

Yrityksen IT-infrastruktuurin kehittäminen Microsoft Intunea hyödyntäen



Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus, Hämeenlinnan korkeakoulukeskus
kevät 2023
Eemeli Ehrnrooth

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli ottaa käyttöön mobiililaitteiden rekisteröinti Microsoft Intune – mobiililaittehallinta ympäristöön ja ottaa käyttöön sovellusten jakelu. Työ aloitettiin opinnäytetyön toimeksiantajan tarpeesta kehittää laitteiden elinkaaren hallintaa ja dokumentointia sekä jatkokehitystä.

Työ on jaettu teoria-, ja käytännön osuuteen. Teoriaosuudessa käsitellään työssä käytettäviä järjestelmiä, niiden tarjoamia mahdollisuuksia sekä historiaa. Opinnäytetyö on toiminnallinen. Toiminnallinen osuus toteutettiin hyödyntäen Microsoftin Endpoint Manageria ja Microsoft Intunea. Käytännön osuudessa syvennytään ensin mobiililaitteiden rekisteröintiin mobiililaittevalmistajien laiterekisteröintiohjelmistoissa sekä Microsoft Intuneessa. Lisäksi tarkastelemme, miten näitä hyödyntämällä saamme jaettua sovelluksia sekä asetettua erinäisiä sääntöjä ja määrittämiä laitteille.

Kehittämistyön perusteella voidaan todeta, että Intune soveltuu yritykselle. Aiemmin manuaalista työtä vaativat tehtävät saatiin automatisoitua ja prosesseja nopeutettua. Toimeksiantaja oli tyytyväinen kehittämistyön tuloksiin sekä jatkokehittämisen mahdollisuuksiin. Opinnäytettyön tuottamat hyödyt näkyvät organisaation tietohallinnon päivittäisessä työskentelyssä.

Avainsanat Microsoft Endpoint Manager, Microsoft Azure, Microsoft Intune, Windows 10,
Pilvipalvelut, MDM, ZT, KME,

Sivut 28 sivua ja liitteitä 1 sivua

Author Eemeli Ehrnrooth

Year 2023

Subject Development of a midsized company's IT-infrastructure using Microsoft Intune

Supervisors Mirlinda Kosova-Alija

ABSTRACT

The purpose of this thesis was to enroll mobile devices in Microsoft Intune – mobile device management service and to distribute software to said devices. This project started on the needs of the company to develop their mobile device lifecycle management, documentation and future development.

This work is divided into theoretical and practical parts. Theory section deals with the systems used in the practical part of the work, their history and use cases.

The practical part focuses on enrolling mobile devices in Intune and distributing software with it.

Keywords Microsoft Endpoint Manager, Microsoft Azure, Microsoft Intune, Windows 10, Cloud services, MDM, ZT, KME

Pages 25 pages and appendices 1 pages

Käsiteluettelo

Azure AD

Azure Active Directory (Azure AD) on Microsoftin pilvipohjainen identiteetin ja pääsynhallintapalvelu, jolla työntekijät kirjautuvat organisaation palveluihin ja järjestelmiin.

MFA

Monivaiheinen tunnistautuminen (Multifactor Authentication) on suojautumismenetelmä, joka hyödyntää esimerkiksi tekstiviestitse tulevaa lisäkoodia kirjautumisen yhteydessä lisäten tietoturvaa.

KME

Samsungin laiterekisteröinti mobiililaitteita varten (Knox Mobile Enrollment) helpottaa Samsungin puhelimien ja tabletti-laitteiden automatisoitua määrittystä ja käyttöönottoa organisaatioissa.

ZT

Androidin laiterekisteröinti mobiililaitteita varten (Zero-Touch Enrollment) helpottaa Android puhelimien ja tabletti-laitteiden automatisoitua määrittystä ja käyttöönottoa organisaatioissa

IoT

Esineiden internet (Internet of Things) tarkoittaa esineiden yhdistämistä internettiin.

On-Premise

Yrityksen tiloissa sijaitseva ja itse ylläpidetty ohjelmisto/järjestelmä.

MEM

Microsoft Endpoint Manager, portaali, josta hallitaan yrityksen laitteita ja näihin liittyviä asetuksia sekä käytäntöjä.

SCCM

Endpoint manageria edeltävä System Center Configuration Manager-hallintaohjelma

MDM

Mobile Device Management. Mobiililaitteiden hallintatyökalu. Esimerkiksi Intune.

Token

Fyysinen tai Digitaalinen varmenne jolla taataan pääsy johonkin

JSON

Ohjelmointikieli

Sisällys

1	Johdanto	1
2	Pilvi ja pilvipalvelut	2
3	Microsoft Azure	3
3.1	Azure Active Directory	3
3.2	Hybrid Azure AD	4
3.3	Azure AD ja tietoturva	5
4	Microsoft Endpoint Manager	6
5	Microsoft Intune	7
5.1	Intune MDM -käyttöönottoprofiilit Androidilla	8
5.2	Microsoft Intunen historiaa	10
6	Kehittämistyön tavoite ja tarkoitus	11
7	Ohjelmistojen jakelu Windows 10/11 -käyttöjärjestelmiin Intunen avulla	12
8	Intune MDM:n käyttöönotto	14
8.1	Enrollment Profiili	15
8.2	Dynaaminen laiteryhmä	16
8.3	Laiterekisteröintiohjelmat	17
8.3.1	Samsung Knox Mobile Enrollment (KME)	17
8.3.2	Android Zero-touch Enrollment (ZT)	18
8.4	Sovellusten lisääminen ja jakelu	20
9	Johtopäätökset ja pohdinta	23
10	Yhteenveto	25
	Lähteet	26

Liitteet

Liite 1	Aineistonhallintasuunnitelma
---------	------------------------------

1 Johdanto

Tässä opinnäytetyössä käsitellään Microsoftin Intune-palvelua ja syvennyttään eri tapoihin kehittää yrityksen infrastruktuuria sitä hyödyntäen. Toimeksiantaja on toivonut pysyvänsä nimettömänä opinnäytetyössä. Toimeksiantajaan viitataan jatkossa sanoilla ”yritys” tai ”toimeksiantaja”. Microsoft Intune on pilvipalvelu, joka keskittyy mobiililaitteiden ja työasemien keskitettyyn pilvipohjaiseen hallintaan. Aihe oli yritykselle ajankohtainen ja opinnäytetyö tehtiin toimeksiantajan tarpeesta säästää yrityksen tietohallinnon resursseja ja helpottaa laitteiden elinkaaren seuranta. Opinnäytetyön aihe oli ajankohtainen ja henkilökohtaisesti minua kiinnostava.

Vuonna 2019 alkanut koronaviruspandemia asetti muutospainetta yritysten IT-järjestelmiin. Etätyöskentelyyn panostetaan entistä enemmän maailmanlaajuisen pandemian vuoksi ja usean keskisuuren yrityksen tietohallinnon resurssit ovat äärimmillään käytössä. Tästä syystä on tärkeää säästää näitä resursseja ja työtunteja aina kun vain mahdollista. Tässä opinnäytetyössä tämä toteutetaan tekemällä käyttöönotto Intunen mobiililaittehallintaan Android-laitteille. Tällä parannetaan yrityksen tietoturvaa, tietosuojaa sekä yleistä hallittavuutta mobiililaitteiden osalta. Työssä otetaan käyttöön myös paketoitu automaattinen tiedostojen jakelu loppukäyttäjien työkoneille, mikä vähentää huomattavasti manuaalista asennustyötä loppukäyttäjien osalta.

Päädyin seuraaviin tutkimuskysymyksiin:

Miten Intunella saadaan automatisoitua aiemmin manuaalista työtä vaativia prosesseja?

Kuinka Intune soveltuu keskisuurelle yritykselle?

Miten Intunea hyödyntämällä pystytään säästämään yrityksen tietohallinnon resursseja?

2 Pilvi ja pilvipalvelut

Pilvipalvelut ovat it-palveluiden, esimerkiksi serverien, tallennustilojen, ohjelmistojen, analytiikan, toimittamista internetin eli ”pilven” yli. Pilvipalveluiden etuina ovat yleensä kustannustehokkuus ja ajatus siitä, että maksetaan vain siitä mitä käytetään. Pilvipalveluita käyttämällä säästetään rautakustannuksissa (hardware), omien datakeskusten ja palvelimien ylläpitokustannuksilta ja näihin liittyviltä sivukustannuksilta kuten sähkö, jäähdytys ja henkilöstökustannukset näiden ylläpitämiseen. (Bigelow, S. & Wesley, C, n.d.a)

Pääsääntöisesti pilvipalvelut jaetaan yleisesti kolmeen ryhmään, IaaS, PaaS ja SaaS.

IaaS on lyhenne sanoista Infrastructure as a Service ja tarkoittaa käytännössä sitä, että organisaatio vuokraa pilvipalveluiden tarjoajalta edellytykset IT-infrastruktuurin pystyttämiseen sitä mukaan, kun niille ilmenee tarvetta. Näitä tarpeita ovat esimerkiksi virtuaalipalvelimet, serverit, tallennustila sekä verkkoratkaisut. Hinnoittelu menee myös tarpeen mukaan riippuen palvelimien ja muiden ratkaisujen määrästä ja käytöstä. (Eronen. H, 2016)

PaaS on lyhenne sanoista Platform as a Service, joka taas tarkoittaa järjestelyä, jossa pilvipalvelun tarjoaja vuokraa ikään kuin pilvialustan palveluna, jota asiakasorganisaatiot voivat kehittää ja käyttää omiin tarpeisiinsa. Suosituimpia PaaS-tuotteita on Salesforcen Lightning-alusta, Amazonin Beanstalk ja Azuren pipeline. (Bigelow, S. & Wesley, C, n.d.b) Tämä mahdollistaa ohjelmistojen kehittämisen ja julkaisun ilman että tarvitsee murehtia alustan ylläpidosta tai resursseista.

Asiakasorganisaatio on tässä ratkaisussa vastuussa siitä mitä sisältöä alustaan tuottaa.

Pilvipalveluiden tarjoaja taas huolehtii palvelimien ylläpidosta ja hallinnoinnista, millä asiakasorganisaation PaaS ratkaisut pyörivät. (Eronen. H, 2016)

SaaS on lyhenne sanoista Software as a Service. Joka tarkoittaa käytännössä sitä, että pilvipalveluntarjoaja toimittaa ohjelmiston pilvipalveluna, johon päästään yleensä kirjautumaan selaimen kautta silloin kun sitä tarvitaan. SaaS tarkoittaa, että ohjelmisto on ylläpidetty pilvipalveluidentarjoajan toimesta ja pienin vastuu, eli vain sovelluksen käyttäminen, jää asiakasorganisaation harteille. Tunnetuimpia esimerkkejä SaaS palveluista ovat M365, Gmail, ja SAP. (Amazon AWS, n.d.a)

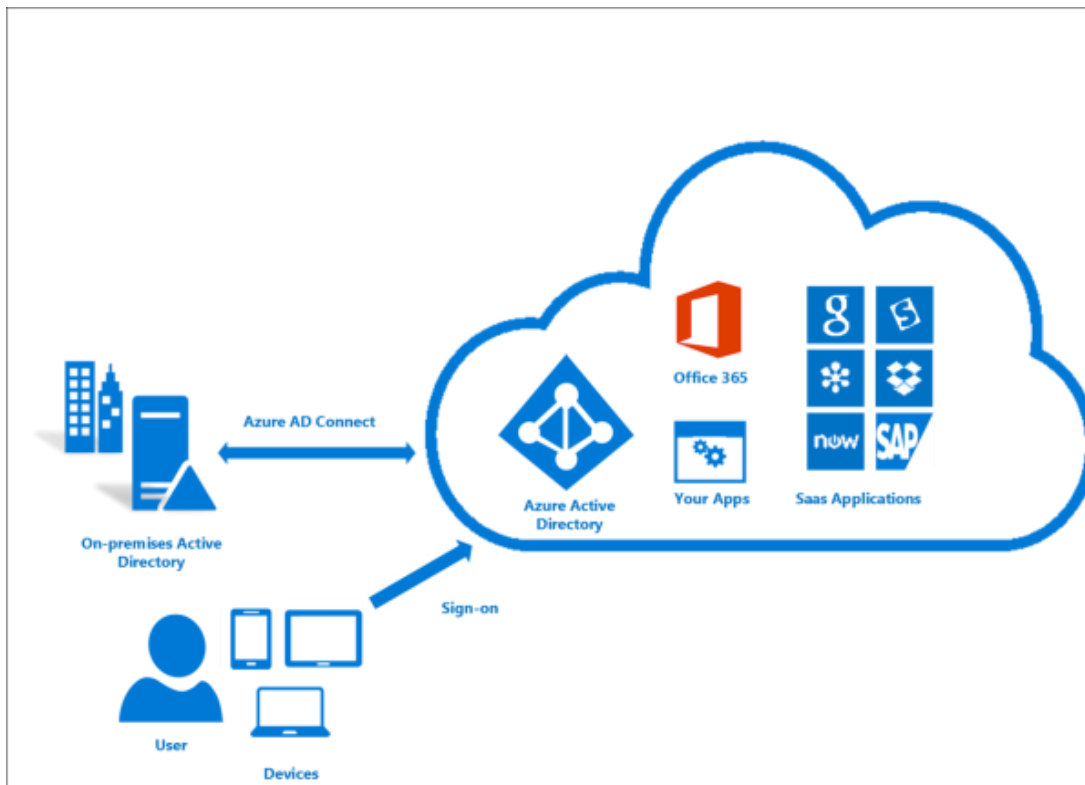
3 Microsoft Azure

Azure on Microsoftin pilvipalvelualusta, johon on yhdistetty yli 200 eri palvelua ja työkalua. Azurella voidaan rakentaa, ajaa ja hallita erilaisia applikaatioita ja pilvipalveluita yli erinäisten pilvipalvelimien ja paikallisten palvelimien. Azurea voidaan käyttää esimerkiksi erilaisiin integraatioihin, IoT-ratkaisuihin, virtuaalipalvelinten hallintaan, verkkopalveluiden hallintaan, käyttäjän/identiteetin hallintaan sekä tietoturvan ajantasaiseen ylläpitämiseen. Azuren sitoutuminen avoimen lähdekoodin ratkaisuihin mahdollistaa laajan räätälöinnin, jolla Azuresta saadaan korvaamaton työkalu minkä kokoisille yrityksille tahansa. (Microsoft, n.d.a)

3.1 Azure Active Directory

Azure AD (Active Directory) on Microsoftin pilvipohjainen identiteetin ja pääsynhallintapalvelu, jolla hallitaan yrityksen työntekijöiden kirjautumista ja autentikointia erinäisiin ulkoisiin ja sisäisiin resursseihin. Kuten esimerkiksi Microsoftin 365-palvelut, Azure portaali ja tuhannet muut SaaS-palvelut. Azure AD:lla voidaan myös hallita kirjautumisia yritysten sisäisiin sovelluksiin ja verkkopalveluihin. Kuva 1 havainnollistaa minkä tyyppisiä palveluita Azure AD tarjoaa, ja miten se yhdistyy loppukäyttäjiin ja mahdolliseen on-premise Active Directoryyn. Azure AD:ta käyttävät IT-järjestelmänvalvojat, sovelluskehittäjät sekä kaikki ketkä omaavat M365-tunnukset. IT-järjestelmänvalvojille Azure AD tarjoaa mahdollisuuksia laidasta laitaan, Azure AD:ssa hallinnoidaan mm. työntekijöiden tilejä, Teams-tiimejä, jakelulistoja, palvelimia, raportteja, VPN-yhteyksiä ja SQL-tietokantoja. (Microsoft, n.d.a)

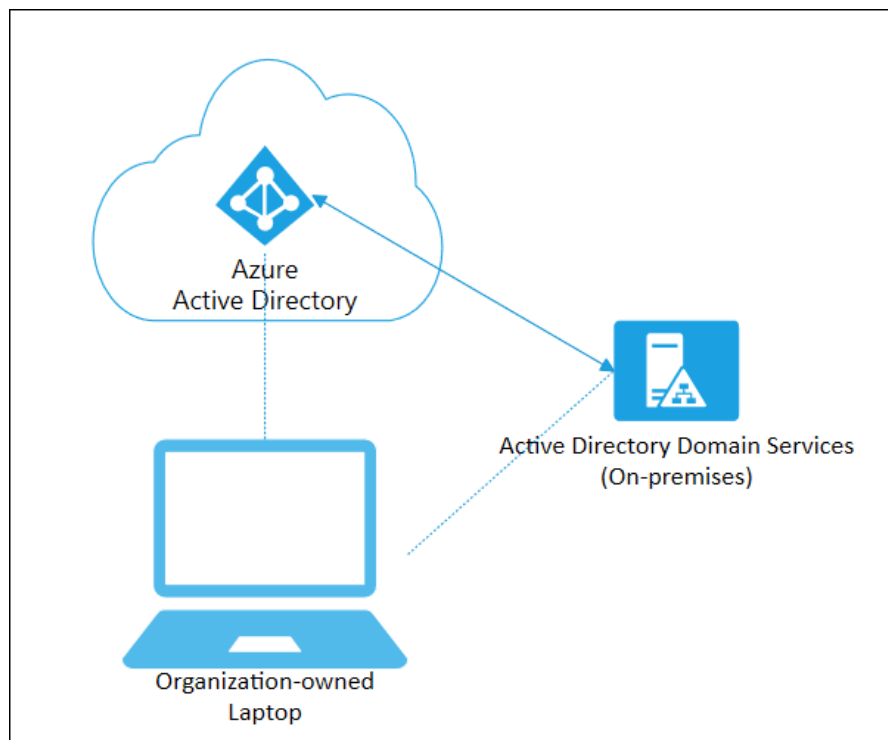
Kuva 1 - Azure AD Connect toimintalogiikka minkä mukaan Azure AD mahdollistaa yhdistämisen eri palveluihin. (Microsoft, n.d.i)



3.2 Hybrid Azure AD

Azure AD mahdollistaa hybridiympäristön käyttöönoton yritysten kohdalla, joilla on jo oma fyysinen palvelinympäristö ja perinteinen Active Directory käytössä. Yritykset voivat hyödyntää joitain Azure AD:n toiminnallisuuksia rekisteröimällä on-premise laitteet Hybrid Azure AD-laitteiksi. Tämän jälkeen laitteen objekti on näkyvissä sekä on-premise AD:ssa että Azure AD:ssa (kuva 2.). Tämä taas mahdollistaa suoraan lisenssien jakamisen sekä Conditional Accessin hyödyntämisen. Conditional Access lisää tietoturvaa ja pitää silti palveluiden käytettävyyden halutulla tasolla. Conditional Access mahdollistaa muun muassa monivaiheisen tunnistautumisen kirjautumisen yhteydessä, sekä kirjautumisen vain luotetuista laitteista. Tyypillisesti Hybrid Azure AD-laitteita otetaan käyttöön, jos yrityksellä on tarvetta käyttää Windows 7 tai 8.1 käyttöjärjestelmällä olevia laitteita, tarve käyttää ryhmäkäytäntöjä laitehallintaa varten tai tarve käyttää Win32-sovelluksia. (Microsoft n.d.b)

Kuva 2 - Hybrid Azure AD liitetty laite. (Microsoft, n.d.h)



3.3 Azure AD ja tietoturva

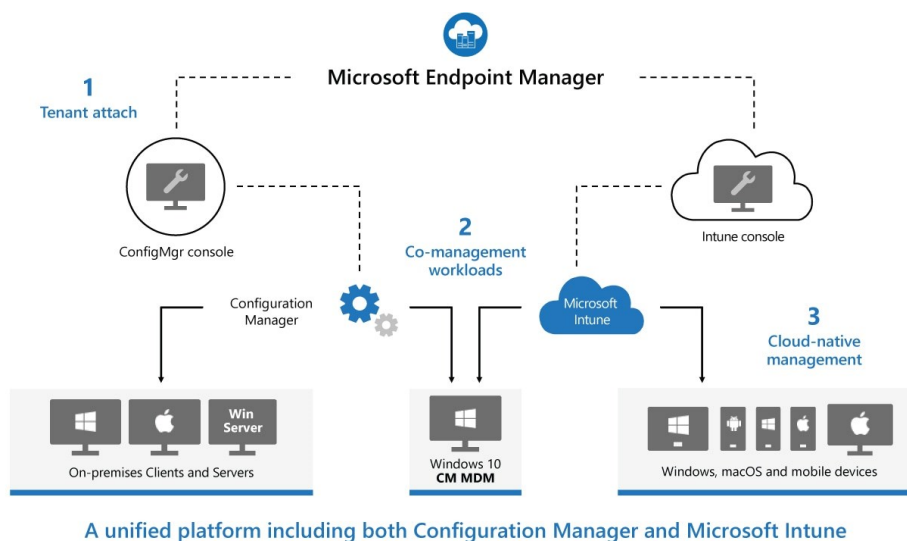
Azure AD mahdollistaa erinomaisen tietoturvan tason yhdistämällä useita eri tapoja parantaa tietoturvaa globaalisti koko yrityksen tasolla. Microsoftilla on kattava dokumentaatio, jossa käydään askel askeleelta läpi tarkistuslista, joka sisältää toimenpiteet hyvän tietoturvan saavuttamiseen. Dokumentaation alussa muistutetaan monivaiheisen tunnistautumisen tärkeydestä. Käytännössä tämä tarkoittaa sitä, että kirjautumisen yhteydessä on käyttäjätunnuksen ja salasanan lisäksi vahvistettava kirjautuminen joko tekstiviestillä, puhelulla tai Microsoft autentikaattorilla. Azure Active Directoryssa tapahtuu päivittäin 50 miljoonaa salasanahyökkäystä, silti vain 20 % kaikista käyttäjistä ja 30 % pääkäyttäjistä käyttävät monivaiheista tunnistautumista. Lokakuussa 2022 Microsoft edellyttää monivaiheisen tunnistautumisen käyttöönoton jokaisessa organisaatiossa. (Microsoft, n.d.c)

4 Microsoft Endpoint Manager

Microsoft Endpoint Manager on hallintaympäristö, mikä yhdistää Desktop Analytics-palvelun, Windows Autopilot-palvelun sekä Microsoft Intunen ja configuration managerin. Endpoint manager otettiin käyttöön SCCM:n technical preview versiossa 1901. Kuvassa 3. näkyy miten miten Microsoftin tekemät muutokset yhdistyvät nykyaikaisessa Endpoint Managerissa, mikä onnistuneesti yhdistää aiemmin erillään olleet palvelut yhdeksi kokonaisuudeksi.

Endpoint Managerissa hallinnoidaan päätelaitteita kuten tietokoneita, puhelimia, tabletteja sekä niiden tietoturvaa ja älykkäitä pilvitoimintoja. Microsoft Endpoint Manager hyödyntää Azure AD:ta laitteiden, käyttäjien, ryhmien ja MFA:n tunnistautumiseen. Microsoft Endpoint Managerin avulla mahdollistetaan päätelaitteiden päivitys pilvipalveluita hyödyntäen. Laitteet saadaan pidettyä ajan tasalla niin tärkeiden tietoturvapäivitysten kuin valinnaisten ohjelmistopäivitysten suhteen. (Microsoft, n.d.d) Forrester Consulting Total Economic Impact™ - tutkimuksen mukaan Microsoft Endpoint Managerin on todettu parantavan organisaation tietoturvaa ja pääoman tuottoa. (Forrester, 2021) Endpoint Manageria hyödynnetään myös sovellusten jakeluun mobiililaitteilla ja tietokoneilla.

Kuva 3 - Intunen ja Configuration managerin eri osa-alueet yhdistettynä uuteen Microsoft Endpoint Manageriin (Microsoft, n.d.e)

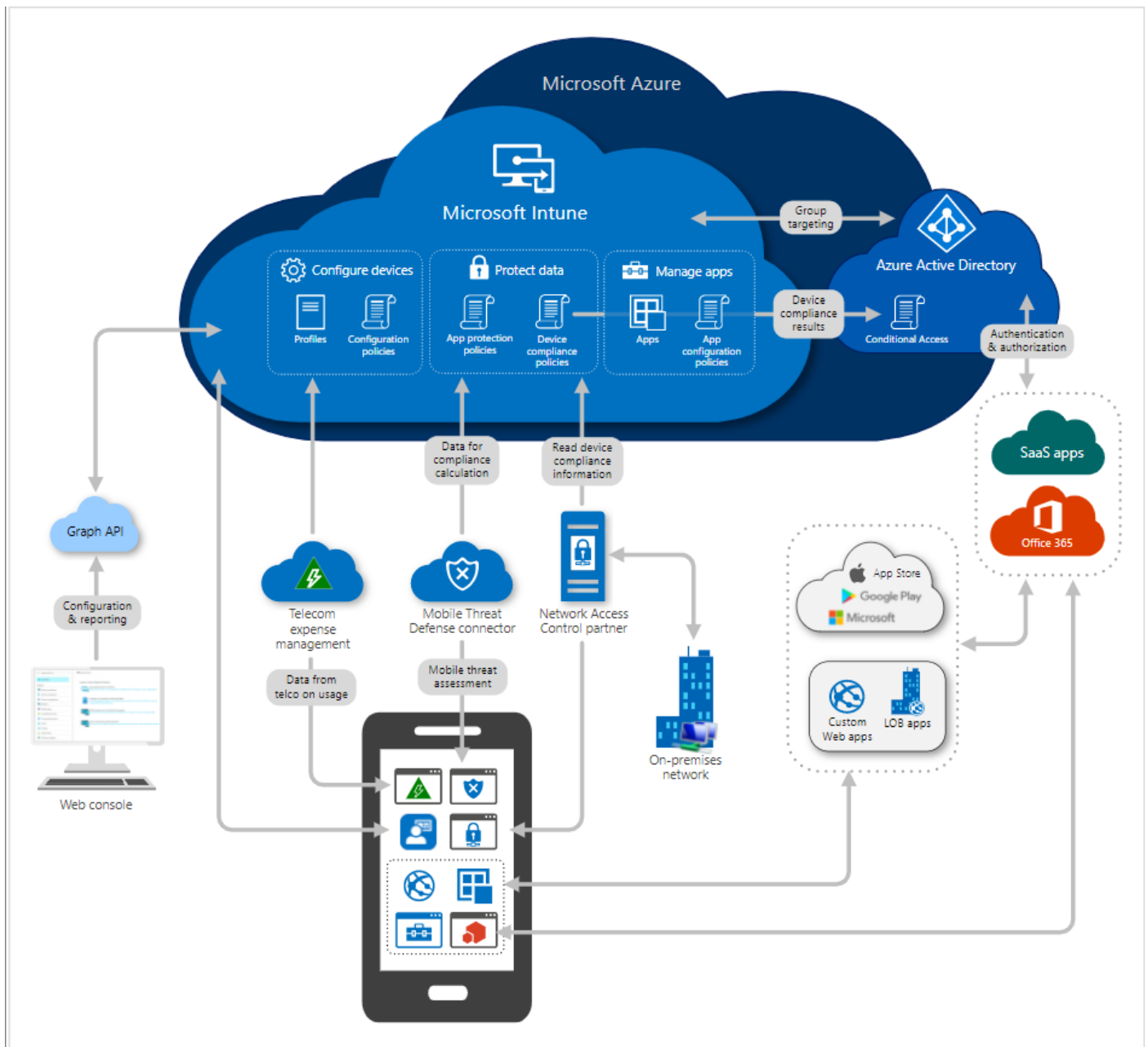


5 Microsoft Intune

Microsoft Intune on pilvipohjainen palvelu, jonka pääpaino on mobiililaitteiden sekä näille kuuluvien applikaatioiden hallinta ja ylläpito. Intune mahdollistaa käytäntöjen ja sääntöjen asettamisen, mitkä määrittelevät miten organisaation laitteita käytetään.

Seuraavaksi muutamia esimerkkejä yleisesti käytetyistä säännöistä ja politiikoista, mitä Intunella on mahdollista saavuttaa; Intunella voi estää esimerkiksi sähköpostien lähettämisen organisaation ulkopuolisille henkilöille, erottaa henkilökohtainen-, ja työpuoli laitteissa sekä halutessaan estää tiedostojen siirto näiden välillä keskenään. Tarkoituksena suojella organisaation dataa ja pitää henkilökohtainen data erillään organisaation datasta. Intunella voi jakaa ohjelmistoja sekä ohjelmistopäivityksiä paketteina loppukäyttäjille pilven ylitse, määritellä salasanaikäytäntöjä puhelimen lukitusnäyttöön sekä määritellä organisaatiossa käytettävien laitteiden ja sovellusten tietoturvamääritykset organisaation tietoturvamääritysten mukaisiksi. Intune on nykyään osa Microsoft Endpoint Manageria, millä pystytään hallitsemaan myös organisaation tietokoneita. (Microsoft, n.d.f) Kuvassa 4. näkyy Intunen toimintalogiikka, sekä miten se yhdistyy eri palveluihin ja järjestelmiin. Kuten loppukäyttäjän puhelimeen, laitteistopolitiikkoihin sekä mahdollisiin ulkoisiin SaaS-palveluihin.

Kuva 4 - Intunen arkkitehtuuri ja toimintalogiikka (Microsoft, n.d.g)

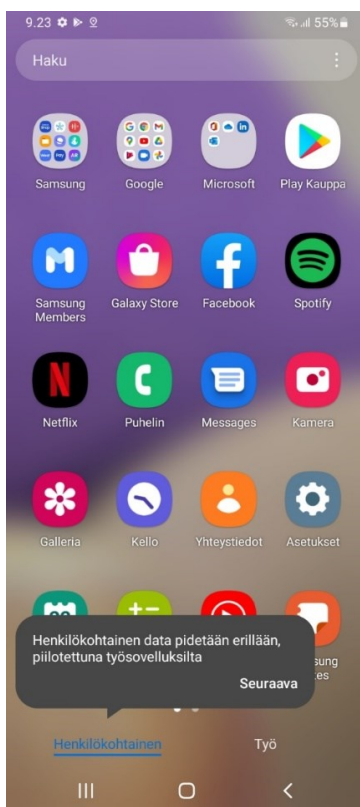


5.1 Intune MDM -käyttöönottoprofiilit Androidilla

Intune mahdollistaa laitteiden hallinnan organisaation tarpeisiin mukautuen ja tarjoaa laitteiden hallinnan osalta useamman eri käyttöönottoprofiilin, joista voi valita organisaatiolleen sopivimman. Näihin vaihtoehtoihin kuuluvat:

1. Personally-owned devices with work profile. Tätä vaihtoehtoa käytetään, jos työntekijällä on oma laite mikä halutaan rekisteröidä yrityksen hallintaan.
2. Corporate-owned dedicated devices. Tätä vaihtoehtoa käytetään laitteissa, joilla on joku selvä käyttötarkoitus ja laite ei ole kenenkään henkilökohtaisessa ja jatkuvassa käytössä (kiosk mode). Eli esimerkiksi jollain työpisteellä oleva yhteisessä käytössä oleva laite, jolla on useampi käyttäjä.
3. Corporate-owned fully managed user devices. Tämä vaihtoehto on yleisimmin käytössä yrityksen omistamissa laitteissa mitkä on määritetty henkilökohtaiseen käyttöön työntekijälle ja on tarkoitettu käytettävän vain työtehtäviin.
4. Corporate-owned devices with work profile. Tämä on yleinen vaihtoehto laitteille, joita työntekijä voi käyttää myös henkilökohtaiseen käyttöön, mutta työasiat ja data halutaan pitää erillään henkilökohtaisista asioista ja datasta. Tässä profiilissa työ-, ja henkilökohtainenprofiili on erotettu toisistaan ikään kuin välilehdillä ja niiden välillä kulkevaa dataa voidaan rajoittaa (kuva 5.). (Tolvanen. M, 2021)

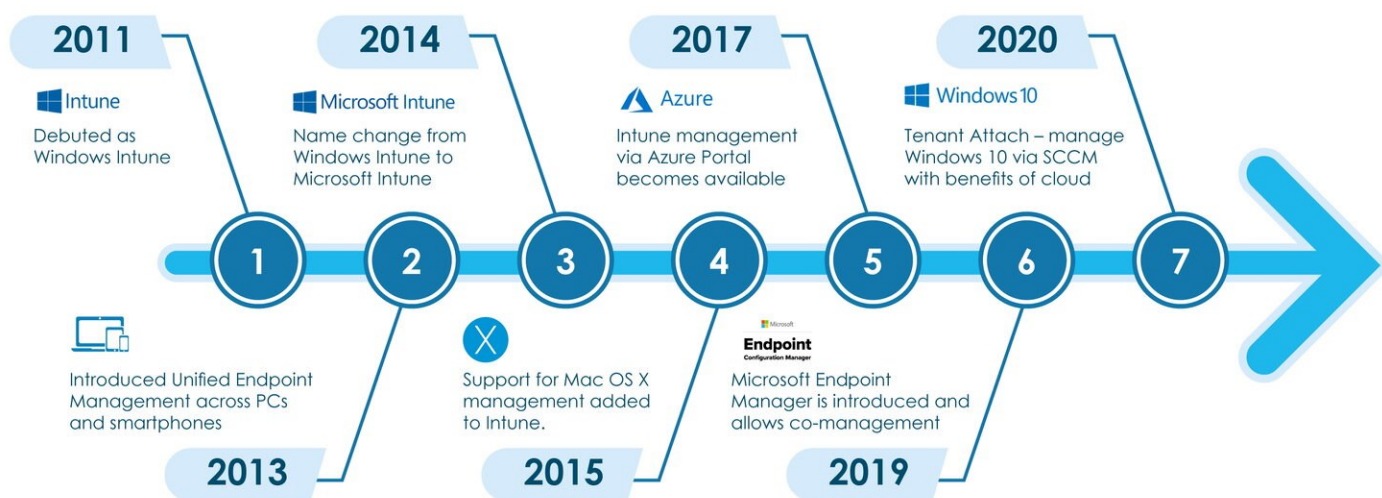
Kuva 5 – Corporate-owned devices with work profile-käyttöönottoprofiililla varustettu puhelimen valikko näkymä, jossa näkyy henkilökohtainen-, ja työpuoli eriteltynä välilehdillä.



5.2 Microsoft Intunen historiaa

Microsoft Intune tuli alun perin avoimeen beta testiin vuonna 2010 nimellä ”Windows Intune”, mitä seurasi virallinen julkaisu vuonna 2011. Intune tuki julkaisussaan Windows-7 käyttöjärjestelmää. Nykyaikana Intune tukee jo melkein kaikkia moderneja käyttöjärjestelmiä. Lukuun ottamatta unixia, linuxia tai windows serveriä. 2013 Intuneen lisättiin yhdistetty tietokoneiden ja mobiililaitteiden hallinta. Microsoft päivitti Windows Intunen nimen Microsoft Intuneksi vuonna 2014. Syynä tähän oli Microsoftin silloinen strategia Intunen brändäykselle. Nimi muutettiin Microsoft Intuneksi, koska Windows ei ollut enää ainoa käyttöjärjestelmä, jota Intunella oli mahdollista hallita. Tuolloin vaihtoehtoina olivat myös Android ja iOS. Tätä edelsi samana vuonna hieman aikaisemmin samankaltainen muutos Azuren nimeen, kun se muutettiin ”Windows Azure cloud computing platform” nimestä pelkästään ”Azureksi”. Tuki Mac OS X:lle lisättiin vuonna 2015. Vielä julkaisun aikaan tuki Macille oli tosi rajoitettua, mutta isoa kehitystä sen jälkeen on tapahtunut. Vuonna 2017 Intune lisättiin osaksi Azuren hallintaportaalia, ja 2019 osaksi Microsoft Endpoint Manageria, mikä toi mahdollisuuden hallita laitteita sekä Configuration Managerin että Intunen kautta. 2020 Endpoint manageriin lisättiin ”Tenant Attach”, mikä tarkoittaa yksinkertaistettuna organisaation yhdistämistä endpoint manageriin. Tällä mahdollistetaan esimerkiksi Configuration Managerissa olevien laitteiden hallinta Intunen portaalista käsin. Kuvassa 6. näkyy Intunen kehityksen historia aikajanan muodossa.

Kuva 6 – Microsoft Intunen tärkeimmät muutokset aikajananalla (Mobilementor, n.d.a)



6 Kehittämistyön tavoite ja tarkoitus

Tämän kehittämisprojektin tarkoituksena oli saada säästettyä keski-suuren yrityksen tietohallinnon, sekä loppukäyttäjien työtunteja automatisoimalla mobiililaitteiden käyttöönottoa ja sovellusten asennusta. Tarkoituksena oli myös parantaa laitteiden sekä yrityksen datan tietoturva.

Tavoitteena oli saada mobiililaitteet heti tilauksen yhteydessä yhdistymään yrityksen järjestelmiin, mikä mahdollistaa sovellusten automaattisen määrittämisen ja jakelun yrityksen työntekijöille. Tämä mahdollistaa myös yrityksen datan tyhjentämisen puhelimesta etänä, jos puhelin sattuisi katoamaan tai joutuisi varastetuksi.

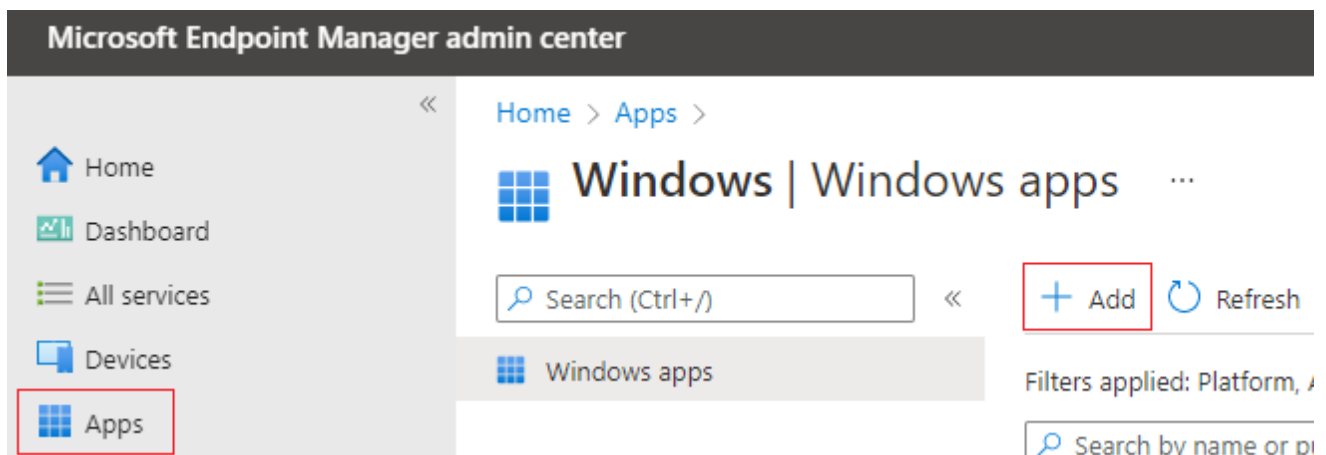
Käyttöönottoprojektin lopullisena tavoitteena on ollut kaikkien tulevien mobiililaitteiden automaattinen liittäminen Microsoft Intuneen. Työtä jatkokehitetään ja edistetään jatkuvasti myös opinnäyttetyön jälkeen.

Menetelmänä työssä on ollut kehittämisprojekti, työssä otettiin käyttöön Microsoft Intune MDM-mobiililaitteiden hallinta yrityksen mobiililaitteille. Menetelmän valinta oli tässä työssä itsestään selvää. Järjestelmään piti perehtyä, tehdä tarvittavat taustatutkimukset ja ottaa se projektiluontoisesti käyttöön tuotantoympäristöön. Tietoa on kerätty päiväkirjamaisesti työn edetessä.

7 Ohjelmistojen jakelu Windows 10/11 -käyttöjärjestelmiin Intunen avulla

Yrityksessä oli tähän asti toimintatapana, että tietohallinto manuaalisesti asentaa kaikki tarvittavat ohjelmistot jokaisen työntekijän koneeseen. Tähän toivottiin muutosta jo olemassa olevilla lisensseillä ja resursseilla. Luonnollinen ratkaisu oli hyödyntää jo käytössä olevaa Microsoft 365 Business Premium lisenssiä, jonka piiriin Intune kuuluu. Työssä käytetään esimerkkinä F-Secure Elements ohjelmistoa, jonka asennuspaketti on .msi – muotoa. Ohjelmistoja lisätään ja konfiguroidaan Microsoft Endpoint Manager - admin centerissä. Lisätäkseen ohjelmiston MEM:iin ensiksi pitää navigoida Apps->Windows->+Add (kts Kuva 7.).

Kuva 7 - Microsoft Endpoint Managerin näkymä, josta päästään lisäämään Windows-yhteensopivia ohjelmistoja



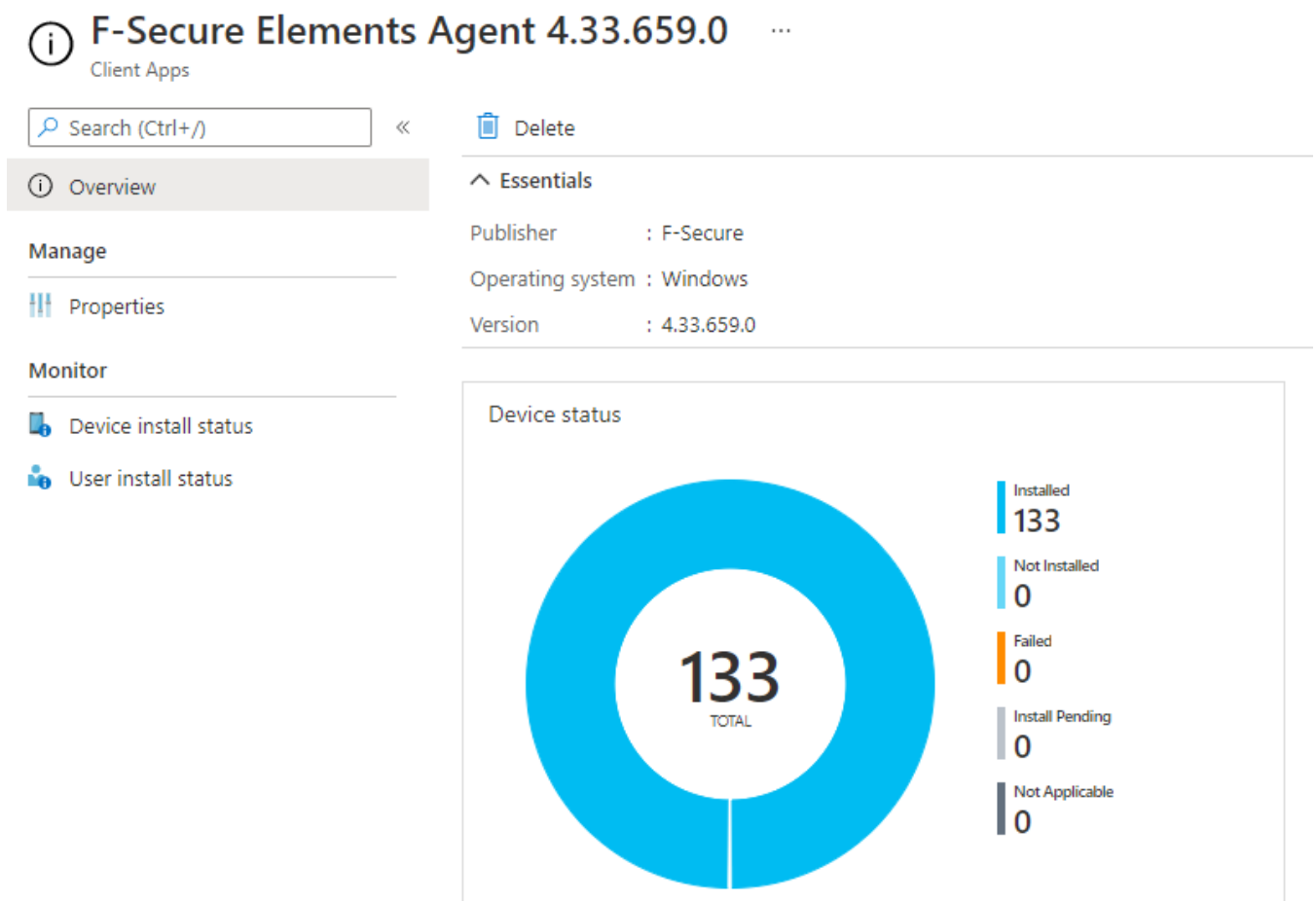
Tämän jälkeen valitaan ohjelmiston tyyppi. Tässä tapauksessa Line-of-Business ohjelmisto, johon sisältyy myös .msi-tiedostopäätteinen windows asennuspaketti. Sen jälkeen ladataan Azureen valitsemasi tiedosto, tässä tapauksessa F-Secure Elementsin .msi-asennuspaketti. Seuraavassa ikkunassa kirjataan tiedoston nimi, kuvaus, julkaisija ja laitetaan komentoriviargumentti, jolla ohjataan käynnistettävän ohjelman toimintaa loppukäyttäjän työasemalla. Tässä instanssissa laitamme argumentiksi "voucher=xxxx-xxxx-xxxx-xxxx-xxxx". X- merkkien tilalle laitetaan lisenssikoodi.

Sen jälkeen määrittelemme, kenelle ohjelmisto jaetaan. Nämä määitykset voidaan tehdä M365-ryhmien, käyttäjien ja laitteiden perusteella. Koska yritys haluaa virusturvan asennettavan kaikille

päätelaitteille, niin valitsemme ”+Add all users”. Seuraavassa ikkunassa tarkistetaan tähän asti syötetyt tiedot ja niiden oikeellisuus.

Ohjelmistojen päivittäminen riippuu pitkälti siitä, minkä tyyppistä ohjelmistoa Intunen avulla loppukäyttäjille jaetaan. Tässä tapauksessa, kun on F-Securen jatkuvasti verkkoon yhteydessä oleva ohjelmisto, joka osaa päivittää itsensä automaattisesti, ei siihen Intunen päästä tarvitse sen enempää muutoksia tehdä. Ohjelmiston monitorointinäköymästä voidaan tarkastella ohjelmiston asennus-statusta käyttäjä- ja laitekohtaisesti sekä konfiguroida asetuksia ja tehdä haluttuja muutoksia ohjelmistoon ja sen jakeluun loppukäyttäjille (kts. Kuva 8.).

Kuva 8 - Lisätyn ohjelmiston monitorointi ja konfigurointi näkymä



8 Intune MDM:n käyttöönotto

Työn tavoitteena oli saada Android laitteille työ-profiilit, jotka erittelevät työasiat henkilökohtaisista asioista. Profiilit mahdollistavat työpuhelimien käytön myös henkilökohtaisena laitteena ilman ylimääräistä yrityksen dataan kohdistuvaa tietoturvaaukkoa. Määritämme erinäisillä mahdollisilla säännöillä muun muassa laitteeseen pakolliseksi salasanan tai vastaavan tunnistautumisvaatimuksen puhelimeen sekä määrittelemme että työprofiilista ei voi siirtää tiedostoja henkilökohtaiselle puolelle.

Intuneen kytketyt mobiililaitteet voidaan myös etänä palauttaa tehdasasetuksille puhelimen kadotessa. Tällä pystytään turvaamaan tärkeitä asiakastietoja sekä muita yrityksen salaisia tietoja. Intune MDM:n käyttöönotto aloitetaan rekisteröitymällä tarvittaviin laiterekisteröintiohjelmiin sekä suorittamalla tarvittavat esivaatimukset Intunen päässä. Managed Google Play-tilin luominen on ensimmäinen askel. Managed Google Play-tili on organisaatioille suunnattu tilityyppi, jonka avulla voidaan hallita Google Play-aplien jakamista ja hallintaa organisaation työntekijöille. Managed Google Play-tili luotiin menemällä Endpoint Managerissa Devices->Android->Android Enrollment->Managed Google Play. Managed Google Playtä napsauttamalla aukeaa ikkuna, josta pääsee tekemään yrityksen "Managed Google Play – tilin". Tilin pystyy yhdistämään omalla domainilla olevalle sähköpostiosoitteelle kuvan 9. mukaisesti.

Kuva 9 - Onnistuneesti linkitetty Managed Google Play – tili. (organisaation tiedot piilotettu)

Managed Google Play

Android enrollment

Disconnect

^ Essentials

Status

Setup

Organization

Google account

Registration date

You must connect Intune to your company's managed Google Play account to manage Android enterprise devices. Follow the steps below to enable Android enterprise enrollment. [Learn more.](#)

1. I grant Microsoft permission to send both user and device information to Google. [Learn more.](#)

☒ I agree.
2. Connect your Intune tenant to an administrative Google account to enable Android enterprise enrollment.

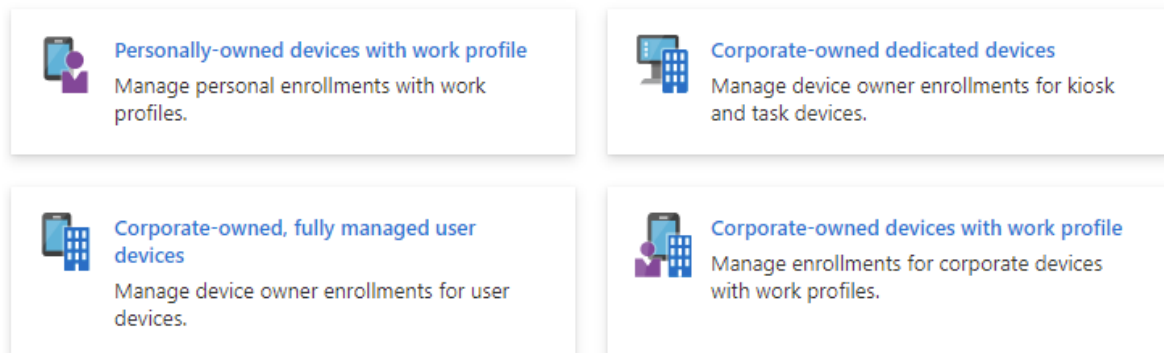
Launch Google to connect now.

8.1 Enrollment Profiili

Android-laitteita varten luodaan seuraavaksi Enrollment profiili, joka toimii hallintamallin profiilina. Vaihtoehtoina ovat kuvassa 10. näkyvät personally-owned devices with work profile, corporate-owned dedicated devices, corporate-owned fully managed user devices ja corporate-owned devices with work profile. Päädyimme corporate-owned devices with work profile (COPE) vaihtoehtoon, sillä se vastaa organisaation tarpeita parhaiten. COPE:ssa on mahdollista tehdä erillinen profiili, mikä toimii puhelimen käyttöjärjestelmässä ikään kuin välilehtenä, joka erottaa työ-, ja henkilökohtaisen puolen toisistaan. Profiilin teko tapahtuu nopeasti, klikataan Corporate-owned devices with work profile-painiketta ja kirjataan profiilille nimi ja kuvaus. Enrollment profiilista haetaan myöhemmin token, mikä käydään myöhemmin liittämässä laiterekisteröintiohjelman käyttöönottoprofiiliin. Täten palveluntarjoajalta ostettu laite, mikä ilmestyy automaattisesti laiterekisteröintiohjelmahan, ilmestyy myös Intuneen.

Kuva 10 – Intunen mobiililaitteiden enrollment-profiilit kuvauksineen

Enrollment Profiles



8.2 Dynaaminen laiteryhmä

Tässä vaiheessa tehtiin dynaamiset laiteryhmät, jotta pystymme kohdistamaan sovelluksia oikeille laitteille. Tämä mahdollistaa enrollatun laitteen automaattisen liittymisen oikeaan ryhmään ja sitä myötä oikeiden sovellusten latautumisen oikeisiin laitteisiin.

Ryhmät luotiin endpoint managerissa valitsemalla kotisivun navigointipalkista ”Groups” ja ”New group”. Tämän jälkeen täytettiin ryhmän nimi, kuvaus ja valitaan oikea group ja membership type ryhmälle. Group type on Security ja membership type on Dynamic Device, kun membership type on muutettu Dynaamiseksi laitteeksi, on mahdollista lisätä dynaamisia kyselyitä, jotka määrittelevät minkä mukaan laitteet liittyvät kyseiseen ryhmään. Samsungin laitteiden ryhmään teimme säännön, joka määrittelee, että jos laitteen valmistaja on yhtä suuri kuin ”Samsung” niin laite liittyy tähän dynaamiseen laiteryhmään. Toinen hyvä vaihtoehto on käyttää kyselyä, joka liittää laitteen ryhmään laitteen enrollment-profiilin nimen perusteella (kuva 11.).

Kuva 11 - Hyviä vaihtoehtoja kyselyille, joilla liittää laite oikeaan dynaamiseen laiteryhmään.

Property	Operator	Value
enrollmentProfileName	Equals	Profiilin nimi
deviceManufacturer	Contains	samsung

8.3 Laiterekisteröintiohjelmat

Laiterekisteröintiohjelmilla pidetään huolta, että yrityksen omistuksessa olevat laitteet siirtyvät heti tilaushetkestä yrityksen mobiililaitteiden hallintaan (MDM), tässä tapauksessa Intuneen. Tällä varmistutaan siitä, että laitteet ovat alusta loppuun koko elinkaarensa ajan yrityksen omistuksessa. Laitetta ei saa asennettua henkilökohtaiseen käyttöön ennen kuin se poistetaan laiterekeröintiohjelmasta. Android laitteita varten luotiin tässä tapauksessa tunnukset ja profiilit kahteen eri laiterekeröintiohjelmiaan, toinen Samsung-laitteita ja toinen OnePlus-laitteita varten.

8.3.1 Samsung Knox Mobile Enrollment (KME)

Samsung Knox on Samsungin laiterekeröintiohjelma, jolla saadaan muun muassa suoraan jälleenmyyjältä tilatut laitteet yhdistettyä mobiililaitteiden keskushallintaan, tässä tapauksessa Microsoft Intuneen. palvelun rekisteröinti ja käyttö on ilmaista. Samsung laitteita varten tarvitsee rekisteröidä Samsung-tunnus ja ottaa käyttöön Samsung Knox Portaali. Kun tunnus on tehty ja yrityksen tiedot täytetty navigoidaan Knox Portaaliin. Knox Portaalista haetaan Knox Mobile Enrollment -ohjelman jäsenyyttä, jonka Samsung aktivoi itse tehtyään tarvittavat taustatyöt yrityksestä kelle laiterekeröintiohjelma ollaan avaamassa. Kyseisissä taustatöissä voi kestää useasta päivästä useaan viikkoon.

Kun Samsung on hyväksynyt pyynnön, navigoidaan varsinaiseen KME-portaaliin. Portaaliin lähdetään liikkeelle siitä, että luodaan kaikille ylläpitäjille tarvittavat henkilökohtaiset tunnukset. Tunnus, jolla KME-profiili on otettu käyttöön, on oletuksena "Super Admin" – roolissa. Knox Portaaliin siirrytään kohtaan "Administrators & Roles" ja kutsutaan ylläpitäjät "Invite Administrator" napin takaa ylläpitämään laitteita ja asetuksia. Ylläpitäjää kutsuessa valitaan rooliksi "Admin" ja määritellään yksityiskohtaisesti oikeudet kutsutulle käyttäjälle. Seuraava vaihe on luoda tuleville laitteille käyttöönottoprofiili. Päävalikon "Knox Mobile Enrollment" painikkeen takaa löytyy "Profiles" ja sen takaa "Create Profile". Vaihtoehtoina ovat Android Enterprise ja Device Admin, joista valitaan Android Enterprise. Seuraavassa ikkunassa valitaan profiilille kuvaava nimi, kuvaus ja MDM-tyyppi. MDM-tyypiksi valitaan Microsoft Intune ja MDM Agent APK-kohtaan laitetaan latauslinkki, josta päätelaite lataa MDM-lisäosan puhelimeen.

rekisteröitymistä varten. Linkki löytyy muun muassa Microsoftin ja Samsungin dokumentaatiosta. Seuraavassa vaiheessa määritetään Android Enterprise profiilin asetukset. Asetuksissa ensimmäisenä kohtana on ”MDM Configuration”. Tähän kohtaan haemme aiemmin Microsoft Endpoint Manageriin luodusta enrollment profiilista tokenin ja liitämme sen seuraavan kuvan JSON-datan sisään lainausmerkkien sisälle. Muut kohdat asetuksista voikin sitten määrittää tapauskohtaisesti, tässä tapauksessa pärjättiin oletusasetuksilla.

Ohjelmakoodi 1 - JSON-data, jolla yhdistetään Knoxin käyttöönottoprofiili Intunen Enrollment profiiliin.

MDM CONFIGURATION

Custom JSON Data (as defined by MDM) ⓘ

```
{"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN":"TÄHÄNTOKENINTUNESTA"}
```

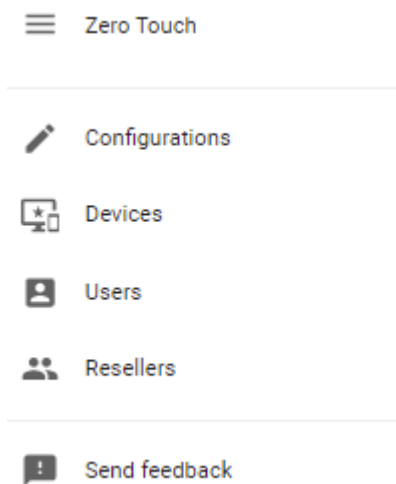
Seuraavaksi on vuorossa jälleenmyyjän rekisteröinti laiterekisteröintiohjelmaan. Tämä mahdollistaa sen, että jälleenmyyjältä ostettu puhelin ilmestyy suoraan laiterekisteröintiohjelmaan ja äskeisten konfiguraatioiden myötä myös Intuneen. Käytännössä tämä tapahtuu siten, että haetaan ”Resellers” kohdan takaa Knox Customer ID ja ilmoitetaan se jälleenmyyjälle. Vastaavasti sitten jälleenmyyjältä pyydetään Knox Reseller ID joka rekisteröidään Knoxin portaaliin. Jälleenmyyjää rekisteröitäessä Knoxin portaaliin valitaan että tältä jälleenmyyjältä ostetut laitteet hyväksytään ja lisätään automaattisesti portaaliin ja sen lisäksi kohdistetaan aiemmin tehty profiili tuleviin laitteisiin. Tämän jälkeen jälleenmyyjältä ostamat laitteet ilmestyvät ”Devices” kohdan alle Knoxin portaaliin.

8.3.2 Android Zero-touch Enrollment (ZT)

Android Zero-Touch Enrollment portaali on huomattavasti yksinkertaisempi ja sisältää vähemmän valintoja ja vaihtoehtoja kuin Samsungin Knox Portaali. Ajatus ja käyttötarkoitus ovat kuitenkin sama. Toisin kuin KME:n käyttöönotossa, Zero-Touchin käyttöönotossa ei tarvitse odottaa vahvistuksia ja erinäisiä hyväksymisprosesseja. ZT:n tapauksessa voit vain pyytää jälleenmyyjääsi

avaamaan portaalin yrityksellesi. Zero-Touch portaalin käyttöliittymä on erittäin selkeä ja yksinkertainen. Mahdollisuuksia tehdä muutoksia ja säätöjä portaalin päässä on huomattavasti vähemmän kuin Samsungilla.

Kuva 11 - Zero-Touch portaalin käyttöliittymän päävalikko



Ensimmäinen askel ZT-portaalissa on sama kuin Knox Portaalissa, eli kutsutaan tarvittavat Admin käyttäjät. Users-painikkeen takaa löytyy ”+”-painike, jonka takaa kutsutaan käyttäjiä (kuva 11.). Sen jälkeen syötetään kutsuttavan henkilön sähköpostiosoite sekä tälle haluttu rooli (Admin tai Owner). Tämän jälkeen konfiguroidaan ZT-portaaliin käyttöönottoprofiili, joka yhdistetään tokenilla varsinaiseen Intunen käyttöönottoprofiiliin/hallintamalliin samaan tyyliin kuin Knoxilla. ZT-portaalin käyttöönottoprofiilin luominen onnistuu painamalla päävalikon ”Configurations” painiketta (kuva 10.) ja sen jälkeen painamalla ”+” painiketta. Seuraavaksi päätetään konfiguraatiolle kuvaava nimi, ja valitaan EMM DPC, eli MDM:n palveluntarjoaja. Tässä tapauksessa se on Microsoft Intune. Konfiguraatio kysyy myös organisaation nimeä, support sähköpostiosoitetta sekä support puhelinnumeroa. Tähän laitettut tiedot ovat loppukäyttäjälle suunnattuja. Laitettu sähköpostiosoite ja puhelinnumero näkyvät puhelimen käyttöönotossa, joista loppukäyttäjä voi tarvittaessa pyytää apua ongelmatilanteessa. Tärkein kohta kuitenkin on DPC extras, johon tulee vastaava JSON-koodi samoin kuin Knoxin profiilin luonnissa. Tällä yhdistetään ZT:n käyttöönottoprofiili varsinaiseen Intunen käyttöönottoprofiiliin. (kuva 12.)

Ohjelmakoodi 2 - JSON-data, jolla yhdistetään ZT-käyttöönottoprofiili Intunen käyttöönottoprofiiliin/hallintamalliin.

DPC extras

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
  "com.google.android.apps.work.clouddpc/.receivers.CloudDeviceAdminReceiver",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
  "I5YvS005hXY46mb01BIRjq4oJJGs2kuUcHvVvKAPEXlg",

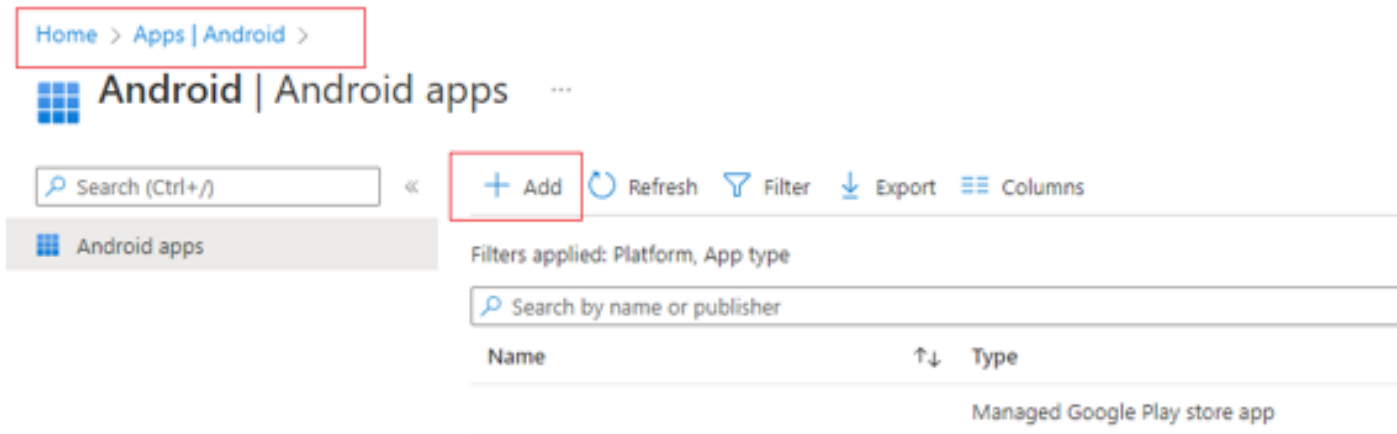
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
  "https://play.google.com/managed/downloadManagingApp?identifier=setup",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
    "com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN": "INTUNETOKENITÄHÄN"
  }
}
```

8.4 Sovellusten lisääminen ja jakelu

Intunessa sovelluksia saadaan lisättyä ja jaettua loppukäyttäjille navigoimalla Endpoint Managerin kotinäkömystä Apps, jonka jälkeen halutun käyttöjärjestelmän mukaan valitaan yksi, tässä tapauksessa Android. Tämän jälkeen avautuu näkymä, tässä tapauksessa "Android Apps". Täältä voidaan lisätä applikaatioita painamalla "+Add"-painiketta kuvan 12. mukaisesti. Tämän jälkeen valitaan Applikaation tyyppi "Managed Google Play Store App".

Kuva 12 – Android ohjelmien lisäys endpoint managerissa



Tämän jälkeen aukeaa ikään kuin virtualisoitu Google Play -kauppa, josta löytyy kaikki Google Play -kaupassa olevat sovellukset. Hakupalkista haetaan toivottua applikaatiota ja hyväksytään se osaksi applikaatiokirjastoasi sekä painetaan yläpalkissa näkyvää "Sync" painiketta. Tämän jälkeen palataan edelliseen kohtaan "Android Apps" ja päivitetään listaus. Applikaatio ilmestyy listaan heti, kun synkronointi on valmis. Prosessi pyörii taustalla ja sitä ei näe, mutta on yleensä todella nopea ja applikaatio nähtävillä melkein saman tien. Sen jälkeen avataan listasta haluttu applikaatio auki, joka avaa applikaation monitorointi- ja hallintanäkymän. Näkymässä näkee muun muassa sovelluksen kehittäjän, sekä kuinka monelle laitteelle sovellus on asennettu.

Seuraavaksi vasemmalta valitaan "properties". Tämä avaa näkymän, joka näyttää sovelluksen tiedot vielä tarkemmin. Sovelluksen kehittäjän, sovelluksen kuvauksen ja nimen, linkin Google Play -kauppaan sekä sovelluksen logon. Näiden alapuolella on kohta "Assignments" ja sen vieressä edit-painike. Edit-painikkeen takaa pystytään määrittämään se, latautuuko sovellus loppukäyttäjien laitteisiin suoraan vai haluaako sen yrityspuolen Google Play -kauppaan ladattavaksi, jossa näkyy vain sovellukset, jotka on erikseen asetettu sinne näkyviksi ja ladattaviksi (Kuva 13.). Eli käytännössä määritellään sovelluksen käyttö pakolliseksi tai vapaaehtoiseksi.

Määritykset tehdään M365-ryhmien avulla. Näin voidaan myös määritellä erinäisillä dynaamisilla säännöillä tiettyjä appeja tietyille laite- tai henkilöryhmille. Samasta paikasta on myös mahdollista määritellä sovelluksen poisto vain tietyiltä käyttäjiltä tai ryhmiltä sen sijaan, että poistaisi koko sovelluksen organisaation sovelluskirjastosta.

Kuva 13 – Applikaatioiden Assignments-valikko, josta määritellään applikaatioiden käyttäjät

Edit application ...

Managed Google Play store app

Assignments Review + save

Required ⓘ

Group mode Group

[+ Included](#) All users

[+ Add group](#) ⓘ [+ Add all users](#) ⓘ [+ Add all devices](#) ⓘ

Available for enrolled devices ⓘ

Group mode Group

No assignments

[+ Add group](#) ⓘ [+ Add all users](#) ⓘ

Available with or without enrollment ⓘ

Group mode Group

No assignments

[+ Add group](#) ⓘ [+ Add all users](#) ⓘ

Uninstall ⓘ

Group mode Group

No assignments

[+ Add group](#) ⓘ [+ Add all users](#) ⓘ [+ Add all devices](#) ⓘ

Review + save

Cancel

9 Johtopäätökset ja pohdinta

Opinnäytetyön tavoitteena oli ottaa käyttöön Microsoft Intune MDM, mobiililaitteiden hallinta- ja ylläpitotyökalu, jolla voitaisiin paremmin hallita ja pitää kirjaa yrityksen laitteista, näiden applikaatioista sekä siitä, että yrityksen laitteet ovat tietoturvapäivitysten osalta ajan tasalla. Intune MDM on otettu yrityksessä käyttöön, joten opinnäytetyön tavoitteessa on onnistuttu. Jatkossa kaikki yritykselle tilattavat mobiililaitteet menevät suoraan Intunen hallinnan piiriin.

Esittämiini tutkimuskysymyksiin sain mielestäni kattavasti vastauksia. Intunen käyttöönotolla saatiin kehitettyä yrityksen IT-infraa eteenpäin. Jatkossa kaikki uudet mobiililaitteet ilmestyvät suoraan tilauksen jälkeen Intunen hallintaportaaliin, josta selviää laitteen käyttäjä, sarjanumero sekä käyttöönoton päivämäärä. Intune soveltuu yritykselle hienosti. Tavoite oli saada kattava kirjanpito laitteista, käyttäjistä ja sarjanumeroista samaan paikkaan. Sen lisäksi Intunen käyttöönotto on vahvistanut yrityksen tietoturvaa mahdollistamalla näytönlukituksien edellytyksiä ja salasana vaatimuksia laitteille. Intunen kuuluessaan jo olemassa oleviin lisensseihin, ylimääräisiä kustannuksia tästä työstä ei yritykselle muodostunut lainkaan.

Jatkokehitysmahdollisuuksia Intunen mobiililaittehallinnalle on lukemattomia ja ideoita sekä ajatuksia onkin jo näistä kertynyt useampia. Esimerkiksi tarkempia tietoturva konfigurointeja ja VPN ratkaisuja. Niiden toteutus onkin kiinni siitä, että miten yrityksessä halutaan priorisoida työtuntien käyttö jatkossa tähän projektiin liittyen.

Toimeksiantajan mukaan nykyisen laitekannan (>250 tietokonetta ja >350 iOS/Android -laitetta) elinkaaren hallintaan MDM -järjestelmän käyttöönotto tuo selkeitä työ- ja kustannussäästöjä. MDM -järjestelmällä voidaan varmistaa, että laitteiden omistajuus teknisesti säilyy yrityksen hallinnassa laitteiden siirtyessä elinkaaren eri vaiheissa . Järjestelmällä voidaan myös automatisoida laitteiden käyttöönottoa, niiden tietoturvaa sekä toimivuutta voidaan keskitetysti parantaa ja myös valvoa.

Helpoin esimerkki elinkaarisäästöistä tulee jo pelkästään laitteen siirtyessä eri vaiheisiin elinkaaren vaiheissa. Työsäästö muodostuu ensin IT -organisaatiolle siitä, että laite toimitetaan suoraan loppukäyttäjälle ilman IT -organisaation työpanosta lukuunottamatta laitetilausta. Seuraavaksi itse

käyttäjä säästää työaikaansa saadessaan hänelle määritetyt perusapplikaatiot, kuten Office:n, sähköpostin sekä muita määritetty ohjelmistoja. Tämän jälkeen työaikasäästöä muodostuu laitteen palautuessa käyttäjältä: Usein keskushallinnoimattomien laitteiden palautuessa laitteet on rekisteröity työntekijän itse omistamalle iCloud tai Google -tilille, ja niiden omistusten liitosten poistaminen etänä ei aina onnistu tai niitä ei muisteta tehdä. Usein laitteiden omistajuus joudutaan todistamaan ostokuitein, mikä tarkoittaa useimmiten kohtuutonta selvitystyötä laitteen jäljellä olevaan käyttöikänsä nähden. Intuneen liitettyjen laitteiden osalta tällaista ongelmaa ei ole lainkaan.

Elinkaarisäästöjen lisäksi keskushallinnointi on osa nykyaikaista tietoturvaa: Laitteiden päivittäminen, asetukset ja asennetut ohjelmistot sekä niiden päivitykset määrittävät mahdollisen tietoturvahyökyksen helppouden. Yrityksen keskushallinnointi on helpottanut ja eritoten antanut mahdollisuuden estää ja parantaa käyttäjien tietoturvan näkökulmasta korkean riskitason valintoja: Intunella on määritetty mm. millä tasolla laite on salattu, kuinka monimutkainen suojakoodi tai salasana laitteella täytyy olla ja minkälaisia muita suoja-asetuksia laitteelle yleensä saa tai pitää vähimmillään määrittää.

10 Yhteenveto

Tutkintakysymyksiin saatiin mielestäni hyvin vastauksia. Intunella saatiin automatisoitua ohjelmiston jakelua mobiililaitteisiin sekä Windows-laitteisiin. Näin ollen sain kehitettyä ja automatisoitua aiempaa manuaalista työtä. Laitteiden elinkaariseuranta on myös nyt paremmin seurattavassa muodossa, kun kaikki askeleet löytyvät pilvipalvelusta. Työllä säästettiin myös jatkoa ajatellen resursseja, kun ohjelmistoja ei tarvitse enää asentaa käsin.

Teoriaosassa halusin käsitellä Microsoft Azurea kokonaisuutena, sekä Azuren alla toimivaa Endpoint Manageria että Intunea. Opinnäytetyön aikana opin itse myös paljon lisää Azuren, Endpoint Managerin sekä Intunen historiasta. Lisäksi opin myös paljon siitä, miten osa tietyistä Azuren osa-alueista yhdistyi vuosien mittaan kokonaisuudeksi nimeltä Endpoint Manager. Vaikka lähteiden määrä ei ole valtava, Microsoftin dokumentaatio sekä eri pilviasiantuntijoiden blogit mahdollistivat erinomaisesti työn etenemisen sekä aiheeseen perehtymisen.

Käytännön osa koostui Intune-palvelun ja laitevalmistajien rekisteröintipalveluiden käyttöönotosta mobiililaitteille, sekä sovelluspakettien jakelusta Mobiili- ja Windowslaitteille. Ongelmia määrittämyksen aikana ei tullut ilmi. Työ aloitettiin laiterekisteröintipalveluiden käyttöönotolla, jota seurasi Microsoft Intunen käyttöönotto. Tämän jälkeen käytiin läpi ohjelmistojen jakelua Intunen avulla sekä mobiili että pc-laitteille.

Lähteet

Amazon AWS (n.d.a) What is cloud computing? Viitattu 15.8.2022

<https://aws.amazon.com/what-is-cloud-computing/>

Bigelow, S. & Wesley, C. (n.d.b) Definition cloud computing Viitattu 15.8.2022

<https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing>

Eronen, H. (2021) IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi Viitattu 5.12.2022

<https://www.planeetta.fi/2016/03/15/iaas-paas-saas-mika-pilvipalvelu-sopii-yrityksellesi/>

Forrester (2021) THE TOTAL ECONOMIC IMPACT™ OF MICROSOFT ENDPOINT MANAGER Viitattu 15.7.2022

<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWCpyn>

Microsoft (n.d.a) What is Azure Active Directory? Viitattu 21.7.2022

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is>

Microsoft (n.d.b) Hybrid Azure AD joined devices Viitattu 21.7.2022

<https://docs.microsoft.com/fi-fi/azure/active-directory/devices/concept-azure-ad-join-hybrid>

Microsoft (n.d.c) Five steps to securing your identity infrastructure Viitattu 27.8.2022

<https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online>

Microsoft (n.d.d) Microsoft Endpoint Manager Viitattu 1.9.2022

<https://www.microsoft.com/en-us/security/business/microsoft-endpoint-manager>

Microsoft (n.d.e) Microsoft Endpoint Manager overview Viitattu 14.8.2022

<https://docs.microsoft.com/en-us/mem/endpoint-manager-overview>

Microsoft (n.d.f) Microsoft Intune is an MDM and MAM provider for your devices Viitattu 5.8.2022.

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>

Microsoft (n.d.g) High-level architecture for Microsoft Intune Viitattu 1.8.2022

https://learn.microsoft.com/en-us/mem/intune/fundamentals/media/high-level-architecture/intunearchitecture_wh.svg

Microsoft (n.d.h) Hybrid Azure AD joined devices Viitattu 21.7.2022

<https://learn.microsoft.com/en-us/azure/active-directory/devices/media/concept-azure-ad-join-hybrid/azure-ad-hybrid-joined-device.png>

Microsoft (n.d.i) What is Azure AD Connect? Viitattu 25.7.2022

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/media/whatis-hybrid-identity/arch.png>

Mobilementor (n.d.a) Microsoft Intune: A Journey to Market Leader Viitattu 1.8.2022

<https://images.squarespace-cdn.com/content/v1/5e740c8fcb9fdf4154a1c6a4/1600701638319-WAFOD3IDHQX2HUIR7OI9/Intune+Journey+to+Market+Leader.jpg?format=1500w>

Puneet, B. (2022) Azure Active Directory (Azure AD): Everything You Need To Know Viitattu 29.8.2022

<https://k21academy.com/microsoft-azure/az-303/azure-active-directory-azure-ad/>

Tolvanen, M. (2021) Moderni mobiililaittehallinta tutuksi – esittelyssä hallintamallit android-laitteille Viitattu 13.8.2022

<https://yrityksille.elisa.fi/ideat/moderni-mobiililaittehallinta-tutuksi-esittelyssa-hallintamallit-android-laitteille/>

Liite 1: Aineistonhallintasuunnitelma

Opinnäytetyössäni käyttämä aineisto on pääosin julkisista Microsoftin dokumentaatioista sekä erinäisistä artikkeleista, mitkä ovat asianmukaisesti merkittynä lähdeluetteloon. Aineisto ja kuvat, mitkä ovat opinnäytetyöni toimeksiantajan organisaatiosta, on toimeksiantajan pyynnöstä esitetty niin, että organisaatio tai siihen liittyviä yksilöitäviä tietoja ei käy ilmi käyttämästäni aineistosta tai kuvista. Soveltavassa osiossa luodut kuvat ovat itse otettuja opinnäytetyön toimeksiantajan M365-ympäristöstä. Opinnäytetyötä ja siihen liittyvää aineistoa säilytetään omalta osaltani 1 vuosi opinnäytetyön hyväksymispäivämäärästä.

Kehitysprojekti:

Opinnäytetyö sekä siinä käytetyt muistiinpanot ja dokumentit ovat tallennettuina asiakkaan M365-ympäristön henkilökohtaiselle OneDrive-tililleni sekä työkäytössä olevan kannettavani kovalevyille. Kannettavalle tietokoneelle kirjautuminen on suojattu MFA:lla. Opinnäytetyössä luotu varsinainen lopputulos on salattu ja löytyy vain yrityksen global adminille, eli pääkäyttäjille, opinnäytetyön toimeksiantajan organisaation pilvipalveluista (Azure, Endpoint manager).