VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Aaron Tammelin

MICROSOFT ENDPOINT MANAGERIN LAITE- JA KÄYTTÄJÄHALLINTA

Liiketalous
2022

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Aaron Tammelin
Opinnäytetyön nimi	Microsoft Endpoint Managerin laite- ja käyttäjähallinta
Vuosi	2022
Kieli	suomi
Sivumäärä	30
Ohjaaja	Päivi Rajala

Tämän opinnäytetyön tarkoituksena oli selvittää, miten Microsoft Endpoint Managerin tarjoamilla palveluilla yritysten ICT-osasto pystyy tehostamaan ja helpottamaan yrityksen laite- ja käyttäjähallintaa.

Ensimmäisen osassa tuodaan esille ongelmia, joita kohtasin työskennellessäni osana ICT-ryhmää ja vastatessani laite- ja käyttäjähallinnasta. Ongelmat olivat luonteeltaan toistuvia ja samankaltaisia.

Toinen osio käsittelee Microsoft Endpoint Managerin tarjoamia palveluita ja niiden eri osa-alueita. Ongelmien ratkaisu havainnollistetaan lukijalle kuvien ja esimerkkitapausten kautta.

Viimeisessä osiossa pohditaan millaisille yrityksille Microsoft Endpoint Managerin palvelut soveltuvat ja mitä sen tuomat hyödyt ovat yritykselle. Yhteenvedossa tuodaan esille toteutuksen tuomat haasteet ja kohderyhmä, jolle työ on suunnattu.

Avainsanat Active Directory, IT-tuki, Microsoft Azure, Laitehallinta

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Business Information Technology

ABSTRACT

Author	Aaron Tammelin
Title	Microsoft Endpoint Manager for device and user management
Year	2022
Language	Finnish
Pages	30
Name of Supervisor	Päivi Rajala

The objective of this thesis was to find out how the services provided by Microsoft Endpoint Manager can make the corporate ICT department more efficient and easier for the company's device and user management.

The first selection studies and highlights the problems I encountered while working as part of an ICT team and in charge of device and user management. The problems were repetitive in nature and similar to each other.

The second section of the thesis discusses the services provided by Microsoft Endpoint Manager and their various components. The solution to the problems is illustrated to the reader through pictures and case studies.

The final section discusses what kind of business Microsoft Endpoint Management services are suitable for and what the benefits for the businesses are. The summary highlights the challenges posed by the implementation and the target group to which the work is directed.

Keywords Active Directory, IT Support, Microsoft Azure, Device Management

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

KÄSITTEET

DOMAIN

Toimialue, jossa Windows-tietokoneita hallitaan lähiverkossa käyttäen Windows-palvelinta. Toimialueen käyttäjille luodaan käyttäjätunnus, joka mahdollistaa toimialueen eri laitteille kirjautumisen ja niiden käyttämisen.

GROUP POLICY

Ryhmäkäytäntö on Windowsin ominaisuus, jolla hallitaan käyttäjiä ja ryhmiä. Hallinta toteutetaan säännöillä. Sääntöjä voidaan määrittää sovellukseen, käyttöjärjestelmään tai käyttäjään.

LÄHIVERKKO

Lähiverkolla tarkoitetaan toimialueen sisäistä tarkasti rajattua tietoliikenneverkkoa. Lähiverkko on sisäinen verkko, jossa sitä käyttävät laitteet eivät ole suoraan yhteydessä internettiin.

WINDOWS IMAGE

Windows-käyttöjärjestelmän näköistiedosto. Näköistiedoston avulla Windows-käyttöjärjestelmä asennetaan ensimmäisen kerran tai uudelleen.

ACTIVE DIRECTORY

Microsoftin kehittämä toimialueen käyttäjätietokanta ja hakemistopalvelu. Tietokanta sisältää tietoja verkkoresursseista, tietokoneista ja käyttäjistä. Active Directorylla ohjataan Windows-toimialuetta.

1 JOHDANTO

Jatkuvan digitalisaation seurauksena yritysten on kohdistettava resurssejaan yhä enemmän mobiililaitteiden ja tietokoneiden hankintaan, hallintaan ja uusintaan. Haastetta yrityksille tuovat mobiililaitteiden ja tietokoneiden suhteellisen lyhyt elinkaari kolmesta viiteen vuoteen ja laitteiden suuri vaihtuvuus, mikä työllistää yritysten ICT-osastoa huomattavasti.

Opinnäytetyön tarkoituksena on tutkia, miten yritysten mobiililaitteiden ja Windows-tietokoneiden hallintaongelmat ovat ratkaistavissa ICT-osaston näkökulmasta. Tämä empiirinen, laadullinen toimintatutkimus perustuu havaintoihini ja työkokemukseen ICT-asiantuntijana yrityksen tietohallinto-osastolla ja työssä havaittuihin ongelmiin laite- ja käyttäjähallinnassa.

Opinnäytetyön empiirisessä osassa tuodaan esille kohdatut ongelmat laite- ja käyttäjähallinnassa sekä konkreettiset esimerkit mobiililaitteiden ja tietokoneiden hallinnan parantamiseksi. Teoriaosuudessa käydään läpi Microsoftin tarjoamat palvelut, joiden pyrkimyksenä on helpottaa ICT-osastojen toimintaa. Lopuksi pohditaan, mitä hyötyä Microsoftin tarjoamasta palvelusta on yritykselle ja loppukäyttäjälle.

Valitsin tämän aiheen opinnäytetyöaiheeksi, koska silloinen esimieheni ehdotti minulle tätä aihetta työskennellessäni osana ICT-osastoa. Aihe herätti mielenkiintoni, koska Microsoft Endpoint Managerin tarjoamilla palveluilla voisin helpottaa omaa työntekoani.

2 KOHDATUT ONGELMAT LAITE- JA KÄYTTÄJÄHALLINNASSA

Tässä kappaleessa käsitellään laite- ja käyttäjähallinnassa kohtaamiani ongelmakohtia työskennellessäni ICT-osastolla. Ongelmat olivat miltei jokapäiväisiä ja ne toistuivat samankaltaisina. Näkemykseni mukaan mainitsemani ongelmat ovat yrityksissä hyvin tyypillisiä ja yrityksen toimialasta riippumattomia. Lähtökohtaisesti ongelmat ovat korjattavissa helposti ja nopeasti, mutta ne sitovat ICT-osaston resursseja. Seuraavissa alakohdissa esitetyt laite- ja käyttäjähallinnan ongelmat pystytään minimoimaan tai lähes kokonaisuudessaan poistamaan käyttämällä Microsoft Endpoint Managerin eri palveluita. Palvelu tarjoaa ratkaisuja miltei rajattomasti, ja täten turhaa työtä voidaan minimoida.

2.1 Uuden tietokoneen tai mobiililaitteen asennus

Uudet työasemat ja mobiililaitteet toimitetaan yritykseen suoraan laitevalmistajan tarjoamilta tukkuliikkeiltä. Tukkuliikkeet toimittavat laitteet yrityksen päätoimipisteeseen, jossa ICT-osasto toimii. ICT-osasto suorittaa laitteen asennuksen. Laite liitetään toimialueeseen ja loppukäyttäjän tarvitsemat ohjelmistot asennetaan sekä päivitetään manuaalisesti ilman automaatiota. Asennettavat sovellukset määräytyvät loppukäyttäjän toimenkuvan mukaan, mutta useassa tapauksessa ongelmaksi muodostuu loppukäyttäjän tietämättömyys siitä, mitä ohjelmistoja hän tulee työssään tarvitsemaan.

Asennuksen jälkeen laite toimitetaan loppukäyttäjälle, joka usein miten toimii eri toimipisteessä tai itsenäisessä työympäristössä. Edellä kerrottu prosessi ilman laitteen suoraa loppukäyttäjälle toimittamista sekä asennuksen ja päivityksen automaatiota vie huomattavan määrän ICT-osaston resursseja.

2.2 Laiterekisterin ylläpito

Laiterekisterin ylläpito on yritykselle erittäin tärkeää. Laiterekisterin tulisi olla integroituna käyttäjienhallintaan, minkä seurauksena laiterekisteri päivittyy auto-

maattisesti esimerkiksi laiterekisterissä olevan laitteen siirtyminen toiselle käyttäjälle. Laiterekisterin avulla yrityksen ICT-osasto on tietoinen yrityksen sisällä käytettävistä tietokoneista ja mobiililaitteista. Rekisteri pitää sisällään tärkeitä tietoja käytettävistä laitteista, kuten valmistajan, mallin ja laitteen nimen. Rekisteriin kirjataan myös laitteen käyttäjä ja käyttöönottopäivämäärät. Käyttöönottopäivämäärän mukaan määräytyy laitteen käyttöikä yrityksessä. Usein rekisteriin kirjataan myös laitteen takuuaika.

Mikäli laiterekisteriä ei ole integroituna käyttäjienhallintaan, ongelmaksi muodostuu laiterekisterin manuaalinen päivittäminen. Tämän seurauksena laiterekisteri ei ole välttämättä ajantasainen ja tiedot saattavat olla virheellisiä.

2.3 Tietokoneiden ja mobiililaitteiden uusiokäyttö

Laitteen uusiokäyttöprosessi vastaa uuden laitteen käyttöönottoa. Erona on ainoastaan, että laite on jo kertaalleen asennettu ja on ollut käytössä. Tietokone tai mobiililaite toimitetaan uusiokäyttöä varten yrityksen päätoimipisteeseen, missä ICT-osasto suorittaa laitteen edellisen käyttäjän tietojen tuhoamisen ja laitteen uudelleen asennuksen.

Uudelleen asennuksen yhteydessä tulee ottaa huomioon laitteen tuleva loppukäyttäjä. Tämän seurauksena jokainen laitteen uudelleenasennusprosessi räätälöityy laitteen tulevan käyttäjän mukaan. Prosessin ongelma on, että tietokone tai mobiililaite on toimitettava fyysisesti ICT-osastolle tietojen tuhoamiseen ja tehdasasetuksiin palauttamiseen sekä uudelleenasennusprosessia varten.

2.4 Ohjelmisto- ja käyttöjärjestelmäpäivitykset

Tietokoneen tai mobiililaitteen asennusvaiheessa ICT-osasto päivittää laitteelle uusimmat käyttöjärjestelmäpäivitykset sekä vastaa käytettävien ohjelmistojen päivityksistä. Laitteet toimitetaan niiden käyttäjille täysin päivitettyinä, olkoon laite uusi tai käytetty.

Jatkossa ohjelmistojen ja käyttöjärjestelmien päivityksistä on vastuussa itse laitteen käyttäjä, minkä johdosta päivitykset eivät pysy pitkään ajantasaisena. Edellä mainitusta johtuen päivittämätön ohjelmisto tai käyttöjärjestelmä voi lakata toimimasta tai ei toimi oikein. Päivittämätön ohjelma tai käyttöjärjestelmä hankaloittaa työntekoa muodostaen samalla erilaisia tietoturvariskejä. Pahimmassa tapauksessa laite palautuu ICT-osastolle käyttökelvottomana vaatien jälleen sen uudelleen asentamista. Prosessi on ICT-osaston ja laitteen käyttäjän kannalta turhauttavaa, aikaa vievää ja vaatii aikataulujen sovittamista, ja olisi vältettävissä automatisoiduilla ja pakotetuilla ohjelmisto- tai käyttöjärjestelmäpäivityksillä.

2.5 Käyttäjän oikeudet tietokoneen muutoksiin

Tietokoneen tai mobiililaitteen käyttäjä ei pysty itse asentamaan tai poistamaan sovelluksia. Sovellusten asentamisesta ja poistamisesta vastaa ainoastaan yrityksen ICT-osasto. ICT-osasto vastaa myös laitteisiin tehtäviä muutoksia ja lisälaitteiden asennuksia.

Järjestelmänvalvojaoikeuksien puuttuminen laitteen loppukäyttäjältä muodostaa työtä yrityksen ICT-osastolle, koska jokaiseen laitteeseen tehtävään muutokseen, ohjelmiston asentamiseen ja poistamiseen tarvitaan järjestelmänvalvojaoikeuksia. Käyttäjien oikeudet määräytyvät Active Directoryyn luotujen ryhmien perusteella. Täten käyttäjille voidaan määritellä eritasoisia käyttöoikeuksia.

2.6 Yrityksen asettamat asetukset laitteille ja käyttäjille

Yrityksen käytössä olevia laitteita ja käyttäjiä hallitaan paikallisella Windows-palvelimelta. Palvelimelta hallinnointi tehdään käyttäen Windows Active Directoryä. Active Directoryssä hallinnointi tehdään käyttäen ryhmiä ja Group Policyjä. Tiedot päivittyvät käyttäjille ja heidän laitteilleen, laitteen ollessa yhteydessä yrityksen lähiverkkoon.

Ongelmaksi tässä muodostuu, että laitteen ja käyttäjän tulee olla yhteydessä yrityksen käytössä olevaan Active Directoryyn lähiverkon kautta. Käyttäjille ja laitteille asetetut asetukset eivät aktivoidu laitteelle tai käyttäjälle, mikäli laite ei ole yhteydessä yrityksen lähiverkkoon.

3 MICROSOFT ENDPOINT MANAGER

Tässä luvussa käsitellään Microsoft Endpoint Managerin palvelu ja sen osa-alueet. Palvelu sisältää ohjelmistokokonaisuuden, jolla tarjotaan yritykselle tarvittavat työkalut käyttäjä- ja laitehallintaan. Microsoft Endpoint Managerin palveluita ovat Microsoft Intune, Microsoft Endpoint Configuration Manager, Windows Autopilot, Edpoint Analytics, Microsoft Defender Endpoint ja Azure AD. Opinnäytetyössäni keskityn osa-alueisiin, jotka koskettavat laite- ja käyttäjähallintaa. Näitä osa-alueita ovat Microsoft Intune, Windows Autopilot sekä Azure AD. Kuviossa 1 eritellään Microsoft Endpoint Manager eri osa-alueet ja niiden tarjoamat palvelut. (Microsoft 2022f.)

Kuvio 1. Microsoft Endpoint Managerin palvelut (Microsoft 2022f).

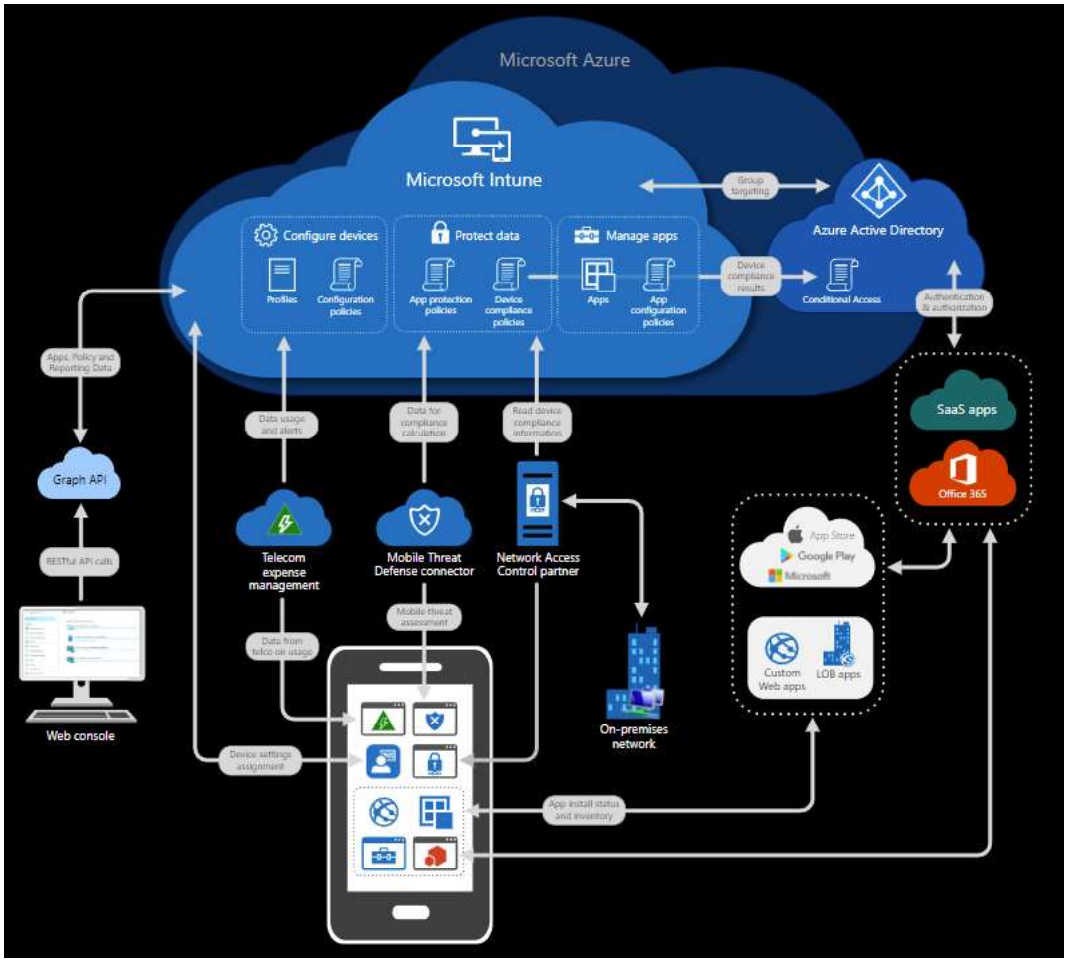
Laitehallinnan osalta opinnäytetyö käsittelee Windows-tietokoneita ja Android-mobiililaitteita. Suurin osa yritysten käyttämistä laitteista on Windows-tietokoneita ja Anroid-mobiililaitteita. Kuviossa 2 on vuoden 2022 eri käyttöjärjestelmien markkinaosuudet. Omassa työssäni ICT-osastolla emme käyttäneet lainkaan IOS- ja MacOS-laitteita. (Statcounter 2022.)

Kuvio 2. Käyttöjärjestelmien markkinaosuudet (Statcounter 2022).

3.1 Microsoft Intune

Microsoft Intune on pilvipohjainen mobiilisovellusten, mobiililaitteiden ja tietokoneiden hallintaan keskittynyt palvelu. Microsoft Intune mahdollistaa yrityksen käytössä olevien mobiililaitteiden ja tietokoneiden hallinnan niiden olinpaikasta riippumatta. Laitteiden asetukset, ominaisuudet ja suojaus ovat muokattavissa yrityksen omien tarpeiden mukaan suoraan Microsoft Intune-portaalista.

Intune-portaalista IT-henkilöstö pystyy tarkastelemaan yrityksen käytössä olevia laitteita. Portaali näyttää kattavasti laitteen tiedot, siihen asennetut ohjelmat, laitteiston päivitykset ja kenellä laite on käytössä. Kuviossa 3 kuvataan Microsoft Intunen eri osa-alueita ja yhteistä kokonaisuutta. (Microsoft 2022g.)



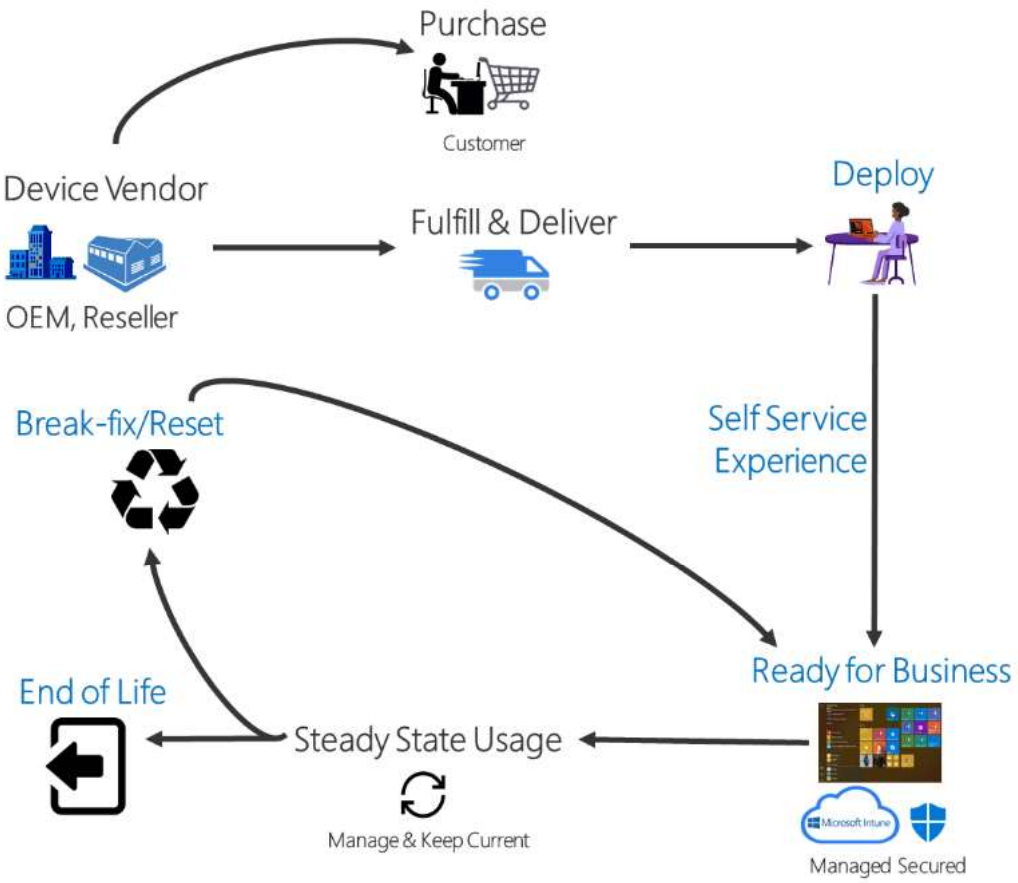
Kuvio 3. Microsoft Intune Azure ympäristössä (Microsoft 2022g).

3.2 Windows Autopilot

Windows Autopilot tarjoaa mahdollisuuden toimittaa Windows-työasemat suoraan loppukäyttäjälle. Tähän prosessiin ei tarvita yrityksen IT-henkilöä, koska tietokoneen käyttöönotto on tehty todella helpoksi ja kuka tahansa osaa tehdä sen. Ainoana vaatimuksena on toimiva internet-yhteys, että laite saadaan käyttökuntoon. Käyttäjä kirjautuu tietokoneelle käyttäen yrityksen hänelle luomaa käyttäjätunnusta.

Tietokone ottaa yhteyden Azure Active Directoryyn. Tämän jälkeen käyttäjälle allokoidut sovellukset alkavat latautua ja asentua tietokoneella automaattisesti. Käyttöönoton jälkeen laitteen ja käyttäjän tiedot päivittyvät yrityksen Intune-portaaliin. Kuviossa 4 kuvataan Windows autopilotin luomaa elinkaarta laitteelle sen

toimitushetkestä käyttäjälle aina laitteen käyttöiän loppumiseen saakka. (Microsoft 2022h.)

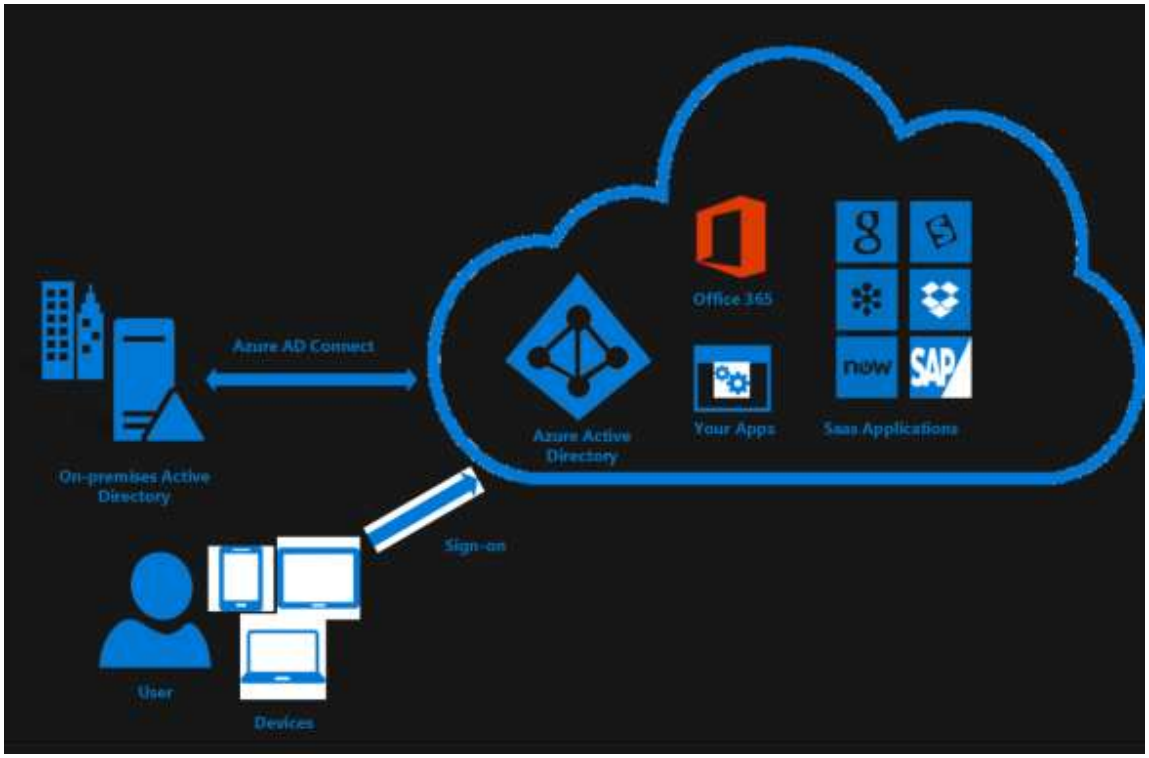


Kuvio 4. Windows Autopilot ja laitteen elinkaari (Microsoft 2022h).

3.3 Azure AD

Azure AD on Microsoftin pilvipohjainen hakemisto- ja identiteettihallintapalvelu. Palvelu mahdollistaa yritysten resurssien ja käyttöoikeuksien turvallisen jakamisen yrityksen käyttäjille. Azure AD toimii alustapalveluna, joka toimii sovellusten, palvelujen ja palvelimien alustana.

Kuviossa 5 on kuvattu hyprid-toteutusta, jossa käyttäjä ja käytössä olevat laitteet ovat yhteydessä pilvipohjaiseen Azure AD:seen ja paikalliseen Windows palvelimella hallittavaan Active Directoryyn. Tämä mahdollistaa käyttäjälle yrityksen resurssien ja käyttöoikeuksien saumattoman käytön. (Microsoft 2022j.)



Kuvio 5. Kuvaus Azure AD (Microsoft 2022l).

4 RATKAISUT ONGELMIIN LAITE- JA KÄYTTÄJÄHALLINNASSA

Tässä luvussa esitellään ratkaisuja ICT-osastolle tulleisiin tukipyyntöihin ja tehtäviin. Tarkastelussa ovat laiteasennuksiin, laiterekisteriin, laitteiden uusikäyttöön ja ohjelmisto- ja käyttöjärjestelmäpäivityksiin liittyvät tehtävät.

4.1 Uuden tietokoneen tai mobiililaitteen asennus

Windows Autopilot mahdollistaa uuden Windows-tietokoneen toimittamisen suoraan sen loppukäyttäjälle. Tukkuliike asentaa tietokoneeseen asiakasyrityksen räätälöimän Windows-käyttöjärjestelmä Imagen. Loppukäyttäjä vastaanottaa tietokoneen tukkuliikkeeltä, käyttäjä kirjautuu siihen käyttäen yrityksen luomaa käyttäjätunnusta. Kirjautumalla tietokoneelle käyttäen yrityksen luomaa personoitua tunnusta, tietokone ottaa yhteyden yrityksen käyttämään pilvipohjaiseen Azure Active Directoryyn. Käyttäjän tunnistautumisen jälkeen tietokone alkaa automaattisesti asentamaan käyttäjälle ennalta määrättyjä sovelluksia, jotka yrityksen ICT-osasto on määrittänyt Microsoft Intuneen. Asentuvat sovellukset määräytyvät käyttäjän työnkuvan mukaan. Tämän jälkeen tietokone on valmis käytettäväksi. (Microsoft 2022m.)

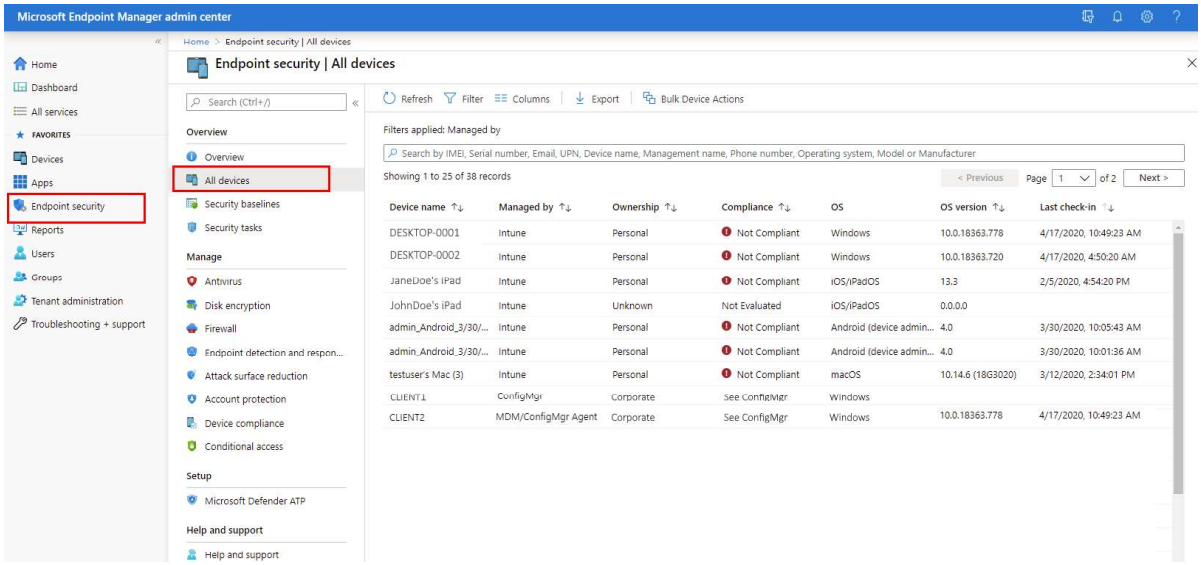
Uuden tietokoneen käyttöönotossa ICT-osaston työtehtävät minimoituvat yrityksen käyttäessä Microsoft Autopilottia. Laite toimitetaan suoraan sen loppukäyttäjälle, joten välikäsiä ei ole ja laitteen käyttöönoton pystyy tekemään sen loppukäyttäjä ilman ICT-osaston apua. ICT-osastolle tehtäväksi uuden laitteen asennuksessa jää ainoastaan käyttäjätunnuksien ylläpito ja niiden käyttöoikeudet.

4.2 Laiterekisterin ylläpito

Laiterekisterin ylläpito automatisoituu ja helpottuu huomattavasti, kun yritys ottaa Microsoft Intunen käyttöön. Laitteet lisätään niiden hankintavaiheessa Intuneen, joko manuaalisesti tai automatisoidusti käyttäen Microsoft Autopilottia.

Manuaalinen lisäys tehdään esimerkiksi mobiililaitteelle, jolla suoritetaan ainoastaan yrityksen asettamia työtehtäviä ja laitetta ei ole kohdistettu yksittäiselle käyttäjälle vaan se on yrityksen yleisessä käytössä. (Microsoft 2022a; Microsoft 2022e)

Microsoft Intunesta ICT-osasto pysyy ajan tasalla yrityksen sisällä käytettävistä mobiililaitteista ja tietokoneista. Laitteista käy ilmi heti Intunen laitesivustolta laitteiden tärkeimmät tiedot kuten nimi, laitteen käyttäjä ja päivämäärä milloin laite on otettu käyttöön. Kuviossa 6 on kuvakaappaus Intunen laitehallinnasta. (Microsoft 2022b.)



Kuvio 6. Intune laitehallinta (Microsoft 2022b).

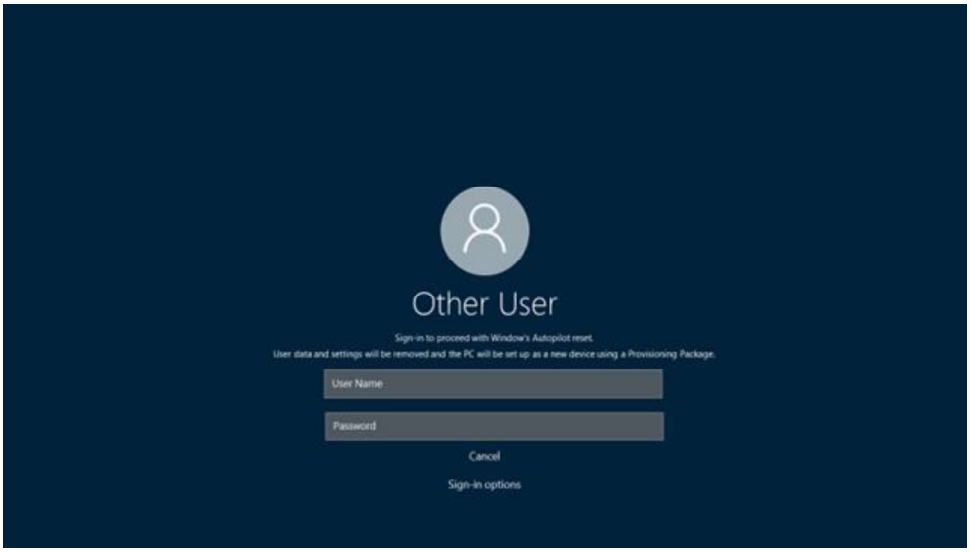
4.3 Tietokoneen ja mobiililaitteiden uusiokäyttö

Microsoft Intune mahdollistaa tietokoneiden ja mobiililaitteiden helpon uusiokäytön. Mikäli uusiokäyttöön tuleva laite on lisättynä Microsoft Intuneen, ICT-osaston ei tarvitse saada laitetta fyysisesti osastolleen. Microsoft Intune mahdollistaa tietokoneen tai mobiililaitteen tietojen tuhoamisen ja tehdasasetuksiin palauttamisen käyttäen Intune-portaalia. Laitteen ollessa kytkettynä toimivaan internet-yhteyteen, laitteen tyhjäys pystytään suorittamaan. Laitteen uusiokäyttövaiheessa käyttäjä kirjautuu laitteelle yrityksen luomalla käyttäjätunnuksella, tämän jälkeen

laitteen uuden käyttäjän tiedot päivittyvät yrityksen Microsoft Intune-portaaliin automaattisesti ja käyttäjälle allokoidut sovellukset alkavat latautua laitteelle.

Laitteen tyhjäystä ja tehdasasetuksiin palauttamista voidaan käyttää myös muihin tarkoituksiin, kuin laitteen uusiokäyttötilanteessa. Mikäli laite on kadonnut tai varastettu, ICT-osasto pystyy tuhoamaan laitteessa olevan datan. Täten yrityksen tiedot eivät joudu vääriin käsiin. (Microsoft 2022i; Microsoft 2022j.)

Kuviossa 7 on Windows Autopilotin mahdollistavasta tietokoneen resetoinnista. Kuvakaappaus on otettu suoraan resetoitavalta laitteelta. Resetointi pystytään suorittamaan suoraan laitteelta tai käyttäen Intunen laitehallintaportaalia. Kuvassa näkyvään käyttäjätunnus- ja salasanatietoon yrityksen ICT-henkilö syöttää järjestelmänvalvojatunnukset. Tämän jälkeen tietokone palautuu tehdasasetuksiin ja laite on mahdollista luovuttaa seuraavalle käyttäjälle tai poistaa se kokonaan käytöstä. (Microsoft 2022m.)



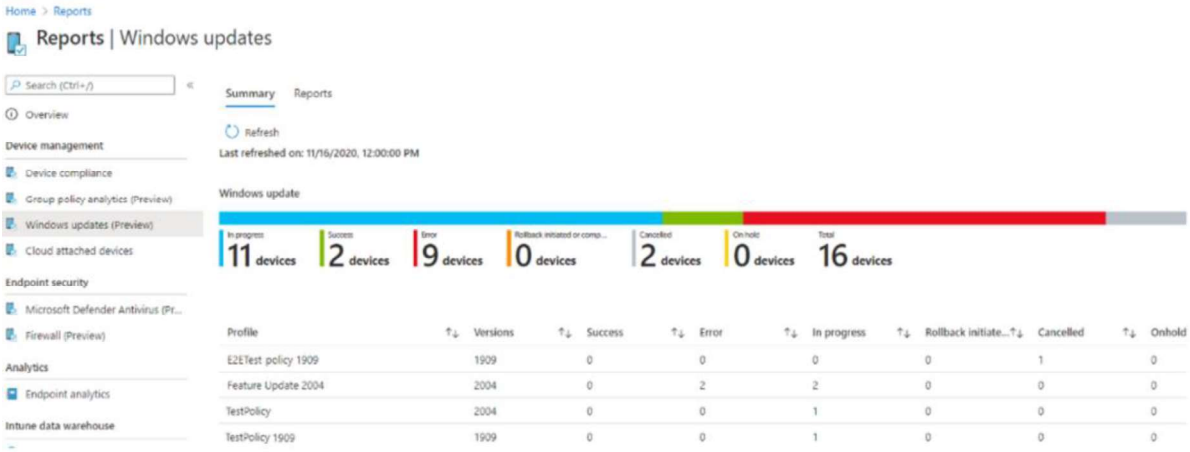
Kuvio 7. Tietokoneen resetointi (Microsoft 2022n).

4.4 Ohjelmisto- ja käyttöjärjestelmäpäivitykset

Microsoft Intunen avulla ICT-osasto pystyy halutessaan pakottamaan tietokoneiden ja mobiililaitteiden käyttäjille ohjelmisto- ja käyttöjärjestelmäpäivitykset. Laitteiden päivitys ei ole jatkossa enää loppukäyttäjän hallinnassa ja vastuulla. ICT-

osasto hallitsee laitteiden päivityksiä ja tämän seurauksena laitteet pysyvät ajan tasalla. (Microsoft 2021d.)

Yrityksen kannattaa kuitenkin tiedottaa käyttäjiä säännöllisistä päivityksistä. Laitteen ollessa yhdistettynä Intuneen laite ilmoittaa käyttäjälle, kun laite aloittaa päivitykset. Mikäli laite tulee käynnistää uudelleen, käyttäjää huomautetaan asiasta, että laite tulee käynnistymään tietynajan kuluttua uudelleen. Päivitykset takaavat ohjelmistojen vakaan toiminnan ja tietoturvallisuuden. Kuviossa 8 on kuvakaappaus Intune portaalista, josta ICT osasto pystyy tarkistamaan mitkä yrityksen käytössä olevat laitteet ovat ajan tasalla ja mihin on päivitetty uusimmat käyttöjärjestelmäpäivitykset. (Microsoft 2022b.)



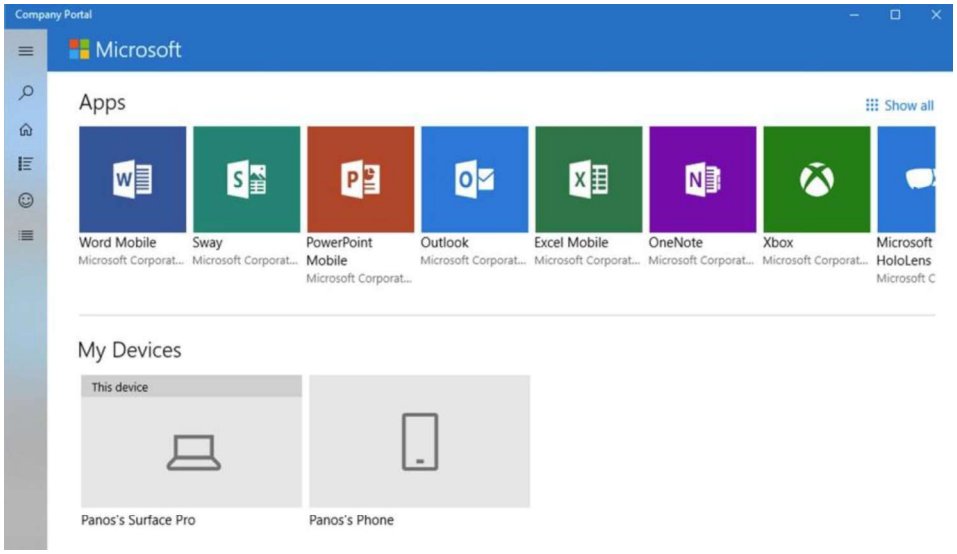
Kuvio 8. Raportti Windows-päivityksistä (Microsoft 2022b).

4.5 Käyttäjän oikeudet tietokoneen muutoksiin

Microsoft Intune mahdollistaa käyttäjilleen ennalta määriteltyjen sovellusten asentamisen ja poiston. Yrityksen ottaessa käyttöön Intune-yritysportaalin, ICT-osasto pystyy määrittelemään sovelluksia, joita loppukäyttäjät pystyvät asentamaan tai poistamaan käyttämältään tietokoneelta tai mobiililaitteelta ilman ICT-osaston apua. (Microsoft 2022o.)

Intune-yritysportaali takaa käyttäjän asentamien sovellusten tietoturvallisuuden. Ohjelmistojen päivitykset ovat ajan tasalla ja ne ovat luotettavia. Täten loppukäyttäjän ei tarvitse ladata työhön tarvitsemiaan sovelluksia suoraan internetistä vaan luotettavalta yrityksen ICT-osaston laatimasta Microsoft Intune-yritysportaalista.

Kuviossa 9 on kuvakaappaus yritysportaalista. Apps-välilehdellä näkyy yrityksen määrittämät sovellukset käyttäjälle. Sovellus-kuvaketta painamalla sovellus alkaa latautua käyttäjän laitteelle. Yritysportaalissa näkyy myös käyttäjän käytössä olevat laitteet.



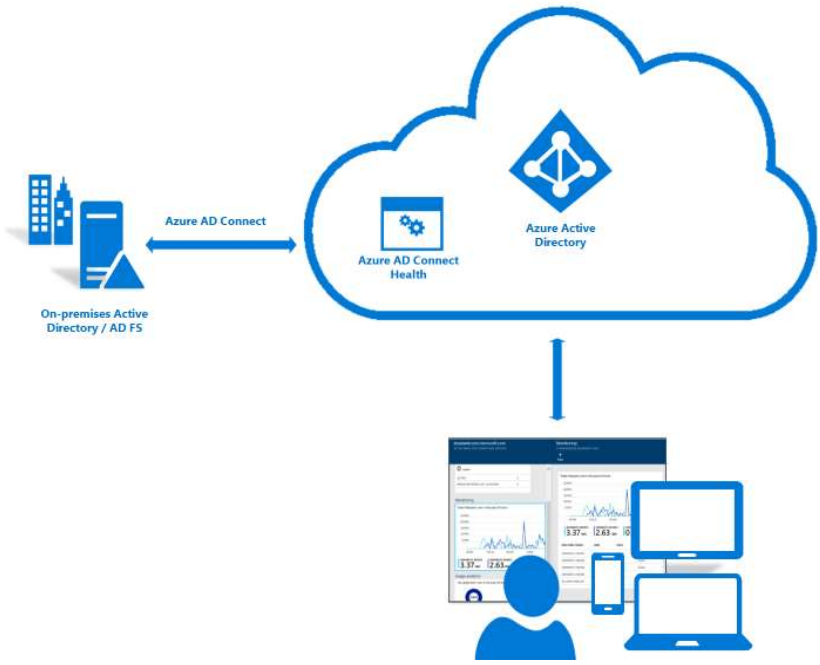
Kuvio 9. Yritysportaali (Microsoft 2022o).

4.6 Yrityksen asettamat asetukset laitteille ja käyttäjille

Pilvipohjainen Azure Active Directory mahdollistaa, että käyttäjien- ja laitteiden hallinta pystytään toteuttamaan niiden olinpaikasta riippumatta. Käyttäjät ja laitteet liitettynä Azure Active Directoryyn ja Microsoft Intuneen mahdollistavat ryhmäkäytäntöjen ja Group Policyjen päivittymisen käyttäjälle ja laitteelle, ilman yhteyttä yrityksen lähiverkkoon. Tähän tarvitaan vain toimiva internetyhteys.

Internetyhteys mahdollistaa laitteen ja käyttäjän yhteyden Azure Active Directoryyn. Kuviossa 10 käyttäjä ja laite ovat yhteydessä pilvipohjaiseen Azure AD:seen.

Pilvipohjaisuuden ansiosta yhteys pystytään muodostamaan, mistä tahansa internetyhteydestä. Yhteyden muodostamiseen ei tarvita laitteen liittämistä yrityksen lähiverkkoon. (Microsoft 2022l.)



Kuvio 10. Käyttäjän ja laitteen yhteys Azure AD:seen (Microsoft 2022l).

5 KÄYTÄNNÖN ESIMERKKEJÄ

Tässä kappaleessa esittelen esimerkkitapauksia ongelmista, joita kohtasin työasema- ja käyttäjähallinnassa työskennellessäni ICT-osastolla. Käytössämme ei ollut Microsoft Endpoint Managerin tarjoamia palveluita. Hallinta oli toteutettu paikallisella Windows-palvelimella. Palvelimelta hallinta toteutettiin käyttäen paikallista Windows Active Directoryä.

Tästä johtuen laitteiden ja käyttäjien tuli olla yhteydessä yrityksen lähiverkkoon, jotta hallintaa pystyttiin tekemään. Tässä luvussa esitellään, miten yleisimmät ICT-tukitehtävät pystytään ratkaisemaan ottamalla Microsoft Endpoint Managerin tarjoamat palvelut käyttöön.

5.1 Salasanan vaihto etäyhteydellä

Käyttäjä työskentelee etäyhteydellä kotoa. Kirjautuessaan tietokoneelle, tietokone ilmoittaa salasanan vanhentuneen. Käyttäjä ei pääse kirjautumaan tietokoneelleen, ennen kuin salasana on vaihdettu uuteen. ICT-osasto pystyy vaihtamaan käyttäjälle uuden salasanan, mutta käyttäjä ei pääse kirjautumaan tällä tietokoneelleen. Tietokone ei ole yhteydessä yrityksen lähiverkkoon. Tässä tapauksessa käyttäjän tulee liittää tietokoneensa yrityksen lähiverkkoon. Tämän jälkeen ICT-osaston vaihtama salasana vaihtuu käyttäjälle, kun tietokone on liitettynä yrityksen sisäverkkoon ja tietokone saa yhteyden paikalliseen Windows Active Directoryyn.

Mikäli yrityksen käyttäjä- ja hakemistopalvelu olisivat rakennettu Azure AD:seen ja laitteet liitetty Microsoft Intuneen, salasanan vaihtaminen onnistuisi mistä tahansa internetverkosta. Intuneen liitettynä laite on yhteydessä pilvipohjaiseen Azure AD:seen. Azure AD:ssa tehdyt muutokset päivittyvät käyttäjälle ja laitteelle, mikäli laite on kytkettynä toimivaan internetyhteyteen.

5.2 Yrityksen tietokone varastetaan

Yrityksen käytössä ollut tietokone varastetaan ja sen sisältämän tiedot ovat vaarassa joutua vääriin käsiin. Varas ei pääse kirjautumaan tietokoneelle, ilman että hän tietäisi käyttäjätunnusta tai salasanaa. Tietokoneen kiintolevy on kuitenkin luettavissa erillisellä lukulaitteella. Tietokone tulisi saada tyhjennettyä yrityksen tiedoista mahdollisimman nopeasti. Tätä ei voida kuitenkaan tehdä ilman, että tietokone löytyy tai laitteen varastanut henkilö saadaan kiinni.

Microsoft Intune mahdollistaa laitteen tietojen tyhjentämisen ja tuhoamisen laitteen olinpaikasta riippumatta. Intunen laitehallintaportaalista laitteelle lähetetään Wipe-komento. Laitteen ollessa seuraavan kerran yhteydessä internettiin, tiedot yrityksen tiedot poistetaan automaattisesti laitteelta.

5.3 Tietokoneelta ei löydy yrityksen yleisohjelmaa

Käyttäjän tietokone vaihtuu uuteen. Uudelle tietokoneelle ei ole asennettu yrityksen liiketoiminnan kannalta tärkeää ohjelmistoa. Ohjelmiston asentaminen ei onnistu ilman järjestelmänvalvojaoikeuksia. Lähtökohtaisesti järjestelmänvalvojaoikeudet ovat ainoastaan yrityksen ICT-osastolla työskentelevillä henkilöillä. Käyttäjän tulee olla yhteydessä ICT-osastoon, että he tekevät ohjelman asennuksen.

Käyttäjä pystyy asentamaan ohjelman omatoimisesti Yritysportaalista. Yritysportaalissa ohjelma on valmiiksi konfiguroitu ja se on heti käyttövalmis. Mikäli sovellusta ei löydy Yritysportaalista, käyttäjän on mahdollista pyytää ICT-osastoa lisäämään sovellus Yritysportaaliin.

5.4 Käyttäjän tietokone rikkoutuu

Käyttäjä ilmoittaa ICT-osastolle, että hänen käytössään ollut tietokone on rikkoutunut. Käyttäjän tulisi saada uusi tietokone mahdollisimman nopeasti. Tässä tilanteessa käyttäjälle tilataan uusi tietokone. Tietokone saapuu laitetoimittajalta en-

sin yrityksen ICT-osastolle. ICT-osastolla laite otetaan käyttöön ja siihen asennetaan käyttäjän tarvitsemat sovellukset. Tämän jälkeen laite toimitetaan käyttäjälle. Tämän lisäksi ICT-osaston ja loppukäyttäjän välillä käydään monia puhelin- ja sähköpostikeskusteluja laitevaihdon aikatauluttamisesta.

Windows Autopilotin ansiosta laite voitaisiin toimittaa suoraan käyttäjälle. Käyttäjä pystyy ottamaan laitteen itse käyttöön. Tähän tarvitaan vain toimiva internetyhteys. Laitteen käyttöönotto on tehty todella helpoksi ja käyttäjän tarvitsemat ohjelmat asentuvat laitteelle automaattisesti. Tämä säästää huomattavasti aikaa ja ICT-osaston resursseja, koska laite toimitetaan jatkossa suoraan loppukäyttäjälle.

6 TULOKSET

Opinnäytetyön tulokset luvussa pohditaan millaisille yrityksille Microsoft Endpoint Managerin tarjoamat palvelut soveltuvat ja mitä käytännön hyötyä niiden käyttöönotto tarjoaa. Arvioin myös opinnäytetyön toteutustapaa, kohtaamiani haasteita ja sekä sitä, kenelle työ on suunnattu.

Microsoft Endpoint Managerin tarjoamat palvelut sopivat mielestäni kaikille yritykselle, jotka haluavat helpottaa ja automatisoida käyttäjä- ja laitehallintaa. Microsoft Endpoint Managerin palvelut mahdollistavat laitteiden käyttäjille yksinkertaisten ja turvallisten toimenpiteiden tekemisen, ilman yrityksen oman ICT-osastoa. Esimerkiksi Yritysportaalista löytyvien sovellusten asentamisen laitteelle ilman järjestelmänvalvojaoikeuksia. Tämän seurauksena ICT-osastolla jää aikaa ja resursseja ICT-osaston ja muiden käytössä olevien palveluiden kehittämiseen.

Microsoft Intunen ja Windows autopilotin tuomat hyödyt mahdollistavat yritysten laitteiden käytön, asennuksen ja uusiokäytön mutkattomasti laitteen käyttöpaikasta riippumatta. Intunen laitehallinta päivittyy automaattisesti ja Intune-portaalista laitteiden tiedot ovat helposti saatavilla. Pilvipohjaisen Azure AD:n ansioista käyttäjät tarvitsevat vain toimivan verkkoyhteyden, jotta heillä on pääsy yrityksen käytössä oleviin ohjelmistoihin ja resursseihin. Käyttäjän ei jatkossa tarvitse olla yhteydessä yrityksen lähiverkkoon, tämän ansiosta esimerkiksi etätyöskentely onnistuu ongelmitta. Laitteet ja käyttäjät ovat aina yhteydessä Azure AD-hallinta palvelimeen, mikäli laite on kytkettynä toimivaan internetyhteyteen.

Omakohtaisesta kokemuksestani, Microsoft Endpoint Managerin tarjoamat hyödyt korostuivat, kun maailmassa puhkesi koronapandemia keväällä 2020. Pandemian seurauksena käyttäjät siirtyivät yhä enenevässä määrin etätöihin. Työskennellessäni ICT-osastolla keväällä 2020 pandemian alkuvaiheessa aloiteltiin työpaikallani Microsoft Endpoint Manageria käyttöönottoa. Käyttöönotto mahdollisti käyttäjien- ja laitteiden hallinnan niiden olinpaikasta riippumatta. Tämä helpotti

huomattavasti päivittäistä työtäni, koska lähtökohtaisesti työpäiväni koostui käyttäjien- ja laitteidenhallinnasta. Tämän ansiosta, minulla jäi aikaa osallistua käynnissä oleviin projekteihin, joiden tarkoituksena oli ICT-osastomme jatkuva kehittäminen.

7 YHTEENVETO

Opinnäytetyön tarkoituksena on herätellä mielenkiintoa Microsoft Endpoint Managerin tarjoamista palveluista, niiden tarjoamista ratkaisuista ja antaa esimerkkien kautta tietoa, miten yritysten ICT-osaston toimintaa voidaan tehostaa ja tiettyjä toimenpiteitä voidaan ehdollistaa laitteiden käyttäjille.

Opinnäytetyön toteuttaminen oli melko haastavaa, koska en ole päässyt kokeilemaan kaikkia Endpoint Managerin tarjoamia palveluita käytännössä. Kyseisten palveluiden käyttöönottoa aloiteltiin hyödyntämään koronapandemian alkuvaiheessa vuonna 2020. Alkuvaiheessa niiden käyttöönotto sitoi paljon aikaa ja resursseja. Lopetin työskentelyn ICT-osaston työtehtävässä huhtikuussa 2021, kun palveluita vielä räätälöitiin yritykselle sopiviksi. Täten kokemus Microsoft Endpoint Managerista jäi suhteellisen lyhyeksi.

Opinnäytetyön tiedonkeruu ja sen ymmärtäminen oli haastavaa, koska lähtökohtaisesti aiheesta löytyvä tieto on englanninkielistä ja välillä vaikeasti ymmärrettävää. Lähteinä käytettiin pääasiassa internetlähteitä, koska aiheesta ei löytynyt kirjallista materiaalia. Ongelmaksi muodostui myös tiedon nopea muuttuminen. Tehdessäni tätä opinnäytetyötä törmäsin ongelmaan, jossa aiheesta löytyvä tieto päivittyy nopeasti. Aiheeni on myös todella laaja, joten käsiteltävää aihealuetta tuli rajata opinnäytetyön selkeyttämisen vuoksi.

LÄHTEET

Microsoft. 2022a. Automatic registration of existing device. Viitattu 10.4.2022. https://docs.microsoft.com/en-us/mem/autopilot/automatic-registration.

Microsoft. 2022b. Intune compliance reports for update. https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-compliance-reports.

Microsoft. 2022c. Manage device with endpoint security in Microsoft Intune Viitattu 10.4.2022. https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-manage-devices.

Microsoft. 2021d. Manage Windows 10 and Windows 11 software updates in Intune. Viitattu 10.4.2022. https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure.

Microsoft. 2022e. Manual registration overview. 10.4.2022. https://docs.microsoft.com/en-us/mem/autopilot/manual-registration.

Microsoft. 2022f. Microsoft Endpoint Manager. Viitattu 10.4. 2022. https://www.microsoft.com/fi-fi/security/business/microsoft-endpoint-manager.

Microsoft. 2022g. Microsoft Intune is an MDM and MAM provider for your devices. Viitattu 10.4.2022. https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft. 2022h. Overview of Windows Autopilot. Viitattu 8.4.2022. https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot.

Microsoft. 2022i. Remove devices by using wipe, retire, or manually unenrolling the device. Viitattu 25.4.2022. https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe.

Statcounter. 2022. Operating System Market Share Worldwide – April 2022. Viitattu 9.5.2022. https://gs.statcounter.com/os-market-share.

Microsoft. 2022j. Use Fresh Start to reset Windows 10 devices with Intune. Viivattu 25.4.2022. https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-fresh-start.

Microsoft. 2022k. What is Azure Active Directory?. Viitattu 22.4.2022. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis.

Microsoft. 2022l. What is Azure AD Connect? Viitattu 29.4.2022. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect.

Microsoft. 2022m. Windows Autopilot. Viitattu 13.4.2022. https://www.microsoft.com/fi-fi/microsoft-365/windows/windows-autopilot.

Microsoft. 2022n. Windows Autopilot Reset. Viitattu 20.4.2022. https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset.

Microsoft. 2022o. Yritysportaali. Viitattu 23.4.2022. https://www.microsoft.com/fi-fi/p/yritysportaali/9wzdncrfj3pz?activetab=pivot:overviewtab.