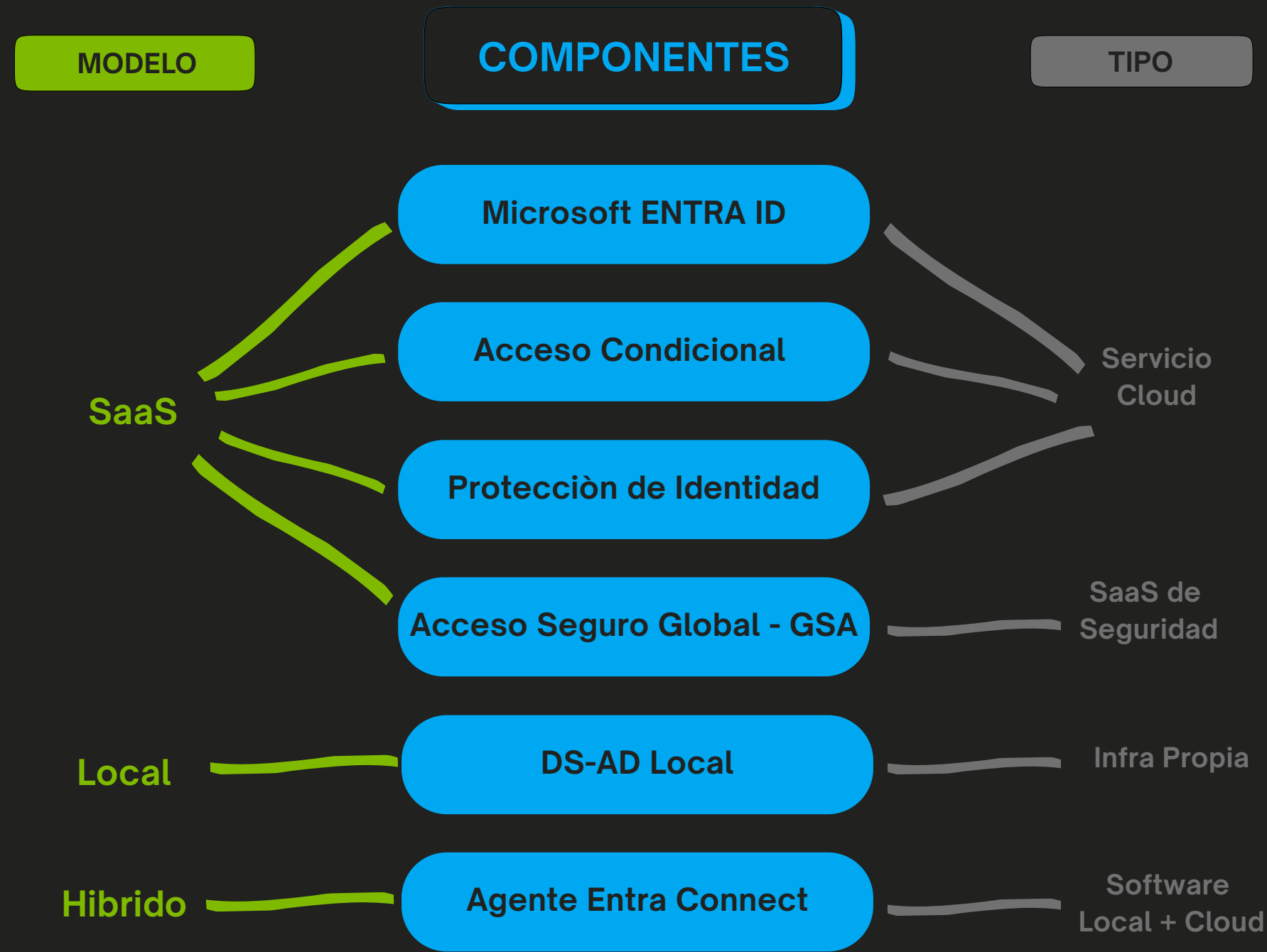
Desafío Actual en el Acceso a Aplicaciones Locales

- Las organizaciones aún mantienen aplicaciones críticas en entornos locales (on-premises).
- El acceso remoto a estos sistemas suele ser inseguro o difícil de controlar.
- Microsoft Entra ID + Global Secure Access permiten integrar identidad, seguridad y acceso sin VPN.
- Más capas de seguridad en Gestión de Acceso a las Identidades, protocolos modernos en procesos de Auth. y AuthZ.
- **Caso Base:** aplicación IIS publicada en entorno corporativo.



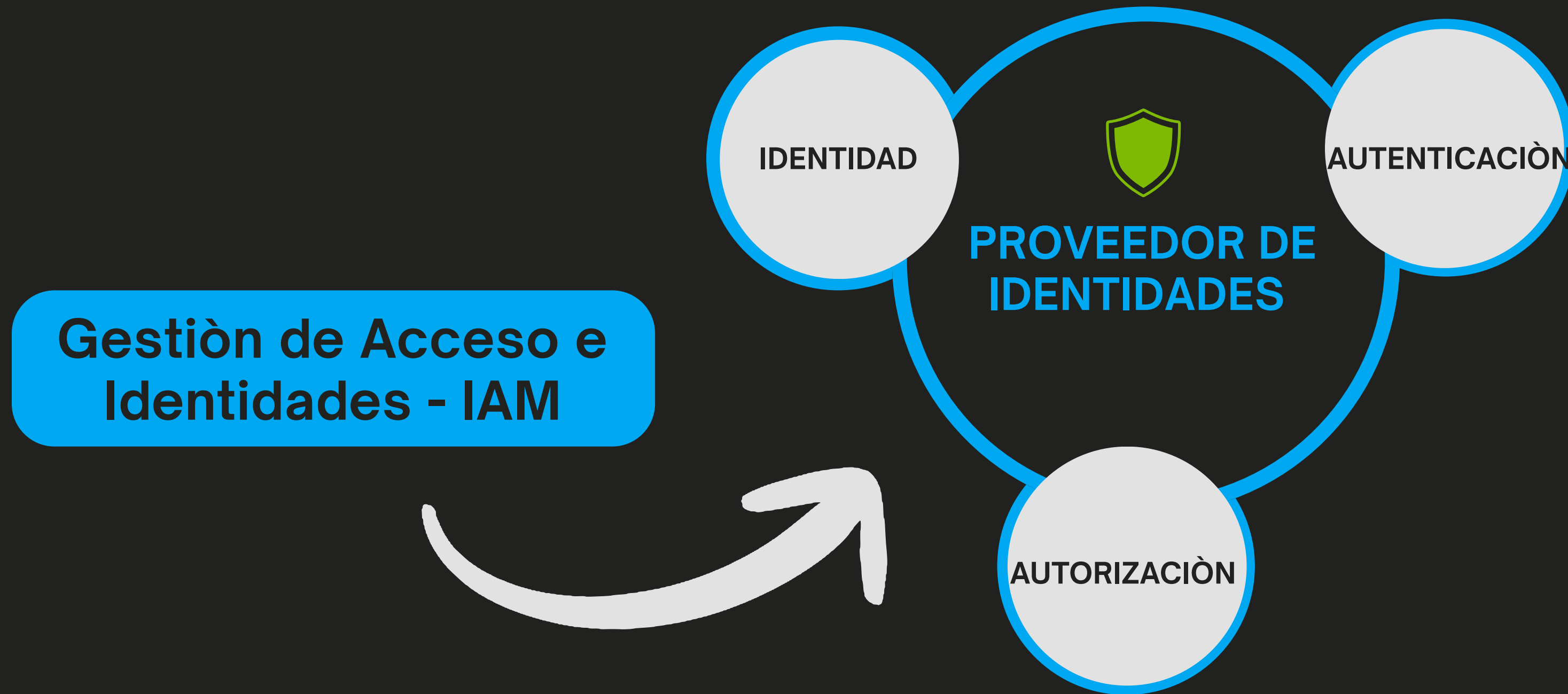
Agregando Capas de Seguridad al Acceso

ENFOQUE HIBRIDO



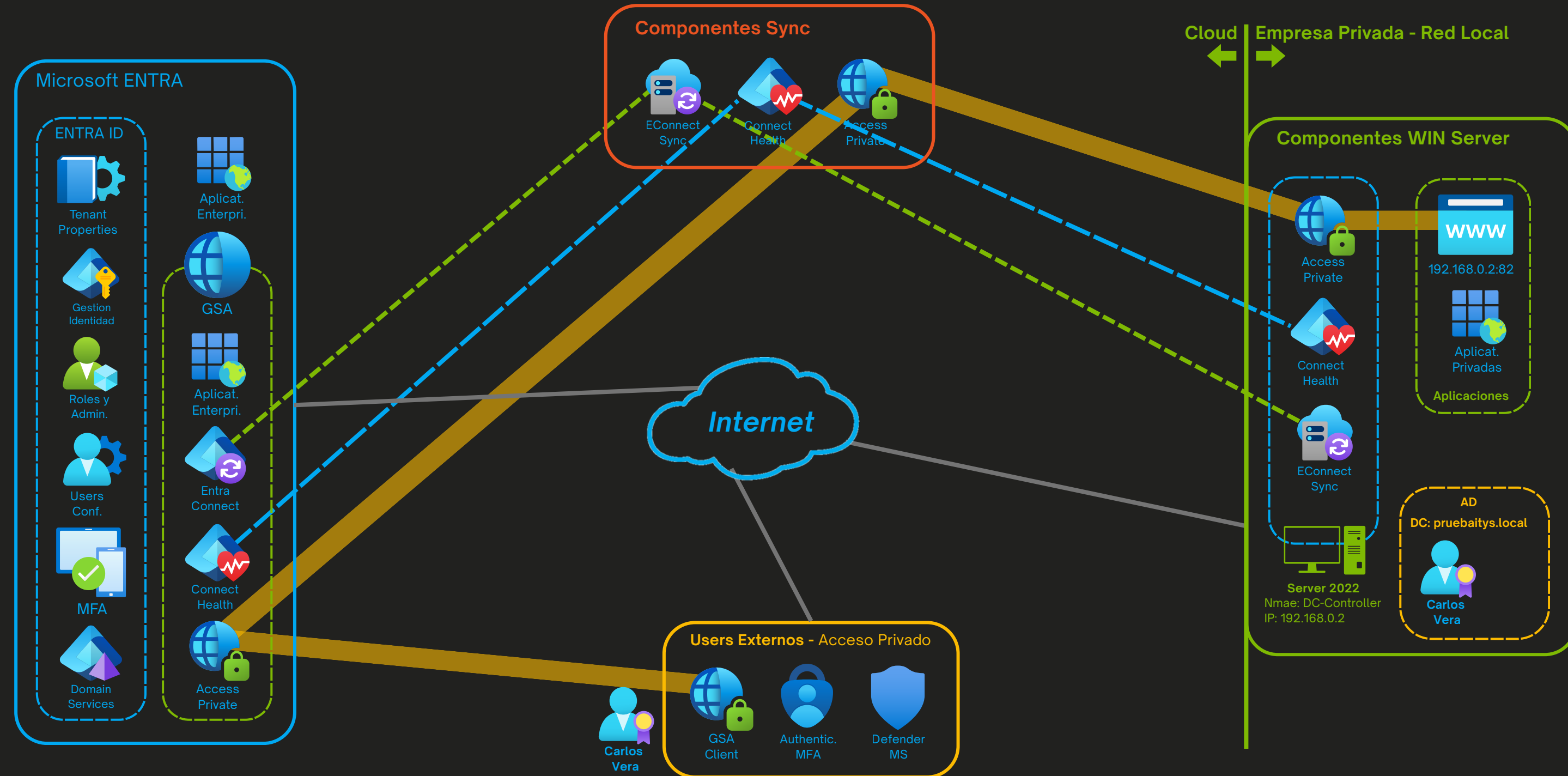
BENEFICIOS

- Sincronización de Identidad (**AD + Entra ID**)
- Gestión de Identidades en la Nube
- Extensión de Directivas Locales - **CA**
- Modernizar AD locales
- Punto de partida para la modernización de Identidades
- AuthN - AuthZ Centralizada y Acceso Unificado (**MFA, SSO**).
- Acceso Privado a Aplicaciones Locales
- Acceso Seguro Global - **GSA**
- Mayores capas de Seguridad en Acceso Privado, mas que una **VPN**.
- Acceso a la Red de Confianza Cero - **ZTNA**
- **App Proxy vs GSA**





MODELO HÍBRIDO DE MICROSOFT



“Menos, es más; escalar con Simpleza, lo último en Seguridad con Menores Costos”



ACCESO CONDICIONAL

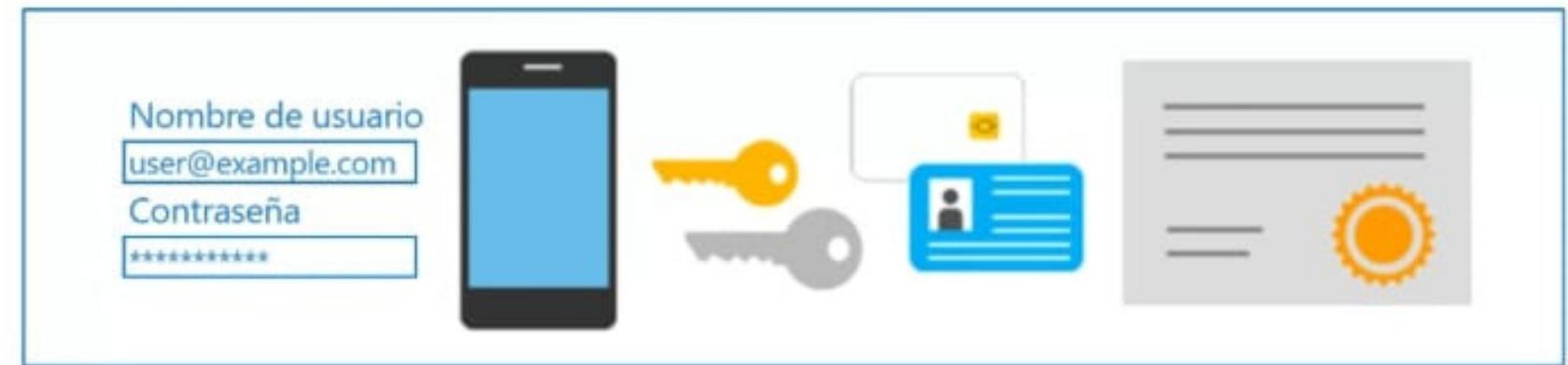
- Usuario o membresía grupal
- Ubicación de la IP
- Dispositivo
- Aplicación
- Detección de Riesgo





AUTENTICACION MULTIFACTOR - MFA

Algo que sabes -- Algo que posees -- Algo que eres



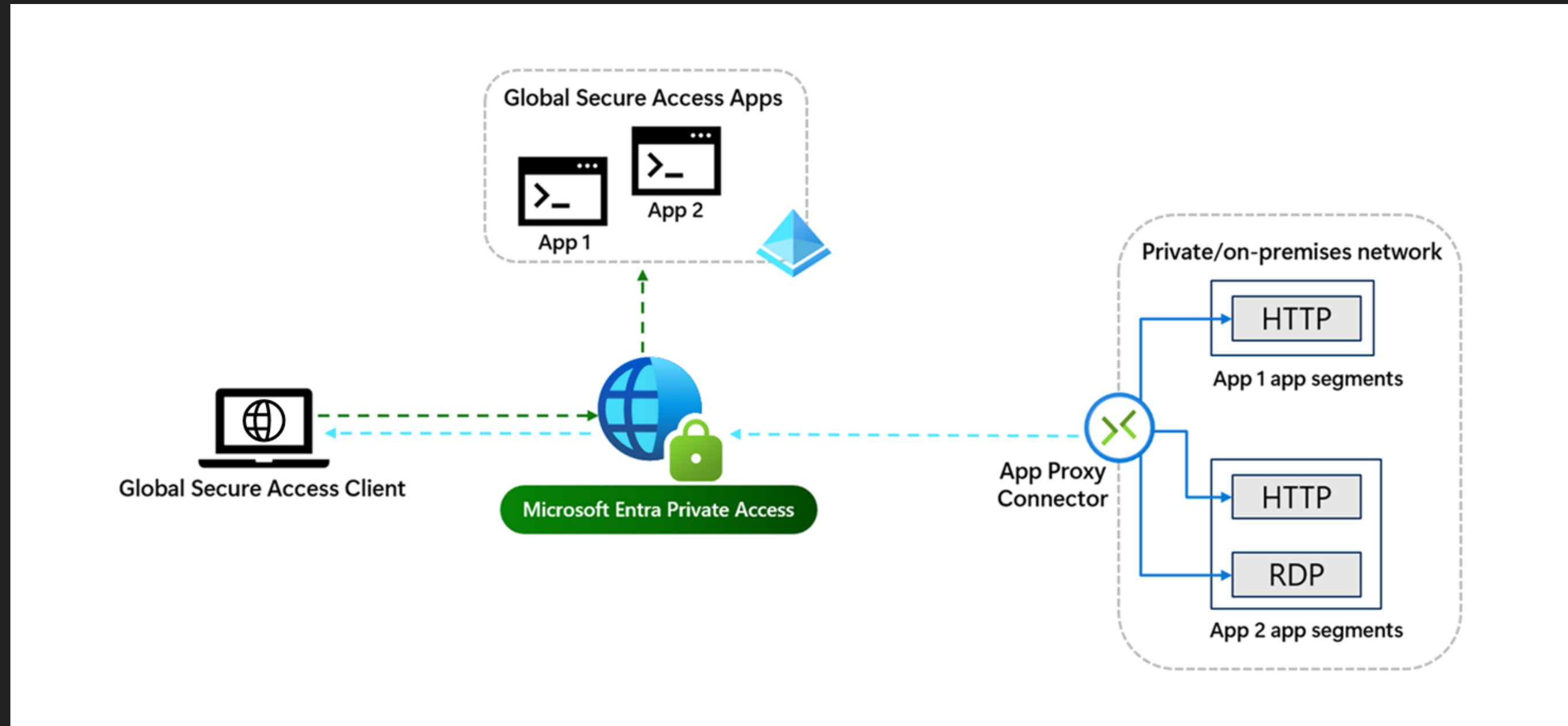
ACCESO A LA RED DE CONFIANZA - ZTNA

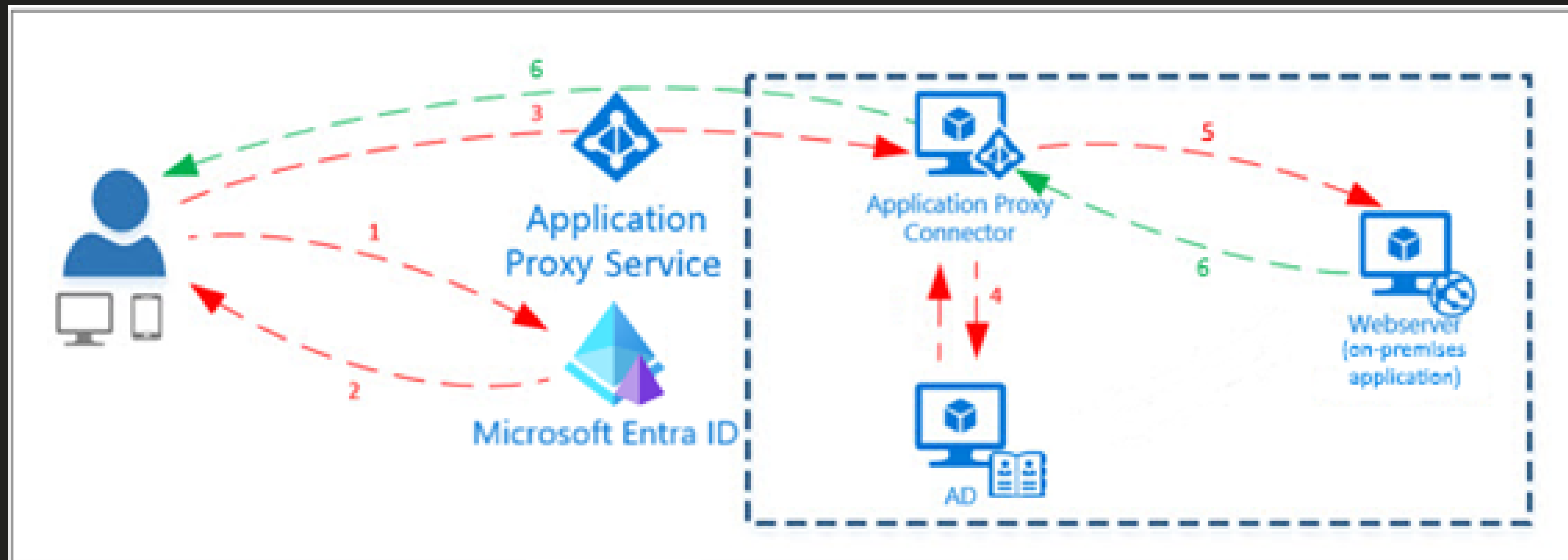




Como funciona?

ACCESO PRIVADO



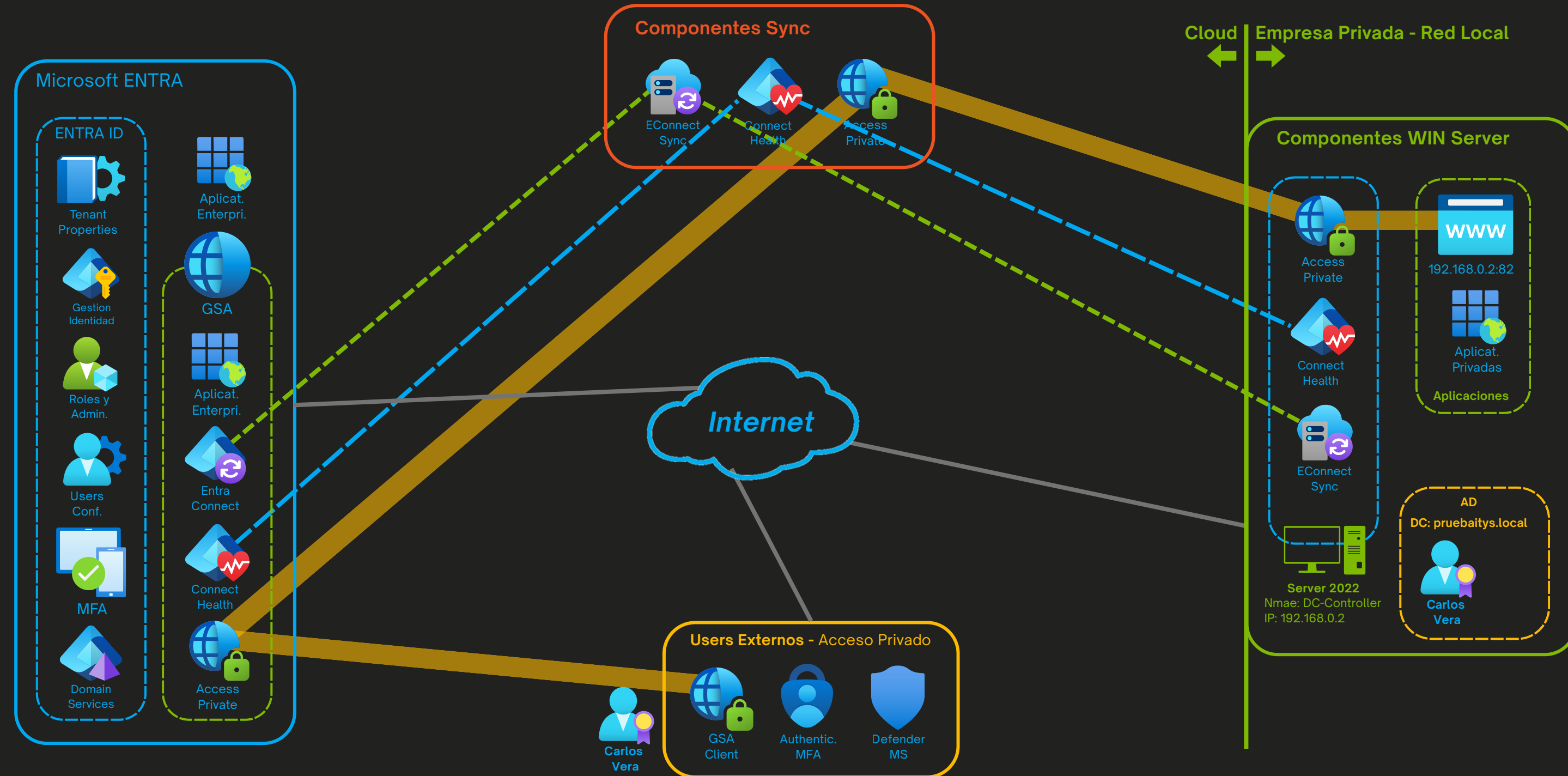


Internet → MyApps (Portal Entra ID) → Autenticación SSO → GSA Perfil Acceso Privado → Servidor IIS (192.168.0.2:82).

Acceso Controlado, Inspeccionado y Registrado



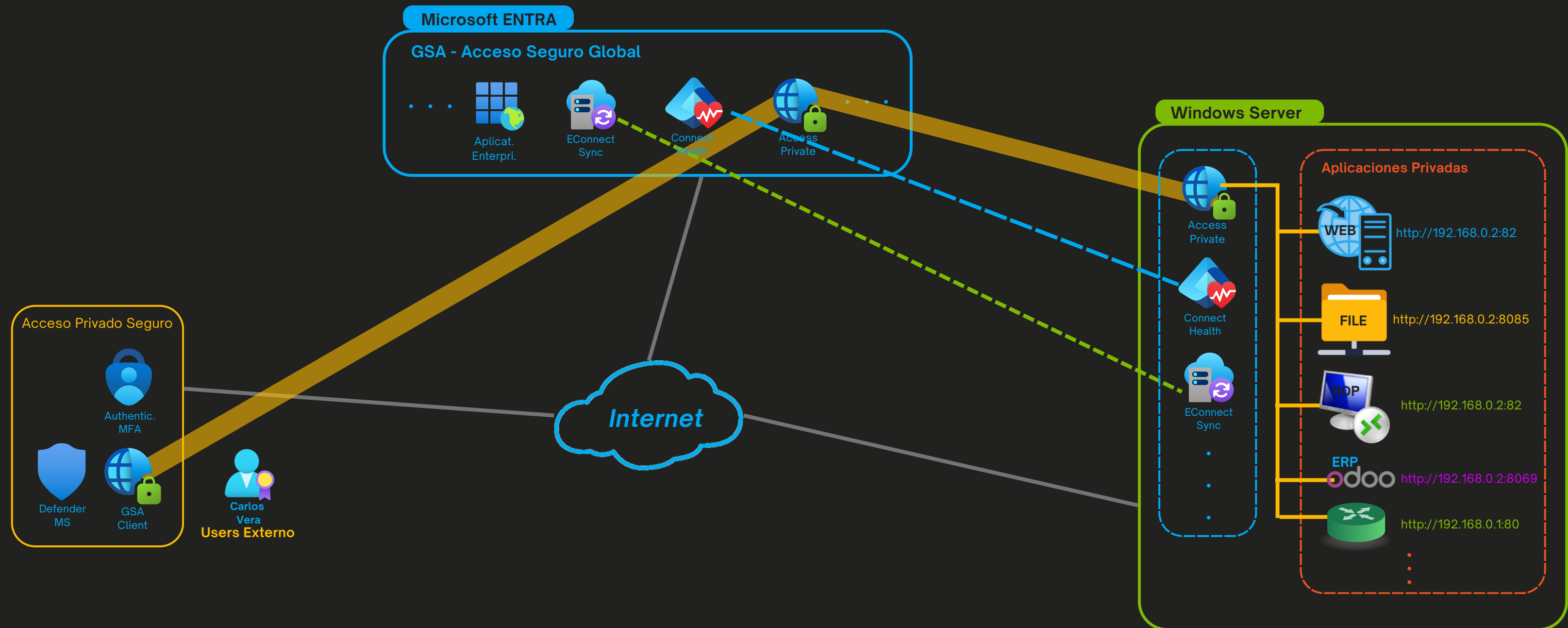
MODELO HÍBRIDO DE MICROSOFT



“Menos, es más; escalar con Simpleza, lo último en Seguridad con Menores Costos”



Acceso Seguro a Aplicaciones y Recursos Privados



“Con Microsoft Entra y GSA Client, cada usuario y cada dispositivo se conecta de forma segura, y la red completa queda invisible para el exterior. El ISP solo provee Internet, pero no ve nada de lo que pasa dentro.”



PROCESOS DEL ACCESO SEGURO

1. Usuarios externos acceden desde Internet mediante portal MyApps.
2. La autenticación se realiza con Microsoft Entra ID.
3. GSA (Global Secure Access) redirige el tráfico hacia la red privada.
4. Perfil de Acceso Privado establece un túnel seguro al servidor IIS (192.168.0.2:82).
5. GSA Client inspecciona y valida el acceso (dispositivo, identidad, riesgo).

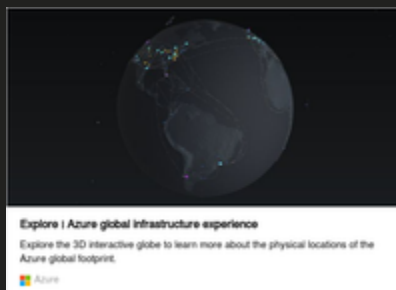
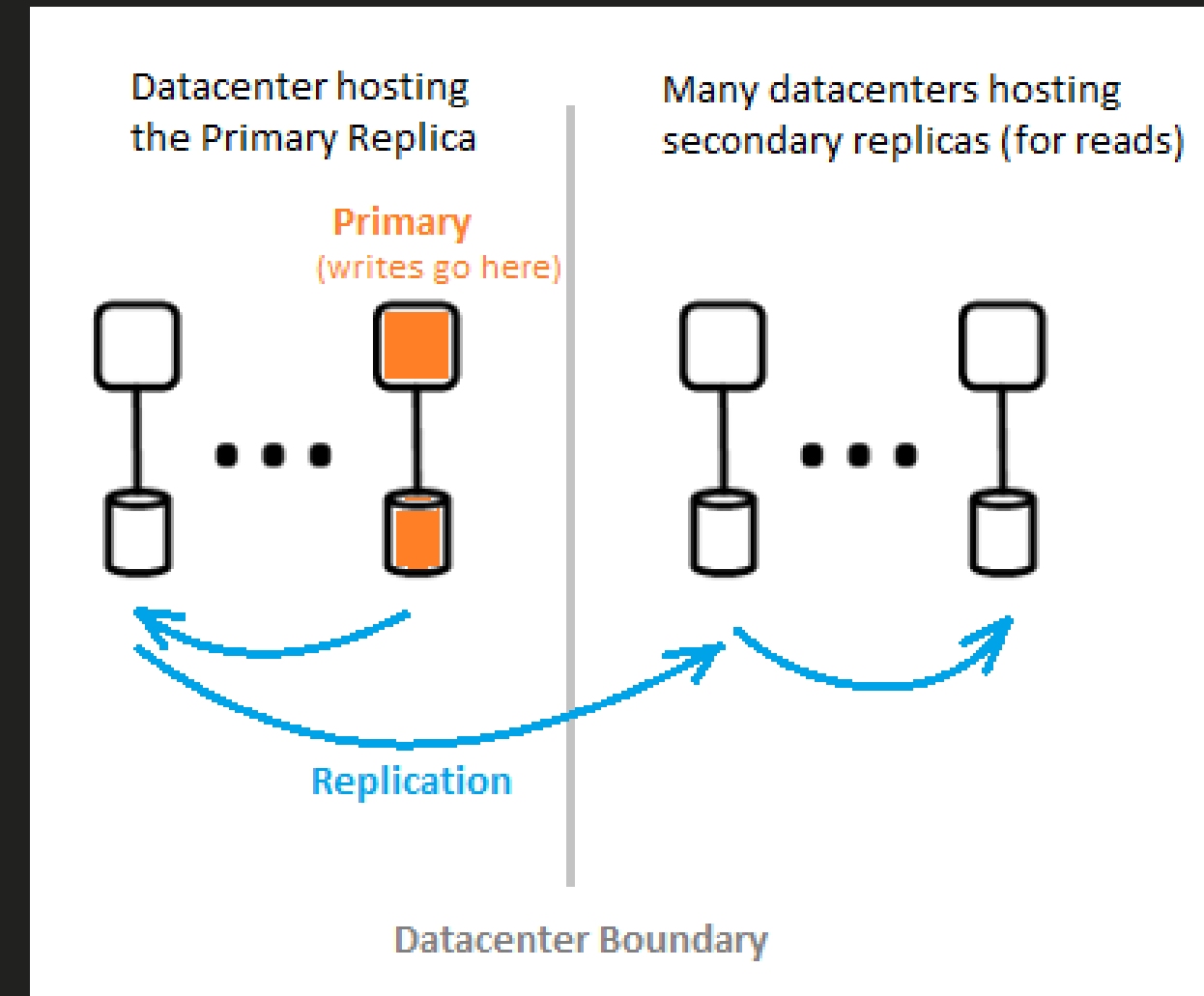
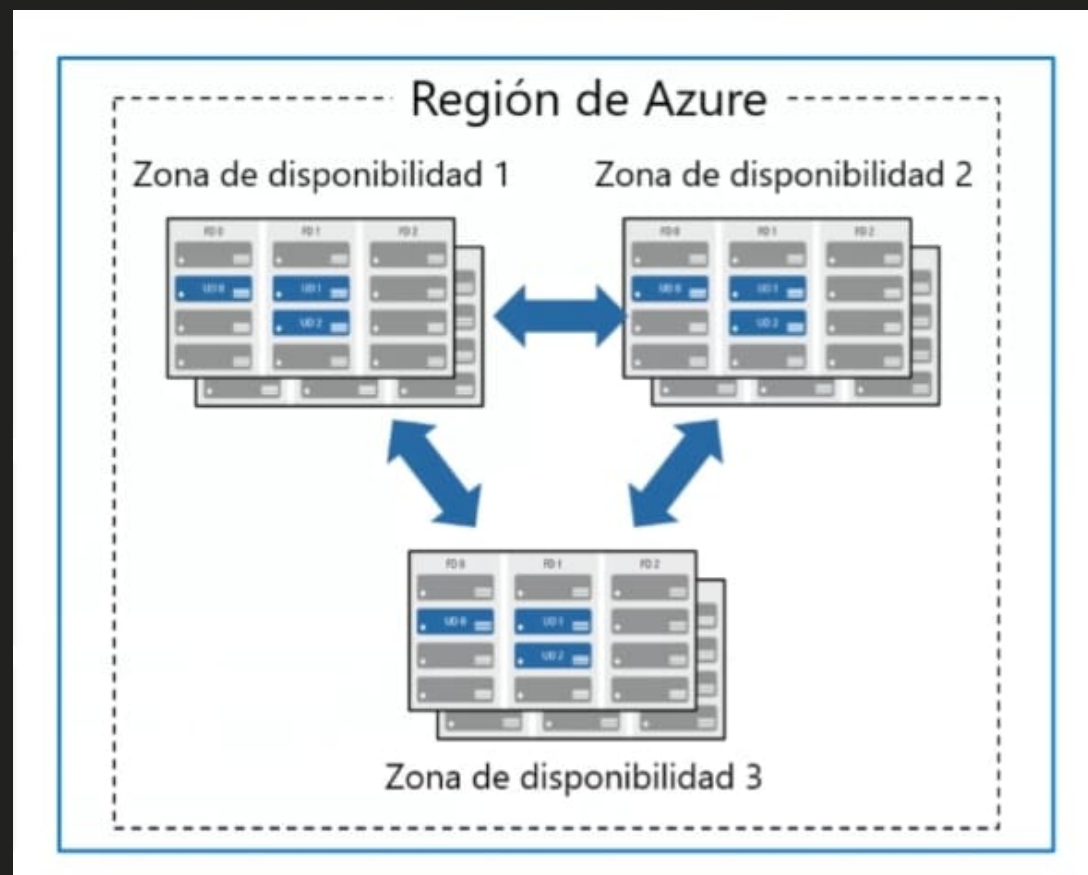


PROPUESTA DE VALOR PARA EL CLIENTE

- Unificación de seguridad y acceso sin necesidad de infraestructura adicional.
- Reducción de superficie de ataque, Mas que una VPN; el modelo basado en identidad y contexto reemplaza el acceso tradicional por VPN.
- Escalabilidad y facilidad de gestión en entornos híbridos.
- Evita exposicion directa de servicios intenos en Internet.
- Ideal para empresas con aplicaciones locales críticas
- Agregando mayores capa de seguridad Auth; Microsoft Entra ID y GSA ofrecen una ruta moderna y segura para acceder a aplicaciones locales.
- Reduce costos de infraestructura y seguridad en cadena de Retail con múltiples sedes-tiendas, Teletrabajo, Colaboradores externos, etc.
- Permite extender la red corporativa a tiendas remotas con Seguridad Granular.



Y CUAL ES LA ARQUITECTURA DETRÁS?



<https://datacenters.microsoft.com/globe/explore>



Ingeniería
Tecnología
Seguridad

“**Con Entra**, su red nacional de tiendas se convierte en un entorno seguro, invisible y escalable. No necesitan invertir en infraestructura local ni preocuparse por ataques externos. Solo pagan la licencia de cada usuario, y Microsoft se encarga de la seguridad de extremo a extremo. Es un modelo rentable, moderno y preparado para crecer.”



Ingeniería
Tecnología
Seguridad

Y LA INFRAESTRUCTURA LOCAL, SERVIDORES?



Microsoft

Active Directory



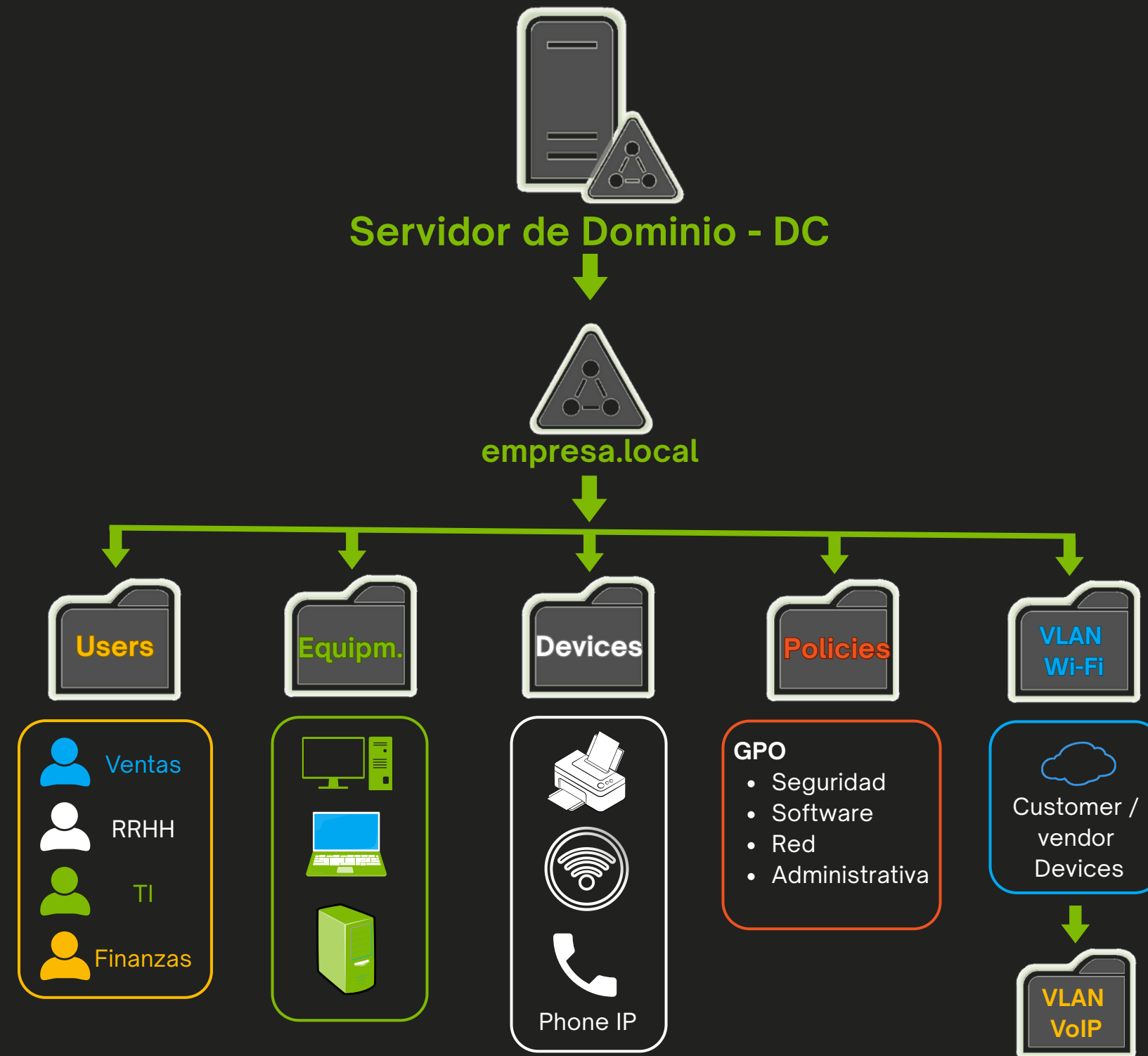
Active Directory



Windows Server®



SERVICIO DE DOMINIO Y ACTIVE DIRECTORY



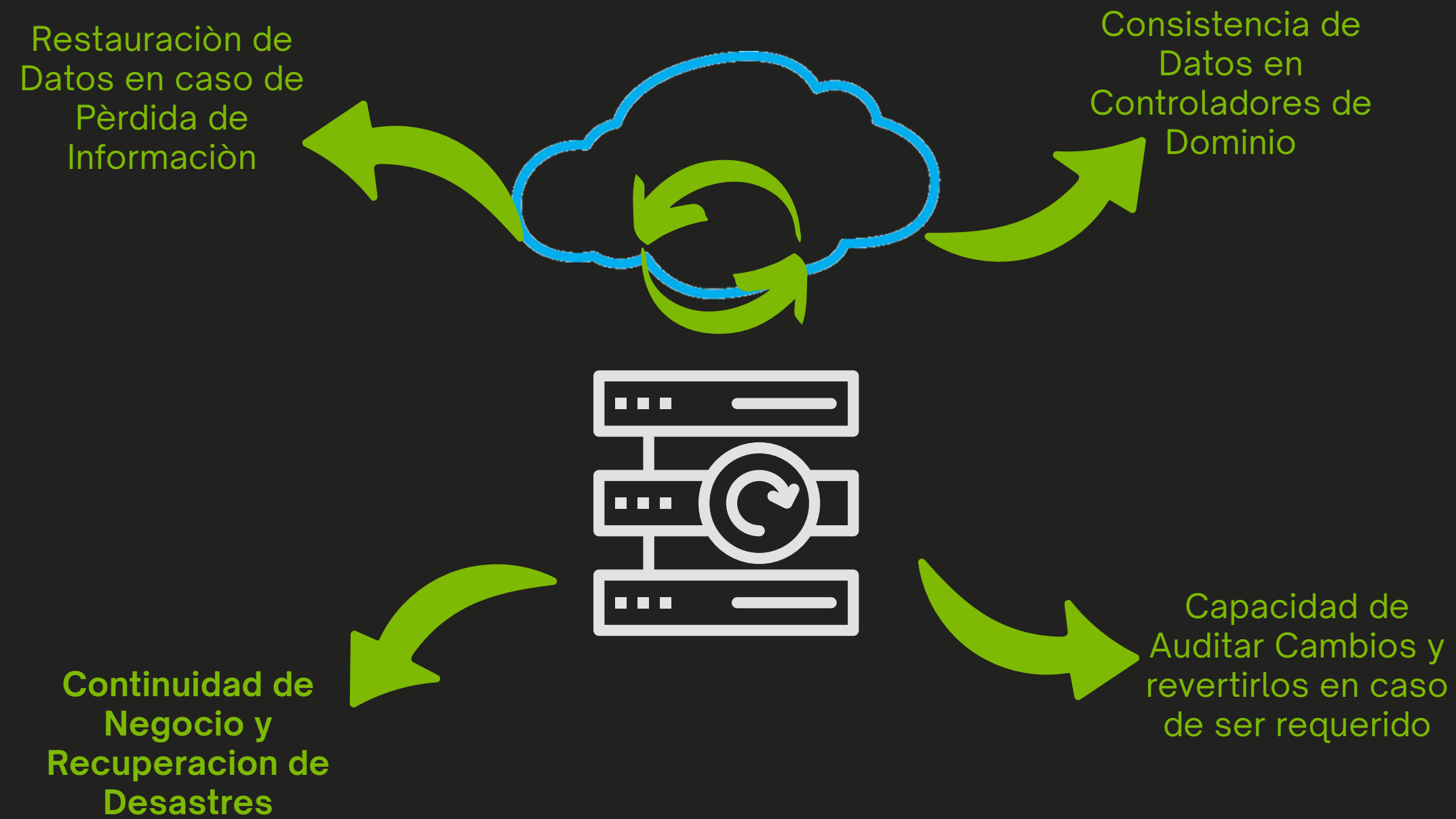


GESTIÓN DE DIRECTIVAS Y GPO





BACKUP DE ACTIVE DIRECTORY





BUENAS PRÁCTICAS PARA BACKUP DE AD

Frecuencia de Backups

Respalda el System State o el Servidor completo de cada DC al menos cada 24 horas

Regla 3-2-1

Tres copias en dos tipos de medios, una fuera del sitio o en la nube

Automatización y Monitoreo

Programas respaldos automáticos y monitorear alertas.

Pruebas de Restauración

Validar periódicamente la integridad mediante restauraciones de prueba

Políticas de Retención

Definir tiempos de conservación según requisitos legales y de negocio

Auditoria y Registro

Mantener Logs detallados de respaldo y restauraciones

Cifrado y Control de Acceso

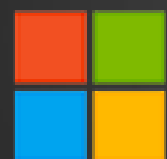
Proteger los Backups con Cifrado y Acceso restringido

Plan de Recuperación ante Desastres - DRP

Incluir AD en el Plan, con Roles y simulacros definidos



Ingeniería, Tecnología y Seguridad



Microsoft Partner
Cloud Solutions Provider

GRACIAS

CONTACTANOS:



+51 943-519-351



requerimiento@itys.pe



www.itys.pe