

7.2.0. Bitlocker 1.5

Thursday, December 11, 2025 12:12

Tietoturva, tietosuoja , kyberturvallisuus ja ISO 27000 standardi

- BitLocker Windows Serverissä (fysisisesti, "maassa olevana") tukee tietoturvaa, tietosuoja ja kyberturvallisuutta, koska se suojaa levyllä olevaa dataa varkauden, katoamisen tai luvattoman käytön varalta.
- ISO/IEC 27001 -standardi ja EU:n GDPR eivät määrään nimenomaan BitLockeria, mutta ne edellyttävät **asianmukaista teknistä suojausta** (kuten levysalausta).

BitLocker Windows Serverissä

- **Tietoturva:** BitLocker käyttää AES-salausta suojaamaan levyjä. Jos palvelin tai levy joutuu väärin käsiin, data ei ole luettavissa ilman avainta.
- **Tietosuoja:** GDPR edellyttää, että henkilötietoja suojataan "asianmukaisin teknisin ja organisatorisin toimin". Levysalaus on suositeltu keino, koska se estää tietojen paljastumisen fysisen varkauden yhteydessä.
- **Kyberturvallisuus:** BitLocker ei estää verkko- tai sovellushyökkäyksiä, mutta se täydentää kokonaisuutta suojaamalla **data at rest** (levyllä oleva tieto). Tämä on osa monikerroksista kyberturvaa.

ISO/IEC 27001 ja BitLocker

- ISO/IEC 27001:2022 on kansainvälinen standardi tietoturvan hallintajärjestelmiille. Se ei määrä tiettyä teknologiaa, mutta vaatii riskienhallintaa ja kontrollien toteutusta.
- BitLocker voidaan dokumentoida osaksi **kontrollia A.10 (Cryptography)** ja **A.18 (Compliance)**.
- Käytännössä BitLocker on yksi tapa osoittaa, että organisaatio hallitsee riskiä fyysisen median katoamisesta.

Lainsäädäntö (EU ja Suomi)

- **GDPR (EU 2016/679):**
 - Edellyttää henkilötietojen suojaamista.
 - Salaus on mainittu yhtenä keinona, ja sen puuttuminen voi johtaa sanktioihin, jos data vuotaa.
- **Suomen tietosuojalaki (1050/2018):** täydentää GDPR:ää.
- **Käytännön tulkinta:** Jos organisaatio käsittelee henkilötietoja Windows Serverillä, levysalaus BitLockerilla on vahva tapa osoittaa "asianmukaiset tekniset toimet".

Riskit ja huomioitavaa

- Ilman keskitettyä hallintaa (AD/Intune) recovery keyt voivat jäädä hajanaisiksi → hallinnollinen riski.
- BitLocker ei yksin riitä: tarvitaan myös käyttööikeuksien hallinta, lokitus, verkon suojaus.
- **Auditointi:** ISO 27001 -sertifioinnissa pitää pystyä osoittamaan, että BitLocker on otettu käyttöön hallitusti ja avainten hallinta on dokumentoitu.

Yhteenveto

- BitLocker Windows Serverissä tukee **GDPR:n ja ISO 27001:n vaatimuksia** suojaamalla dataa levyllä.
- Laki ei määrä juri BitLockeria, mutta **salaus on käytännössä välittämätön** tietosuojan ja kyberturvallisuuden kannalta.
- Pienissä yrityksissä BitLocker voi olla nopea ratkaisu, suurissa se on osa hallittua ISMS-järjestelmää.

#####

Vmworkstation (windows server manager + Entra id / azure)

Hybridimallissa BitLocker-avaimet voidaan tallentaa sekä **Active Directoryyn (AD)** että **Entra ID / Intuneen**, mutta tämä edellyttää oikeanlaista konfiguraatiota. Jos asetukset eivät ole yhtenäiset, osa avaimista voi jäädä vain AD:hen, jolloin niitä ei näy Intune/Entra ID -portaalissa

BitLocker-avainten tallennus hybridimallissa

- **Active Directory (on-prem):** Perinteisesti BitLocker-avaimet tallennetaan AD:n tietokantaobjekteihin. Tämä toimii hyvin, jos hallinta on täysin on-prem.
- **Entra ID (Azure AD):** Kun laite on **Azure AD-joined** tai **hybrid-joined**, BitLocker-avaimet voidaan varastoida myös Entra ID:hen. Admin voi tarkistaa ne **Entra admin centeristä** (Devices → Recovery keys).
- **Intune:** Jos BitLocker on otettu käyttöön Intune-politiikalla, avaimet varmuuskopioidaan automaattisesti Entra ID:hen. Intune tarjoaa myös hallintpaneelin, josta avaimet löytyvät. Käyttäjät voivat hakea omat avaimensa **myaccount.microsoft.com**-portaalista.

Käytännön huomioita hybridissä

- **Sekava tilanne:** Hybrid-joined laitteilla osa avaimista voi tallentua vain AD:hen, vaikka asetuksissa olisi määritetty myös Azure AD. Tämä johtuu usein GPO-asetusten ja Intune-politiikan päällekkäisydestä.
- **Ratkaisu:**
 - Varmista, että **Intune BitLocker policy** on otettu käyttöön ja että se vaatii avainten varmuuskopioinnin Entra ID:hen.

- Jos laitteet on jo salattu AD:n kautta, avaimet pitää **migroida** tai **uploadata** Entra ID:hen erikseen (PowerShell-skriptit tai Microsoftin migraatio-ohjeet).
- Dokumentoi, kumpi on “source of truth” (AD vai Entra ID), jotta auditointi ja palautus onnistuvat.

Riskit ja haasteet

- **Inconsistent storage:** Jos osa avaimista jää vain AD:hen, Intune/Entra ID-portaalissa näkyy “BitLocker recovery key missing”.
- **Auditointi:** Yrityksen compliance-vaatimukset voivat edellyttää, että kaikki avaimet löytyvät yhdestä hallintakanavasta.
- **Käyttäjäkokemus:** Jos avain ei ole Entra ID:ssä, käyttäjä ei voi hakea sitä itsepalveluportaalista, vaan adminin pitää kaivaa se AD:stä.

VMware-labissa ja testaat hybridimallia:

1. Konfiguroi GPO niin, että avaimet tallennetaan AD:hen.
2. Ota Intune BitLocker policy käyttöön, joka pakottaa avaimet myös Entra ID:hen.
3. Testaa hybrid-joined VM: varmista, että avain näkyy sekä AD:ssä että Entra ID:ssä.
4. Dokumentoi prosessi: miten admin hakee avaimen AD:stä vs. Entra ID:stä. Tämä on tärkeää auditointia ja käyttäjätukea varten.
5. Yritys voi saada BitLocker-avaimet näkyviin Intune/Entra ID-portaalissa hybridimallissa, mutta se vaatii oikean politiikan ja mahdollisesti migraation jo salatuista laitteista.

Hybridimallissa (AD + Entra ID/Intune) BitLocker-avainten hallinnassa voi syntyä useita **riskejä ja haasteita**, jotka eivät aina näy heti, mutta voivat aiheuttaa isoja ongelmia myöhemmin.

Keskeiset riskit ja haasteet

- **Avainten tallennuspaikan epäselvyys**
 - Jos GPO ohjaa avaimet AD:hen ja Intune-politiikka Entra ID:hen, osa avaimista voi tallentua vain toiseen paikkaan.
 - Admin ei välttämättä tiedä, mistä avain löytyy kriittisessä palautustilanteessa.
- **Auditointi ja compliance**
 - Jos yritys ilmoittaa, että kaikki avaimet löytyvät Entra ID:stä, mutta osa onkin vain AD:ssä, syntyy auditointiriskejä.
 - Tämä voi rikkoa esim. ISO 27001 tai GDPR-vaatimuksia, jos avaimia ei hallita keskitetysti.
- **Käyttäjäkokemus**
 - Käyttäjät voivat hakea avaimensa itsepalveluportaalista (myaccount.microsoft.com), mutta vain jos avain on Entra ID:ssä.
 - Jos avain on vain AD:ssä, käyttäjä joutuu ottamaan yhteyttä IT-tukeen → lisää kuormaa.
- **Migraatiohaasteet**
 - Jo salatut laitteet eivät automaattisesti siirrä avaimiaan Entra ID:hen.
 - Tarvitaan PowerShell-skriptejä tai Microsoftin migraatiotyökaluja, mikä voi olla työlästää.
- **Hybrid-joinin epäselvyyydet**
 - Laitteen tila (AD-joined, Azure AD-joined, hybrid-joined) vaikuttaa siihen, minne avain tallentuu.
 - Jos join-tila ei ole selkeä, avaimet voivat jäädä väärään paikkaan.
- **Politiikkojen ristiriidat**
 - GPO ja Intune voivat antaa ristiriitaisia asetuksia (esim. pakollinen tallennus AD:hen vs. Entra ID:hen).
 - Tämä voi johtaa siihen, että BitLocker ei aktivoi oikein tai avaimet eivät varmuuskopioi.

Muita sekaannuksia, joita voi ilmetä

- **Monen hallintakanavan käyttö**
 - Adminit joutuvat tarkistamaan sekä AD:stä että Entra ID:stä → lisää hallintatyötä.
- **Varastointiformaattien erot**
 - AD tallentaa avaimet objektiin attribuutteihin, Entra ID tallentaa ne portaalin kautta.
 - Tämä voi aiheuttaa eroja raportoinnissa ja automaattisessa avainten haussa.
- **Hybridilaitteiden offboarding**
 - Kun käyttäjä poistuu, laitteen avaimet voivat jäädä vain AD:hen, vaikka yritys haluaisi ne Entra ID:hen.
- **Intune-politiikan viiveet**
 - Jos Intune ei ehdi puskea asetuksia ennen kuin BitLocker käynnistyy, avain tallentuu vain AD:hen.

Miksi tämä on tärkeää

- **Palautustilanteet:** Jos avain ei löydy nopeasti, käyttäjä voi menettää pääsyn dataan.
- **Compliance:** Yrityksen pitää pystyä osoittamaan, että kaikki avaimet ovat hallinnassa.
- **Hallinnan selkeys:** Yksi “source of truth” vähentää virheitä ja nopeuttaa tukiprosesseja.
- suurin riski on **avainten hajautuminen kahteen eri paikkaan** ja siitä seuraava **epäselvyys hallinnassa, auditoinnissa ja käyttäjätuessa**.

Lisenssitaso ja muu minimaallisuus tasot

Lisenssitaso vaikuttaa suoraan siihen, miten BitLocker-avainten hallinta toimii hybridimallissa (AD + Entra ID + Intune).

Lisenssitasojen vaikutus BitLocker-avainten hallintaan

Lisenssi	Mitä saat	BitLocker-avainten hallinta	Mahdolliset sekaannukset
Azure/Entra	Perus Azure AD (Entra ID) ominaisuudet	BitLocker-avaimet eivät tallennu Entra ID:hen.	Jos yritys luulee, että avaimet näkyvät pilvessä, syntyy sekaannusta. Käyttäjät eivät voi hakea
Free		Avainten varmuuskopioointi onnistuu vain AD:hen.	

Entra ID P1	Hybrid join, Conditional Access, perus Intune-integraatio	BitLocker-avaimet voidaan tallentaa Entra ID:hen, mutta hallinta on rajallista. Avainten näkyvyys adminille onnistuu, mutta ei laajaa raportointia.	avaimiaan itsepalveluportaalista. Jos osa laitteista on vain AD-joined, avaimet jäävät AD:hen. Hybrid join voi aiheuttaa ristiriitoja, jos GPO ja Intune asetukset eivät ole linjassa.
Entra ID P2	Advanced security, Identity Protection	Sama kuin P1, mutta parempi auditointi ja riskienhallinta. Avainten hallinta selkeämpää.	Vähemmän sekaannusta, mutta jos osa laitteista ei ole Intunen hallinnassa, avaimet voivat silti hajautua.
Intune (lisensi vaaditaan erikseen)	Endpoint management, BitLocker policy	BitLocker-avaimet tallentuvat automaattisesti Entra ID:hen, näkyvät Intune-portaalissa ja käyttäjien itsepalvelussa.	Jos Intune ei ole käytössä, avaimet eivät siirry pilveen → ristiriita odotusten ja todellisuuden välillä.

⚠ Riskit minimitasolla (Free/P1 ilman Intunea)

- **Avaimet vain AD:ssä** → Pilvhallinta puuttuu, käyttäjät eivät voi hakea avaimiaan itse.
- **Hybrid join ei riitä yksinään** → Pelkkä hybrid join ei takaa, että avaimet tallentuvat Entra ID:hen.
- **Lisenssien väärinymmärrys** → Yritys voi olettaa, että "Azure AD join" = avaimet pilvessä, vaikka todellisuudessa se vaatii Intune-politiikan.
- **Auditointi ja compliance** → Free/P1 ei tarjoa keskitettyä raportointia avaimista → vaikeampi osoittaa hallintaa auditojille.

✓ Yhteenveto

- **Free-tasolla:** BitLocker-avaimet jäävät vain AD:hen → pilvhallintaa ei ole.
- **P1-tasolla:** Avaimet voidaan tallentaa Entra ID:hen, mutta hallinta on rajallista ja helposti syntyy sekaannusta, jos osa laitteista ei ole Intunen hallinnassa.
- **Intune + Entra ID:** Vasta tämä yhdistelmä tuo selkeän, keskitetyn hallinnan ja vähentää ristiriitoja.

Minimitason lisenssit **tuovat sekaannusta ja ristiriitoja**, koska yritys voi luulla saavansa pilvhallinnan "ilmaiseksi", vaikka todellisuudessa BitLocker-avainten hallinta pilvessä vaatii Intune-politiikan ja vähintään P1-lisenssin.

#####

Maasta pilveen (Windows server >> Azure (Entra))

Kun yritys (tai itse labissa) siirtyy **Windows Serveristä kohti pilvipalveluita** (Entra ID, Intune, Azure), kyse ei ole vain teknisestä migraatiosta vaan myös **hallinnan, kustannusten ja riskien uudelleenajattelusta**. Tämä koskee myös BitLocker-avainten hallintaa, mutta laajemmin koko infrastruktuuria.

📝 Mitä testata ja tarkistaa pilvisiirtymässä

- **Hybrid join toimivuus**
 - Testaa, että laitteet liittyvät oikein sekä AD:hen että Entra ID:hen.
 - Varmista, että avaimet tallentuvat sinne minne pitää (AD vs. Entra ID).
- **GPO vs. Intune politiikat**
 - Tarkista, ettei päällekkäisiä asetuksia ole.
 - Testaa, kumpi voittaa jos molemmat ohjaavat BitLockeria.
- **Käyttäjäkokemus**
 - Simuloi palautustilanne: pystyykö käyttäjä hakemaan avaimen itse Entra ID:stä?
 - Testaa tukiprosessi: admin löytääkö avaimen nopeasti?
- **Vianmääritys**
 - Hybrid join virheet (esim. device registration failure).
 - Avainten tallennus epäonnistuu → tarkista event logit ja Intune compliance-raportit.
 - Testaa eri skenaarioita: uusi laite, jo salattu laite, offboarding.
- **Palveluiden integraatio**
 - AD CS (sertifikaatit), GPO:t, Intune-politiikat → varmista, että ne eivät ole ristiriidassa.
 - Testaa myös, miten pilvipalvelut toimivat VMware-labissa (rajallinen internet-integraatio).

⌚ Kustannusten vertailu

Kun mietit pilvipalveluun siirtymistä, kustannukset eivät ole vain lisenssejä, vaan myös **piilokuluja ja säästöjä**:

- **Lisenssit**
 - Entra ID Free vs. P1 vs. P2 → vaikuttaa siihen, missä avaimet tallentuvat ja mitä hallintaa saat.
 - Intune → erillinen lisenssi, mutta tuo keskitetyn hallinnan.
- **Infrastruktuuri**
 - On-prem Windows Server = laitteistonkustannukset, ylläpito, sähkö, varmistukset.
 - Pilvi = kuukausimaksut, mutta ei laitteistohuolia.
- **Hallinta ja tuki**
 - On-prem: adminit hallitsevat AD:tä ja GPO:ta.
 - Pilvi: Intune/Entra ID vähentää manuaalista työtä, mutta vaatii uutta osaamista.
- **Riskit ja compliance**
 - Jos avaimet hajautuvat, auditointi voi maksaa enemmän (lisätyö, riskit).

- Pilvessä raportointi ja compliance helpottuvat, mutta lisenssitaro ratkaisee.

Suositeltu eteneminen

1. Labissa testaa hybrid join + BitLocker avainten tallennus molempien paikkoihin.
2. Dokumentoi vianmääritysprosessit: mitä logeja tarkistat, mistä avaimet löytyvät.
3. Vertaa kustannuksia:
 - AD + Windows Server ylläpito vs. Entra ID + Intune lisenssit.
 - Laske myös piilokulut (sähkö, ylläpito, auditointi).
4. Pohdi compliance-näkökulmaa: missä avaimet pitää olla, jotta auditointi onnistuu.

Windows Serverin roolin pienentyminen ja pilvipalvelun siirtyminen vaikuttaa suoraan BitLocker-avainten hallintaan ja tuo mukanaan testaus- ja kustannusvertailun tarpeen.

Käyttäjien määrä ja testauksessa

Missä testauksen laajuus ja yrityksen koko alkavat vaikuttaa siihen, kuinka monta päivää tai viikkoja kannattaa varata. Hyvä lähtökohta on aina aloittaa pienestä, hallitusta pilotista ennen kuin laajennat muihin tiimeihin.

Hyvä lähtökohta testaukselle

- Aloita itsestäsi / labista
 - Testaa ensin VMware-ympäristössä: hybrid join, BitLocker-avainten tallennus AD:hen ja Entra ID:hen.
 - Dokumentoi kaikki vaiheet ja virheet → tämä toimii pohjana myöhemmälle skaalauselle.
- Pieni pilotti (10 käyttäjää)
 - Valitse eri rooleista (HR, laskutus, myynti) muutama testikäyttäjä.
 - Näet, miten politikit ja avainten hallinta toimivat eri tiimien laitteilla.
 - Tämä vaihe vie yleensä **päiviä**, ei viikkoja.
- Keskkokoinen pilotti (50–100 käyttäjää)
 - Tässä vaiheessa huomaat, miten **tuki ja prosessit** kestävät kuormaa.
 - Testaa palautustilanteet: pystyykö IT löytämään avaimet nopeasti, ja osaavatko käyttäjät hakea ne itsepalvelusta.
 - Tämä voi viedä **1–2 viikkoa**, koska ongelmia alkaa tulla enemmän.
- Laajempi testaus (200–500 käyttäjää)
 - Tässä kohtaa järjestelmänvalvoja ei enää pärjää yksin. Tarvitaan **lisäksiä muista tiimeistä** (helpdesk, infra, tietoturva).
 - Prosessit pitää olla dokumentoitu ja automatisoitu (Intune-politiikat, raportointi).
 - Tämä vaihe voi viedä **useita viikkoja**, koska mukana on jo organisaation eri osastot ja compliance-vaihtumiset.

Mitä "pilotti" tarkoittaa IT-ympäristössä

- Pilotti = kokeilu / testivaihe ennen laajempaa käytöönottoa.
- Siinä otetaan **pieni määrä laitteita tai käyttäjiä** mukaan, jotta voidaan testata asetuksia, politiikkoja ja prosesseja käytännössä.
- Tavoite on löytää virheet, ristiriidat ja käytännön ongelmat ennen kuin koko organisaatio siirtyy uuteen malliin.

Käyttäjät vs. järjestelmä

- Pilotti voi olla **10 käyttäjää eri tiimeistä** (esim. HR, myynti, laskutus), jolloin näet miten eri roolit ja laitteet reagoivat.
- Se voi myös olla **vain IT-tiimin testilaitteet**, jos haluat ensin varmistaa teknisen toimivuuden ennen kuin otat loppukäyttäjät mukaan.
- Eli "pieni pilotti" ei ole yksi käyttäjä, vaan **rajattu joukko** – yleensä 5–20 käyttäjää tai laitetta.

Miksi pilotti tehdään

- **Riskien hallinta:** jos asetukset eivät toimi, vain pieni ryhmä kärsii, ei koko organisaatio.
- **Dokumentointi:** saat selville, mitä pitää muuttaa ja voit kirjoittaa ohjeet valmiiksi.
- **Tukiprosessit:** näet, miten helpdesk tai admin löytää avaimet ja ratkaisee ongelmat.

"pienestä pilotista", tarkoitan pientä testikäyttäjäryhmää tai testilaitteiden joukkoa, ei yksittäistä käyttäjää.

Mitä vaikuttaa testauksen kestoon

- **Yrityksen koko ja tiimirakenne**
 - Mitä enemmän käyttäjiä ja rooleja, sitä enemmän variaatiota laitteissa ja prosesseissa.
- **Lisenssitaro (Free vs. P1 vs. Intune)**
 - Jos käytössä on vain AD + Free, testaus keskittyy AD:hen.
 - Jos mukana on Intune, pitää testata myös pilvipolitiikat ja raportointi.
- **Tukiprosessit**
 - Jos IT-tiimi on pieni, testaus vie enemmän aikaa.
 - Jos mukana on helpdesk ja infra, työ jakautuu.
- **Dokumentointi ja vianmääritys**
 - Hyvä dokumentointi nopeuttaa skaalaumista.
 - Jos dokumentaatio puuttuu, jokainen uusi vaihe vie enemmän aikaa.

Suositus etenemiselle

1. Testaa ensin itse labissa → saat varmuuden peruspolitiikoista.
2. Pilotti 10 käyttäjällä → nopea, hallittu, eri roolit mukana.

3. Laajenna 50–100 käyttäjään → testaa tukiprosessit ja itsepalvelu.
4. Skaala 200–500 käyttäjään → vasta tässä vaiheessa kannattaa ottaa koko organisaatio mukaan.

Kannattaa **aloittaa itsestäsi ja pienestä pilotista** ennen kuin laajennat muihin tiimeihin. Mitä suurempi käyttäjämääriä (10 vs. 500), sitä enemmän aikaa ja tiimien välistä yhteistyötä tarvitaan.

Tämä liittyy suoraan siihen, mitä tapahtuu jos yritys **ei skaala pilvipalveluihin** vaan jää Windows Server + AD -malliin, vaikka käyttäjämääriä kasvaa.

Mitä riskejä syntyy jos ei skaala pilveen (200–500 käyttäjää)

- **Hallinnan monimutkaistuminen**
 - AD + GPO toimii hyvin pienessä ympäristössä, mutta 200–500 käyttäjällä politiikkojen, sertifikaattien ja BitLocker-avainten hallinta muuttuu raskaaksi.
 - Järjestelmänvalvoja joutuu tekemään paljon manuaalista työtä, ja virheiden riski kasvaa.
- **Avainten hajautuminen**
 - Jos avaimet jäävät vain AD:hen, käyttäjät eivät voi hakea niitä itsepalvelusta.
 - Tukiprosessi kuormittuu, koska jokainen palautustilanne vaatii adminin apua.
- **Kustannukset pitkällä aikavälillä**
 - On-prem Windows Server vaatii laitteistokuluja, ylläpitoa, sähköä ja varmistuksia.
 - Kun käyttäjämääriä kasvaa, nämä kulut voivat nousta pilvipalvelua kalliimmiksi.
- **Auditointi ja compliance**
 - Suuremmassa organisaatiossa auditointivaatimukset (ISO, GDPR, NIS2) korostuvat.
 - Jos avaimet ja hallinta ovat vain AD:ssä, raportointi ja läpinäkyvyys ovat heikompia.
- **Joustavuuden puute**
 - Pilvessä Intune ja Entra ID tarjoavat automaattisen avainten tallennuksen, raportoinnin ja itsepalvelun.
 - Jos pysyt vain AD:ssä, et saa näitä hyötyjä → vaikeampi tukea etätyötä ja hajautettuja tiimejä.

Mitä jos skaalaat vain osittain (300, 350, 400 käyttäjää pilveen, loput AD:ssä)

- **Sekava hallinta**
 - Osa avaimista pilvessä, osa AD:ssä → adminin pitää tarkistaa molemmista.
 - Tukiprosessi monimutkaistuu, koska ei ole yhtä "source of truth".
- **Käyttäjäkokemuksen eriarvoisuus**
 - Pilveen siirretyn käyttäjät voivat hakea avaimensa itsepalvelusta.
 - AD-käyttäjät joutuvat aina ottamaan yhteyttä IT-tukeen. Tämä voi aiheuttaa tyytymättömyyttä.
- **Lisenssien ja kustannusten sekaannus**
 - Jos osa käyttäjistä on Intunen piirissä ja osa ei, lisenssien hallinta vaikeutuu.
 - Yritys voi maksaa turhaan kahdesta eri hallintamallista.
- **Migraation vaikeutuminen myöhemmin**
 - Jos siirto tehdään osissa, myöhemmin joudut tekemään lisämigraatioita → enemmän työtä ja riskejä.

Suositus

- **Alle 200 käyttäjää:** AD + GPO voi riittää, jos kustannukset ja compliance eivät ole kriittisiä.
- **200–500 käyttäjää:** kannattaa siirtyä pilveen (Intune + Entra ID), koska hallinta, kustannukset ja compliance helpottuvat.
- **Osittainen skaalaus (300–400 käyttäjää pilveen, loput AD:ssä):** teknisesti mahdollista, mutta sekaannusta syntyy → ei suositeltavaa pitkällä aikavälillä.

Jos ei skaala pilveen, riskit liittyvät **hallinnan monimutkaisuuteen, kustannuksiin ja complianceen**. Osittainen skaalaus tuo **sekavuutta ja eriarvoisuutta** käyttäjien välillä.

Ei maailma kaudu, jos yritys ei skaala pilveen koko 200–500 käyttäjän joukkoa – mutta **riskit, kustannukset ja elinkaarivaikutukset** kasvavat merkittävästi, ja ne kannattaa hahmottaa etukäteen.

Mitä tapahtuu jos ei skaala pilveen

- **Hallinta pysyy on-prem AD:n varassa**
 - BitLocker-avaimet, GPO:t ja sertifikaatit jäävät Windows Serverin alle.
 - Tämä toimii, mutta hallinta kuormittuu, kun käyttäjämääriä kasvaa.
- **Ei katastrofi, mutta enemmän manuaalityötä**
 - Adminit joutuvat tekemään enemmän vianmääritystä ja tukityötä.
 - Käyttäjät eivät saa itsepalvelua (avainten haku, compliance-raportit).
- **Kustannukset voivat nousta**
 - Laitteistot, ylläpito, sähkö, varmistukset → skaalautuvat huonosti.
 - Pilvessä kustannukset ovat ennustettavampia, mutta lisenssit maksavat.

Elinkaari ja pitkän aikavälin vaikutukset

- **Teknologian elinkaari**
 - Windows Server + AD on kypsä ja toimiva, mutta Microsoftin kehitys painottuu pilveen (Entra ID, Intune).
 - Uudet ominaisuudet tulevat pilveen, ei on-prem AD:hen.
- **Käyttäjämäärin kasvu**
 - 50–100 käyttäjää → AD riittää.

- 200–500 käyttäjää → hallinta monimutkaistuu, compliance-vaatimukset kasvavat.
- Yli 500 käyttäjää → pilvihallinta käytännössä välttämätön, muuten tukiprosessit ylikuormittuvat.
- **Organisaation elinkaari**
 - HR, laskutus, myynti, IT → eri tiimit tarvitsevat yhtenäisen hallintamallin.
 - Jos osa on pilvessä ja osa AD:ssä, syntyy sekava “kaksijakoinen elinkaari”.

Mitä hahmottaa ja ymmärtää suurissa käyttäjämääriissä

- **Prosessit vs. teknologia**
 - Teknologia toimii, mutta prosessit (tuki, auditointi, käyttäjäkokemus) voivat kaatua, jos hallinta ei skaalaudu.
- **Compliance ja riskit**
 - Suuremassa organisaatiossa auditointi ja tietoturva korostuvat.
 - Pilvi tarjoaa valmiit compliance-raportit, AD ei.
- **Käyttäjäkokemus**
 - 500 käyttäjää → jokainen palautustilanne ilman itsepalvelua kuormittaa IT:tä.
 - Pilvessä käyttäjät voivat hakea avaimensa itse → säästää aikaa ja rahaa.
- **Strateginen näkökulma**
 - Jos yritys aikoo kasvaa, pilvi on elinkaaren kannalta järkevämpi.
 - Jos pysyy pienenä, AD voi riittää, mutta kehitys jää jälkeen.

Yhteenveto

- Ei ”maailman kaatumista”, jos pysytään AD-mallissa → se toimii, mutta skaalautuvuus ja elinkaari kärsivät.
- Osittainen skaalaus (murto-osa pilveen, loput AD:ssä) tuo sekavuutta ja eriarvoisuutta käyttäjien välillä.
- Suuremissa käyttäjämääriissä (200–500+) kannattaa hahmottaa:
 - **Hallinnan kuormitus**
 - **Compliance-vaatimukset**
 - **Kustannusten ennustettavuus**
 - **Käyttäjäkokemus ja itsepalvelu**

Pilveen siirtyminen ei ole pakollista, mutta elinkaaren ja skaalautuvuuden kannalta se on järkevä, kun käyttäjämääri kasvaa yli ~200–500.