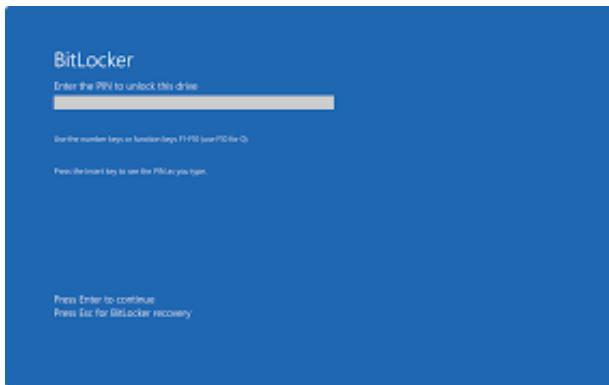


7.2. Bitlocker - 1

Friday, December 5, 2025

17:44

BitLocker Windows Serverissä on **levynsalaus** työkalu, jota käytetään suojaamaan dataa varkausilta ja luvattomalta käytöltä. IT-adminille se tuo hallittavuutta ja tietoturvaa, käyttäjälle se tarkoitaa, että data pysyy turvassa myös laitteen kadotessa. Riskit liittyvät avainten hallintaan ja TPM-haavoittuvuuksiin, mutta oikein toteutettuna se on erittäin hyödyllinen. Palautusavaimet voidaan säilyttää esimerkiksi Active Directoryssä tai Microsoft Endpoint Managerissa.



🔒 Teoria: BitLocker ja Active Directory (fyysisen ympäristö)

1. BitLocker perusidea

- BitLocker on **levyn salausratkaisu**, joka suojaa dataa, jos laite joutuu väriin käsiin.
- Se salaa koko levyn, ja avain tarvitaan käynnistykseen yhteydessä (TPM, PIN, USB-avain).
- Työasemissa tämä on kriittistä, koska ne liikkuvat käyttäjien mukana. Palvelimissa käyttö on harvinainen, mutta mahdollista.

2. Active Directoryn rooli

- AD Domain Services voi toimia BitLocker-avainten **escrow-säilytyspaikkana**.
- Kun GPO:t om määritetty oikein, jokainen domainiin liitetty kone tallentaa BitLocker-palautusavaimen automaattisesti AD:hen.
- Tämä tarkoittaa, että jos käyttäjä unohtaa PIN-koodin tai TPM menee lukkoon, IT voi hakea avaimen AD:stä ja palauttaa koneen käyttöön.
- Käytännössä AD toimii siis **hallintakerroksena BitLockerille** fyysisessä ympäristössä.

3. Hallintakäytännöt työasemien palautuksessa/vaihdossa

- **Fyysisen palautus IT:lle**
 - Yleisin käytäntö, koska kone voidaan tyhjentää, poistaa AD:stä ja varmistaa, että BitLocker-avaimet ovat tallessa.
 - IT voi tehdä "secure wipe" ja valmistella koneen uudelle käyttäjälle.
- **Etähallinta AD:n kautta**
 - Mahdollista vain, jos kone on yhteydessä domainiin (LAN tai VPN).
 - GPO:n kautta voidaan pakottaa resetointi, mutta käytännössä tämä on hankala ilman MDM:tä.
 - Jos kone ei saa yhteyttä AD DNS:ään, se ei voi vastaanottaa uusia GPO-päivityksiä.

☞ Tästä syystä perinteisessä AD-ympäristössä **fyysisen palautus on käytännössä standardi**, ja etähallinta toimii vain rajatusti (VPN-yhteyden kautta).

4. DNS ja GPO-yhteydet

- Domain-joined kone tarvitsee yhteyden **domain controlleriin ja sen DNS:ään**.
- Ilman VPN:ää etätyöasema ei saa GPO-päivityksiä eikä voi raportoida AD:lle.
- Tämä on yksi suurimmista rajoitteista fyysisessä AD-mallissa: hallinta toimii vain, kun kone on yrityksen verkossa.

5. Teoreettinen malli

Voit ajatella kokonaisuutta näin:

- **BitLocker** = tekninen salausratkaisu levylle.
- **Active Directory** = hallintajärjestelmä, joka säilyttää avaimet ja varmistaa, että IT voi palauttaa koneen käyttöön.
- **GPO** = politiikkamekanismi, jolla pakotetaan BitLocker käyttöön ja määritetään, että avaimet tallennetaan AD:hen.
- **DNS + DC-yhteys** = välttämätön, jotta työasema saa politiikat ja raportoi tilansa.
- **Fyysisen palautus** = käytännön tapa hallita koneen vaihto/palautus, koska etähallinta on rajallista ilman VPN:ää.

- Fyysisessä AD-ympäristössä BitLocker toimii parhaiten, kun avaimet escrowataan AD:hen.
- Työaseman palautus/vaihto tehdään yleensä fyysisesti IT:ssä, koska etähallinta on rajoittunut.
- DNS ja GPO-yhteydet vaativat VPN:n, jos kone on yrityksen verkon ulkopuolella.
- Tämä malli on selkeä, mutta rajoittuu siihen, että hallinta on sidottu fyysiseen verkkoon ja domainiin.

#####
#####

Miksi BitLocker Windows Serverissä?

- **Tietoturva:** Salaa koko levyn, jolloin data ei ole luettavissa ilman oikeaa avainta. Tämä suojaa erityisesti palvelimia ja kannettavia, jos levy varastetaan.
- **Compliance:** Monissa toimialoissa (esim. finanssi, terveydenhuolto) vaaditaan salattua dataa levyllä. BitLocker täyttää nämä vaatimukset.
- **Integraatio AD:n kanssa:** Palautusavaimet voidaan automaattisesti tallentaa Active Directoryyn, jolloin IT-admin voi palauttaa salauksen hallitusti.

Hyödyt IT-adminille

- **Keskitetty hallinta:** BitLocker voidaan hallita Group Policyillä, SCCM:llä tai Intunella. Tämä mahdollistaa automaattisen käyttöönnoton ja seurannan.
- **Avainhallinta:** Palautusavaimet voidaan kerätä AD:hen tai pilvipalveluun, jolloin IT-admin voi auttaa käyttäjää ongelmatilanteessa.
- **Auditointi:** Mahdollistaa raportoinnin siitä, mitkä koneet ovat salattuja ja mitkä eivät.

Työaseman palautus/vaihto AD-ympäristössä

- **Fyysisen palautus IT:lle**
 - Yleisin käytäntö, jos käyttäjä vaihtaa konetta tai palauttaa sen.
 - IT voi varmistaa, että kone poistetaan AD:stä, BitLocker-avaimet on tallessa (jos ne on escrowattu AD:hen), ja levy voidaan tyhjentää hallitusti.
 - Tämä on turvallisimpien tapa, koska kone on fyysisesti hallinnassa eikä jää riskiä, että salattua dataa kulkee mukana.
- **Etähallinta (GPO, SCCM, Intune, PowerShell Remoting)**
 - Mahdollista, jos kone on vielä verkossa ja yhteydessä AD:hen.
 - Voit etänä käynnistää **resetoinnin, poistaa AD-objektiin, tyhjentää BitLocker-avaimen** jne.
 - Ongelmana: jos kone ei ole VPN:n tai LAN:n kautta yhteydessä domainiin, etäkomennot eivät mene perille.
 - Käytännössä etähallinta toimii vain, jos kone on vielä "elossa" ja yhteydessä yrityksen verkkoon.

DNS ja yhteydet etänä

- Työasema, joka on **domain-joined**, tarvitsee yhteyden yrityksen DNS:ään ja DC:hen (domain controller) saadakseen GPO:t ja AD-päivitykset.
- Jos kone on yrityksen verkon ulkopuolella, se ei saa yhteyttä AD:hen ilman **VPN-yhteyttä**.
- Microsoftin tarjoama tapa:
 - **VPN + GPO** → kone saa päivitykset domainista.
 - **Intune / Azure AD Join** → kone saa politiikat pilvestä ilman VPN:ää.
- Perinteisessä AD:ssä ei ole mitään "taikakanavaa" ilman VPN:ää – DNS ja DC-yhteys on pakollinen.

Yhteenvetto

- AD-ympäristössä koneen palautus/vaihto tehdään yleensä **fyysisesti IT:ssä**, mutta etänä onnistuu vain jos kone on VPN:n kautta yhteydessä domainiin.
- DNS ja GPO-päivitykset eivät toimi etänä ilman VPN:ää.
- Jos halutaan hallita koneita ilman VPN-riippuvuutta, käytä **Intune/Azure AD** → politiikat tulevat pilvestä.

#####

GPO-päivitykset etätöitäväälle

- **Normaalisti:** Domain-joined kone hakee GPO:t vain, jos se saa yhteyden **domain controlleriin (DC)** ja sen DNS:ään.
- **Toimistoläppärin käytäntö:** Jos VPN:ää ei ole, kone saa politiikat vain silloin kun se käy fyysisesti yrityksen verkossa. Tämä on se "pari kertaa viikossa toimistolla"-malli.
- **Kikka kolmonen etänä:**
 - VPN-yhteys → kone näkee DC:n ja saa GPO:t.
 - Ilman VPN:ää ei ole mitään virallista tapaa saada GPO:t, koska ne eivät tule internetin yli.
 - Joissain ympäristöissä käytetään **DirectAccess** tai **Always On VPN** (Microsoftin ratkaisut), jolloin kone on "virtuaalisesti" aina domainissa. Mutta nämäkin ovat VPN-teknikoita, ei mitään taikakanavaa.

 kyllä, ilman VPN:ää koneen pitää käydä toimistolla saadakseen GPO:t. Tämä on fyysisen AD:n rajoite.

BitLocker ja varastettu/kadonnut kone

- **BitLocker suojaa levyn sisällön.** Jos levy on salattu, varas ei pääse dataan ilman avainta.
- **USB-porttien estäminen GPO:lla:**
 - Voidaan tehdä, mutta se ei ole BitLocker-suojausta vaan erillinen Device Installation Restriction -politiikka.
 - BitLocker ei ole "purkautettavissa" pelkällä USB:llä, ellei varas saa käynnistysavainta (esim. jos organisaatio käyttää USB-startup key).
- **MFA työasemaan:**
 - Fyysisessä AD:ssa ei ole nativisti MFA-kirjautumista työasemalle.
 - Käytännössä suojaus on **BitLocker + AD-kirjautuminen (salasana, mahdollisesti SmartCard)**.
- **Käytännön suojaus:**
 - BitLocker pitää olla **pakotettuna GPO:lla** ja palautusavaimet escrowattuna AD:hen.
 - USB-porttien estäminen voi vähentää riskiä, mutta ei ole välttämätöntä BitLockerille.
 - Jos kone varastetaan, tärkeintä on että levy on salattu ja avaimet tallessa IT:llä.

Yhteenveto

- Fyysisessä AD-ympäristössä ilman VPN:ää koneen on **pakko käydä toimistolla** saadakseen GPO:t.
- BitLocker suojaa levyn sisällön, eikä varas voi "purkaa" sitä USB-portin kautta, ellei organisaatio käytä USB-avainkäynnistystä.
- USB-porttien estäminen GPO:lla on lisäsuojia, mutta ei BitLocker-riippuvainen.
- MFA ei ole nativisti osa fyysisistä AD-työaseman kirjautumista – käytännössä suojaus on BitLocker + AD-salasana/SmartCard.

- BitLockerin idea on nimenomaan se, että sitä **ei voi purkaa "kikka kolmosella"** – se on suunniteltu estämään juuri sen kaltaiset ohitukset.

BitLocker-suojaus

- BitLocker käyttää **vahvaa salausalgoritmia (AES)** ja avainhallintaa (TPM, PIN, palautusavain).
- Jos levy on salattu, sen sisältö on käytännössä **hyödyttömässä muodossa** ilman oikeaa avainta.
- Ei ole mitään "takaporttia" tai helppoa keinoa ohittaa suojausta – tämä on koko teknologian tarkoitus.

Mitä IT voi tehdä hallitusti

- **Palautusavaimet:** Jos GPO on määritetty oikein, palautusavaimet tallentuvat Active Directoryyn. IT voi hakea ne sieltä ja avata levyн.
- **Recovery Agent:** Organisaatio voi määrittää EFS/BitLocker Recovery Agentin, jolla voidaan hallitusti palauttaa data.
- **Hallittu resetointi:** Jos avaimia ei ole tallessa, ainoa vaihtoehto on tyhjentää levy (wipe) ja asentaa kone uudelleen.

Mitä ei voi tehdä

- Ei ole mitään "USB-trikkiä" tai komentoa, jolla BitLocker ohitetaan.
- Ei voi murtaa salauksen järkevässä ajassa ilman avainta – se on kryptografisesti suunniteltu estämään sen.
- Jos palautusavainta ei ole tallessa, data on menetetty. Tämä on osa tietoturvamallia.

Yhteenveto

BitLocker on turvallinen juuri siksi, että sitä ei voi purkaa ilman avainta.

- **IT:n keinot:** palautusavaimet AD:stä, Recovery Agent, hallittu resetointi.
- **Varas/ulkopuolinen:** ei realistista keinoa päästää dataan ilman avainta.

#####

Administrator ja loppukäyttäjät

Administratorin kannalta olennaiset asiat BitLockerista

- **Avainten hallinta**
 - BitLocker-palautusavaimet tulee **pakottaa talteen Active Directoryyn** GPO:n avulla.
 - Administrator ei koskaan luovuta avaimia käyttäjälle, ellei ole erityinen tarve (esim. tukitilanne).
 - Avainten escrow AD:hen varmistaa, että jos käyttäjä unohtaa PIN-koodin tai TPM menee lukkoon, IT voi palauttaa koneen käyttöön.
- **Politiikat ja asetukset**
 - GPO:lla voidaan pakottaa BitLocker käyttöön kaikilla levyillä (OS, data, removable).
 - Vähintään OS-levy tulee olla salattu.
 - TPM + PIN on suositeltu yhdistelmä, mutta jo pelkkä TPM riittää monessa ympäristössä.
 - USB-startup key kannattaa estää, koska se lisää riskiä (avaimen voi kopioida).
- **Käytännöt varastutilanteessa**
 - Jos kone katoaa, BitLocker suojaa datan.
 - Administrator voi poistaa koneen AD:stä ja merkitä sen kadonneeksi.
 - Avainta ei koskaan anneta ulkopuoliselle – se on vain IT:n hallussa.

Käyttäjän kannalta

- **Tarkistaminen, että BitLocker on päällä**
 - Käyttäjä voi itse tarkistaa BitLocker-tilan ilman admin-oikeuksia:
 - Avaa **Control Panel → System and Security → BitLocker Drive Encryption**.
 - Tai komentorivillä: manage-bde -status (näyttää salauksen tilan).
 - Tämä on täysin ok ja jopa suositeltavaa, että käyttäjä voi itse varmistaa salauksen olevan aktiivinen.
- **Käyttäjän rooli avaimen suhteen**
 - Käyttäjä ei normaalista tee mitään palautusavaimen kanssa.
 - Avaimet tallennetaan AD:hen automaattisesti, eikä käyttäjän tarvitse käsitellä niitä.
 - Jos BitLocker kysyy palautusavainta (esim. TPM resetoinnin jälkeen), käyttäjä ottaa yhteyttä IT:hen, joka hakee avaimen AD:stä.
- **Käyttäjän mahdollisuudet**
 - Käyttäjä ei voi poistaa BitLockeria ilman admin-oikeuksia, jos GPO on pakottanut sen päälle.
 - Käyttäjä voi nähdä tilan, mutta ei hallita avaimia.

Tärkeimmät asetukset ja käytännöt

- **Pakota BitLocker käyttöön GPO:lla** (OS-levy vähintään).
- **Escrowaa palautusavaimet AD:hen.**
- **Estä USB-startup key** (vain TPM/PIN).
- **Käytä TPM:tä** (vähintään versio 2.0).
- **Dokumentoi prosessi:** mitä tehdään, jos kone katoaa, jos käyttäjä unohtaa PINin, jos TPM menee lukkoon.

- **Käyttäjälle ohje:** miten tarkistaa, että BitLocker on päällä, ja että avaimia ei tarvitse käsittellä itse.

Yhteenvetö

- Administrator hallitsee avaimet ja politiikat, käyttäjä ei koskaan käsittele avaimia.
- Käyttäjä voi itse tarkistaa, että BitLocker on päällä, mutta ei voi poistaa sitä.
- Tärkein sääntö: **avaimet escrowataan AD:hen ja niitä ei luovuteta ulos.**
- Käytännöt varmistavat, että kadonneen koneen data pysyy suojaattuna ja IT voi hallitusti palauttaa koneen käyttöön.

BitLocker saatavuus eri Windows-versioissa

BitLocker on saatavilla vain **Windows 10/11 Pro, Enterprise ja Education**-versioissa. **Home-versiossa BitLocker ei ole natuivisti mukana**, mutta siellä voi olla rajattu "Device Encryption" joissakin uusissa laitteissa.

Windows-versio	BitLocker-tuki	Huomioita
Windows 10/11 Pro	<input checked="" type="checkbox"/> Kyllä	Täysi BitLocker-tuki, hallittavissa GPO:lla ja AD:llä.
Windows 10/11 Enterprise	<input checked="" type="checkbox"/> Kyllä	Sama kuin Pro, mutta laajemmat hallintaominaisuudet (esim. MBAM, lisäpolitiikat).
Windows 10/11 Education	<input checked="" type="checkbox"/> Kyllä	Täysi BitLocker-tuki, suunnattu oppilaitoksiille.
Windows 10/11 Home	<input type="checkbox"/> Ei natuivisti	Ei sisällä BitLockeria. Joissakin laitteissa on Device Encryption , joka on kevyempi versio. Vaihtoehtona: päivitä Pro-versioon tai käytä kolmannen osapuolen salausratkaisuja.

Tärkeät huomiot

- **Home-versio:** BitLocker ei ole virallisesti mukana, mutta joissakin uusissa laitteissa (esim. Surface, OEM-läppärit) voi olla **Device Encryption**, joka toimii automaattisesti Microsoft-tilin kautta. Tämä ei ole sama kuin täysi BitLocker.
- **Pro/Enterprise/Education:** Näissä versioissa BitLocker voidaan hallita keskitetyisti Active Directoryn ja GPO:n avulla, jolloin palautusavaimet escrowataan AD:hen.
- **Käytännön suositus yrityksille:** Käytä vähintään Pro-versiota, jotta saat BitLocker-hallinnan ja avainten tallennuksen AD:hen. Home-versio ei sovella yrityskäytöön, jos halutaan täysi hallinta.

#####

Työasema - tilanne

BitLocker ja varastettu / rikkoutunut työasema

1. Jos kone varastetaan

- **BitLocker suojaa levyn sisällön:** ilman avainta varas ei saa dataa auki.
- Administratorin rooli:
 - Varmista, että palautusavaimet on escrowattu AD:hen.
 - Poistaa koneen AD:stä ja merkitsee sen kadonneeksi.
 - Ei ole mitään etäkäskyä, joka "purkaa" BitLockerin – se on tarkoituksesta mahdotonta.
- Käyttäjälle ei anneta avaimia, vaan IT hallitsee niitä. Käyttäjä voi vain raportoida koneen kadonneeksi.

2. Jos kone rikkoutuu / ei käynnisty

- BitLocker ei estä **tehdasasetusten palautusta** tai uudelleenasennusta, mutta salattu levy pitää ensin avata palautusavaimella.
- Administratorilla pitää olla valmiudet hakea avain AD:stä.
- Käyttäjälle voidaan antaa ohje: "Ota yhteys IT:hen, jos kone kysyy BitLocker-avainta."
- Jos levy on fyysisesti rikki, dataa ei voi palauttaa ilman varmuuskopioita – BitLocker ei auta eikä estää tässä.

3. Etähallinta ja yhteys

- **Ilman WiFi/VPN-yhteyttä** kone ei saa mitään etäkäskyjä AD:ltä.
- Tämä koskee kaikkia GPO-päivityksiä, etälukituksia ja resetointeja.
- Käytännössä:
 - Jos kone on kadonnut, etäkäsky ei mene perille, ellei kone ole verkossa.
 - BitLocker suojaa datan riippumatta siitä, onko kone verkossa vai ei.
- Tämä on tärkeä ero: **BitLocker ei tarvitse verkkoa suojatakseen dataa** – se toimii paikallisesti.

4. Käytännön malli

- **Administratorin valmiudet:**
 - Avainten escrow AD:hen.
 - Prosessi kadonneen koneen käsittelyyn (poisto AD:stä, ilmoitus tietoturvalle).
 - Ohjeistus käyttäjälle, mitä tehdä jos kone kysyy BitLocker-avainta.
- **Käyttäjän rooli:**
 - Voi tarkistaa, että BitLocker on päällä.
 - Raportoi IT:lle, jos kone katoaa tai kysyy avainta.
 - Ei käsitlele avaimia itse.

Yhteenveto

- Ilman WiFi/VPN-yhteyttä kone ei saa etäkäskyjä, mutta BitLocker suojaa datan silti.
- Administratorin pitää varmistaa, että avaimet on tallessa AD:ssä ja prosessi kadonneen koneen käsittelyyn on selkeä.
- Käyttäjä voi tarkistaa BitLocker-tilan, mutta ei hallitse avaimia.
- BitLocker toimii "offline-suojana" – se ei tarvitse verkkoa ollakseen tehokas.

Mitä tapahtuu **työaseman (A-koneen) hajoamisen tai katoamisen jälkeen** ja miten se liittyy BitLockeriin, Active Directoryyn ja sovellusten siirtoon B-koneelle.

BitLocker-näkökulma

- BitLocker suojaa **vain levyn dataa**.
- Jos A-kone katoaa tai hajoaa, BitLocker varmistaa, ettei ulkopuolin pääse käsiksi levyä sisältöön.
- BitLocker ei kuitenkaan siirrä sovelluksia, asetuksia tai käyttäjäprofiileja automaattisesti B-koneelle.
- Administratorin tehtävä on varmistaa, että avaimet ovat escrowattu AD:hen ja että kone voidaan poistaa hallinnasta.

Active Directory + DNS ympäristön rooli

- AD hallitsee käyttäjätilejä, ryhmäpolitiikkoja (GPO) ja koneobjekteja.
- Kun käyttäjä siirtyy B-koneelle:
 - Käyttäjä voi kirjautua sisään omalla domain-tilillään.
 - GPO:t ja AD-politiikat latautuvat B-koneelle, kun se on yhteydessä domainiin (LAN/VPN).
- DNS varmistaa, että kone löytää domain controllerin ja saa poliikit.
- Tämä tarkoittaa: **käyttäjäprofiili ja poliikit siirtyvät, mutta sovellukset eivät automaattisesti kopioudu**.

Sovellusten siitto A → B

- Windows-ympäristössä sovellukset eivät siirry automaattisesti AD:n kautta.
- Käytännön vaihtoehdot:
 - **SCCM / Configuration Manager / GPO Software Deployment** → IT voi asentaa samat sovellukset B-koneelle automaattisesti.
 - **Kasin asennus** → IT asentaa sovellukset uudelleen B-koneelle.
 - **Roaming profiles / Folder Redirection** → käyttäjän tiedostot ja asetuksia voivat siirtyä, mutta sovellukset eivät.
- Sovellusten siitto riippuu siitä, onko organisaatiossa käytössä **sovellusten hallintaratkaisu (SCCM, MDT, GPO)**. Ilman näitä, B-koneelle pitää asentaa ohjelmat uudelleen.

Käytännön malli

1. A-kone katoaa/hajoaa → BitLocker suojaa datan.
2. Administrator poistaa koneen AD:stä ja varmistaa, että avaimet ovat tallessa.
3. B-kone otetaan käyttöön → liitetään domainiin.
4. Käyttäjä kirjautuu sisään → saa omat AD-politiikat ja profiilin.
5. Sovellukset asennetaan uudelleen → joko automaattisesti (SCCM/GPO) tai käsin.

Yhteenveto

- BitLocker suojaa datan, mutta ei siirrä sovelluksia.
- AD + DNS varmistaa, että käyttäjä voi kirjautua B-koneelle ja saa poliikit.
- Sovellusten siitto vaatii erillisen hallintaratkaisun (SCCM, GPO Software Deployment, MDT).
- Käytössä: **profiilit ja poliikit siirtyvät, mutta sovellukset eivät automaattisesti kopioudu**.

Tietojen tallennus

BitLocker ja datan siirto

- **BitLocker suojaa levyn sisällön** salauksella, mutta se ei ole varmuuskopioointityökalu.
- Jos A-kone katoaa, hajoaa tai varastetaan, BitLocker varmistaa vain sen, että **ulkopuolin ei pääse käsiksi dataan**.
- BitLocker ei auta siirtämään keskeneräistä projektia B-koneelle – se ei tee automaattista migraatiota.

Käytännön siirto A → B

- Jos A-kone on vielä toimiva:
 - Data voidaan siirtää hallitusti (esim. kopioimalla, käyttämällä varmuuskopiojärjestelmää, OneDrive/DFS, tai manuaalisesti).
 - BitLocker ei estää siirtoa – kun levy on auki ja käyttäjä kirjautunut sisään, tiedostot toimivat normaalisti.
- Jos A-kone hajoaa tai katoaa:
 - Ilman varmuuskopioita data on menetetty, koska BitLocker estää ulkopuolisen pääsyn.
 - Tässä kohtaa BitLocker suojaaa, mutta ei auta palauttamaan.

Kannattaako tallentaa kaikkea työasemalle?

- Ei ole paras **käytäntö** tallentaa kaikkea vain paikalliselle C-levylle.
- Yrityskäytöissä suositellaan:
 - **Verkkolevyt / DFS / file serverit** → AD-integraatio, varmuuskopointi.
 - **Folder Redirection / Roaming Profiles** → käyttäjän tiedostot siirtyvät automaattisesti uuteen koneeseen.
 - **Varmuuskopointi** → keskeneräiset projektit eivät jää vain yhden koneen varaan.

Yhteenveto

- BitLocker suojaa dataa, mutta ei siirrä sitä uuteen koneeseen.
- Jos halutaan, että keskeneräiset projektit säilyvät A-koneen katoamisen jälkeen, ne pitää olla **varmuuskopioitu tai tallennettu verkkoon**.
- Administratorin rooli: varmistaa, että käyttäjät eivät säilytä kriittistä dataa vain paikallisella C-levyllä.
- Käyttäjän rooli: käyttää ohjeistettuja tallennuspaikkoja (verkko, pilvi, varmuuskopiojärjestelmä).

#####

Withsecure & Windows server (bitlocker)

BitLocker yritysympäristössä

- BitLocker on Windowsin oma levyn salausratkaisu, joka suojaa dataa, jos laite katoaa tai varastetaan.
- Se toimii **paikallisesti käyttöjärjestelmän tasolla** ja voidaan hallita Active Directoryn kautta (avainten escrow, GPO-pakotus).
- BitLocker ei itsessään sisällä pilvhallintaa, vaan se on osa Windowsin sisäistä turvakerrosta.

WithSecure (entinen F-Secure) ja BitLocker

- WithSecure tarjoaa **pilvipohjaisia tietoturvaratkaisuja**: endpoint protection, EDR, MDM-tyyppisiä hallintaratkaisuja.
- Se ei korvaa BitLockeria, vaan voi **tukea sen hallintaa** osana kokonaisuutta.
- Käytännössä:
 - BitLocker hoitaa **levyn salauksen**.
 - WithSecure voi valvoa, että koneen tietoturvalainsät (esim. salaus päällä, USB-porttien käyttö estetty) ovat kunnossa ja raportoida hallintaan.
 - Näin WithSecure toimii enemmän **valvontakerroksena**, ei salausratkaisuna.

Kumpi on "parempi"?

- **BitLocker**: vältämätön, jos halutaan nativisti Windowsin levyn salaus ja AD-integraatio.
- **WithSecure**: hyvä lisä, jos halutaan pilvipohjainen valvonta, raportointi ja laajempi tietoturva (haittaohjelmat, EDR, compliance).
- Ne eivät ole vaihtoehtoja toisilleen, vaan **täydentävät toisiaan**:
 - BitLocker = salaus.
 - WithSecure = hallinta, valvonta, uhkien torjunta.

Käytännön malli

Yrityksen Windows Server + AD -ympäristössä:

1. **BitLocker pakotetaan GPO:lla** ja avaimet escrowataan AD:hen.
2. **Administrator hallitsee avaimet**, käyttäjä ei koskaan käsittele niitä.
3. **WithSecure** voi raportoida, että BitLocker on päällä ja kone on compliant, mutta itse salaus on edelleen BitLockerin vastuulla.

Windows Server + BitLocker (ilman lisäpalveluja)

- **Windows Server + Active Directory + GPO** tarjoaa jo valmiiksi:
 - BitLocker-pakotuksen työasemille.
 - Palautusavainten escrowauksen AD:hen.
 - Käytännön hallinnan (avainten haku, resetointi, politiikat).
- Tämä riittää monelle organisaatiolle, jos tavoitteena on **vain levyn salaus ja avainten hallinta**.
- Administrator saa käytöönsä kaikki olennaiset työkalut: GPO, ADUC (Active Directory Users and Computers), manage-bde, PowerShell, raportointi.

WithSecure + BitLocker

- **WithSecure** ei korvaa BitLockeria, vaan toimii sen päällä.
- Se tuo lisäarvoa:
 - Keskitetty raportointi ja compliance (näyttää, että BitLocker on päällä).
 - Laajempi tietoturva: haittaohjelman torjunta, EDR, uhkien havaitseminen.
 - Pilvipohjainen hallinta, jolloin ei tarvita VPN:ää GPO-päivityksiin.
- **Kustannus**: tulee lisenssistä. Eli se on enemmän kustannusta, mutta tuo myös enemmän näkyvyttä ja suojaaa.
- **Tehokkuus**: parantaa hallintaa ja valvontaa, mutta ei tee BitLockerista itsessään vahvempaa – se vain varmistaa, että BitLocker on käytössä ja raportoi sen tilan.

Kannattaako käyttää?

- Jos yrityksen malli on **puhdas fyysinen AD + Windows Server**, BitLocker + GPO riittää peruslevyn salaukseen ja avainten hallintaan.
- WithSecure on **lisäplussa**, jos halutaan:
 - Pilvipohjainen hallinta ilman VPN-riippuvuutta.
 - Laajempi tietoturva (haittaohjelmat, EDR, compliance).
 - Raportointi ja näkyvyys johdolle / tietoturvaliimille.
- Jos tavoitteena on vain BitLocker ja AD-avainten hallinta, **Windows Serverin omat työkalut riittävät**.
- Jos halutaan kokonaisvaltainen tietoturva ja näkyvyys, **WithSecure tuo lisäarvoa, mutta maksaa enemmän**.

Yhteenvetö

- **Windows Server + BitLocker** = riittää peruslevyn salaukseen ja avainten hallintaan.
- **WithSecure** = lisäplussa, tuo näkyvyyttä ja laajemman tietoturvan, mutta lisää kustannuksia.
- Administratorille Windows Serverin omat työkalut riittävät BitLocker-hallintaan, mutta WithSecure voi helpottaa valvontaa ja compliance-raportointia.