# Felhasználó központú IT

Harmath Zoltán
zoltanh@exchange.microsoft.com

A biztonsági fenyegetettségek száma és területe gyorsan változik.

De nem csak a támadók dolgoznak ezen, a végfelhasználók is sokat tesznek ezért.

## **2009** körülhatárolt környezet

## **2014** perimeter eltűnése

Mobilitás a perimeter alapú biztonság megszűnését eredményezi.

A perimeter hálózatod kifakul, vagy már kifakult.

BYOD fontos és megoldandó kérdéseket tár fel.

De nem ez az egyedüli kérdéskör amit meg kell oldani.

Windows fejlesztésével a támadókat új taktika használatára kényszerítettük.

A támadók a figyelmüket az identity lopásokra irányították így a rendszerekbe a nevedben lépnek be.

# Tökéletes a vihar

BYOD növeli az eszközök számát amik a vállalati erőforrásokhoz kapcsolódnak

és a legtöbbször kevésbé vagy egyáltalán nincsenek úgy menedzselve ahogy kellene vagy szeretnénk

# A megoldandó feladatok komponensei


## Felhasználók

A felhasználók azt várják, hogy **bárhonnan dolgozhassanak** és hozzáférhessenek a munkához szükséges erőforrásokhoz

## Eszközök

A **végfelhasználói eszközök robbanásszerű változása** erodálja a vállalati IT standard alapú megközelítését

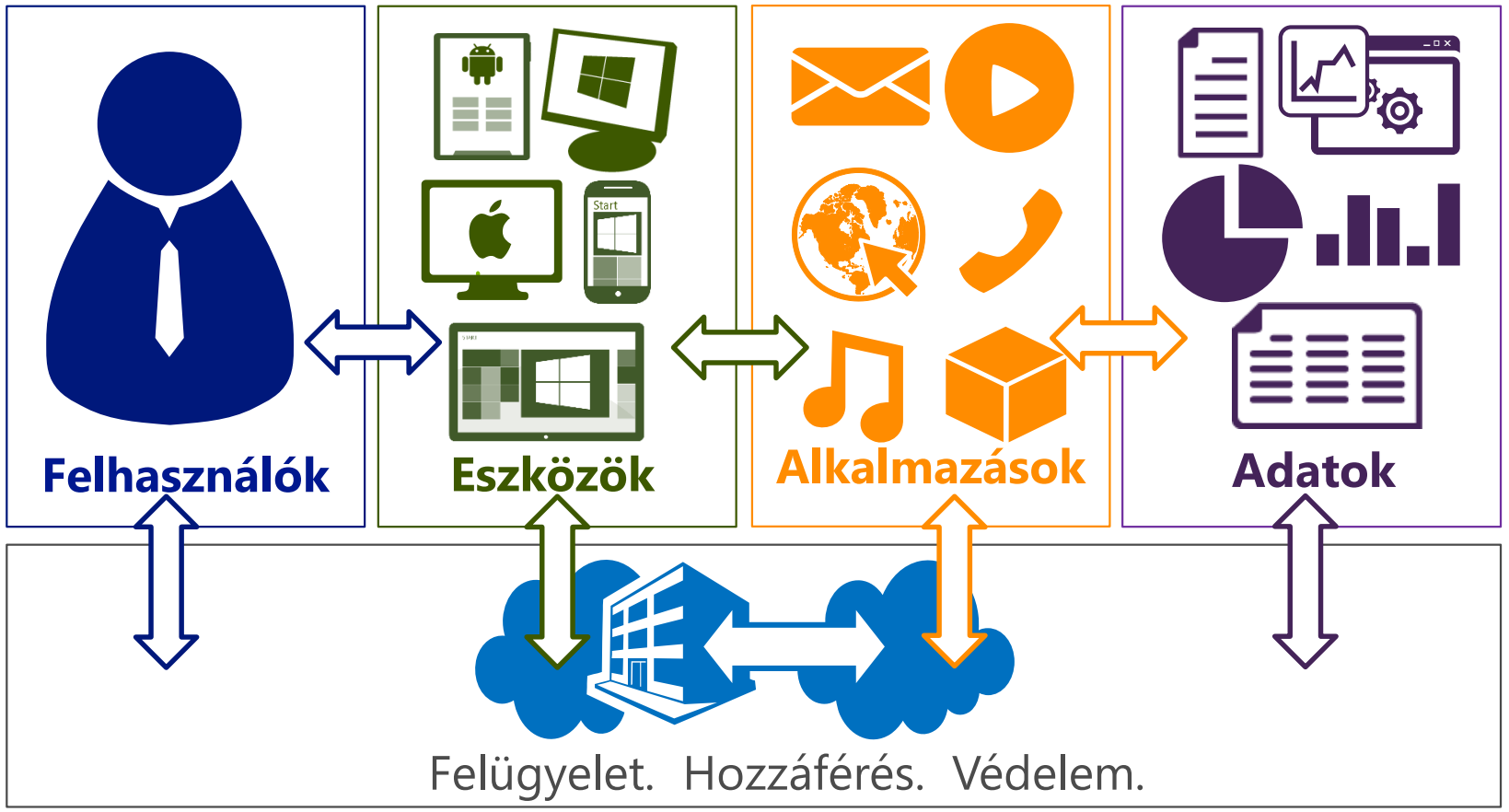
## Alkalmazások

A **platformokon átnyúló** alkalmazások terítése és felügyelete bonyolult.

## Adat

A felhasználók produktivitását úgy kell biztosítani, hogy közben **meg kell felelni a szabályozási elvárásoknak** és **csökkenteni kell a kockázatokat**

# A felhasználó központú IT




## A felhasználók felszabadítása

Tegyük lehetővé, hogy a felhasználók az általuk választott eszközzel dolgozhassanak, és biztosítsunk konzisztens adat-hozzáférést.

## Egyesített felügyeleti környezet

Biztosítsunk egységes alkalmazás- és eszközfelügyeletet

## Adatvédelem

Modern eszközökkel védjük a vállalati információkat és csökkentsük a kockázatokat.

ADRMS

PhoneFactor

Dynamic Access Control

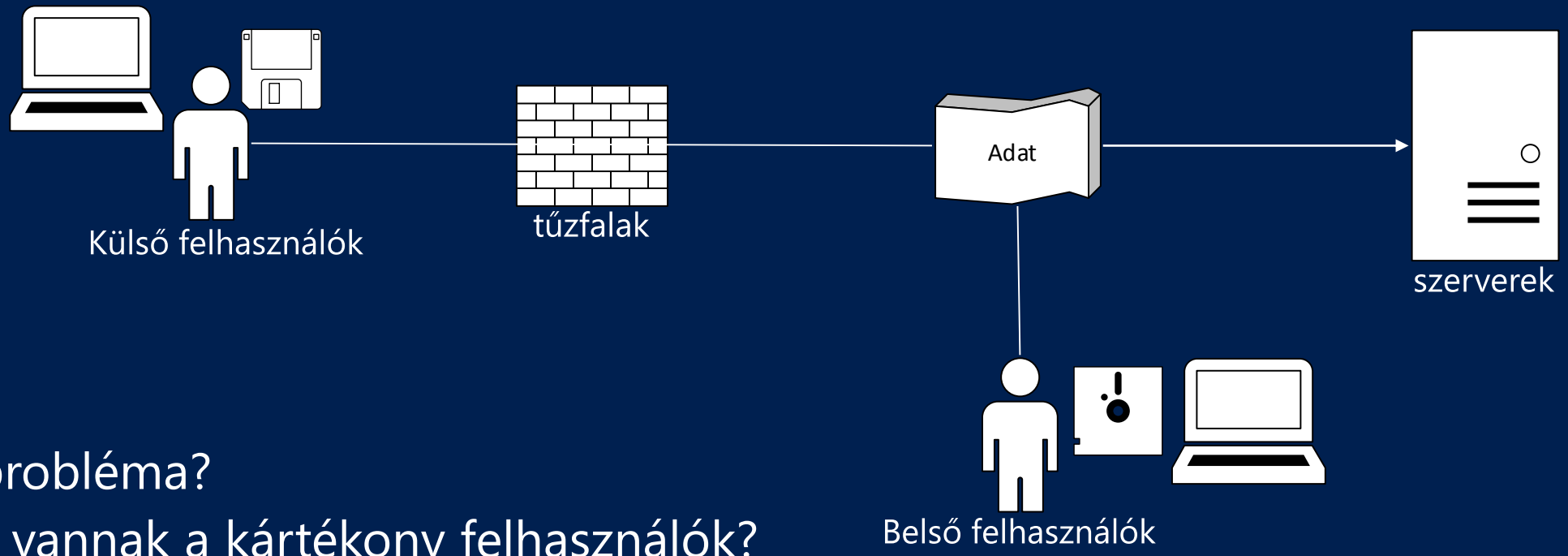
Web Application Proxy

Work Folders

Workplace Join

# ADRMS

# Jelenlegi állapot – úgy általában

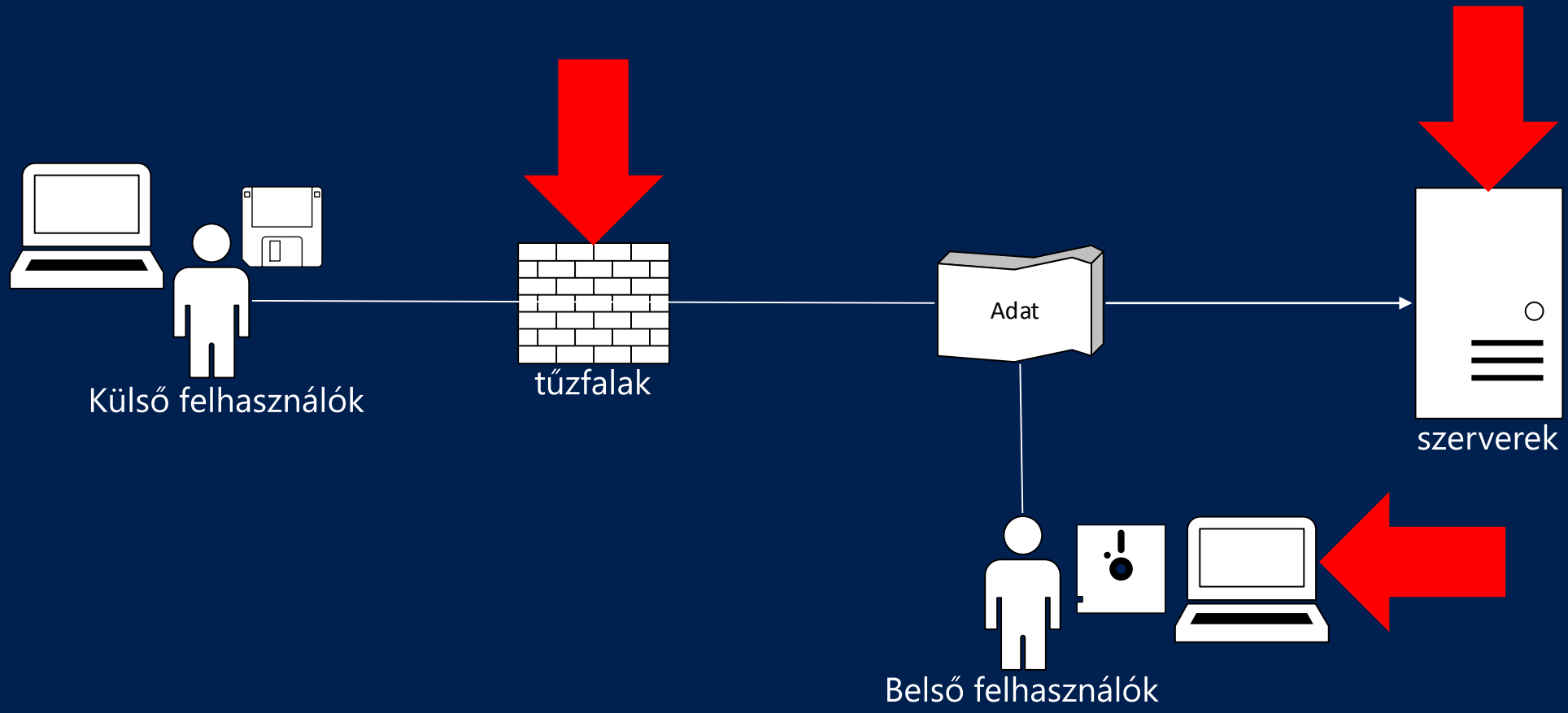



Mi a probléma?

- Hol vannak a kártékony felhasználók?
- Hogyan védjük az adatmásolatokat?
- A tűzfalak látják az adatforgalmat?
- Megbízhatóak a kliens számítógépek?

# A megoldás kézenfekvő!?

- Legyen hát DLP
  - Amivel a lehetséges szivárgási pontokat felügyeljük



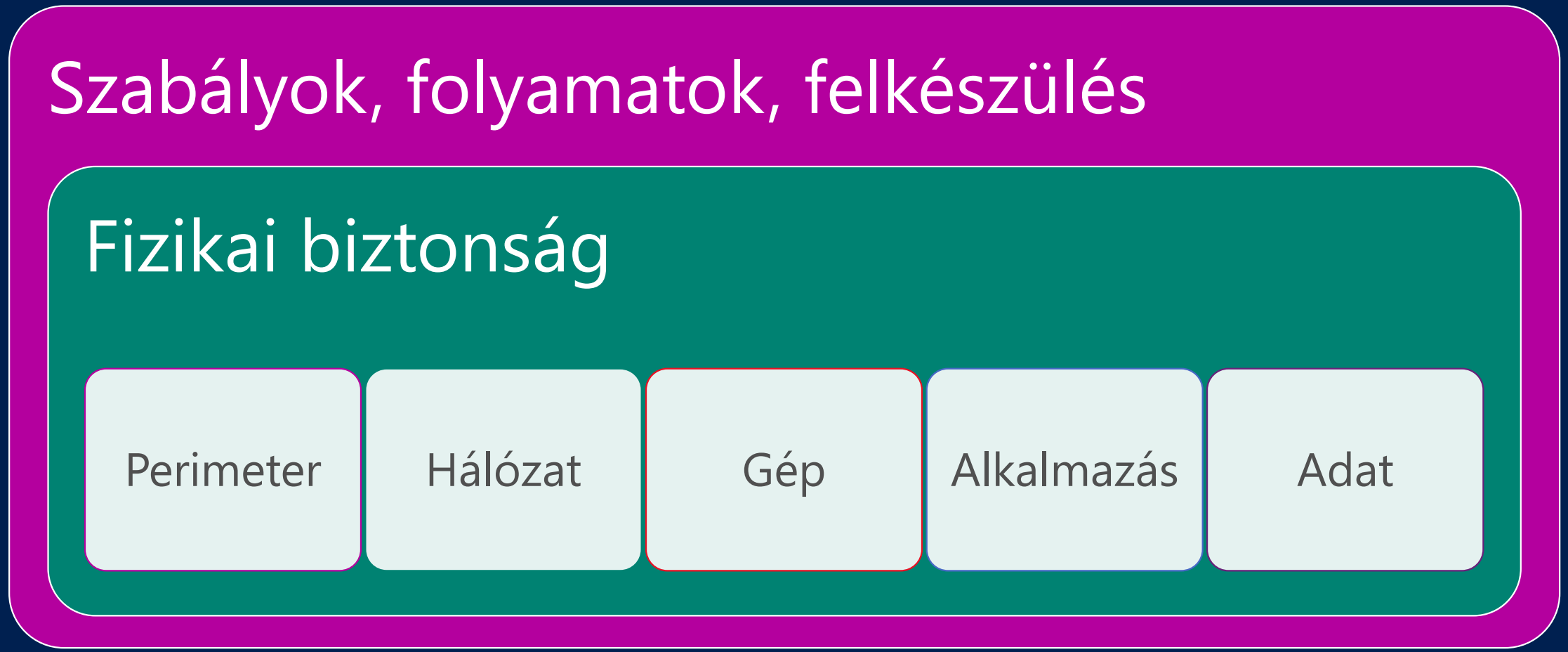
# Problémák

- Minden lehetséges szivárgási pont felügyelhető?
  - Biztosan nem
- Szükséges, hogy „kintről” és nem felügyelhető gépekről is elérhető legyen az adat?
  - Úgy általában igen. Ha más nem, akkor a főnök biztosan szeretné elérni iPAD-ról
- Hogyan kezeljük a titkosított adatkapcsolatokat?
  - Kapcsoljuk ki a titkosítást…várjunk épp javítani és nem rontani szeretnénk…
- Minden tűzfal, minden levelezőrendszer stb. támogatott?
  - Úgy általában nem. Nosza cseréljük le őket.

# Mi erről egy kicsit másként gondolkodunk

- A klasszikus DLP megoldások úgy általában a host és a network rétegre összpontosítanak, ami nehéz
- A mi javaslatunk az, hogy mindezt ha lehet akkor a problémás réteghez a lehető legközelebb oldjuk meg
  - A problémás réteg az adatréteg
- Mik ezek a rétegek?

# Mélységi védelem



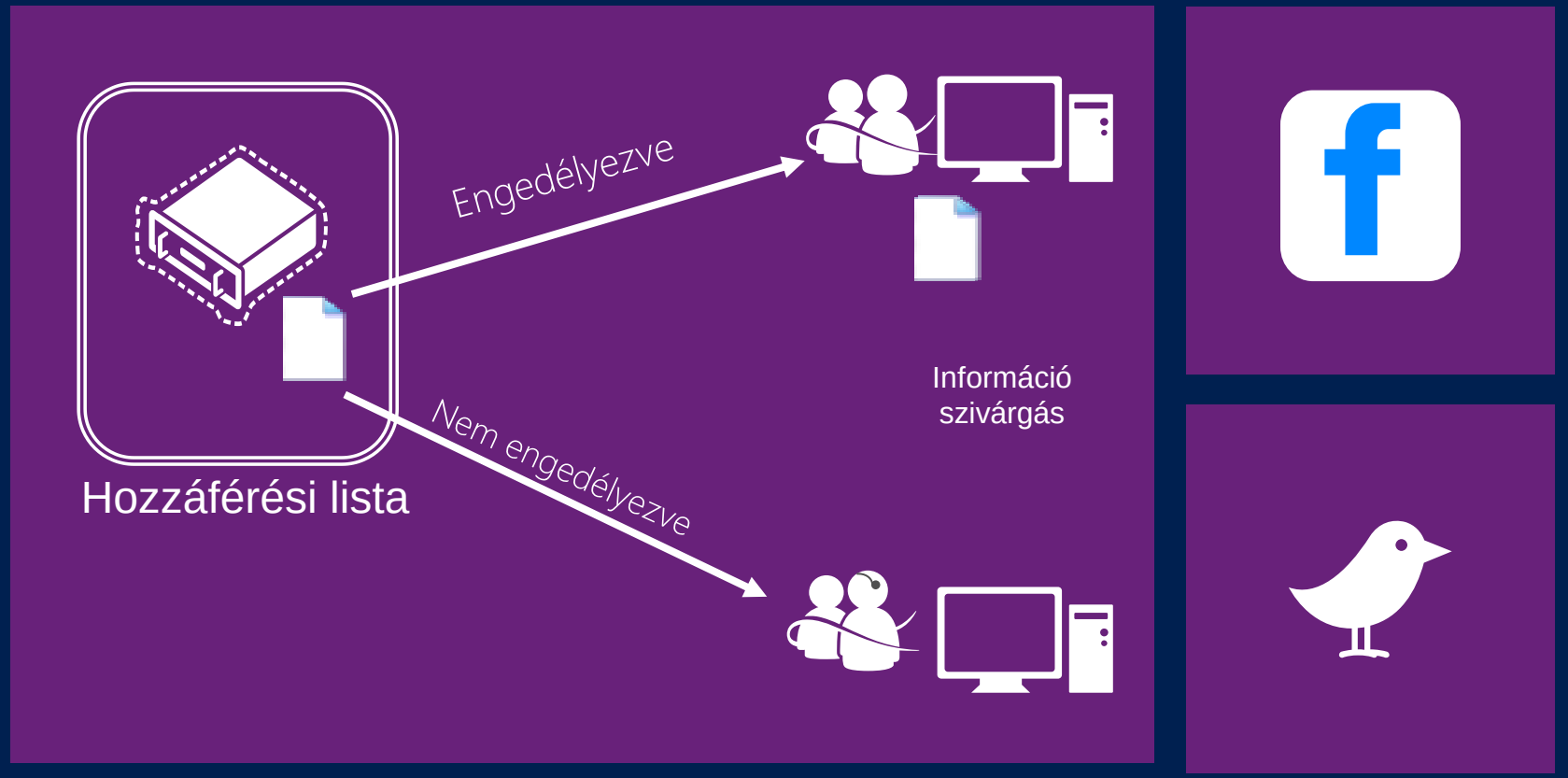
# Adatrétegben történő kezelés

- Evidens → titkosítás
- Ha titkosítjuk az adatot, akkor az elég sok problémát megold


Zavar az, hogy…

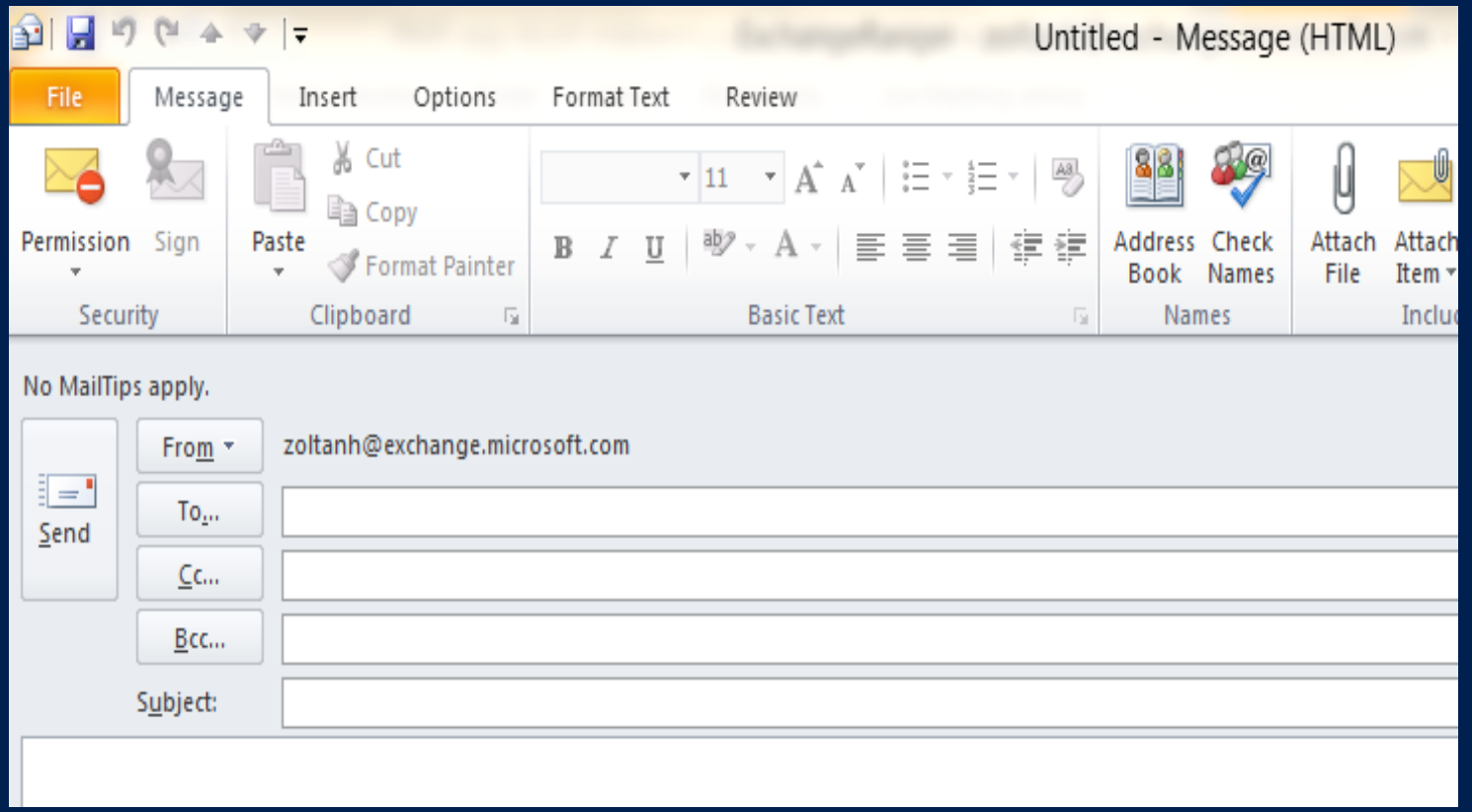
- …nem biztonságos gépről érik el a titkosított adatot?
- …ha a titkosított adat kikerül a házból?
- …ha külső meghajtókon van a titkosított adat?

# Áttekintés

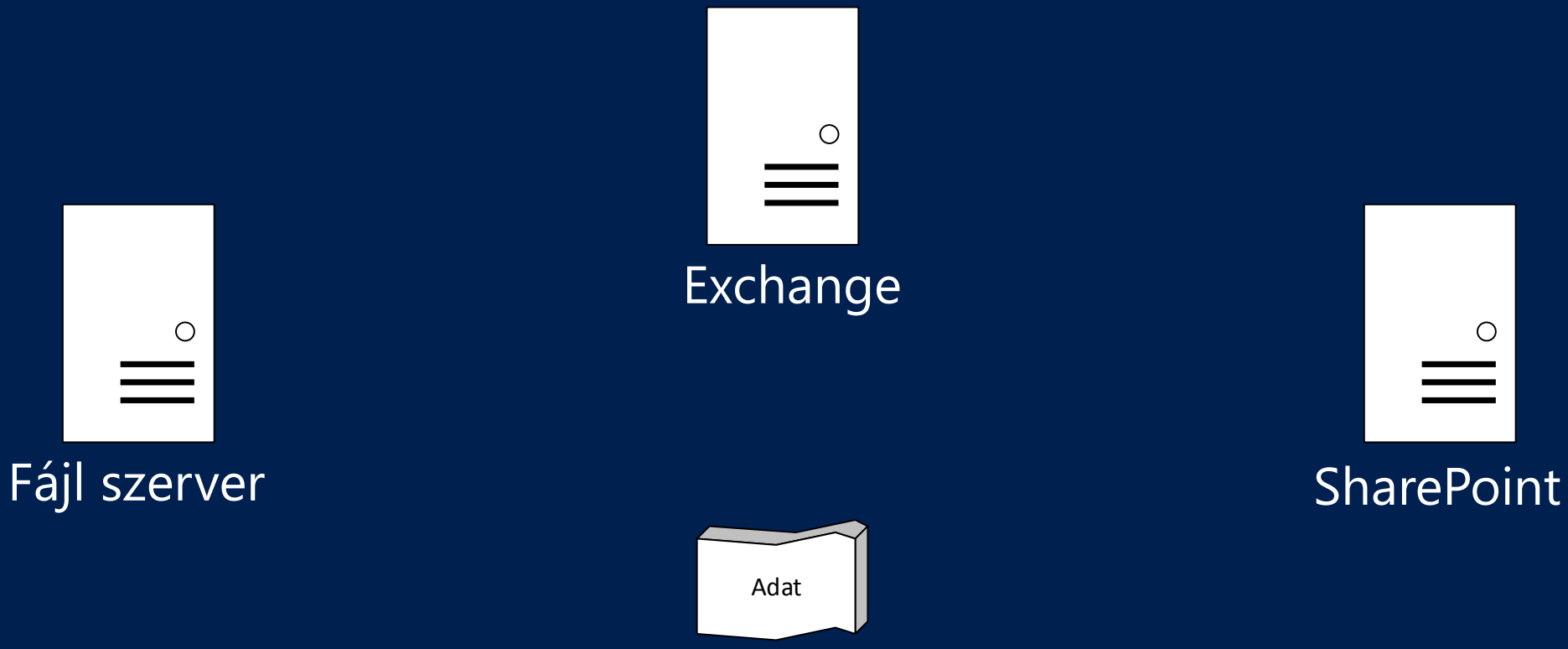

Engedélyezve
Nem engedélyezve
Hozzáférési lista
Információ szivárgás

# Az analóg módszerek továbbélnek


# A leggyengébb láncszem



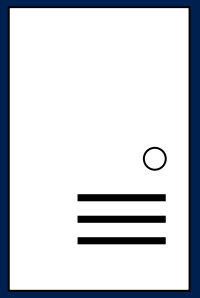

# Egy lehetséges adat titkosítási megoldás




ADRMS – integrálva a meglevő adattárolási pontokkal
FIPS 140-2 compliant adattitkosítási módszer

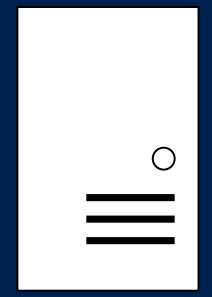
# Fájl szerver

- Jellemzők
  - Real-time titkosítás
  - Kulcsszó alapján
  - Adat klasszifikáció
  - Reguláris kifejezések alapján
  - Központilag definiálható
  - Független attól, hogy melyik fájl szerverünk, melyik mappájában van az adat



Fájl szerver

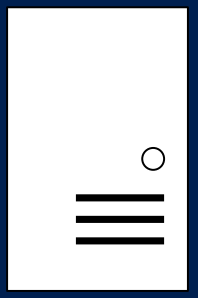
# Exchange




- Adattovábbítás során titkosítás használható
- In-transit az adattitkosítás levehető, hogy a vállalati szabályokat végrehajthassuk
- Adatkeresések számára az adat látható, tehát nem kell attól tartani, hogy így akarnak elrejteni valamit a dolgozók
- Végfelhasználó tud keresni a titkosított adatokban

# SharePoint

- Adattárakon a védelem beállítható
- Minden a dokumentumtárban elhelyezett adat titkosítva lesz



# Nitro Announces New Microsoft RMS Integration with Nitro Pro

## Nitro Pro with RMS Introduces User-Based File Security for Businesses

SAN FRANCISCO, Jun 03, 2014 (BUSINESS WIRE) -- Nitro, a leading provider of document productivity and collaboration solutions, today announced a new integration with Microsoft RMS (Rights Management Service) to provide enhanced security for document workflows. Demonstrating Nitro's continued commitment to document security, Nitro Pro with RMS now enables users to protect and securely exchange digital documents with anyone in their collaboration circle.

Microsoft and Nitro's increased investment in RMS helps enable the secure sharing of all file types – including PDF and Microsoft Office formats – on all devices. Nitro Pro with RMS protects at the file level, leveraging encryption technology to ensure that only those with permission can access your sensitive documents, whether they are inside your organization or outside the firewall. Nitro Pro also offers several additional security features including password and permissions settings, certificate security based on public/private key security, and basic encryption for sharing and tracking PDF documents.

"From the desktop to the cloud, documents and how we share them can have a significant impact on an organization's success," said Mimi Hoang, VP, Product at Nitro. "The increasing flow of shared information has exposed vulnerabilities in traditional document security, making it difficult to control who can access sensitive files. Whether someone accidentally forwards an email or a user has malicious intent, the end result is that sensitive information can wind up in unintended hands. Providing users with peace of mind and more control over who can access documents irrespective of their destination, our integration of Microsoft RMS with Nitro Pro means our customers can comfortably share digital documents as intended between both employees and third parties."

Key features of Nitro Pro with RMS include the following:

- **PDF File Encryption** – The Microsoft RMS integration encrypts PDF files so that only those who have permission are granted access. Each user identity is verified to ensure documents can only be accessed and modified by authorized personnel within the internal network or beyond the corporate firewall.

https://portal.aadrm.com/home/download/

Microsoft RMS

## Protect. Share.

Our service lets you protect and share files securely with others, on your terms.

Learn More

# Microsoft Rights Management

Click on your favorite device below to download the RMS sharing application. The application can open and create protected pictures, text, and .pfile

Computers

Mobile Devices

The following applications support RMS

Want your app added to this list? Click here.

# Demo

# Kifejezés alapú ACL

# Beszéljünk a claim-ekről

## BOARDING PASS

Please keep this document until the end of your trip.

KLM SKYTEAM

**Sec. nr.:**KL1972: **007**, DL0233: **002**

Name HARMATH, ZOLTAN
Passport B[redacted]
E-ticket # 0742464646906
Frequent flyer KL/203[redacted] Silver

FOLD LINE

| FLIGHT | DATE | FROM | TO | DEPARTURE | GATE | BOARDING | CLASS | SEAT |
|---|---|---|---|---|---|---|---|---|
| **KL1972** | 29OCT | BUDAPEST 2A | AMSTERDAM | **06:25** | unknown | 05:45 | M | 05C |
| **KL6033** | 29OCT | AMSTERDAM | SEATTLE | **10:40** | unknown | | Y | 19J |
| | | OPERATED BY DELTA AIR LINES | | | | | | |

Verify terminal and gate at airport

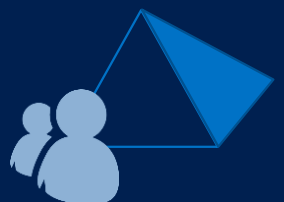
# Az adatkezelés kihívásai

# Az adatkezlés kihívásai

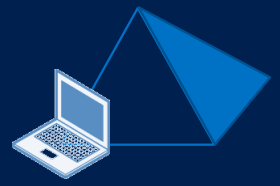
- Ki férhet hozzá az adatokhoz?
- Kevesebb biztonsági csoport?
- Az érzékeny adatokat védeni kell!

# Koncepció

| Adat osztályozás | Kifejezés alapú auditálás | Kifejezés alapú hozzáférés biztosítása | Titkosítás |
|---|---|---|---|
| Az AD-ban tárolt erőforrás tulajdonságok alapján az adatok besorolása<br><br>Automatikus besorolás a dokumentum tartalma alapján | Célzott, hozzáférési auditálás, a dokumentum besorolása és / vagy az eszköz / felhasználó adatai alapján<br><br>Központilag tárolt Audit konfiguráció alapján | Rugalmas hozzáférési lista, a dokumentum besorolása és / vagy az eszköz / felhasználó adatai alapján<br><br>Központilag tárolt hozzáférési konfiguráció alapján | Automatikus RMS titkosítás a dokumentum besorolása alapján |



AD DS



File Server

# Data classification – az adat felismerése

Adat osztályozás

Az AD-ban tárolt erőforrás tulajdonságok alapján az adatok besorolása

Automatikus besorolás a dokumentum tartalma alapján

- Besorolás a dokumentum tartalma, helye alapján, egyéb tulajdonságai alapján
- Automatikus / manuális osztályozás
- Data Classification Toolkit

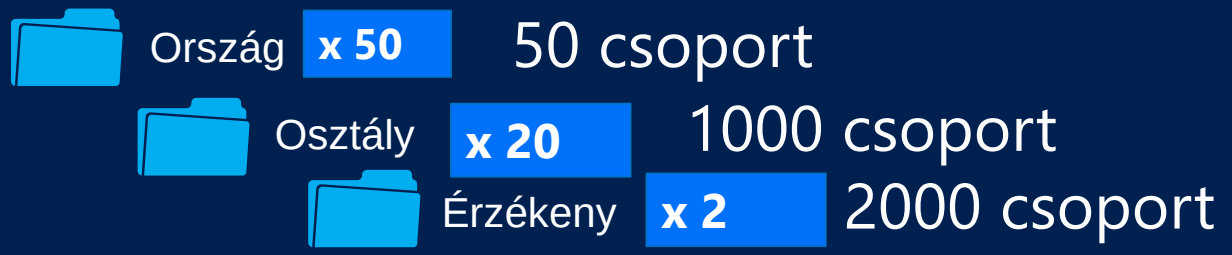
# Kifejezés alapú hozzáférés

**Kifejezés alapú hozzáférés**

Rugalmas hozzáférési lista, a dokumentum besorolása és / vagy az eszköz / felhasználó adatai alapján

Központilag tárolt hozzáférési konfiguráció alapján

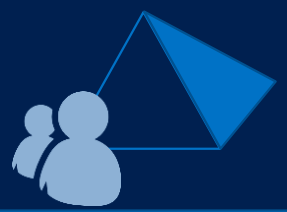
- Kevesebb biztonsági csoport segítségével, rugalmasabb jogosultság kezelés



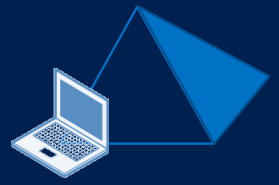

Ugyanez Windows Server 2012 segítségével: 71 csoport
Ország + Osztály + Sensitive

És hogy miért?

# Központi hozzáférési szabályok



AD DS



File Server

**Felhasználó claim-ek**
User.Department = Finance
User.Clearance = High

**Eszköz claim-ek**
Device.Department = Finance
Device.Managed = True

**Erőforrás tulajdonságok**
Resource.Department = Finance
Resource.Impact = High

**Hozzáférési szavály**

Alkalmazva: @File.Impact = High
Allow | Read, Write | if (@User.Department == @File.Department) AND (@Device.Managed == True)

# Központi hozzáférési szabályok (Central Access Policy)

Active Directory címtárban:

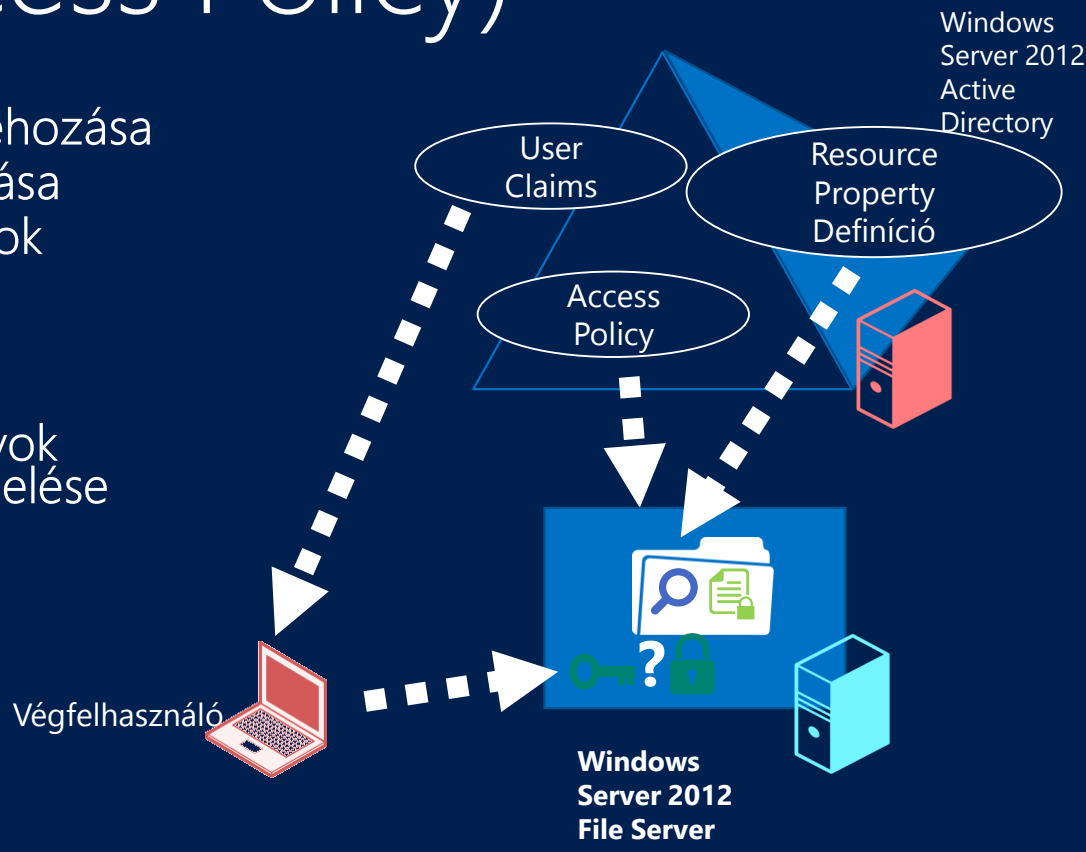
- Erőforrás tulajdonságok létrehozása
- Központi szabályok létrehozása
- Felhasználói claim objektumok létrehozása

File Server-en:

- Adatok osztályozása
- Központi hozzáférési szabályok erőforrásokhoz történő rendelése

Futási időben:

- Felhasználó hozzáférésének ellenőrzése



# Központi hozzáférési szabályok

Security csoportok felhasználása (minimális infrastruktúra frissítés szükséges)

Applies to: Exists(File.Country)
Allow | Read, Write | if (User.MemberOf(US_SG)) AND (File.Country==US)
Allow | Read, Write | if (User.MemberOf(Canada_SG)) AND (File.Country==CA)
Allow | Read, Write | if (User.MemberOf(France_SG)) AND (File.Country==FR)
…

Applies to: Exists(File.Department)
Allow | Read, Write | if (User.MemberOf(Finance_SG)) AND (File.Department==Finance)
Allow | Read, Write | if (User.MemberOf(Operations_SG)) AND (File. Department==Operations)
…

Felhasználói claim-ek használata (adattisztítás szükséges az AD-ban)

Applies to: Exists(File.Country)
Allow | Read, Write | if (User.Country==File.Country)

Applies to: Exists(File.Department)
Allow | Read, Write | if (User.Department==File.Department)



PM példa

# PhoneFactor

# Mi az a multi-factor (másként kétfaktor, 2FA, multi-factor, MFA, erős azonosítás...)?

## Bármelyik kettő vagy több faktor ezek közül:

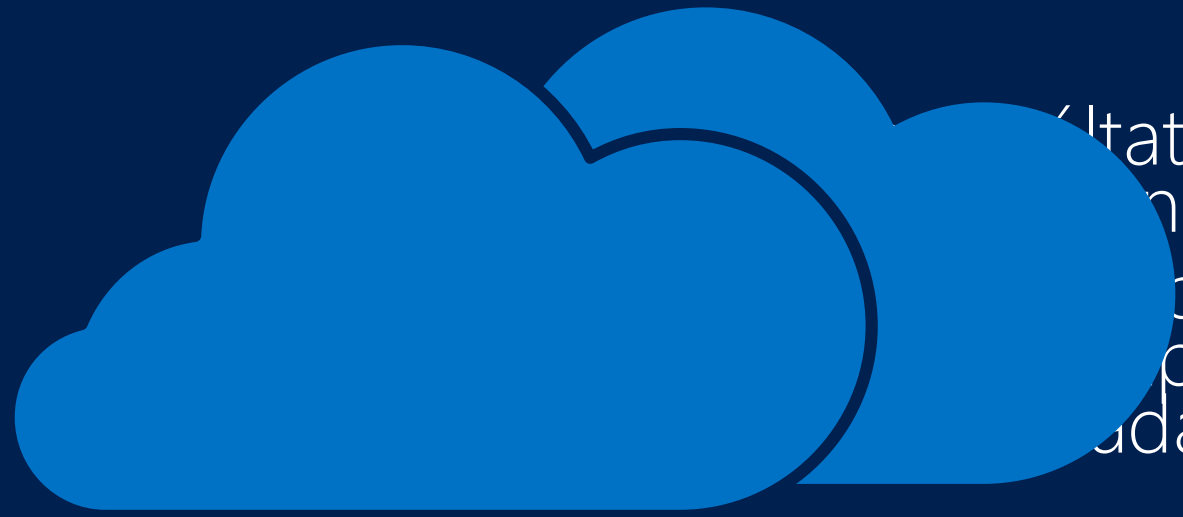
Valamit ismerszt - password vagy PIN
Valamit birtokolsz – telefon, bankkártya vagy hardware token
Valaki vagy - újjlenyomat, retina szken vagy egyéb biometrikus adat
Erősebb, jobb az AuthN ha több faktort használunk a fentiek közül (out-of-band)

## Tipikus kialakítás

Hardware OTP Token
Tanúsítvány
Smart Card

Telefon alapú azonosítás:
- Telefonhívás, SMS, Push értesítés,
- Software alapú OTP Token

# Windows Azure Multi-Factor Authentication?



ltatás, amit a
nk biztosít
rid cloud
pont tárcsáz ki, de
adattárolás helyben

Több ezer ügyfél és nagyvállalat bízik benne és használja

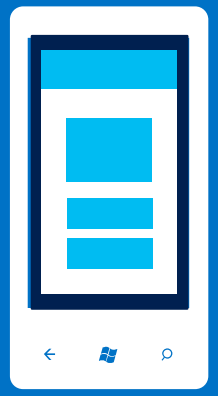
Biztosítja az erős azonosítást a helyben- és felhőben üzemeltetett szolgáltatások részére

# Hogyan működik?

## Mobile alkalmazás

Push Notification

One-Time Passcode (OTP) Token

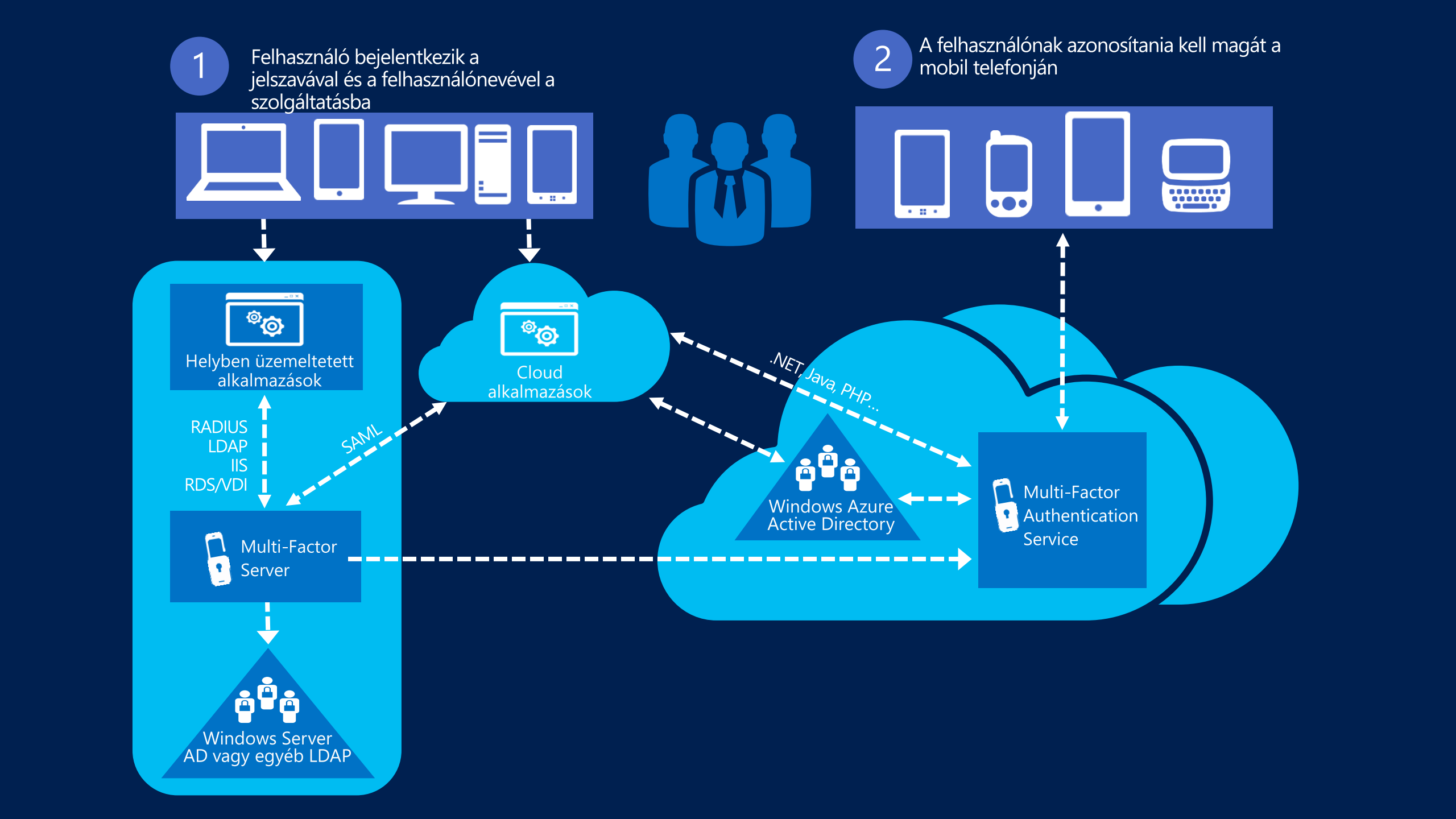


## Telefonhívás

Phone Call

## SMS üzenet

SMS


1
Felhasználó bejelentkezik a jelszavával és a felhasználónevével a szolgáltatásba
2
A felhasználónak azonosítania kell magát a mobil telefonján
Helyben üzemeltetett alkalmazások
RADIUS
LDAP
IIS
RDS/VDI
SAML
Multi-Factor Server
Windows Server AD vagy egyéb LDAP
Cloud alkalmazások
.NET, Java, PHP...
Windows Azure Active Directory
Multi-Factor Authentication Service

# Kinek miért jó?

Felhasználók

# Felhasználók

- A felhasználó életében a telefon központi helyen szerepel, ezt használjuk ki, szeretni fogja
- Megengedhetjük, hogy a felhasználó válasszon (SMS, telefonhívás, szoftver OTP)
- Eszközfüggetlen, ellenben egy smart-card vagy tanúsítvány alapú azonosítással
- Több metódust és több telefonszámot is támogat a rendszer, így flexibilis és kényelmes

Adminisztrátorok

# Adminisztrátorok, IT üzlet

- Nem kell eszközt vásárolni és annak életciklusát üzemeltetni (tanúsítvány, smart-car)
- Nem kell felhasználói oktatást végezni
- A meglevő rendszerekkel könnyen integrálható
- Teljesen automatizálható
- Elvesztett eszköz esetén egyszerű annak cseréje (telefon)
- Önkiszolgáló szolgáltatás a felhasználóknak

# Security

- Erős multi-factor azonosítás
- Valósidejű fraud riasztás
- PIN opcióval tovább növelhető a biztonság
- Jelentéskészítés és naplózás az auditálhatósághoz
- NIST 800-63 level 3, HIPAA, PCI DSS megfelelőséget segíti

# Skálázható

- Működik a legtöbb helyben üzemeltetett alkalmazással – VPN, web alkalmazások, RDP, stb.
- ADFS SAML alapú alkalmazásokkal integrálható
- Azure Active Directory alapú, azért, hogy az Office365 alapú szolgáltatások használhassák
- Publikus SDK elérhető, így saját alkalmazásokkal is integrálható
- Megbízható, jól skálázódó szolgáltatás, ami a masszív nagyszámú azonosítást is képes kiszolgálni

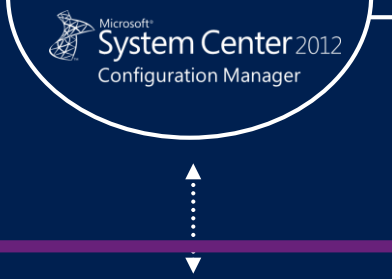
# Munka bárhonnan

Users can **work from anywhere** on their device with access to their corporate resources.

Users can **enroll devices** for access to the **Company Portal** for easy access to corporate applications

Windows Intune

Microsoft System Center 2012 Configuration Manager

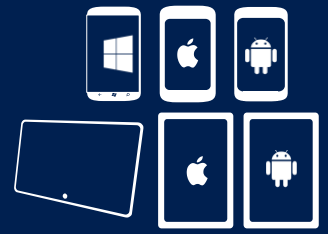


Windows Server RDS Gateway

Client VM

Session host

IT can publish **Desktop Virtualization (VDI)** resources for external access



Windows Server Web Application Proxy

Published Apps

IT can **publish access** to resources with the **Web Application Proxy** based on device awareness and the users identity

Users can register devices for **single sign-on** and access to corporate data with **Workplace Join**

Windows Server Active Directory

Windows Server Remote Access

LOB Apps

Files

IT can provide seamless corp. access with **DirectAccess** and automatic connections with **app-triggered VPNs**

# Web Application Proxy


Céges hálózat elérése bárhonnan, céges vagy nem céges gépről egyaránt

Az eszköz lehet menedzselt vagy nem menedzselt is

Single Sign On (SSO)


Céges alkalmazások szelektív publikálása

Alkalmazás, user, számítógép alapú szabályozás

Jobb védelem a pre-authentication segítségével

Nem kell változtatni az alkalmazásokon

Nem kell változtatni az eszközökön

# Hogy véd a WAP?

## Preauthentication

Csak azonosított forgalom éri el a céges szervereket

## Hálózat izoláció

Közvetlenül nem éri el az Internetes kliens az alkalmazásszervereket. Minden a WAP-on keresztül megy.

## Szelektív publikáció

Meghatározott alkalmazás / path publikálható

## DDoS védelem

A bejövő forgalom lassítható, sorba állítható, ezáltal védhető a backend szerver réteg

# Proxy képességek

## Web protokollok: HTTP, HTTPS

## URL Translation

A belső és a külső domain név lehet eltérő: https://portal.contoso.com → http://portal/
HTTP fejlécben a nevek cserélhetőek. HTML vagy JavaScript-ben cserét ma nem tudunk elvégezni

## Csak HTTPS kintről

Bent lehet HTTP vagy akár HTTPS is

## Egyben ADFS Proxy is

A szabályok és az authorizációs szabályok tárolását és kiértékelését az ADFS végzi

# Preauthentication

## Opcionális

Nem kötelező, a végfelhasználó azonosíthatja magát a back-end rendszeren is közvetlenül.

## Az azonosítás az ADFS szerveren történik

Erős függelem az ADFS-től

A felhasználói azonosítóval, eszköz azonosítóval, az elérendő alkalmazáson és a hálózati helyen múlik, hogy milyen azonosítást használunk

Minden ADFS képesség támogatott: smart card, phone factor, soft password lockout stb.

Az átirányítás a következő protokollokra támogatott: standard HTTP, Office kliens, OAuth2

Nincs redirect: HTTP Basic vagy NTLM authantication

## Single Sign-On (SSO)

Az első azonosítás után nincs több authentikációs prompt

# Bridge between Claims and Kerberos

## SSO for Kerberos backend applications

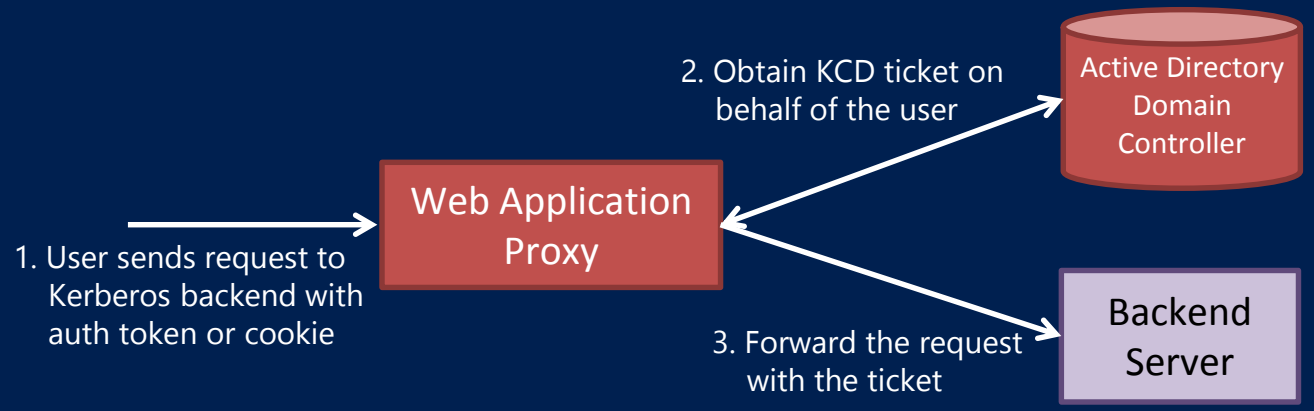
Web Application Proxy can use Kerberos Constrain Delegation (KCD) to authenticate the user to backend applications that support Kerberos / Integrated Windows Authentication (IWA).

This works only when preauthentication is not pass-through.

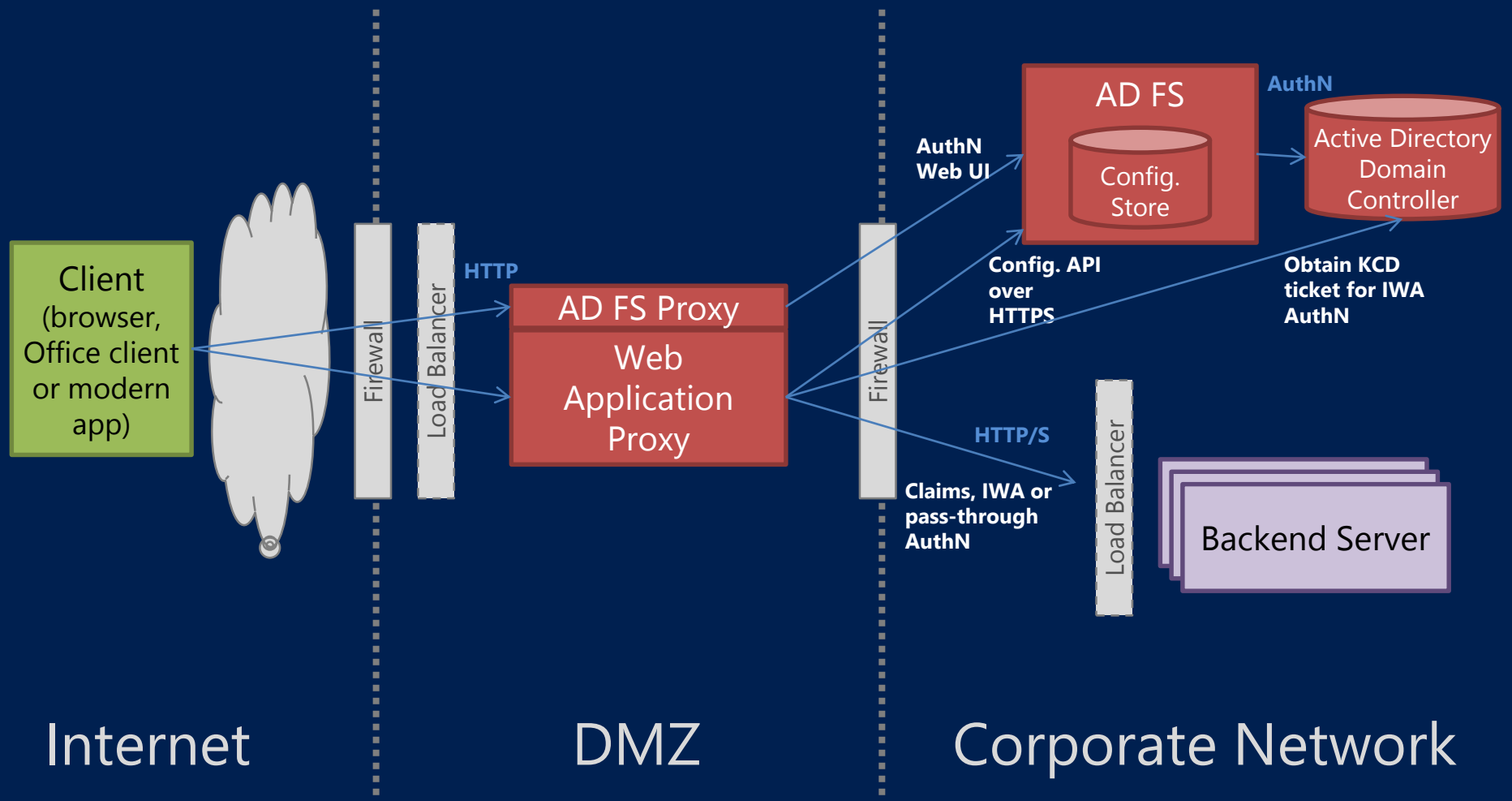
## AD FS authentication & authorization policies

AD FS in Windows Server 2012 R2 allows the configuration of non claims aware relying party.

These RPs are used by Web Application Proxy to enforce AD FS authentication and authorization policies for those applications.



# Network topology



# Experience with Microsoft Applications


SharePoint is working with preauthentication in AD FS when the SharePoint authentication is claims or Windows/Kerberos (via KCD).

Known limitation: Web Application Proxy does not support wildcard domain publishing (e.g. https://*.apps.contoso.com) so when publishing SharePoint Apps, their domains shall be published explicitly.


OWA can be published with preauthentication and KCD.

ActiveSync and Outlook Anywhere could be published with pass-through preauthentication.

Known limitations: Outlook Anywhere doesn't work on the preview release (fixed for RTM); Some old ActiveSync clients do not support SNI.


Lync mobility could be published using pass-through authentication. Known limitations: no support for HTTP interfaces, some Lync clients do not support SNI.

Lync SIP traffic shall be handled by Lync Edge.

Note: Web Application Proxy does not certify a specific application or its versions

# Built for scale, stability and ease of admin

| | | | |
|---|---|---|---|
| Fully functional API using PowerShell and WMI | Admin UI integrated with the Remote Access Management Console (VPN, DA) | Integration into Server Manager. Installed as a role service. | Performance Counters |
| SCOM Pack | Best Practices Analyzer (BPA) | Windows Event Log | Can easily scale to many symmetric servers |

# Work Folders

# Trusted File Servers

Original server workload

Exabytes deployed annually

Rich ecosystem

Simple and efficient

# Introducing Work Folders

- Allow information workers to access their individual data
- … that is centrally located on a traditional file server
- … from all of their devices
- … from wherever they are
- … while remaining in compliance with policies

# File Sync Solutions

| | Consumer / personal data | Individual work data | Team / group work data | Personal devices | Data location |
|---|---|---|---|---|---|
| SkyDrive | ✓ | | | ✓ | Public cloud |
| SkyDrive Pro | | ✓ | ✓ | ✓ | SharePoint / Office 365 |
| Work Folders | | ✓ | | ✓ | File server |

# Client Deployment Options

- Manual
  - Auto-discovery of server URL based on email address
  - Explicit entry of sync server URL
- Opt-in
  - Settings delivered via Group Policy, SCCM or Intune
  - User decides if they want to use Work Folders on that device
- Mandatory
  - Settings delivered via Group Policy, SCCM or Intune
  - No user action required

# Logical System Overview

Work Folders Server

## File and Storage Services sub-role

Server Manager provides a consolidated view of sync activity across your servers

An additional access protocol

Sync Share

## Multiple Sync Shares per server

Each share maps to a file system location

Users/groups associated with a single share

Policy defined per share

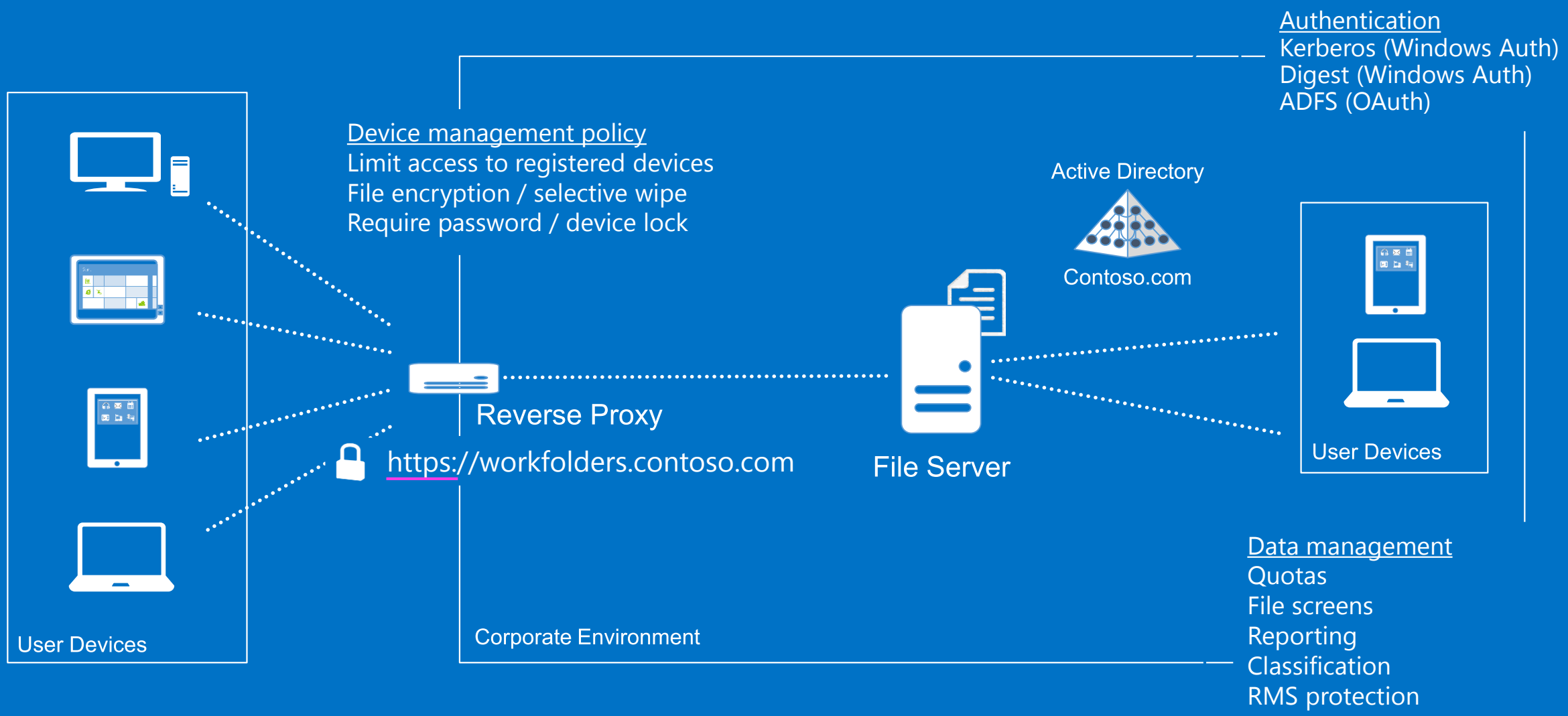
User devices

## Files stay in sync across all devices

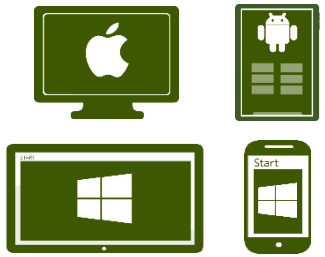
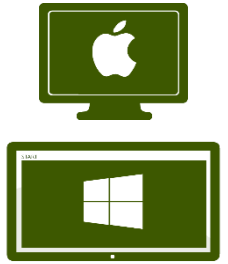
Local changes sync back to server and then to other devices

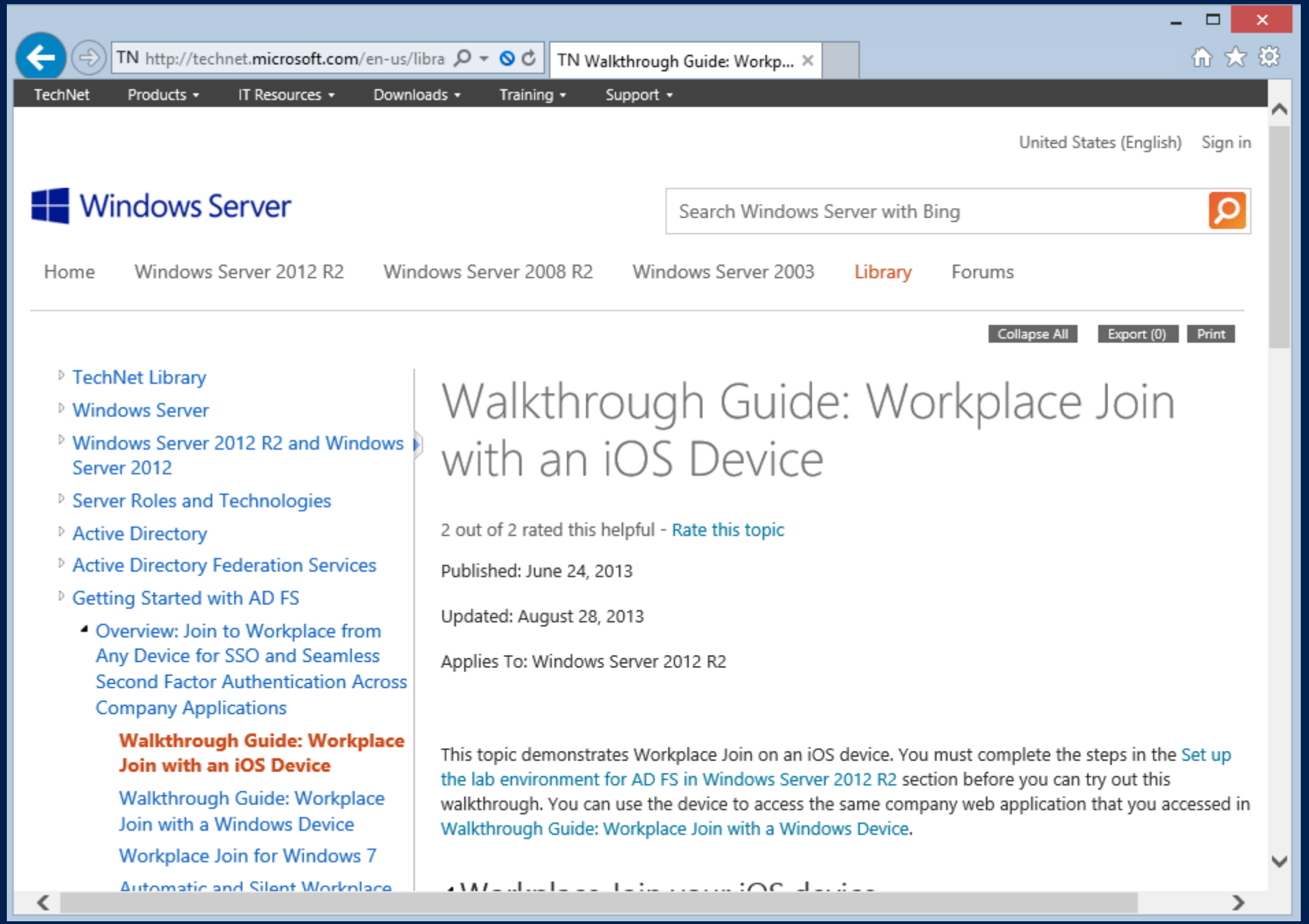
SMB clients can continue to work directly with server files

# Single Server Deployment



# Egyszeri bejelentkezés és eszköz regisztráció

| | Nem csatlakoztatott | Csatlakoztatott | Tartománytag |
|---|---|---|---|
| |  |  |  |
| | A felhasználó eszköze “ismeretlen” nincs felette semmilyen IT kontrol. Részleges hozzáférés esetleg engedélyezett. | A regisztrált eszköz „ismert” az IT számára, és az eszközhitelesítés lehetővé teszi az IT számára, hogy feltételes hozzáférést biztosítson a vállalati információkhoz | A tartománytag gépek az IT teljes kontrollja alatt állnak és teljes hozzáférésük lehet a vállalati információkhoz. |
| Böngésző munkamenet egyszer bejelentkezés | ✓ | ✓ | ✓ |
| Könnyű 2-faktoros hitelesítés Web alkalmazásokhoz | ✗ | ✓ | ✓ |
| Vállalati alkalmazások SSO | ✗ | ✓ | ✓ |
| Desktop SSO | ✗ | ✗ | ✓ |


TN http://technet.microsoft.com/en-us/libra
TN Walkthrough Guide: Workp...
TechNet
Products
IT Resources
Downloads
Training
Support
United States (English)
Sign in
Windows Server
Search Windows Server with Bing
Home
Windows Server 2012 R2
Windows Server 2008 R2
Windows Server 2003
Library
Forums
Collapse All
Export (0)
Print
TechNet Library
Windows Server
Windows Server 2012 R2 and Windows Server 2012
Server Roles and Technologies
Active Directory
Active Directory Federation Services
Getting Started with AD FS
Overview: Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications
Walkthrough Guide: Workplace Join with an iOS Device
Walkthrough Guide: Workplace Join with a Windows Device
Workplace Join for Windows 7
Walkthrough Guide: Workplace Join with an iOS Device
2 out of 2 rated this helpful - Rate this topic
Published: June 24, 2013
Updated: August 28, 2013
Applies To: Windows Server 2012 R2
This topic demonstrates Workplace Join on an iOS device. You must complete the steps in the Set up the lab environment for AD FS in Windows Server 2012 R2 section before you can try out this walkthrough. You can use the device to access the same company web application that you accessed in Walkthrough Guide: Workplace Join with a Windows Device.

# Az egyesített felügyelet különböző szintjei

| | Nem regisztrált | Regisztrált | MDM felügyelet | Teljes felügyelet |
|---|---|---|---|---|
| E-mail publikálás (EAS) | Igen | Igen | Igen | Igen |
| Work Folderek publikálása a felhasználóknak | Igen | Igen | Igen | Igen |
| Kondíció alapú hozzáférés a felhaaználó, az eszköz és a hely alapján | Csak eszköz blokkolás | Igen | Igen | Igen |
| Audit naplózás és monitorozás | | Igen | Igen | Igen |
| Egyesített eszköz felügyelet | | | Igen | Igen |
| Egyesített alkalmazás felügyelet | | | Igen | Igen |
| Szelektív adat-törlés | | | Igen | Igen |
| Megfelelőségi jelentések | | | Igen | Igen |
| Csoportházirendek és bejelentkezési scriptek | | | | Igen |
| OS terítés és lemezkép kezelés | | | | Igen |
| Konfiguráció kezelés | | | | Igen |
| Felügyelt szoftverfrissítés | | | | Igen |
| Anti malware felügyelet | | | | Igen |
| Teljes alkalmazás felügyelet | | | | Igen |
| BitLocker felügyelet | | | | Igen |


Microsoft