HAMK
Hämeen ammatti-
korkeakoulu

Pilvipalvelut Finnvera Oyj:n IT-ympäristössä

Pilvipalveluiden vertailu

Ammattikorkeakoulun opinnäytetyö
Tieto- ja viestintätekniikka, insinööri (AMK)
Kevät 2024
Janne Haatanen

HAMK
Hämeen ammatti-
korkeakoulu

Tieto- ja viestintätekniikka
Tekijä Janne Haatanen
Työn nimi Pilvipalvelut Finnvera Oyj:n IT-ympäristössä
Ohjaaja Teemu Järvenpää

Tiivistelmä
Vuosi 2024

Tällä opinnäytetyöllä oli kaksi päätavoitetta. Ensimmäinen tavoite oli ottaa selvää pilvipalveluista, joista voisi olla hyötyä toimeksiantajalle. Toinen tavoite oli selvittää, miksi toimeksiantaja on valinnut nykyisen pilvipalveluratkaisunsa. Opinnäytetyön toimeksiantajana toimi Finnvera Oyj.

Pilvipalvelut yleistyvät monella eri alalla ja opinnäytetyössä käytiin läpi pilvipalveluiden erilaisia muotoja sekä niille olennaisia termejä, kuten julkinen pilvipalvelu ja yksityinen pilvipalvelu. Opinnäytetyön tutkimusosassa käytiin läpi kolmea eri pilvipalvelua, Microsoft Entraa, Amazon Web Servicen palveluita sekä Google Cloudia. Pilvipalveluita tarkasteltiin niiden laite- ja käyttäjähallinnan osalta.

Microsoftin Entraa käytiin huomattavasti eniten läpi opinnäytetyön aikana. Entrasta tuotiin esille sen hyviä laite- sekä käyttäjähallinnan ominaisuuksia. Kolmesta vertailutusta pilvipalvelusta, Entra oli lupaavin toimeksiantajan tarpeisiin nähden. Amazon Web Servicen palveluista käytiin läpi WorkSpacesia, OpsWorksia sekä hieman Systems Manageria. Amazon Web Servicen tarjoamat palvelukokonaisuudet osoittautuivat olemaan liian hankalia sekä laajoja toteuttaa niistä saataviin hyötyihin nähden. Amazon Web Servicen palveluissa, tämän opinnäytetyön selvityksen perusteella, ei löydy suoraan vertaista palvelua kuin Microsoftilla. Kolmas pilvipalvelu, jota käytiin läpi opinnäytetyössä, oli Google Cloud ja tarkemmin Google Endpoint Management. Google Endpoint Management osoittautui potentiaaliseksi järjestelmäksi laitteiden hallintaa varten. Google Endpoint Managementista kumminkin puuttui ominaisuuksia, joita esimerkiksi Microsoft tarjoaa, kuten turvallisuuteen liittyviä ominaisuuksia. Google Endpoint Management oli käyttöliittymältään yksinkertaisin verrattuna opinnäytetyön kahteen muuhun pilvipalveluun.

Toimeksiantajalla, Finnvera Oyj:llä, on pääosin käytössä Microsoftin tarjoamat pilvipalveluratkaisut. Opinnäytetyön aikana selvisi syy, miksi toimeksiantaja on valinnut Microsoftin palvelut. Microsoft tarjoaa kattavimman ja helpoiten lähestyttävän pilvipalveluratkaisun laite- ja käyttäjähallintaan nähden. Pilvipalvelut ulottuvat myös pidemmälle kuin laite- ja käyttäjähallintaan, joita on täten mahdollista laajentaa Microsoftin pilvipalveluratkaisuiden avulla.

Avainsanat AWS, Microsoft, pilvipalvelut
Sivut 23 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Information and Communication Technology Abstract
Author Janne Haatanen Year 2024
Subject Cloud Services in Finnvera Oyj's Cloud Environment
Supervisor Teemu Järvenpää

This thesis had two main objectives. The first objective was to investigate cloud services that could benefit the commissioning party. The second objective was to determine why the commissioning party had chosen their current cloud service solution. Finnvera Oyj was the commissioning party of this thesis.

Cloud services are becoming more common in various fields, and the thesis explored different kinds of cloud services as well as essential terms associated with them, for example public cloud services and private cloud services. In the research portion of the thesis, three different cloud services were examined: Microsoft Entra, Amazon Web Services and Google Cloud. The analysis of cloud services focused on their device and user management aspects.

Microsoft's Entra was extensively examined during the thesis. Entra was highlighted for its good device and user management features. Among the compared three cloud services, Entra appeared to be the most promising for the needs of the commissioning party. Amazon Web Services' services included WorkSpaces, OpsWorks and to some extent, Systems Manager. The services provided by Amazon Web Services were found to be too complex and extensive to implement relative to the benefits they provided. Based on this thesis's findings there is no directly comparable service between Amazon Web Services and Microsoft Entra. The third cloud service reviewed in the thesis was Google Cloud, specifically Google Endpoint Management. Google Endpoint Management lacked security features that Microsoft offers, therefore making it a worse candidate. Google Endpoint Management had the simplest interface compared to the other two cloud services discussed in the thesis.

Finnvera Oyj mainly uses cloud service solutions provided by Microsoft. During the thesis, it was made apparent why the commissioning party had chosen Microsoft's services. Microsoft offers the most comprehensive and easily accessible cloud service solutions for device and user management. Cloud services extend beyond device and user management, and it is possible to expand them with the help of Microsoft's cloud service solutions if needed.

Keywords AWS, cloud services, Microsoft
Pages 23 pages

Sisällys

Kuvat, taulukot ja kaavat

1 Johdanto

Tässä opinnäytetyössä selvitetään, mikä julkinen pilvipalvelu soveltuu parhaiten Finnvera Oyj:n nykyisen tietojärjestelmän hallintaan. Pilvipalveluiden soveltuvuutta tutkitaan vertailemalla erilaisia pilvipalveluita keskenään ja tarkastelemalla, kuinka kukin pilvipalvelu sopisi toimeksiantajan, Finnvera Oyj:n, IT-ympäristöön. Finnvera Oyj on Suomen valtion omistama erityisrahoitusyhtiö. Finnveran tarjoamiin palveluihin kuuluu erilaiset takaukset, lainat ja vientitakuut (Finnvera, n.d.). Finnvera kuvaa toimintaansa internet-sivuillaan seuraavasti: ”Valtion omistamana rahoitusyhtiönä Finnvera täydentää rahoitusmarkkinoita ja jakaa rahoitukseen sisältyvää riskiä muiden rahoittajien kanssa.” (Finnvera, n.d.) Rahoitusyhtiönä Finnvera tarvitsee tietynlaisia ominaisuuksia omilta järjestelmiltään esimerkiksi, yritysten tietojen turvaamista ja joustavaan työskentelyyn mahdollistavia ominaisuuksia.

Opinnäytetyön aihe valikoitui Finnveran kanssa käytyjen keskustelujen perusteella. Finnvera suorittaa tällä hetkellä pilvisiirtymää, jonka vuoksi pilvipalveluiden läpikäynti ja erilaisten pilvipalveluiden tutkiminen todettiin hyödylliseksi Finnveran kannalta. Pilvipalveluiden tarjoamat palvelut sekä rakenteet ovat erittäin laajoja, joten tämä työ päätettiin rajata Finnveran IT-ympäristön laite- ja käyttäjähallintaan.

Työssä tullaan käymään läpi yleistä tietoa tunnetuista pilvipalveluista ja sen lisäksi esitellään konkreettisia esimerkkejä laite- sekä käyttäjähallinasta näiden pilvipalveluiden sisällä. Työssä tullaan myös esittelemään Finnveran tämänhetkisen IT-ympäristön pilvipalveluratkaisua ja siihen mahdollisia parannuksia tai perusteluita, joista käy ilmi miksi Finnvera on päätynyt kyseiseen ratkaisuun.

2 Yleistä pilvipalveluista

Pilvipalvelu lyhyesti selitettynä tarkoittaa käyttötarpeen mukaan valittua palvelua, joka korvaa fyysisesti omistettavat tuotteet (Magic Cloud, n.d.). Pilvipalveluita käytetään maailmalla moniin eri tarkoituksiin, yritysten sekä yksityishenkilöiden toimesta. Ehkä tunnetuimpia pilvipalveluita yksityishenkilöille ovat, Microsoftin Onedrive, Google Drive ja iCloud. Yrityksille taas tyypillisiä pilvipalveluita ovat Amazonin tarjoama Amazon Web Services ja Microsoftin tarjoama Entra ID, entiseltä nimeltään Azure Active Directory.

Yritysten valitessa pilvipalveluratkaisuja, täytyy niiden pohtia minkälainen ratkaisu olisi paras yrityksen tarpeisiin. Ratkaisuja löytyy kolmea erilaista, yksityinen pilvipalvelu, julkinen pilvipalvelu tai molempien yhdistelmä. Yksityiselle pilvipalvelulle ominaista on, että se on rakennettu ainoastaan yhden organisaation tai yrityksen käytettäväksi. Pilvipalvelussa olevaan dataan tai sovelluksiin päästään ainoastaan käsiksi yrityksen toimesta. Tämänkaltaista ratkaisua käyttävät yritykset tai organisaatiot, joilla on paljon arkaluonteista dataa, kuten esimerkiksi terveydenhoitopalvelut sekä pankit. (Citrix, n.d.)

Yksityisen pilvipalvelun vastakohtana toimii julkinen pilvipalvelu. Julkinen pilvipalvelu perustuu palvelun tarjoamiseen monelle asiakkaalle internetin välityksellä (Citrix, n.d.). Yleisimpiä pilvipalvelunmuotoja löytyy kolmea erilaista, Software As A service, Platform As A Service ja Infrastructure As A Service. Näistä puhutaan yleisemmin lyhenteillä, SaaS, PaaS ja IaaS. (Magic Cloud, n.d.) Nämä kyseiset pilvipalvelumuodot ovat yleisiä julkisessa pilvipalvelussa. Julkisen pilvipalvelun isoin hyöty löytyy sen skaalautumisesta. Sen avulla yritykset pystyvät jakamaan resursseja helpommin ja tehokkaammin omille työntekijöilleen. (Citrix, n.d.)

Kahden aiemman pilvipalveluratkaisun yhdistelmästä voidaan puhua hybridi nimityksellä. Hybridiratkaisussa käytetään julkisen ja yksityisen pilvipalveluratkaisun tiettyjä osa-alueita. Kyseinen hybridiratkaisu voisi esimerkiksi pitää sisällään yksityiselle ratkaisulle ominaisen datan salaamisen ja julkisesta ratkaisusta sovelluksiin ja resursseihin pääsyn yrityksen päivittäistä toimintaa varten, kuten kommunikaatiota varten. Hybridiratkaisun saavuttamiseksi pilvipalvelun tarjoaja voi tarjota sovelluksen, jonka avulla pystytään kommunikoimaan julkisen ja yksityisen pilvipalvelun välillä. (Citrix, n.d.)

SaaS on tunnetuin pilvipalvelumuoto. Siihen sisältyy muun muassa verkkopohjaiset sähköpostipalvelut ja erilaiset pilvitallennustilat, kuten Dropbox ja Microsoft 365. SaaS-sovellusten avulla käyttäjät voivat jakaa ja hallita erilaisia tietoja joustavasti paikasta ja

laitteesta riippumatta. IaaS-palvelulla voidaan luoda infrastruktuuria yritykselle, jossa on mahdollista käyttää esimerkiksi SaaS-sovelluksia. IaaS mahdollistaa joustavan toiminnan ilman IT-infrastruktuurin fyysistä omistamista. Amazon Web Services on yksi hyvä esimerkki IaaS palveluntarjoajasta. Pilvipalveluntarjoaja vastaa esimerkiksi palvelimista sekä sovellusten palomuureista. PaaS-palvelu mahdollistaa alustan erilaisten sovellusten kehittäjille. PaaS-palvelut ovat yleensä verkkopohjaisia ja ne tarjoavat eri ohjelmointikieliä, käyttöjärjestelmiä sekä tietokantoja. (Citrix, n.d.)

Yritykset voivat käyttää omiin IT-ratkaisuihin suuren määrän rahaa sekä resursseja. Tähän voisi kuulua muun muassa omien palvelinsalien rakentaminen ja ylläpito. Pilvipalvelut helpottavat tämänkaltaisissa hankinnoissa. Pilvipalveluiden avulla yritykset voivat skaalata palvelut tarpeidensa mukaan. Maksusuunnitelmat pilvipalveluissa perustuvat yleensä kuukausi- ja vuosimaksuihin. Tämä mahdollistaa helpon tavan budjetoida IT-hankintoja ja hallita IT-ympäristön kasvua tai supistumista ilman oman IT-infrastruktuurin omistamista. Pilvipalveluiden käyttö luo yrityksille myös joustavuutta. Palveluita voidaan ostaa tarpeen mukaan ja niistä päästään myös eroon ilman suurempia kuluja. (Citrix, n.d.)

3 Microsoft Entra

Entra on Microsoftin tarjoama kokonaisuus, joka pitää sisällään kaikki Microsoftin käyttäjätietoratkaisut ja verkon käyttöoikeusratkaisut. Microsoft Entra muodostaa yhden osan Microsoftin Security -kokonaisuudesta. Tähän kyseiseen kokonaisuuteen kuuluvat myös Microsoft Purview, Microsoft Priva, Microsoft Defender sekä Microsoft Sentinel. Entra paljastettiin yrityksille ja kuluttajille toukokuussa 2022. (Microsoft, n.d.-a)

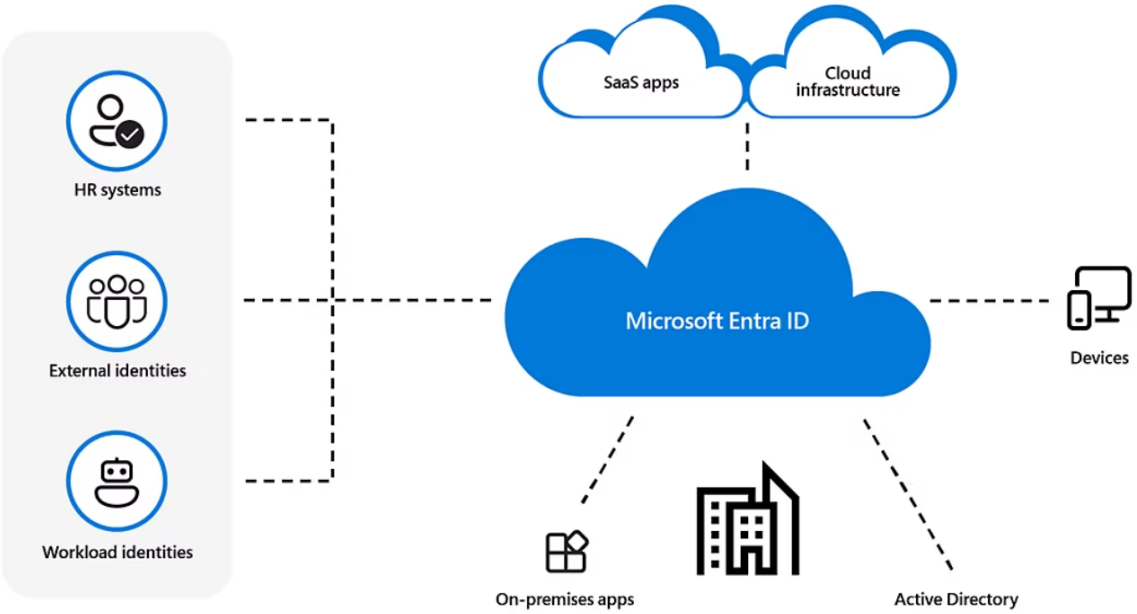
Julkaisu hetkellä Microsoft Entra piti sisällään Azure Active Directoryn (Azure AD), jonka avulla pystytään hallitsemaan muun muassa käyttäjäoikeuksia sekä käyttäjätunnuksia. Azure Active Directoryn nimi vaihdettiin Entran julkaisun myötä vastaamaan nykyistä tuoteperhenimitystä. Nykyään Azure AD tunnetaan nimellä Microsoft Entra ID. (Microsoft, n.d.-a)

3.1 Microsoft Entra ID

Microsoft Entra ID on pilvipalvelu, jonka avulla voidaan hallita yrityksen käyttöoikeus- ja käyttäjätunnuspalveluita. Entra ID:n avulla yritys saa käyttöönsä tuhansia SaaS-sovelluksia, esimerkiksi Microsoft 365 -tuoteperheen mukana tulevan Word kirjoitusohjelman. Yritysten

sisäisten sovellusten, intranetin ja pilvipalveluiden avulla luotuja sovelluksia voidaan myös hallita Entra ID:n avulla. (Microsoft Learn, n.d.-c) Kuvassa 1 tuodaan visuaalisesti esille, yksi Entra ID:n ominaisuuksista, jossa käy ilmi, kuinka Microsoft Entra ID:tä voidaan käyttää esimerkiksi yhdistämään yrityksellä jo olemassa olevia sovelluksia uusien SaaS-sovellusten kanssa. (Microsoft, n.d.-b)

Kuva 1. Microsoft Entra ID:n käyttösoveltuvuus (Microsoft Learn, n.d.-b).



Yrityksissä työntekijöillä on erilaisia työrooleja, jotka Entra ID on ottanut myös huomioon. Riippuen omasta työtehtävästä, pystyt hyödyntämään Entra ID:n ominaisuuksia tietyin tavoin. IT-palveluiden ylläpitäjät voivat esimerkiksi hallita käyttöoikeuksia eri sovelluksiin, hallita kaksivaiheista tunnistautumista ja jakaa sovelluksia eri työasemille työtehtävistä riippuen. Microsoft on myös lisännyt sovellusten tuottajille ominaisuuksia Entra ID:en. Tuottajat voivat muun muassa luoda ”single sign-on” mahdollisuuden jo olemassa oleviin sovelluksiin. ”Single sing-on”, tunnetaan yleisesti lyhenteellä SSO, mahdollistaa kirjautumisen jo valmiina olevilla tunnuksilla toiseen sovellukseen. (Microsoft Learn, n.d.-c)

3.2 Microsoft Intune

Microsoft Intune on yksi Microsoft Entran palveluista, joka mahdollistaa ja helpottaa yrityksen sisäisten resurssien hallintaa. Sisäisiksi resursseiksi voidaan luokitella yrityksen käytössä olevat puhelimet, tietokoneet, käyttäjätunnukset ja sovellukset. (Microsoft Learn, n.d.-g)

Intune on yhteensopiva useiden eri käyttöjärjestelmien kanssa. Tämmöisiä käyttöjärjestelmiä ovat muun muassa Android, Linux Ubuntu, iOS, macOS ja Windows. Intune toimii verkkoselaimen kautta olevalla ”admin” konsolilla. Admin konsolilla voidaan automatisoida sovellusten-, laitteiden- ja tietoturvankäytäntöjä. Käytäntöjen lisäksi Intunen admin konsolin avulla sovellusten jakaminen ja päivittäminen yrityksessä oleville työntekijöille tai laitteille on mahdollista. (Microsoft Learn, n.d.-g)

Microsoftin omia ja kolmansien osapuolten sovelluksia voidaan yhdistää Intunen kanssa. Windowsin autopilot-järjestelmän avulla laitteiden käyttöönotto tai uudelleen konfigurointi voidaan tehdä suoraan Intunen välityksellä. Tämä mahdollistaa laitteen toimituksen suoraan loppukäyttäjälle tavarantoimittajan toimesta. Aiemmin mainittuihin sovellusjakoihin voisi kuulua esimerkiksi Microsoft 365 -sovellukset. Näitä sovelluksia voidaan päivittää sekä ladata yrityksen hallinnassa oleville tietokoneille. Intunen mobiililaitehallinnan avulla kolmansien osapuolten sovelluksia sekä käytäntöjä on mahdollista ottaa mukaan yrityksen toimintaan. Yhdistämällä esimerkiksi Applen käyttöoikeussertifikaatit Intunen kanssa, voidaan Intunen kautta päästä käsiksi Applen tarjoamiin sovelluksiin ja ladata näitä sovelluksia eri laitteille. Samankaltainen toiminto löytyy myös Android käyttöjärjestelmää varten. (Microsoft Learn, n.d.-g)

Etäyhteyden muodostaminen yrityksen verkkoon on mahdollista VPN:n, eli virtuaalisen erillisverkon, avulla. VPN yhteys voidaan määrittää Intunen avulla. Ciscon, NetMotionin ja Microsoft Tunnelin sekä lukuisten muiden VPN-tarjoajien yhteydet toimivat Intunen kanssa. Etäyhteyksien lisäksi Intunen avulla voidaan määritellä erilaisia langattoman lähiverkonasetuksia. Langattomaan verkkoon voidaan määritellä autentikointimetodit tai määrittää automaattinen verkkoon liittyminen sijainnin perusteella. Langattomaan verkkoon liittyminen voidaan määrittää myös SSO-sisäänkirjautumisella. SSO-kirjautuminen on myös mahdollista määrittää muille sovelluksille Intunen avulla. (Microsoft Learn, n.d.-g)

3.3 Käyttäjätunnusten ja ryhmien hallinta Intunella

Yritysten IT-pääkäyttäjät, IT-adminit, ovat vastuussa IT-ympäristössä olevista käyttäjistä sekä erilaisista käyttöoikeusryhmistä. Näiden ryhmien hallintaan monella yrityksellä on käytössä Microsoftin tarjoama Active Directory, joka toimii paikallisena hallintaympäristönä. (Microsoft Learn, n.d.-f) Paikallisessa hallintaympäristössä on yleistä omistaa tai ostaa palveluna, palvelimia ja hallita niitä etäyhteyksien kautta. Jos ei haluta omistaa tai ostaa palvelinpalveluita, voidaan käyttää tähän samaan tarkoitukseen Intunea.

Intunella käyttäjien ja ryhmien hallinta toimii samanlaisilla periaatteilla kuin Active Directory -ympäristöissä, joitain poikkeuksia lukuun ottamatta. Käyttäjiä voidaan luoda Intuneen muutamalla eri tavalla. Jos yrityksellä on jo valmiina Active Directory -ympäristössä luotuja käyttäjiä ja ryhmiä, voidaan ne tuoda Intuneen käyttämällä Microsoft Entra Connect ominaisuutta. Käyttäjiä on mahdollista luoda myös CSV-tiedoston avulla. Luodaan CSV-tiedosto, jossa on tiedot olemassa olevista ryhmistä sekä käyttäjistä ja tuodaan se suoraan Intuneen. Microsoft 365 -palveluita käyttävät käyttäjät ovat automaattisesti myös Intunessa. Näiden kolmen lisäksi käyttäjiä sekä ryhmiä on mahdollista luoda suoraan ilman mitään olemassa olevia käyttäjä- tai ryhmätietoja. (Microsoft Learn, n.d.-f)

Intunen sisällä on myös omat admin-tason oikeusryhmät. Näiden ryhmien avulla voidaan määritellä, millaisia oikeuksia kukin admin pystyy käyttämään. Oikeusryhmien avulla voidaan rajata tiettyjä toimintoja kuulumaan vain muutamalle henkilölle tilanteen tai työtehtävän vaatiessa. On myös mahdollista ottaa väliaikaisesti käyttöön jokin oikeusryhmä, jos työtehtävä sitä vaatii, esimerkiksi tietokoneiden poisto Intunesta vaatii Intune Service Administrator -oikeusryhmän. (Microsoft Learn, n.d.-f) Intunea ei välttämättä tarvitse olla jatkuvasti muokkaamassa, joten tämänkaltainen oikeus voidaan laittaa vain väliaikaisesti.

Erilaisten laitteiden, kuten tietokoneen, ensimmäisellä käyttöönottokerralla määrittyy kyseisen laitteen ”omistaja”. Käyttäjän ottaessa laite käyttöön, tulee kyseiseen laitteeseen kaikki käytäntömääritelmät käyttäjätunnuksen mukana. Lisättäessä käytäntöjä käyttäjätunnukselle, samat käytännöt tulevat automaattisesti voimaan käyttäjän jokaiseen laitteeseen, joissa on ”omistajana”. Intunen ollessa pilvipalvelu myös sen käyttöoikeusmäärittelyt poikkeavat paikallisten palvelimien määrittelyistä. Paikallisten palvelimien oikeudet perustuvat hierarkkiseen menetelmään. Englanniksi tätä menetelmää kutsutaan LSDOU, tarkoittaen local, site, domain ja OU (Organizational Unit). Hierarkkinen järjestys kyseisessä menetelmässä kulkee oikealta vasemmalle. Intunen ratkaisu oikeuksien määrittelyyn on yksinkertaisempi. Oikeudet määritellään suoraan käyttäjätunnuksille sekä ryhmille, joista oikeudet valuvat eteenpäin laitteisiin. (Microsoft Learn, n.d.-f)

Käyttäjiä voidaan suojata Intunella neljällä eri tavalla, Nolla luottamus (Zero trust), monivaiheinen tunnistautuminen, sertifikaatteihin perustuva tunnistautuminen ja Windowsin ”Hello for Business” -palvelu (Microsoft Learn, n.d.-f). Monivaiheinen tunnistautuminen on erittäin yleinen tapa turvata käyttäjätunnuksia. Kyseisessä tavassa sisäänkirjautumisen yhteydessä vaaditaan toinen tapa tunnistautua salasanan ja käyttäjätunnuksen lisäksi, esimerkiksi todennus-sovelluksen tai tekstiviestin avulla. Sertifikaatteihin perustuva tunnistautuminen tapahtuu nimensä mukaan sertifikaattien kautta. Hyöty sertifikaattien

käytössä tulee niiden joustavuudesta. Käyttäjien ei tarvitse käyttää omia käyttäjätunnuksia eikä salasanoja tässä tunnistautumistavassa. Oletettu käyttäjä on jo varmennettu sertifikaatin avulla, jonka ansiosta hän pääsee käsiksi yrityksen materiaaleihin. Sertifikaatti varmenne tapahtuu yleensä langattoman verkon tai virtuaalisen erillisverkon avulla. (Microsoft Learn, n.d.-f) Windowsin ”Hello for Business” vie välikäden pois tunnistautumistavasta ja salasanojen sijaan käyttää PIN-koodia tai biometrisiä tunnistautumistapoja, esimerkiksi kasvojentunnistusta. Normaali tilanteissa salasanojen ja käyttäjätunnusten tunnisteet pidetään palvelimella. Käyttäjän syötettäessä tunnistetietonsa, sivusto tai vastaava palvelu, hakee internetin välityksellä palvelimelta kyseisen käyttäjän tunnistetiedot ja tarkistaa vastaavatko ne syötettyjä tunnistetietoja. Nämä tiedot on mahdollista kaapata, jos palvelimelle päästään jollain tapaa käsiksi ja täten tunnistautumistiedot ovat haavoittuvaisia. ”Hello for Business” tallentaa tunnistautumistiedot paikallisesti palvelimien sijaan. Tällä tavoin tunnistetiedot pysyvät aina kyseisessä laitteessa, eikä murtautumisvaaraa täten synny. (Microsoft Learn, n.d.-f)

Nolla luottamuksella tarkoitetaan turvallisuusarkkitehtuuria, jonka tehtävänä on suojata käyttäjiä sekä laitteita. Laitteiden ja käyttäjien suojaaminen voidaan toteuttaa muutamalla eri tavalla. Intunella on mahdollista määrittää laitteille vaatimuksia, jotka laitteen täyttäessä, antavat oikeudet yrityksen eri resursseihin. Intunella on myös mahdollista tehdä sovellusten jakokäytäntöjä ja muita turvallisuusasetuksia, kuten määritellä haittaohjelmien torjuntaohjelma Microsoftin tai kolmansien osapuolien valikoimasta. Edellä mainitut kolme käytäntöä muodostavat Nolla luottamuksen kolme ydinkohtaa. (Microsoft Learn, n.d.-h)

3.4 Laitteiden hallinta Intunella

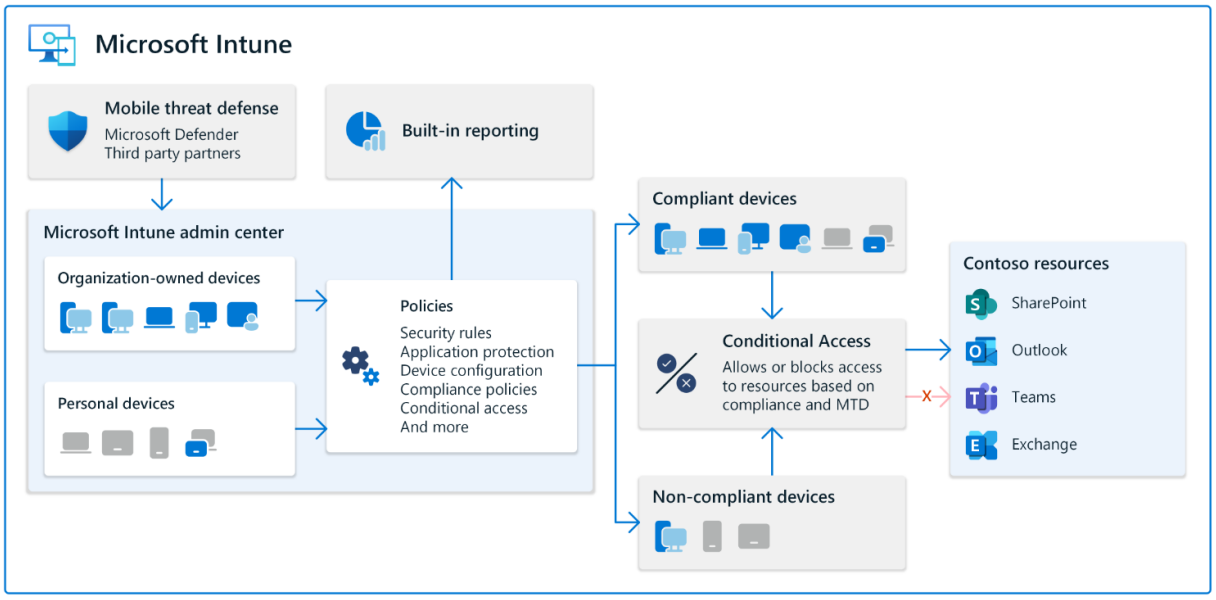
Laitteiden hallinta on yksi Intunen ydin ominaisuuksista. Yritykset voivat luoda Intunen avulla erilaisia määritelmiä yrityksen omistuksessa oleville laitteille tai työntekijöiden omille laitteille, mikäli yritys sallii omien laitteiden käytön. Turvallisuus ja käyttöoikeudet järjestelmiin sekä sovelluksiin ovat esimerkkejä näistä määritelmistä. Intunen avulla yritykset voivat muun muassa vaatia tietynlaisia pääsykoodi- ja palomuuriominaisuuksia käytettäville laitteille. Turvallisuuden kannalta laitteita voidaan hallita etäyhteyksien avulla, jos laite on hävinnyt tai epäillään sen joutuneen vääriin käsiin. Laite voidaan tarvittaessa esimerkiksi lukita, käynnistää uudelleen, paikantaa sekä tyhjentää tehdasasetuksille. (Microsoft Learn, n.d.-e)

Omien laitteiden ja yrityksen omistamien laitteiden Intune -määrittelyissä on yleisesti eroavaisuuksia. Työntekijöiden omiin laitteisiin määritellään vähemmän käyttöön liittyviä käytäntöjä kuin yrityksen omistamiin laitteisiin. Yritys voi vaatia työntekijän oman laitteen

lisäämistä Intunen laitehallintaan, jotta laitteelle voidaan määritellä tarvittavat käytännöt. Laitehallinnan lisäksi on myös mahdollista kohdistaa hallinta ainoastaan käytettäviin sovelluksiin. Tällä tavoin suojataan sovelluksissa oleva data väärinkäytöltä. Näitä kahta tapaa hallita laitteita kutsutaan sovellusten suojaamiseksi ja laitteiden rekisteröinniksi. Yritysten on mahdollista käyttää tapoja yhdessä määrittäessä työntekijöiden omien laitteiden hallintaa. Yrityksen omistamat laitteet tulisi aina olla täysin yrityksen omassa hallinnassa riippumatta siitä kuka laitetta käyttää. Tällä tavoin varmistetaan, että jokainen laite saa tarvittavat käytännöt yrityksen resurssien suojaamiseksi. (Microsoft Learn, n.d.-e)

Laitteiden hallinnan helpottamiseksi Intunen sisällä voidaan luoda laiteryhmiä. Näillä laiteryhmillä on mahdollista määritellä ominaisuuksia laitekohtaisesti käyttäjästä riippumatta, esimerkiksi voidaan estää bluetooth-yhteyksien muodostaminen. Laiteryhmien lisäksi laitteiden yhteensopivuus on yksi Intunen laitehallintaan liittyvä ominaisuus. Varmistamalla laitteiden yhteensopivuus määriteltyjen käytäntöjen ja sääntöjen noudattamiseksi, edistää se laitteiden turvallista käyttöä yrityksen sisällä. Intunella yritys määrittelee vähimmäisvaatimukset käytettäville laitteille. Vähimmäisvaatimuksia ovat esimerkiksi käyttöjärjestelmän versio, palomuurimääritelmät ja monimutkaiset salasanat. Laitteiden yhteensopivuuden monitoroinnilla on helppo seurata, mitkä laitteet ovat ajan tasalla ja mitkä tarvitsevat päivityksiä tai uudelleen määrityksiä. (Microsoft Learn, n.d.-e) Laitteiden hallinnan ymmärtämistä voidaan helpottaa visuaalisesti kuvalla 2. Kuvasta käy ilmi, kuinka Intunen laitehallinta-arkkitehtuuri muodostuu.

Kuva 2. Microsoft Intunen laitehallinta-arkkitehtuuri (Microsoft Learn, n.d.-e).



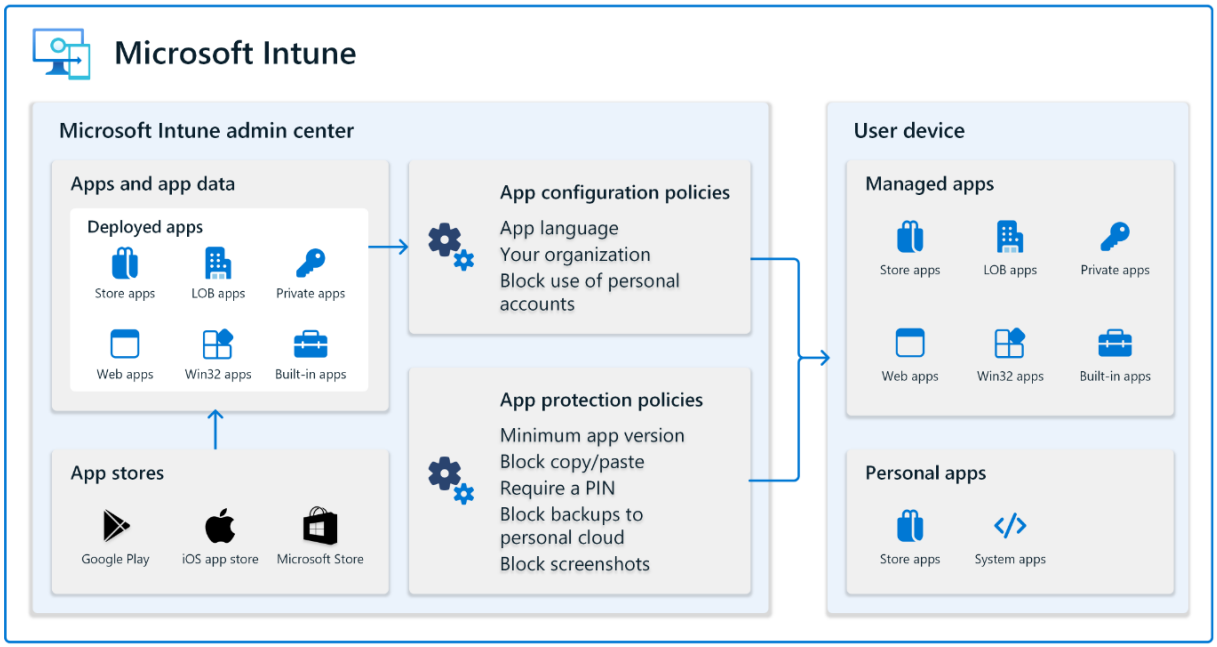
3.5 Sovellusten hallinta Intunella

Sovellusten hallinta on tärkeä osa yritysten loppukäyttäjä hallintaa. Hallitsemalla sovelluksia voidaan turvata niissä oleva, yrityksille tärkeä, data sekä suojata sovelluksia mahdollisilta haittaohjelmilta tai haittatekijöiltä. Sovellusten hallinta helpottuu huomattavasti Intunen avulla. Intunella pystyy jakamaan, päivittämään, määrittelemään ja suojaamaan sovelluksia. Intune tukee muun muassa Android, iOS, macOS ja Windows laitteita sovellusten hallintaa ajatellen. (Microsoft Learn, n.d.-d)

Android-, iOS-, macOS- ja Windows -laitteet yhdistävät suoraan omiin sovelluskauppoihinsa, kun ne tuodaan Intuneen. Intunen sisällä, esimerkiksi sovellusten jaot, toteutetaan Intune Admin -konsolin avulla. Eri käyttöjärjestelmien laitteille on myös mahdollista yhdistää yrityskohtaisia tilejä tai koulutilejä, joiden avulla on mahdollista käyttää, esimerkiksi lisensseillä rajattuja sovelluksia. Riippumatta laitteen käyttöjärjestelmästä, jokaisella laitteella on käytettävissä erilaiset internetin kautta käytettävät sovellukset, sekä yrityksen alakohtaiset sovellukset. Alakohtaiset sovellukset yleisesti luodaan yrityksen toimesta ja laitetaan Intuneen jakoa varten. Alakohtaisista sovelluksista käytetään termiä LOB, joka on lyhenne sanoista line-of-business. Ennen sovellusten jakamista laitteille, niihin on yleisesti tehty erilaisia konfiguraatioita yrityksen käytäntöjen mukaisesti. (Microsoft Learn, n.d.-d)

Intune Admin -konsolin avulla yrityksen IT-pääkäyttäjät voivat luoda sovellukseen konfiguraatioita ennen sen jakoa. Sovellukseen voidaan luoda PIN-koodi vaatimus, valita ohjelman käyttökieli sekä estää henkilökohtaisten tunnuksien käyttäminen. Henkilökohtaisia tunnuksia voisi esimerkiksi käyttää Teams-sovelluksessa. Sovelluksia on mahdollista konfiguroida milloin tahansa Intune Admin -konsolin avulla. Sovelluksiin tehtävät käytännöt voidaan määritellä laitteille niiden käyttöönoton yhteydessä tai käyttöönoton jälkeen, jos sovellusta ei vielä käytetty ennen laitteen käyttöönottoa. Sovellusten konfiguraatio kohdistuu jokaiseen sovellukseen, jolla käsitellään yrityksen resursseja. Tämän takia työntekijöiden henkilökohtaisille laitteille voidaan myös tehdä sovellusmäärityksiä, mikäli niitä käytetään työn tekoon. Tällä tavoin voidaan suojata esimerkiksi työsähköpostin käyttö henkilökohtaisella laitteella. (Microsoft Learn, n.d.-d) Kuvassa 3 tuodaan pääpiirteittäin esille, kuinka sovellusten hallinta Intunella tapahtuu.

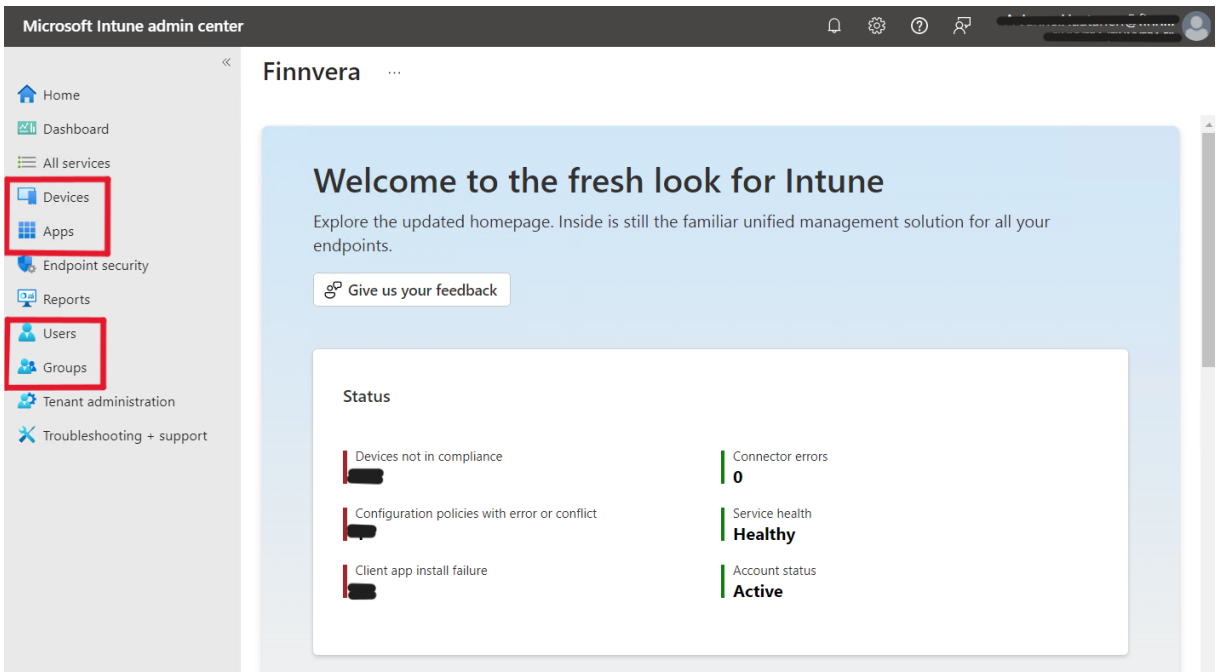
Kuva 3. Sovellusten hallinta-arkkitehtuuri Intunen sisällä (Microsoft Learn, n.d.-d).



3.6 Intunen käyttöliittymä

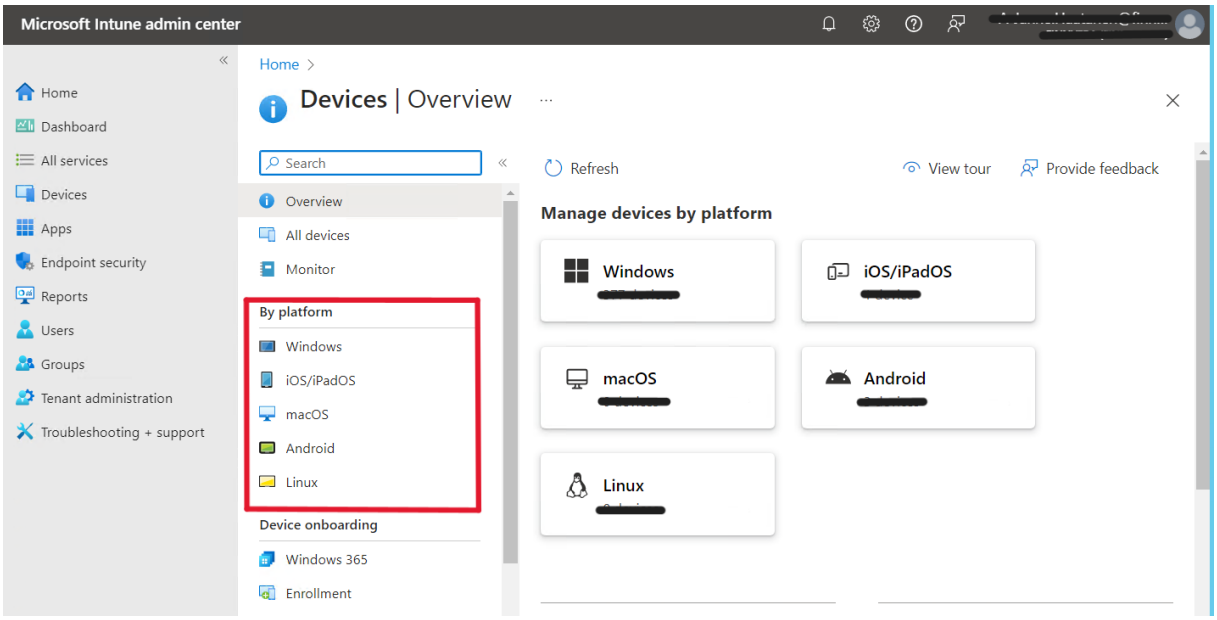
Intunen käyttöliittymä on selkeä ja helppo oppia. Kuvassa 4 nähdään osa Finnveran Intunen kotisivusta.

Kuva 4. Finnveran Intunen kotisivu näkymä (Finnvera, henkilökohtainen tiedonanto, n.d.).



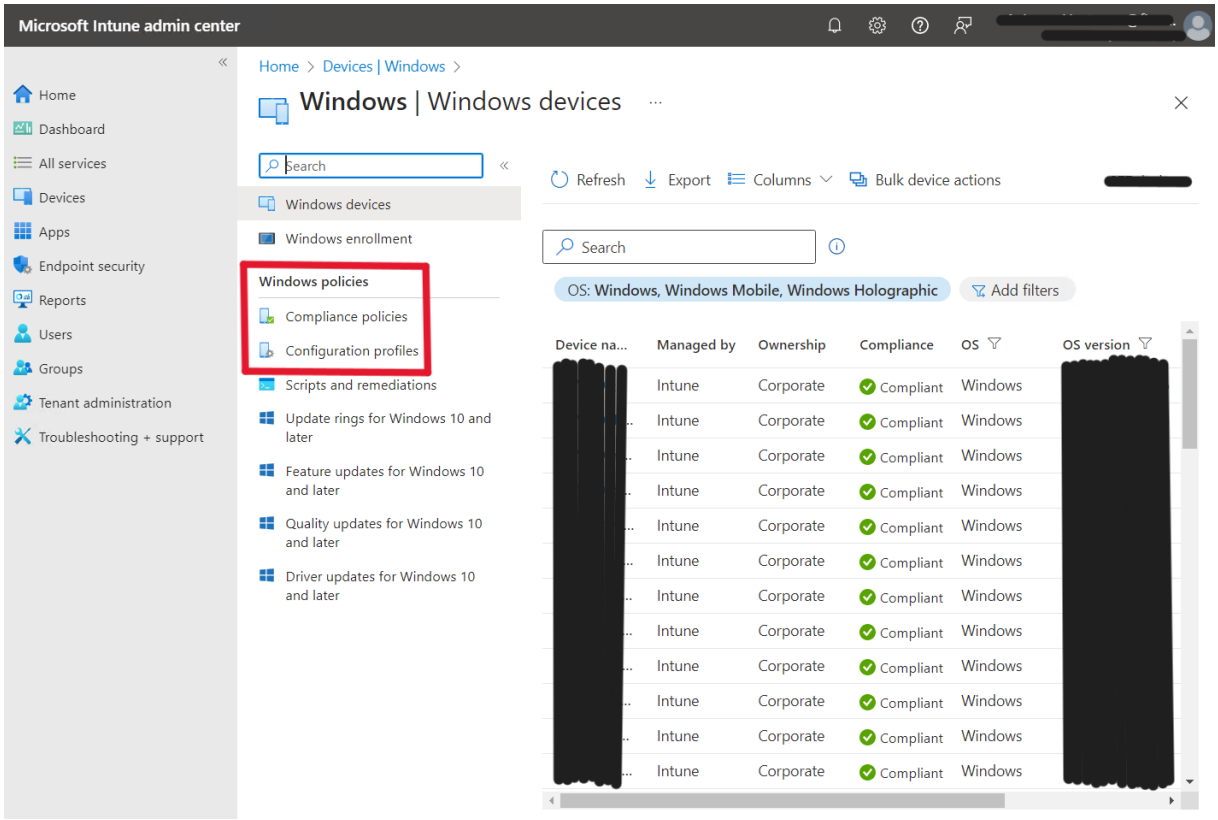
Punaisella rajatuilla alueilla on Finnveran laite- sekä käyttäjähallinnan kannalta oleellisia valikkoja. Ylemmästä laatikosta löytyy ”Devices” eli laitteet, ja ”Apps” eli sovellukset. Alemmasta laatikosta löytyy ”Users” eli käyttäjät ja ”Groups” eli ryhmät. Laitteet kohdasta päästään laitteet näkymään, kuva 5, josta voidaan tarkastella Finnveran hallinnassa olevia laitteita.

Kuva 5. Finnveran Intunen laitteet näkymä (Finnvera, henkilökohtainen tiedonanto, n.d.).



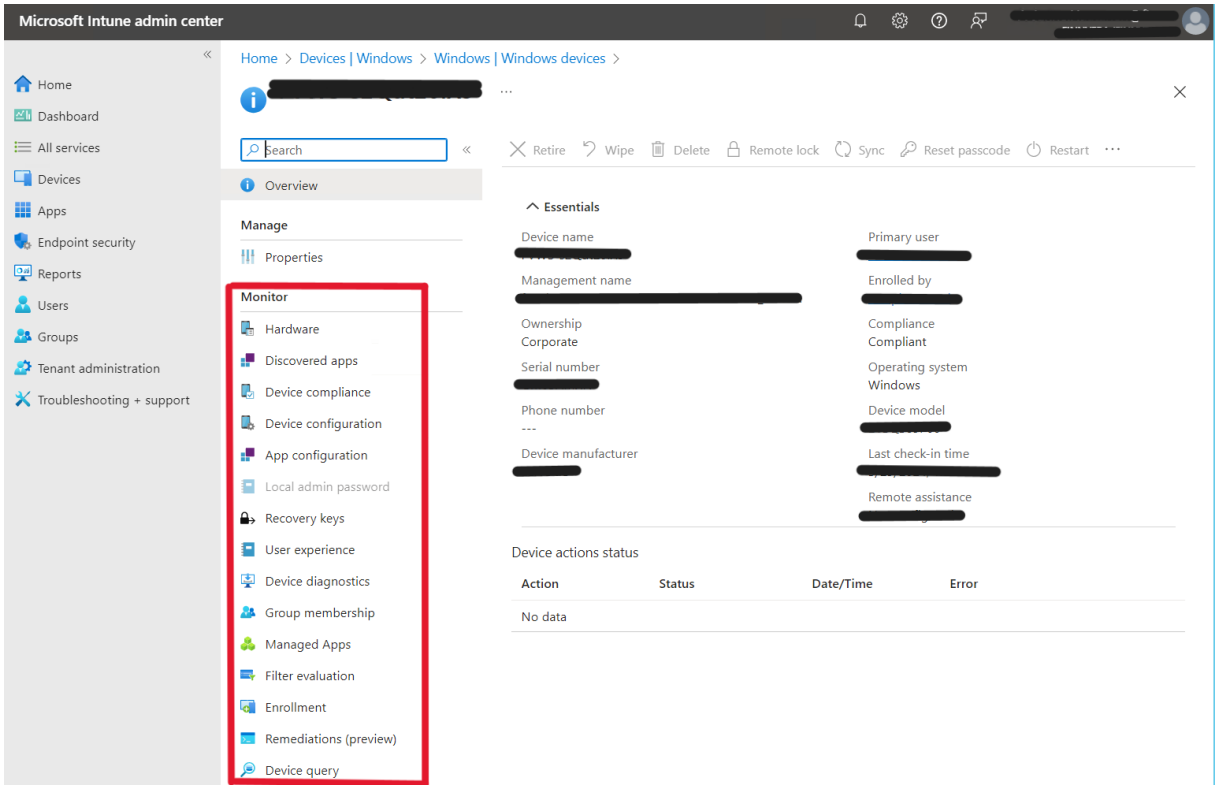
Laitteet on lajiteltu Intunessa käyttöliittymien mukaan selkeyden ja työn helpottamiseksi. Windows-laitteita voidaan tarkastella ”Windows” kohdan alta, kuten kuvassa 5 näkyy. Kun ”Windows” kohta avataan, päästään näkymään, kuva 6, jossa on koottuna yrityksen Windows-laitteet.

Kuva 6. Finnveran Intunen Windows-laitteet näkymä (Finnvera, henkilökohtainen tiedonanto, n.d.).



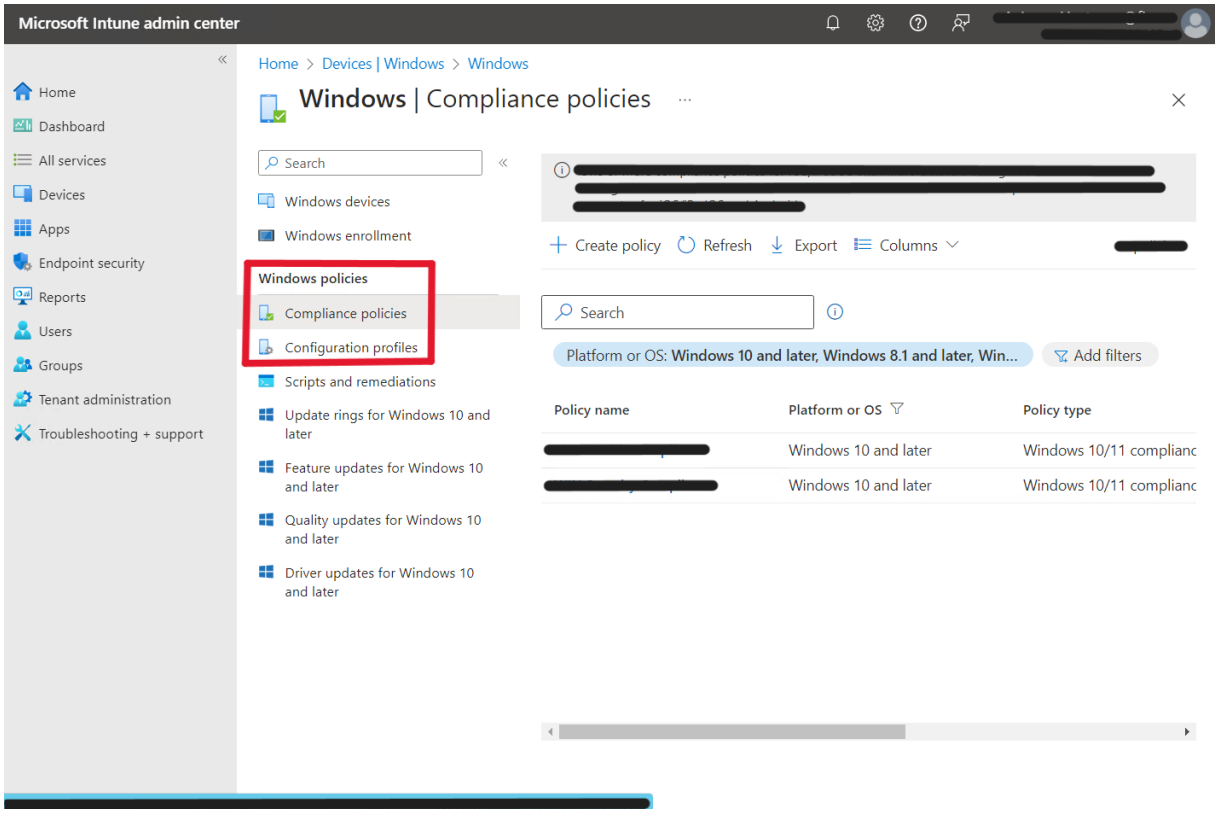
Windows-laitteet näkymässä voidaan tarkastella yrityksen hallinnassa olevia Windows-laitteita, sekä on mahdollista tarvittaessa katsoa tietyn laitteen ominaisuuksia tarkemmin. Kuvassa 7 näytetään yhden laitteen oma näkymä, josta voidaan katsoa esimerkiksi seuraavat asiat: laitteen nimi, ensisijainen käyttäjä, laitteen sarjanumero, laitteen malli, käyttöjärjestelmä ja milloin viimeksi laitteelle on kirjauduttu.

Kuva 7. Finnveran Windows laitteen oma näkymä Intunessa (Finnvera, henkilökohtainen tiedonanto, n.d.).



Kuvassa 7. olevassa punaisesta laatikosta löytyy laitehallintaan olennaisia kohtia. On mahdollista katsoa, mitä sovelluksia laitteella on kohdasta ”Discovered apps” tai tarkistaa onko Windows Autopilot käyttöönotto onnistunut ”Enrollment” kohdasta. Kun palataan kuvassa 6 (s.12) olevaan näkymään, löytyy punaisesta laatikosta ”Windows policies”, joka pitää sisällään ”Compliance policies” sekä ”Configuration profiles”. Näiden kahden kohdan takaa löytyy laitteen sääntölinjaukset, joilla varmistetaan laitteen yhteensopivuus yrityksen käytäntömääritelmiin nähden, sekä konfiguraatioprofiilit, joita laitteelle on laitettu tai voidaan laittaa. Kuvassa 8. näytetään sääntölinjaus näkymää hieman tarkemmin.

Kuva 8. Finnveran Windows laitteen ”Compliance policy” näkymä (Finnvera, henkilökohtainen tiedonanto, n.d.).



4 Amazon Web Servicen resurssien hallintapalvelut

Amazon Web Services, lyhyesti AWS, on tällä hetkellä maailman suurin pilvipalveluiden tarjoaja. AWS tarjoaa tällä hetkellä yli 200 palvelua maailmanlaajuisesti omien datakeskuksien avulla. Palvelut jakautuvat muun muassa tietokantoihin, koneoppimiseen, tekoälyyn, pilvitallennustilaan ja virtuaalitietokoneisiin. Amazonin yksi myyntikorteista on, heidän mukaansa, suurin ja syvin ymmärrys kyseisistä palveluista verrattuna kilpailijoihin. Tähän samaan kategoriaan voidaan liittää myös turvallisuus. AWS on rakennettu olemaan yksi turvallisimmista pilvipalvelualustoista, joita markkinoilta löytyy. Tämän takia esimerkiksi pankit, maanpuolustusorganisaatiot ja muut organisaatiot, jotka käsittelevät arkaluontoista dataa, käyttävät Amazon Web Servicen palveluita. (Amazon AWS, n.d.-b)

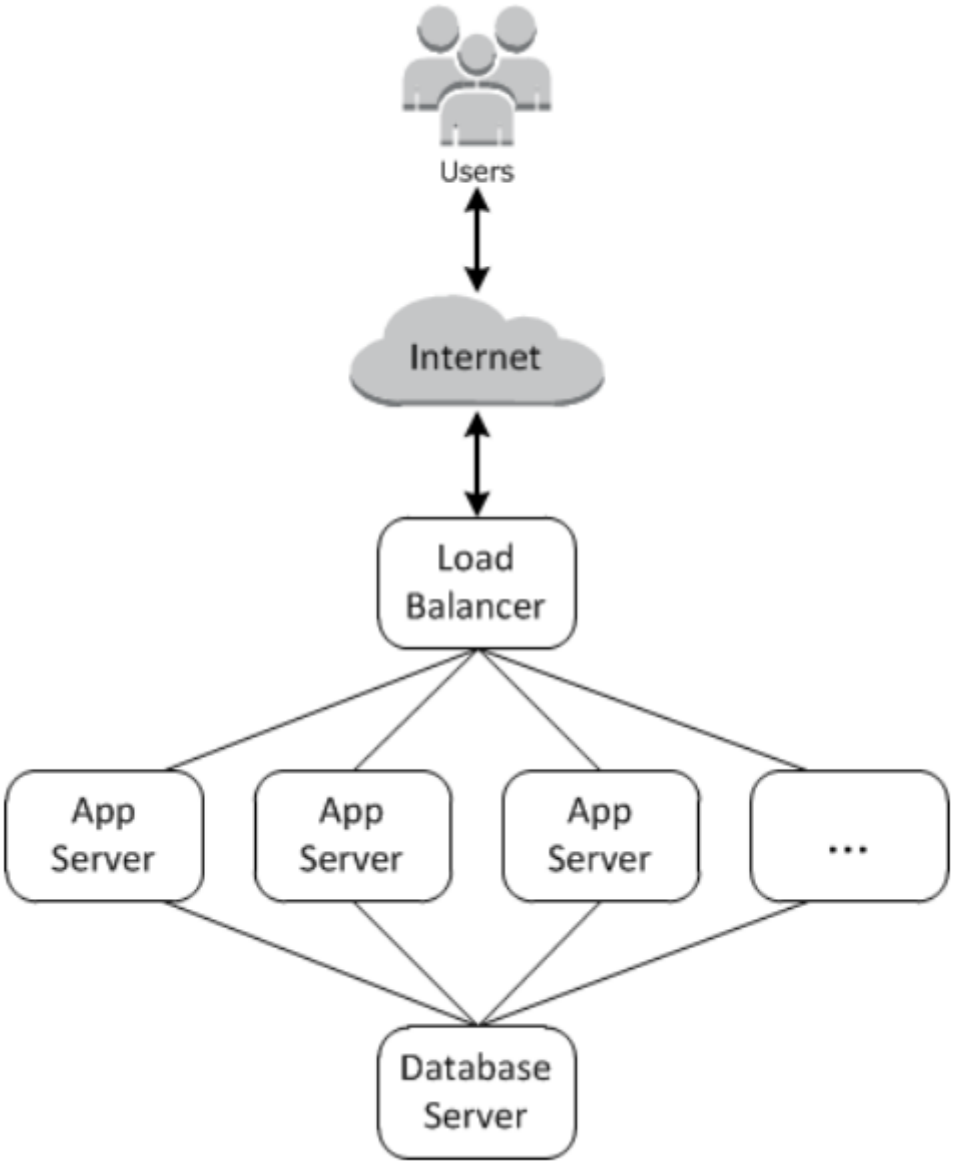
AWS Systems Manager on hallintakeskus, johon on keskitetty AWS-resurssien hallintaa. Systems Managerin sisällä on useita muita hallintaohjelmia, joiden avulla AWS ympäristö on

helposti hallittavissa. Näitä hallintaohjelmia ovat esimerkiksi ”Application Manager” ja ”Change Manager”. Systems Manager tulee tulevaisuudessa korvaamaan AWS OpsWorksin. OpsWorksin Stack -rakenne tulee myös muuttumaan OpsWorkin loputtua. (Amazon AWS Docs, n.d.-c) Yhdistyessä täysin Systems Managerin kanssa OpsWorks Stack tulee saamaan Systems Managerille olennaisia ominaisuuksia, kuten parannellun resurssien hallinnan sekä paremman konfiguraatiohallinnan.

Amazon Web Servicen tarjoamat palvelut, OpsWorks ja WorkSpaces, luovat yhdessä Microsoftin Intune palvelun, kaltaisen kokonaisuuden. Verrattuna Microsoftin Intuneen, OpsWorks sekä WorkSpaces eivät yhdessä tarjoa täysin samanlaisia hallintaympäristömahdollisuuksia. Yksi huomattava eroavaisuus Intunen ja OpsWork sekä WorkSpacesin yhdistelmän välillä on päätelaitehallinnan puute.

OpsWorks on Amazon Web Servicen tarjoama palvelinten konfiguraatio- ja hallintajärjestelmä. OpsWorks käyttää Chef ja Puppet nimisiä automaatiotyökaluja palvelinten ylläpitämiseen. Näiden kahden lisäksi OpsWorks sisältää ohjelman nimeltä AWS OpsWorks Stacks. Stacks saa nimensä sen rakenteesta. Rakennettaessa jonkinlaista web-sovellusta, siihen tarvitaan osia. Näitä osia voivat muun muassa olla tietokantapalvelimet, sovellusten palvelimet ja kuormituksen jakajat. (Amazon AWS Docs, n.d.-b) Näiden yhdistelmää kutsutaan stackiksi, suomennettuna kasaksi tai pinoksi. Kuvassa 9. näytetään erittäin yksinkertainen esimerkki stack ympäristöstä.

Kuva 9. OpsWorks Stack esimerkki (Amazon AWS Docs, n.d.-b).



Amazon WorkSpaces on Amazon Web Servicen tarjoama palvelu, jonka avulla on mahdollista luoda virtuaalisia työpöytäympäristöjä. Työpöytäympäristöjä on mahdollista luoda käyttäen eri käyttöjärjestelmiä, kuten Microsoftin Windowsia, Amazonin Linuxia sekä Ubuntu Linuxia. Näitä virtuaalisiatyöpöytiä on mahdollista käyttää internetin välityksellä selaimen avulla tai laitteilla, joihin on mahdollista saada asiakassovellus. Sovellus on saatavilla muun muassa Windows tietokoneille, macOS tietokoneille, iPadeille, Chromebookeille ja Android laitteille. WorkSpaces tukee suurinta osaa käyttöjärjestelmistä, kuten Windowsia, macOS ja Linuxia. Jokaisella näistä on mahdollista käyttää WorkSpacesin tarjoamia palveluita

internetin selaimen kautta. WorkSpaces tarjoaa monia eri kustomointi vaihtoehtoja virtuaalistentyöpöytien suhteen. On mahdollista valita käyttöjärjestelmä, virtuaalisen tietokoneen käyttöteho, sovellusten konfiguraatiot sekä maantieteellinen alue, jossa haluaa virtuaalisen työpöydän sijaitsevan. Amazon Web Services tarjoaa WorkSpacesiin valmiiksi rakennettuja kokonaisuuksia eri käyttötarkoituksiin. Valmiiksi rakennettujen kokonaisuuksien lisäksi on myös mahdollista luoda täysin itse kustomoitu WorkSpaces kokonaisuus. (Amazon AWS Docs, n.d.-d)

Käyttäjäkokemus sekä -turvallisuus on otettu myös huomioon WorkSpacesissa. WorkSpacesin pääkäyttäjät voivat rajoittaa IP-osoitteita, joilla on oikeus päästä käsiksi WorkSpacesissa luotuihin virtuaalisiin työpöytiin. Tämän lisäksi on mahdollista luoda kaksivaiheinen tunnistautumismenetelmä. Helpottaakseen, esimerkiksi työntekoa, virtuaalisiin työpöytiin on mahdollista tuoda jo olemassa olevia sovelluksia ja niihin oikeuttavia lisenssejä. Tämä ominaisuus on tosin rajattu ainoastaan Windowsia käyttäville työpöydille. Jotta käyttäjien ei tarvitsisi luoda uusia käyttäjätunnuksia käyttääkseen virtuaalisia työpöytiä, käyttäjiä on mahdollista hallita jo olemassa olevien tietojen perusteella. Tämän kaltainen järjestely tarkoittaisi siis sitä, että jo olemassa oleva käyttäjähallinta järjestelmä, esimerkiksi konesaliympäristössä oleva AD-järjestelmä, voidaan tuoda osaksi WorkSpacesia. Jos aiempaa käyttäjähallintaa ei ole, se on mahdollista luoda WorkSpacesin sisälle. (Amazon AWS Docs, n.d.-d)

5 Google Cloud

5.1 Google Cloudin infrastruktuuri

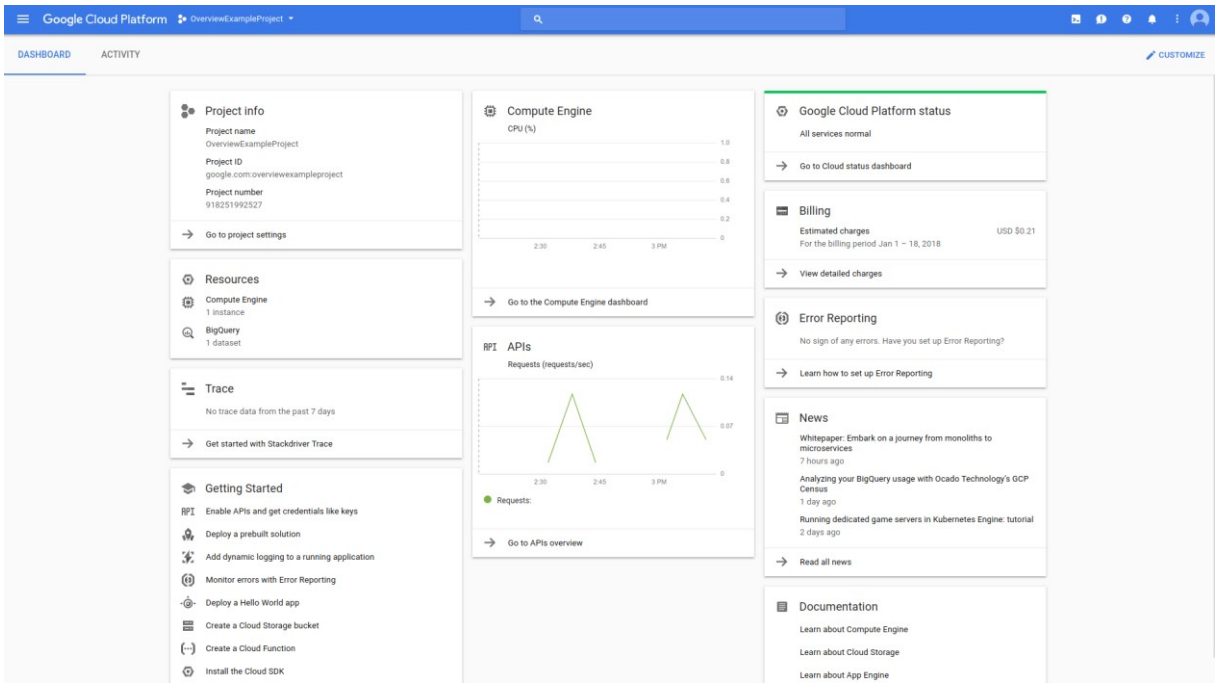
Google Cloud on Googlen tarjoama pilvipalvelu. Google Cloudin infrastruktuuri perustuu ympäri maapalloa sijaitseviin datakeskuksiin. Näissä datakeskuksissa sijaitsee tietokoneita, kovalevyjä sekä palvelimia, joilla on virtuaalisia tietokoneita. Googlella on yli 100 erilaista tuotetta Google Cloud -palvelussa. Tunnetuimpia tai käytetyimpiä palveluita ovat Compute Engine, Cloud Storage ja Cloud SQL. Compute Enginellä voidaan luoda ja käyttää virtuaalisia tietokoneita, Cloud Storagessa voidaan säilyttää dataa turvallisesti sekä skaalautuvasti ja Cloud SQL:llä voidaan luoda sekä ylläpitää SQL-tietokantoja. (Google Cloud Docs, n.d.)

Google Cloud käyttöliittymä toimii ”projektien” avulla. Projekti on ikään kuin säiliö sille, mitä lähdetään rakentamaan Google Cloudilla. Jokaisella projektilla täytyy olla nimi,

projektitunniste eli ID ja projektinumero. Projekti pitää sisällään asetuksia sekä oikeuksia, jotka jaetaan projektin sisällön kanssa. Resurssien jakaminen on mahdollista projektin sisällä, mutta projektien välinen jakaminen vaatii erillisen ohjelman nimeltään ”Shared VPC”. (Google Cloud Docs, n.d.)

Googlen pilvipalveluita on mahdollista hallita kolmella eri tavalla. Mieluisin ja yksinkertaisin tapa hallita palveluita on todennäköisesti Google Cloud -konsoli. Google Cloud -konsoli on graafinen internetselaimeen pohjautuva hallintaympäristö. Kuvassa 10 nähdään esimerkki Google Cloud -konsolin käyttöliittymästä.

Kuva 10. Google Cloud -konsolin käyttöliittymä (Google Cloud Docs, n.d.).



Toinen palveluiden hallinta vaihtoehto on ”Command-line interface” eli komentorivinäkymä. Komentorivinäkymä eroaa Google Cloud -konsolista olemalla graafisesti paljon suppeampi, kuten kuvassa 11. näkyy. Hallinta tapahtuu komentorivien avulla.

Kuva 11. Google Cloud -komentorivinäkymä (Google Cloud Docs, n.d.).

Kolmas tapa hallita Google Cloud -resursseja on käyttää Goolgen rakentamia asiakaskirjastoja. Kirjastot on luotu niin, että niissä voidaan käyttää tietyn resurssin luomiseen alkuperäistä ohjelmointikieltä, kuten Pythonia. (Google Cloud Docs, n.d.)

5.2 Google Endpoint Management

Google Endpoint Management on osa Google Workspace kokonaisuutta. Google Workspace pitää sisällään käyttäjille valmiita sovelluksia, jotka on luotu helpottamaan työntekoa, kuten Gmail, Google Calendar sekä Google Drive. Eroavaisuus Google Workspacesin ja Google Cloudin välillä löytyy niiden käyttötarkoituksista. Google Cloud on tarkoitettu enemmän asioiden kehittämiseen sekä luomiseen, esimerkiksi sovellusten kehittäminen, kun taas Google Workspace keskittyy jo valmiiden sovellusten avulla asioiden hallintaan. (OnsiteHelper, n.d.)

Google Endpoint Managementin avulla voidaan hallita päätelaitteita, kuten tietokoneita, samankaltaisesti kuin Microsoftin Intunella. Google Endpoint Management mahdollistaa käyttäjäystävällisen tavan hallita laitteita ja integroituu hyvin muiden Google Workspace -sovellusten kanssa. Laitehallinta on mahdollista yleisimmille käyttöjärjestelmille, kuten Androidille, iOS:lle, Mac:lle ja Windowsille Google Enpoint Managementin avulla. Laitehallintaan Google Endpoint Managementissa kuuluu muun muassa sovellusten- ja turvallisuusmääritysten hallinta. (OnsiteHelper, n.d.)

6 Pilvipalvelut Finnveran IT-ympäristössä

IT-ympäristö Finnveralla voidaan tällä hetkellä jakaa uuteen ja vanhaan. Finnveralla on tällä hetkellä omia konesaleja, joiden avulla hoidetaan osaa IT-ympäristöstä. Konesalijärjestelmää voidaan pitää nykyisin vanhana mallina ylläpitää IT-ympäristöjä. Uutena järjestelmänä

Finnvera käyttää Microsoftin Entraa ja sieltä tarkemmin Entra ID:tä sekä Intunea. Intunea käytetään pääosin laitehallintaan ja käyttäjienhallinta tapahtuu suurimmaksi osin Active Directoryn avulla. Active Directory tietokoneet sijaitsevat konesaleissa olevilla palvelimilla. Konesaleissa olevilla tietokoneilla ylläpidetään muun muassa Finnveran käyttäjätunnuksia ja niihin liittyviä asioita, kuten sähköpostia ja käyttöoikeuksia. Käyttöoikeuksien hallinnan avuksi on myös otettu käyttöön IAM.

Identity and Access Management, lyhyesti IAM, on viitekehys, jonka avulla hallitaan IT-ympäristön käyttäjätunnuksia sekä käyttöoikeuksia. Finnvera käyttää IAM viitekehystä käyttäjätunnusten hallintaan, joka pitää sisällään muun muassa käyttäjätunnusten luonnin ja poiston sekä käyttöoikeuksien lisäämisen ja poistamisen. IAM toimii Finnveralla yhdessä Active Directoryn kanssa. Saatuaan ilmoituksen uudesta työntekijästä, Finnveran muiden palveluiden kautta, IAM aloittaa uuden käyttäjätunnuksen luonnin. IAM luo automaattisesti Active Directoryyn uuden käyttäjän, jolle tulee muutamia vakiokäyttöoikeuksia tunnuksen aktivoitumisen yhteydessä. Käyttäjätunnus on yleensä ajastettu IAMin toimesta siten, että se tulee voimaan työsuhteen alkamispäivänä. Työntekijällä ja hänen esihenkilöllään on mahdollisuus pyytää tai lisätä käyttöoikeuksia työtehtävien mukaan. Kun pyyntö tulee työntekijältä, täytyy esihenkilön hyväksyä oikeuden lisäys, jotta se tulee voimaan. Esihenkilö voi myös itse lisätä tarvittavia oikeuksia omille alaisilleen. Finnveralla IAM on poistanut manuaalisen työn määrää huomattavasti IT-työntekijöiltä. IAMin avulla IT-työntekijät voivat keskittyä paremmin IT-ympäristön kehittämiseen sekä ylläpitoon käyttäjätunnusten jatkuvan hallinnan sijaan. Tiivistettynä, IAM automatisoi käyttäjätunnusten luontia ja käyttöoikeuksien lisäystä.

Laitehallinta Finnveralla tapahtuu pääosin Intunella. Osa laitteiden määrittelyistä on kumminkin vielä sidoksissa AD ympäristöön, esimerkiksi tietokoneiden käyttöä rajataan Group Policyjen avulla. Lyhyesti selitettynä Group Policyllä tarkoitetaan IT-infrastruktuuria, jossa on mahdollista tehdä määrittelyjä käyttäjille ja työlaitteille, kuten tietokoneille. Group Policyt ovat rajoitettuja konesaliympäristöihin ja niiden hallintaan vaaditaan aina pääsy kyseiselle palvelimelle, jossa muokattava Group Policy sijaitsee. Intune sen sijaan toimii pilvipalveluna ja tämä mahdollistaa monipuolisemman ja ketterämmän laitehallinnan, koska laitehallinta tapahtuu internetin välityksellä Intunen admin -konsolin avulla, eikä yhteyttä palvelimelle vaadita. Intunen rooli laitehallinnassa korostui entisestään Finnveran uusien tietokoneiden hankinnan myötä. Tietokoneiden käyttöönotossa hyödynnettiin Windows Autopilot ominaisuutta.

Windows Autopilot prosessi on luotu helpottamaan laitteen käyttöönottoa. Prosessissa laite on mahdollista konfiguroida tavarantoimittajan toimesta valmiiksi ennen laitteen lähettämistä käyttäjälle. Laitteeseen ladataan OEM versio Windows käyttöjärjestelmästä, jonka avulla Windows imageja ei tarvitse luoda ja asentaa uudelleen niiden vanhetessa (Microsoft Learn, n.d.-a). Kun laite otetaan käyttöön Autopilotin avulla, yrityksen IT-työntekijöillä ei tarvitse olla kovin suurta infrastruktuuria laitteiden ylläpitoa varten. Käyttäjän näkökulmasta Autopilot on myös hyvä ratkaisu, koska useimmiten käyttäjälle jää tehtäväksi erittäin vähän käyttöönottoon liittyviä vaiheita. Kun tietokone otetaan käyttöön käyttäen Autopilottia, se ilmestyy automaattisesti Intuneen hallittavaksi laitteeksi. Intunessa laitteille valmiiksi tehdyt käytäntömääritykset tulevat Autopilotin mukana laitteeseen sen rekisteröidyttyä Intuneen Autopilot prosessin aikana. Laitteiden automaattinen lisääminen Intuneen mahdollistaa niiden hallinnan Intunen avulla.

7 Johtopäätökset ja pohdinta

Työssä verrattiin kolmea eri pilvipalvelun tarjoajaa Microsoftia, Amazon Web Serviceä ja Googlea. Pilvipalveluiden tarjoajia vertailtiin soveltuvuudessa, kattavuudessa sekä helppokäyttöisyydessä. Pilvipalveluja vertailtiin Finnveran käytössä oleviin Microsoftin tarjoamiin pilvipalveluratkaisuihin. Microsoftin tarjoamat palvelut ovat osoittautuneet Finnveralle sopivimmiksi niiden monimuotoisuuden ja helppokäyttöisyyden takia. Esimerkiksi Microsoft Entran avulla hallitaan laitteita ja jo käytössä olevat konesalipalvelut integroituvat hyvin helposti Microsoftin pilvipalveluiden kanssa. Helppokäyttöisyys Microsoftin palveluissa ei täysin vedä vertoja Googlen Endpoint Managementille, mutta on silti helpommin lähestyttävissä kuin esimerkiksi Amazon Web Servicen palvelut.

Amazon Web Servicen tarjoamat palvelut eivät täysin sovi Finnveran tarpeisiin. Amazon Web Services tarjoaa joustavaa pilvipalvelurakennetta, esimerkiksi palvelinten ylläpidossa sekä hallinnassa. Finnveran palvelinten ollessa jo konesaleissa, ei nähdä tarpeelliseksi lähteä siirtämään palvelinten ylläpitoa Amazon Web Servicen tarjoamille palvelimille. Amazon Web Servicen tarjoamat laitteiden- ja käyttäjätunnusten hallintapalvelut ovat erittäin paljon monimutkaisemmat kuin Microsoftin tai Googlen tarjoamat palvelut. Täysin samanvertaista hallintajärjestelmää laitteiden hallintaan sekä käyttäjätunnusten hallintaan, kuin Microsoft Entra, ei tämän tutkimuksen avulla löytynyt Amazon Web Serviceltä. Amazon Web Services tarjoaa erilaisten resurssien hallinta- ja ylläpitopalveluita, mutta silloin täytyisi siirtyä suurimmaksi osaksi heidän tarjoamiin palveluihin, joka ei sopisi Finnveran tarpeisiin eikä tavoitteisiin.

Googlen tarjoama Endpoint Management on hyvin yksinkertainen ja helposti opittavissa oleva hallintaympäristö. Jos Finnvera olisi paljon pienempi yritys, olisi Google Endpoint Management hyvä vaihtoehto Microsoftin tarjoamien palveluiden tilalle tai rinnalle. Finnvera vaatii järjestelmiltään monimuotoisuutta sekä turvallisuutta. Googlen Endpoint Management ei ole yhtä turvallinen kuin kilpailijansa. Microsoftin tarjoama Intune mahdollistaa esimerkiksi enemmän turvallisuuteen liittyviä asetuksia Google Endpoint Managementtiin verrattuna (OnsiteHelper, n.d.).

Finnveran tarpeisiin soveltuu Microsoftin pilvipalveluratkaisut parhaiten, koska Microsoftilta löytyy tällä hetkellä parhaimmat työvälineet Finnveran nykyisen tietojärjestelmän hallintaan. Osa Amazon Web Servicen tarjoamista palveluratkaisuista ovat kattavuudeltaan vajanaiset Finnveran käyttötarpeisiin nähden. Helppokäyttöisyys on myös huomattavasti alhaisempi Amazon Web Servicen palveluilla kuin Microsoftin palveluilla. Helppokäyttöisyyden puolesta Googlen tarjoamat palvelut voisivat sopia Finnveralle. Helppokäyttöisyys itsessään ei kumminkaan riitä Finnveralle, kun kyseessä on tietojärjestelmän hallintaan tarkoitettu pilvipalvelu. Google ei pärjää palveluiden kattavuudessa eikä soveltuvuudessa Microsoftin palveluille.

Lähteet

Amazon AWS. (n.d.-a). *IAM.*
https://aws.amazon.com/iam/

Amazon AWS. (n.d.-b). *What is aws.*
https://aws.amazon.com/what-is-aws/

Amazon AWS Docs. (n.d.-a). *IAM introduction.*
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Amazon AWS Docs. (n.d.-b). *AWS OpsWorks.*
https://docs.aws.amazon.com/opsworks/latest/userguide/welcome.html

Amazon AWS Docs. (n.d.-b). *AWS OpsWorks.* [kuva 4]
https://docs.aws.amazon.com/opsworks/latest/userguide/welcome.html

Amazon AWS Docs. (n.d.-c). AWS Systems Manager.
https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html

Amazon AWS Docs. (n.d.-d). *Amazon Workspaces.*
https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html

Citrix. (n.d.). *What is a cloud service.*
https://www.citrix.com/solutions/digital-workspace/what-is-a-cloud-service.html

Finnvera. (n.d.). *Tietoa Finnverasta.*
https://www.finnvera.fi/finnvera/tietoa-finnverasta

Google Cloud Docs. (n.d.). Google Cloud Overview.
https://cloud.google.com/docs/overview

Google Cloud Docs. (n.d.). Google Cloud Overview. [kuva 10]
https://cloud.google.com/docs/overview

Google Cloud Docs. (n.d.). Google Cloud Overview. [kuva 11]
https://cloud.google.com/docs/overview

Magic Cloud. (n.d.). *Mikä on pilvipalvelu.*
https://magiccloud.fi/mika-on-pilvipalvelu/

Microsoft. (n.d.-a). *Microsoft Entra.*
https://www.microsoft.com/fi-fi/security/business/microsoft-entra

Microsoft. (n.d.-b). *Microsoft Entra ID.*
https://www.microsoft.com/fi-fi/security/business/identity-access/microsoft-entra-id

Microsoft. (n.d.-b). *Microsoft Entra ID* [kuva 1].
https://www.microsoft.com/fi-fi/security/business/identity-access/microsoft-entra-id

Microsoft Learn. (n.d.-a). *Microsoft autopilot.*
https://learn.microsoft.com/en-us/autopilot/windows-autopilot

Microsoft Learn. (n.d.-b). *Microsoft AWS to Azure services comparison.*
https://learn.microsoft.com/en-us/azure/architecture/aws-professional/services

Microsoft Learn. (n.d.-c). *Microsoft Entra Fundamentals What is.*
https://learn.microsoft.com/fi-fi/entra/fundamentals/whatis

Microsoft Learn. (n.d.-d). *Microsoft Intune Fundamentals, Manage apps.*
https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-apps

Microsoft Learn. (n.d.-d). *Microsoft Intune Fundamentals, Manage apps.* [kuva 3]
https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-apps

Microsoft Learn. (n.d.-e). *Microsoft Intune Fundamentals, Manage devices.*
https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-devices

Microsoft Learn. (n.d.-e). *Microsoft Intune Fundamentals, Manage devices.* [kuva 2]
https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-devices

Microsoft Learn. (n.d.-f). *Microsoft Intune Fundamentals, Manage identities.* https://learn.microsoft.com/en-us/mem/intune/fundamentals/manage-identities

Microsoft Learn. (n.d.-g). *Microsoft Intune Fundamentals, What is intune?* https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft Learn. (n.d.-h). *Microsoft Intune Fundamentals, Zero trust with Microsoft Intune.* https://learn.microsoft.com/en-us/mem/intune/fundamentals/zero-trust-with-microsoft-intune

OnsiteHelper. (n.d.). *Microsoft Intune vs Google Endpoint Management.* https://onsitehelper.com/microsoft-intune-vs-google-endpoint-management/