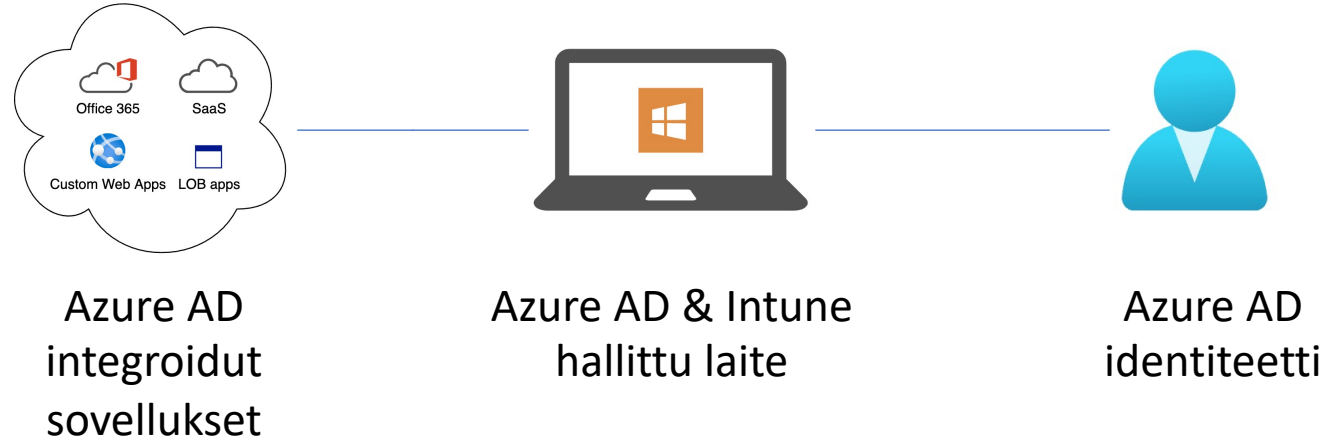
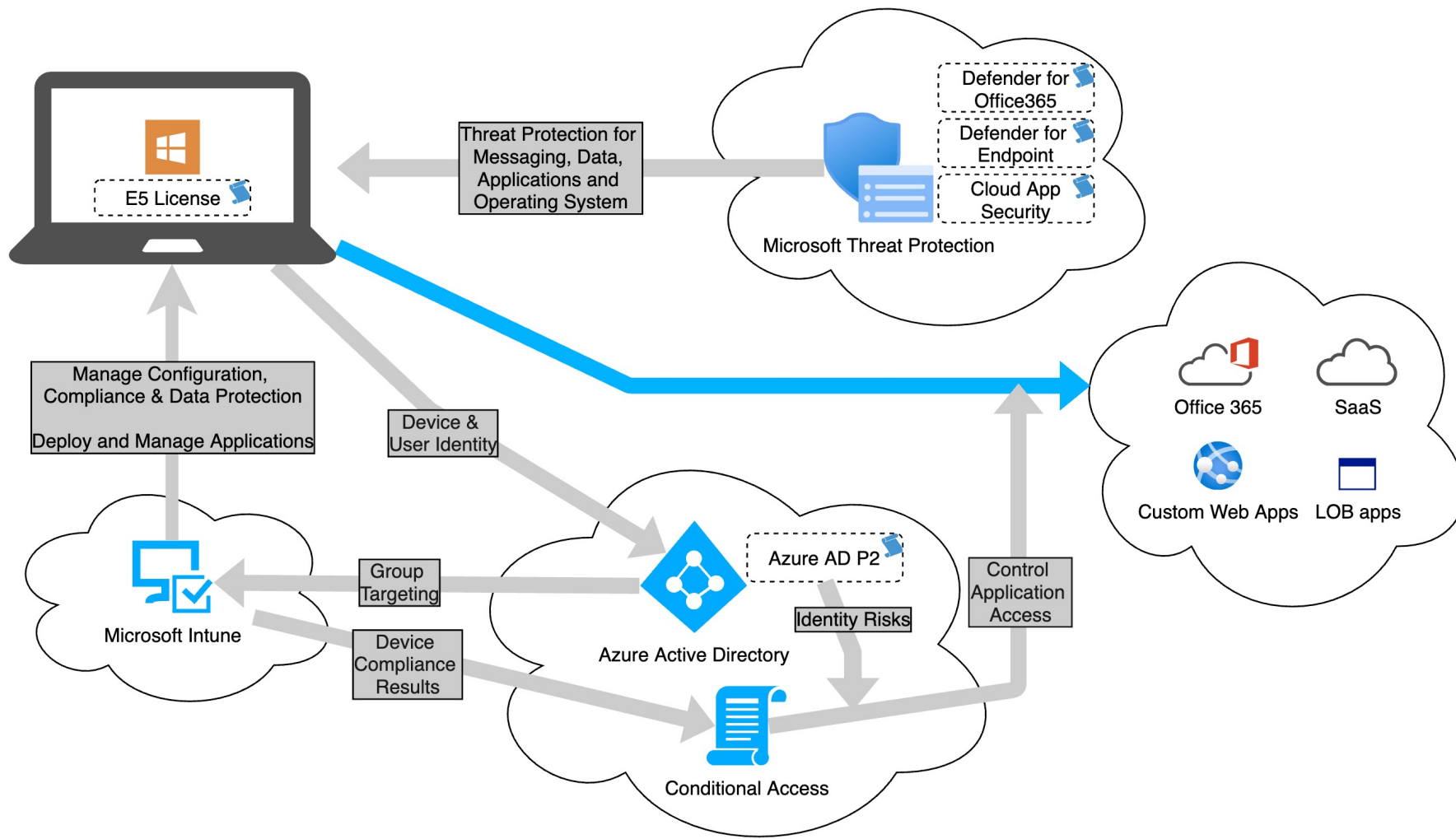


# Tietoturva pilvipalveluissa: Windows 10 ja Microsoft 365

08/2021

*“Miltä näyttää pilvihallittu, internetiin kytketty ja tietoturvallinen Windows 10 päätelaite, jolta käytetään M365- ja muita SaaS-palveluita?”*



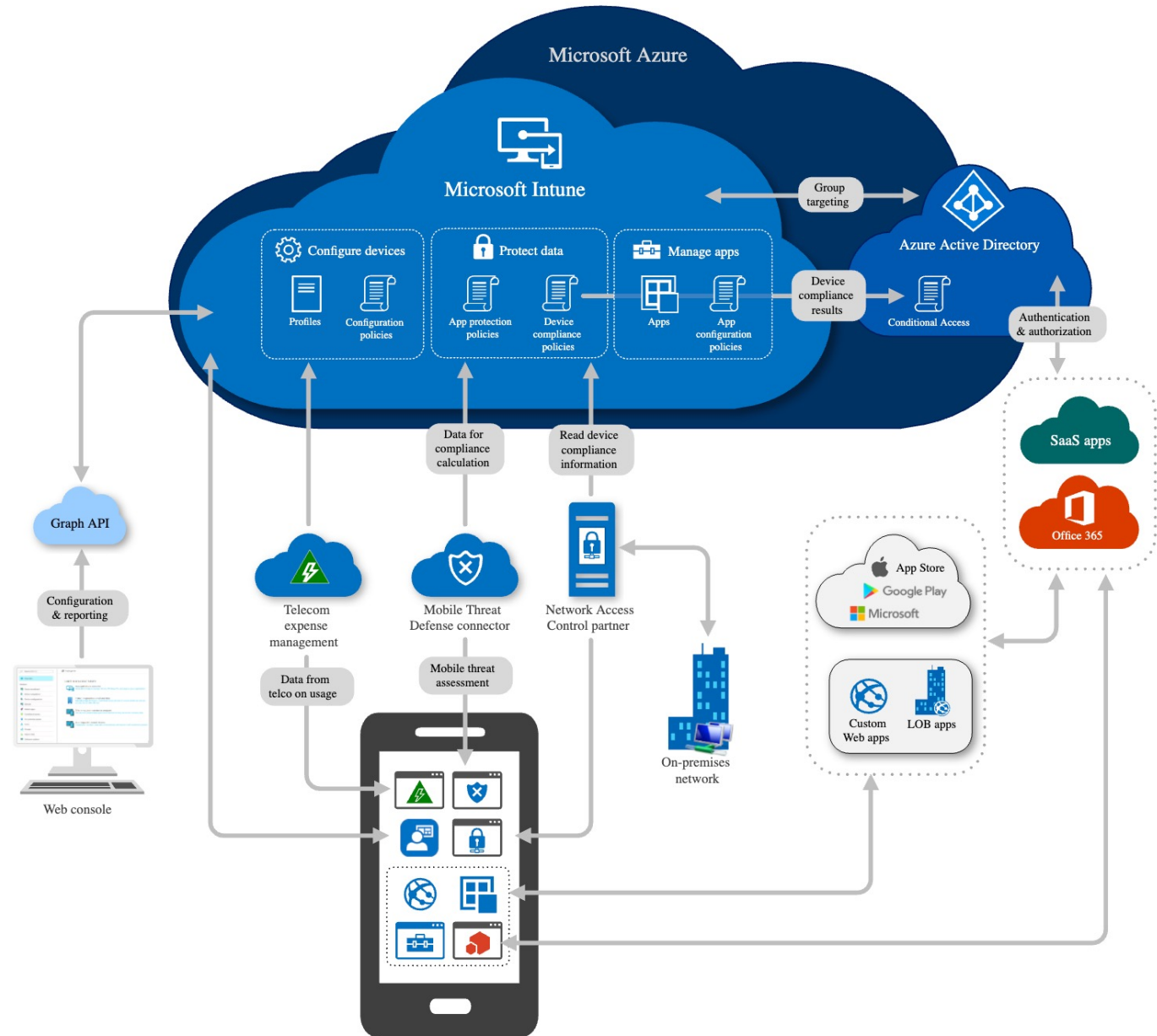


## Laitehallinnan keskeisenä palveluna Intune:

- Mobiililaitteet ja työasemat.
- BYOD ja yrityslaitteet.
- Windows, MacOS, Android, iOS.

## Ydinominaisuudet:

- Sovellusten hallinta ja jakelu.
- Laitteilla käsiteltävän tiedon suojaaminen.
- Laitteiden konfiguraation ja tietoturvaominaisuuksien hallinta.



**Laitteen pilvi-identiteetin** keskiössä Azure AD, johon laitteet voidaan kytkeä seuraavin tavoin:

### Azure AD Registered

- Henkilökohtainen BYOD-työasema tai mobiililaite.
- Kirjautuminen lokaalilla tunnuksella.
- Asetusten tietoturvasoa voidaan valvoa Intunella.

Käyttöjärjestelmätuki:  
Windows 10  
Android, iOS, MacOS

### Azure AD Joined

- Yrityksen omistama pilvinatiivi työasema.
- Kirjautuminen yritysidentiteetillä.
- Voidaan hallita Intunella.

Käyttöjärjestelmätuki:  
Windows 10  
Server 2019 Azuressa

### Azure AD Hybrid Joined

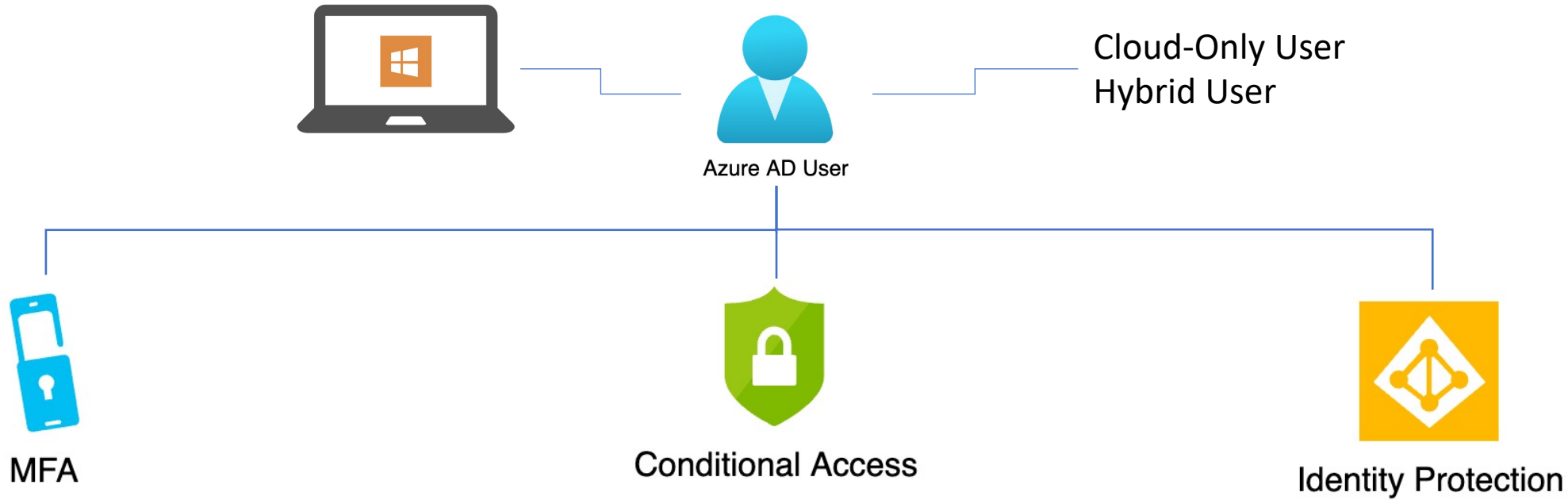
- Yrityksen omistama hybridi-työasema.
- Kirjautuminen yritysidentiteetillä.
- Voidaan hallita Intune, SCCM ja Group Policyn yhdistelmällä.

Käyttöjärjestelmätuki:  
Windows 7, 8.1, 10  
Server 2008 tai uudempi

Paikkariippumaton

Sisäverkko

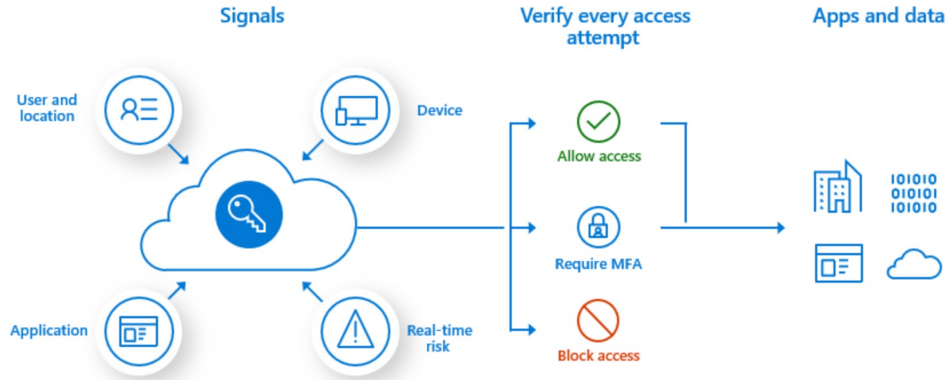
# Käyttäjän identiteetti pilvessä



Microsoft  
bala@contoso.com

## Verify your identity

- Approve a request on my Microsoft Authenticator app
- 123 Use a verification code from my mobile app
- Text +X XXXXXXXX40
- Call +X XXXXXXXX40



### Risk detection type

- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked Credentials

## Salasanaton kirjautuminen laitteelle

Mitä on salasanaton kirjautuminen

- PIN-koodi tai biometrinen tunnistus

Miksi parempi kuin salasana

- Sidottu fyysiseen laitteeseen
- Suojattu laitteen rautatasolla (TPM-siru)

Tekniikat Windows 10-koneilla

- Windows Hello for Business
- Authenticator App
- FIDO2 avaimet

### Use Windows Hello with your account

Your organization requires you to set up your work or school account with Windows Hello Face, Fingerprint, or PIN.

If you've already set up Windows Hello on this device, we'll automatically add it for this account. You may be asked to re-verify with Windows Hello.

If your organization requires a more complex PIN, Windows will prompt you to change it.



### Four steps to passwordless freedom

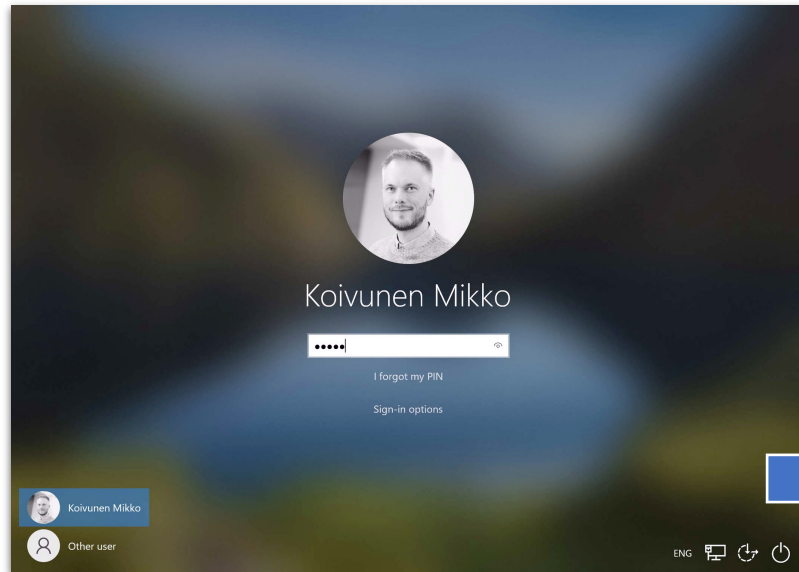
1. **Develop** a password replacement offering
2. **Reduce** user-visible password surface area
3. **Transition** into a passwordless deployment
4. **Eliminate** passwords from the identity directory

Lähde:

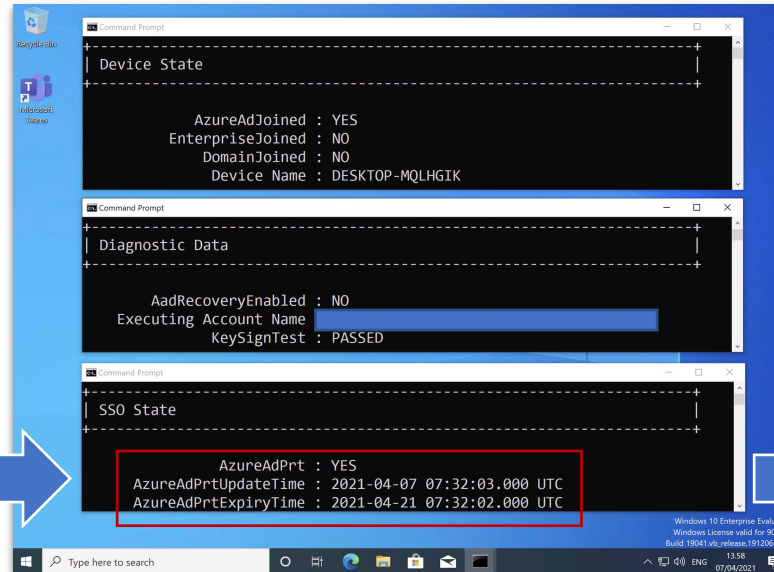
[Passwordless Strategy - Microsoft 365 Security | Microsoft Docs](#)

# Salasanaton kirjautuminen, SSO ja MFA

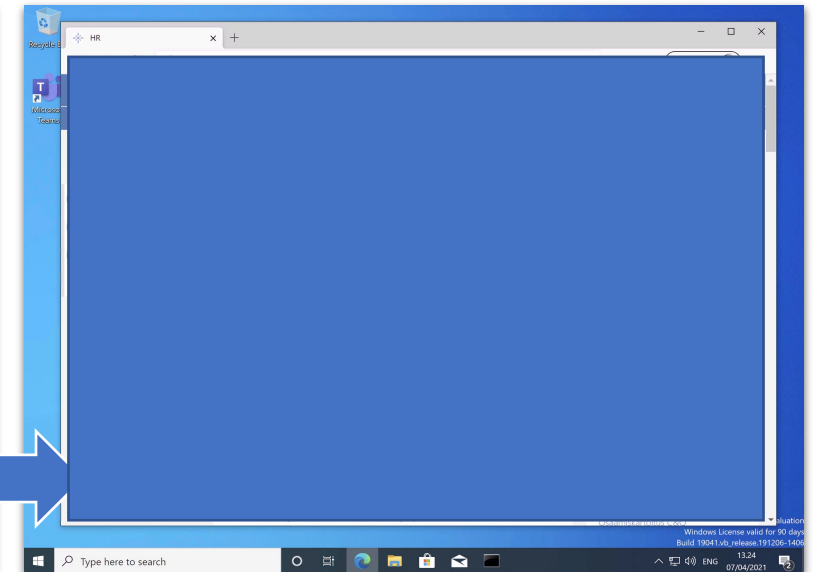
## Win10 PIN-kirjautuminen



## Windows saa AAD:lta tokenin



## SSO & MFA pilvisovelluksiin



Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓
Require MFA for External Usage	require multi-factor authentication		Success

OperationName	Sign-in activity
AuthenticationRequirement	multiFactorAuthentication
DeviceDetail_displayName	DESKTOP-MQLHGK
AppDisplayName	Office 365 SharePoint Online
DeviceDetail_trustType	Azure AD joined
Status_additionalDetails	MFA requirement satisfied by claim in the token



## Sovellusten käyttö pilvityöasemalta

### SaaS-sovellukset

Tavoitteeksi kannattaa ottaa Azure AD kirjautuminen kaikkiin SaaS-palveluihin.

SaaS-palveluiden käyttöä ja riskejä voidaan seurata ns. CASB tuotteilla.

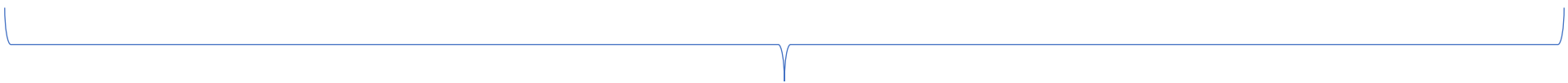
### Web-sovellukset

Aiemmin VPN/VDI-käyttöä vaatineet sisäverkon web-sovellukset voidaan julkaista turvallisesti esimerkiksi Azure AD App Proxy palvelulla.

### Legacy-sovellukset

Client-server sovellukset sopivat heikosti pilvipohjaiseen työasemaan.

Käytännössä tarvitaan työpöytä- tai sovellusvirtualisointia.



Tietoturvasoaa voidaan korottaa kytkemällä palveluiden julkaisu ja kirjautuminen osaksi zero-trust arkkitehtuurin mukaista keskitettyä pääsynhallintapalvelua.

## Tietoturvaluottot

<b>Defender for Endpoint</b>	<ul style="list-style-type: none"><li>• Päätelaitteiden suojaus haittaohjelmilta</li><li>• Päätelaitteuhkien ja haavoittuvuuksien hallinta</li></ul>
<b>Defender for Office 365</b>	<ul style="list-style-type: none"><li>• Viestinnän ja kollaboraatiopalveluiden suojaus haittaohjelmilta, tietojen kalastelulta ja huijauksilta.</li></ul>
<b>Cloud App Security</b>	<ul style="list-style-type: none"><li>• SaaS-palveluiden riskien tunnistaminen.</li><li>• Varjo-IT havainnointikyky.</li><li>• Tiedon luokittelu ja tietovuotojen tunnistus.</li></ul>
<b>Windows 10 built-in</b>	<ul style="list-style-type: none"><li>• Bitlocker</li><li>• Windows Defender anti-virus</li><li>• Windows Firewall</li><li>• AppLocker</li><li>• Ransomware protection (OneDrive)</li></ul>



### Endpoints

Deliver preventive protection, post-breach detection, automated investigation, and response for endpoints.

[Learn about Microsoft Defender for Endpoint >](#)



### Cloud apps

Get visibility, control data, and detect threats across cloud services and apps.

[Learn about Microsoft Cloud App Security >](#)



### Email and documents

Secure your email, documents, and collaboration tools with Microsoft Defender for Office 365.

[Learn about Microsoft Defender for Office 365 >](#)