

# **TIETOTURVALLISUUS OSANA PILVIPALVELUIDEN KÄYTTÖÄ**



Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

kevät 2022

Olli Lehmuskanta

Tietojenkäsittelyn koulutus

Tekijä Olli Lehmuskanta

Työn nimi Tietoturvallisuus osana pilvipalveluiden käyttöä

Ohjaaja Ismo Turve

Tiivistelmä

Vuosi 2022

---

Opinnäytetyön tarkoituksena oli selvittää yleisesti pilvipalveluiden tietoturvallisuutta yritystoiminnan näkökulmasta katsottuna. Opinnäytetyö on tutkimuksellinen opinnäytetyö. Työssä käytettiin menetelmänä vertailua uuden tiedon saamiseksi.

Opinnäytetyö käsittelee aluksi teoriaosuudessa tietoturvaa ja tietosuoja kokonaisuutena. Osiossa myös käydään läpi tietoturvaa yritystoiminnan näkökulmasta. Toisessa osiossa kerrotaan pilvipalveluista yleisesti, niiden palvelu- ja hankintamalleista, hyödyistä, haitoista sekä pilvipalveluiden tietoturvallisuudesta.

Opinnäytetyön käytännön osuudessa otettiin käyttöön kolme eri pilvipalvelualustaa: Google Cloud Platform, Microsoft Azure ja Amazon Web Services. Käyttöönoton jälkeen alustojen käytettävyyttä vertailtiin yleisellä tasolla. Käytettävyyden jälkeen alustojen tietoturvaan perehdyttiin aluksi taulukkoa hyödyntäen, jonka jälkeen alustojen tietoturvaa käytiin läpi laajemmin. Tietoturvan osalta käytiin läpi parhaita käytäntöjä, ongelmia ja pilvialustojen tietoturvan tulevaisuutta. Myös alustojen tietosuoja käytiin läpi.

Johtopäätöksenä voidaan todeta, että alustojen kesken käyttöönotossa ei havaittu isoja eroavaisuuksia. Tietoturvan osalta tärkeät tietoturvatoimet löytyivät jokaisesta alustasta. Ongelmana pilvipalveluissa ovat tietomurrot ja tulevaisuudessa tietoturvaan liittyvien kyberuhkien torjuminen muodostuu entistä tärkeämmäksi. Tietosuojan osalta alustojen palveluntarjoajat noudattavat tarkasti tietosuojaan kohdistuvia säännöksiä ja lakeja.

Materiaali opinnäytetyöhön kerättiin eri tieteellisistä julkaisuista, kirjoista ja muista aiheeseen liittyvistä julkaisuista.

Avainsanat Pilvipalvelut, tietoturva, Google Cloud Platform, Microsoft Azure, Amazon Web Services.

Sivut 44 sivua ja liitteitä 1 sivu

Degree Programme in Business Information Technology  
Author Olli Lehmuskanta  
Subject Information security as a part of cloud services  
Supervisors Ismo Turve

Abstract  
Year 2022

---

The purpose of this thesis was to research information security of cloud services from business point of view. This thesis is a research-typed thesis. As a method, comparison was used to get new information.

The theory section of this thesis covers information security and data protection as a whole. In this section information security is viewed from business point of view. In the second section cloud services are explained. Their service models, advantages, disadvantages, and information security of cloud services were explained.

In the practical implementation three different cloud platforms were deployed: Google Cloud Platform, Microsoft Azure, and Amazon Web Services. After the deployment, their availability was compared in general. After comparison of availability, information security of cloud services was familiarized with utilization of a table which contains every important security measure. After that, information security of cloud services was examined. Best practices, challenges and future of cloud service security were processed also. Data security of cloud services were processed as well.

As a conclusion, when looking at availability there were no big differences between platforms. All major information security measures were found on each platform. Major problem in cloud services are data breaches. Prevention of cyberthreats related to information security are in major role in the future. Regarding data protection, cloud services providers comply with different laws and statutes.

Material in this thesis was gathered from different scientific publications, books and other publications related to the topic.

Keywords Information security, cloud services, Google Cloud Platform, Microsoft Azure, Amazon Web Services.

Pages        44 pages and appendices 1 page

## Sanasto

GDPR	EU:n Yleinen tietosuoja-asetus
IaaS	Infrastructure as a Service, pilvipalvelumalli
SaaS	Software as a Service, pilvipalvelumalli
PaaS	Platform as a Service, pilvipalvelumalli
IoT	Internet of Things. Suomeksi esineiden internet
AWS	Amazon Web Services, Amazonin tarjoama pilvipalvelualusta
Kryptaus	Tiedon salaamista vaikeaksi luettavaan muotoon
Koventaminen	Palvelimien suojauksen parantaminen
Rightsizing	Toimenpide, jolla saadaan resurssien ja kapasiteetin käyttö pysymään sopivana
TLS	Transport Layer Security. Tietoliikennesalausprotokolla
SSL	Secure Sockets Layer. Tietoverkkosalausprotokolla
VPN	Virtual Private Network. Virtuaalinen erillisverkko. Tapa, jolla voidaan yhdistää verkkoja julkisen verkon yli muodostaen näennäisesti yksityisen verkon
Hostaus	Palvelintilan ja tietojärjestelmäpalveluiden tarjoaminen muille itse ylläpitämänä omalla laitteistollaan
AES	Salausalgoritmi, jolla suojataan tietoja salaamalla ne

## Sisälllys

1	Johdanto .....	1
2	Tietoturva .....	2
2.1	Tietosuoja.....	3
2.1.1	GDPR.....	3
2.1.2	GDPR yritystoiminnassa .....	3
2.1.3	Asetusten soveltaminen.....	4
2.2	Tietoturvallisuus yritystoiminnassa .....	4
3	Pilvipalvelut .....	6
3.1	Pilvipalveluiden ominaisuudet.....	6
3.2	Pilvipalveluiden palvelumallit .....	7
3.2.1	Ohjelmistoresurssi-palvelumalli.....	8
3.2.2	Alustaresurssipalvelu .....	8
3.2.3	Infrastruktuuriresurssipalvelu .....	8
3.3	Pilvipalveluiden hankintamallit.....	9
3.3.1	Yksityinen pilvipalvelu .....	9
3.3.2	Yhteisöpilvipalvelu .....	10
3.3.3	Julkinen pilvipalvelu .....	10
3.3.4	Hybridipilvipalvelu.....	11
3.4	Pilvipalveluiden hyödyt .....	11
3.5	Pilvipalveluiden haasteet .....	12
3.6	Tietoturvallisuus pilvipalveluissa .....	13
3.7	Pilvipalveluiden turvallisuuden arviointi.....	14
4	Vertailtavat alustat .....	16
4.1	Google Cloud Platform.....	16
4.2	Microsoft Azure.....	16
4.3	Amazon Web Services.....	17
5	Alustojen käyttöönotto .....	18
5.1	Google Cloudin käyttöönotto.....	18
5.2	Microsoft Azuren käyttöönotto .....	20
5.3	Amazon Web Servicen käyttöönotto.....	22
6	Alustojen vertailu .....	26
6.1	Käytettävyys.....	26
6.2	Tietoturva.....	29

6.2.1	Tietoturvamenetelmien tarkempi läpikäynti .....	30
6.2.2	Palomuurit.....	30
6.2.3	Monitorointi .....	32
6.2.4	Tunnistautuminen .....	34
6.2.5	Tuki .....	36
6.2.6	Hyviä käytäntöjä alustojen tietoturvassa.....	36
6.2.7	Tietomurrot .....	37
6.2.8	Pilvialustojen tietoturvan tulevaisuus.....	38
6.3	Alustojen tietosuoja .....	38
7	Johtopäätökset .....	40
8	Yhteenveto .....	41
	Lähteet.....	42

## Kuvat, ohjelmakoodit ja taulukot

Kuva 1	Pilvipalveluiden palvelumallien vastuujako (Kyberturvallisuuskeskus, 2020).....	9
Kuva 2	Yhteenveto pilvipalvelun palvelu- sekä hankintamalleista (Kyberturvallisuuskeskus, 2014, s. 6) .....	11
Kuva 3	Tarvittavat tiedot käyttäjästä alustan käyttöön .....	19
Kuva 4	Alustan käyttöönoton toinen vaihe .....	20
Kuva 5	Näkymä osasta tarvittavista tiedoista .....	21
Kuva 6	AWS käyttöönoton toinen vaihe .....	23
Kuva 7	Näkymä neljännestä vaiheesta .....	24
Kuva 8	Näkymä tuen valitsemisesta .....	25
Kuva 9	Yleisnäkymä AWS:än pääikkunasta .....	27
Kuva 10	Yleisnäkymä Azuren pääikkunasta.....	28
Kuva 11	Yleisnäkymä Google Cloud Platformin pääikkunasta .....	28
Kuva 12	Näkymä uuden palomuurin luomisesta Azuressa .....	31
Kuva 13	Uuden palomuurisäännön luominen Google Cloud Platformissa .....	32
Kuva 14	Näkymä Microsoft Defender for Cloud -palvelusta.....	33
Kuva 15	AWS:än GuardDutyn näkymä .....	33
Kuva 16	AWS:än kaksivaiheisen tunnistautumisen aktivointi.....	34

Kuva 17 Esimerkinäkymä AWS:än sisäänkirjautumisesta MFA päällä .....	34
Kuva 18 Azuren näkymä kaksivaiheisen tunnistautumisen aktivoinnista.....	35
Kuva 19 Google Cloud Platformin tuen hinnoittelu .....	36
 Taulukko 1 Kooste alustojen tärkeimmistä tietoturvatoinista.....	29

## **Liitteet**

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



## 1 Johdanto

Nykypäivänä tietoturvallisuus on tärkeässä roolissa tietoteknisessä maailmassa. Tietoturvan merkitys on korostunut ja se täytyy ottaa huomioon käyttäessä eri sovelluksia tai palveluja. Myös pilvipalveluiden käyttö on yleistynyt viime vuosien aikana sekä työ- että yksityiskäytössä. Yhä useammat organisaatiot ja yritykset rakentaa tai ovat rakentaneet infraansa pilvipalveluiden pohjalle tehosteakseen yrityksensä toimintaa. Opinnäytetyön tavoitteena on lisätä tietoa tietoturvasta sekä sen vaikutuksesta pilvipalveluiden käytössä. Opinnäytetyö keskittyy pilvipalveluihin ja tietoturvaan yritysmaailman näkökulmasta.

Tässä opinnäytetyössä käydään läpi tietoturvaa yleisellä tasolla sekä käydään läpi tietoturvaan liittyviä asioita sekä pilvipalveluiden tietoturvallisuutta. Työssä otetaan käyttöön ja vertaillaan kolmea eri pilvipalvelua ja niiden tietoturvallisuutta yrityskäytössä. Opinnäytetyön tavoitteena on vastata asetettuihin tutkimuskysymyksiin ja tarjota lukijalle tietoa tietoturvan tärkeydestä pilvipalveluissa yritysmaailman näkökulmasta.

Opinnäytetyöhön asetetut tutkimuskysymykset:

1. Mitä täytyy ottaa huomioon tietoturvan kannalta, kun käytetään pilvipalveluita?
2. Miten työssä vertailut palvelut eroavat toisistaan tietoturvallisuuden kannalta?
3. Miten organisaatiot voivat omalta osaltaan harjoittaa tietoturvallista toimintaa?

## 2 Tietoturva

Tietoturva terminä voidaan käsittää tiedon tai tietojärjestelmien turvaamista ja suojaamista sillä tavoin, että sen oikeellisuus, luottamuksellisuus tai sen olemassaolo ei mahdollisesti vaarannu. Organisaatioissa tietoturva on osa sen riskienhallintaa, valvontaa sekä johtamista turvallisesti. Tietoturvallisuus koskee sekä manuaalista, että sähköistä tiedonkäsittelyä. Aktiivinen tietoturvallinen toiminta on jokapäiväistä toimintaa yrityksen sisällä, että sen ulkopuolella, jotta tämä toiminnallinen tavoite voidaan turvata. (LLKY, 2019, s. 2)

Hyvin hoidettu tietoturva mahdollistaa sen, että organisaatio pääsee kehittymään riskit halliten. Kaikkien yritysten työntekijöiden ei tarvitse olla tietoturvan ammattilaisia, mutta kaikkien tulee olla tietoisia omasta roolistaan, sekä tiedon merkityksestä organisaatiolle. Jotta onnistunutta tietoturvaa voidaan toteuttaa, tarvitaan jatkuvaa viestintää ja kouluttamista. Näin voidaan käsitellä tietoa sen vaatimalla huolellisuudella. (Oksala, 2012, s. 12)

Tietoturva koostuu neljästä eri osa-alueesta: tiedon saatavuudesta, tiedon luottamuksellisuudesta, tiedon eheydestä sekä todentamisesta ja kiistämättömyydestä. Tiedon saatavuudella tarkoitetaan sitä, kun mahdollinen tieto on sen oikeutettujen henkilöiden saatavilla tai tieto on käytettävissä, kun niitä mahdollisesti tarvitaan. Tiedon luottamuksellisuus on sitä, että tiedot ovat vain henkilöillä tai organisaatioilla, joilla on oikeus tietoihin eivätkä pääse ulkopuolisten tietoon. Tiedon eheydellä tarkoitetaan tietojen säilyvyyttä sekä muuttumattomuutta mahdollisten inhimillisten virheiden tai järjestelmävikojen vuoksi. Viimeinen osa-alue todentaminen ja kiistämättömyys on käyttäjän todentamista ja heidän tietojen käytön todistamista. (LLKY, 2019, s. 2)

Tietoturvaan lisäksi kuuluvat myös laitteistojen, tietoliikenteen, tietoaineistojen, ohjelmistojen sekä tilojen ja toiminnan turvaaminen. Kokonaisuutena tietoturva muodostuu tietoturvasta, tietosuojasta ja myös näiden hallinnasta ja suunnittelusta. (LLKY, 2019, s. 2)

## **2.1 Tietosuoja**

Olennainen osa tietoturvaa on tietosuoja. Tietosuoja on henkilön yksityisyyden suojaamista ja sen tarkoituksena on turvata henkilön tietoja, oikeuksia sekä luottamusta. EU:n uusi yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö määrittelee tietosuojan vaatimuksia. Lainsäädännön avulla rekisterinpitäjä suunnittelee ja osoittaa henkilötietojen lainmukaisen käsittelyn. Suojaus kattaa tiedon käsittelyn, säilytyksen sekä siirron riippumatta tietojen tallennusmuodosta tai uhan luonteesta, joka tietoon kohdistuu. Tietoon kohdistuvaa uhkaa on erilaista. Uhka voi olla sekä tahallista tai tahatonta. Näitä uhkia ovat muun muassa järjestelmäviat, tapaturmat, tiedon tahallinen urkinta, huolimattomuus ja luonnonkatastrofit. (LLKY, 2019, s. 9)

### **2.1.1 GDPR**

GDPR on lyhenne englanninkielisistä sanoista General Data Protection Regulation. Suomeksi voidaan puhua yleisestä tietosuoja-asetuksesta (EU) 2016/679). Asetus määrettiin soveltavaksi 25.5.2018 koko EU:n alueella. (Hanninen, Laine, Rantala, Rusi, Varhela, 2017, s. 13)

Yhtenä keskeisenä GDPR:n tavoitteena on yhdenmukaistaa EU:n alueella olevien jäsenvaltioiden tietosuojalakeja ja siihen liittyvää sääntelyä sekä helpottaa palvelun tarjoamista kansallisrajojen yli. (Hanninen, ym., 2017, s. 13)

### **2.1.2 GDPR yritystoiminnassa**

GDPR vaikuttaa lähes kaikkien yritysten toimintaan riippumatta niiden koosta. Jokaisessa yrityksessä tapahtuu henkilötietojen käsittelyä, joten tietosuoja-asetuksen määräyksiltä yksikään yritys ei voi välttyä. Lähes jokaiselta yritykseltä löytyy ainakin yksi asiakas, jolla on omassa asiakasrekisterissään ainakin yksi yhteyshenkilö. Jo tämä riittää siihen, että tietosuoja-asetusta tulee soveltaa. Myös, jos yrityksellä on yksikin työntekijä, asetusta tulee sovellettavaksi. (Hanninen ym., 2017, s. 16)

Tärkeimmät asiat GDPR:ään liittyen yritysten kohdalta ovat osoitusvelvollisuus henkilötietojen käsittelyssä. Kaikilla henkilöillä, kuten yritysten yhteyshenkilöillä tai kuluttajilla on siis oikeus tietää mitä tietoa heistä on kerätty, kuinka pitkäksi aikaa ja mihin tarkoitukseen. Tämä pitää olla henkilölle läpinäkyvä. Tiedon keruu pysyy samana, mutta tiedon keräämisen peruste pitää olla mietittynä. Myös tietojen täytyy pysyä ajantasaisena, joten rekisterit pitää olla ajan tasalla. (Suomen Asiakastieto, 2018)

### **2.1.3 Asetusten soveltaminen**

Tietosuoja-asetuksen soveltavuus painottuu henkilötietojen käsittelyyn. Käsittely on osittain tai kokonaan automaattista. Sitä sovelletaan myös henkilötietojen käsittelyyn, joka on muussa kuin automaattisessa muodossa, ja ne muodostavat osan rekisteriin. Tietosuoja-asetus täytyy ottaa huomioon aina kun yrityksen tietojärjestelmissä käsitellään henkilötietoja. Myös tietojen manuaalinen käsittely kuuluu asetuksen piiriin. (Hanninen ym., 2017, s. 19)

Lisäksi asetusta sovelletaan henkilötietojen käsittelyyn Euroopan unionin alueella sijaitsevassa henkilötietojen käsittelijän tai rekisterinpitäjän toimipaikassa riippuen siitä sijaitseeko rekisterinpitäjä Euroopan unionin alueella vai ei. (Hanninen ym., 2017, s. 19)

## **2.2 Tietoturvallisuus yritystoiminnassa**

Tietoturvallisuus yritystoiminnassa koskee koko yrityksen ihmisten, tekniikan ja prosessien muodostamasta kokonaisuudesta. Tietoturvallisuus ei ole siis vain tietotekniikkakysymys. Toteuttaessa tietoturvatavoimia, vastuun ei tulisi olla vain IT-osastolla vaan vastuun tulisi heijastua koko yritystoimintaan. Tietoturvallisuuden ulottuvuus koskee näin tuotteita, ihmisiä, prosesseja, tuotantolaitoksia, järjestelmiä, laitteita, verkostoja, menettelytapoja, toimintapolitiikkoja sekä tietoa. (Keskuskauppakamari, 2020, s. 8)

Tietoturvallisuutta tulisi organisoida ja toteuttaa siten, että se tukee organisaatioiden perustehtäviä ja strategian mukaisten tavoitteiden saavuttamista mahdollisimman parhaalla tavalla. Tietoturvallisuus onkin osa hyvää hallintotapaa ja lain noudattamista. Tietoturvallisen toteutuksen tulee myös olla mahdollisimman kustannustehokasta. Keskeistä

tietoturvallisuudessa on myös tavan velvoitteet, jotka perustuvat siihen, että tietoturvalla on tärkeä asema sekä tietohallintotoiminnan, että turvallisen tietoteknisen ympäristön ylläpitämisessä ja kehittämisessä. (Andreasson & Koivisto, 2013, s. 32)

Organisaatiossa tietoturvallisuuden tulisi olla luonteva osa toimintaa ja erityisesti osa sen kokonaisvaltaista riskienhallintaa. Näin se muodostaa myös perustan toiminnan toimintavarmuudelle ja jatkuvuussuunnittelulle. Päätöksiä tai toimintaa tukevien tietojen tulee olla tarvittaessa saatavilla tai organisaation toiminta saattaa vaarantua. Luvattomasti tai virheelliseen muutettuun tietoon perustuvat päätökset saattavat aiheuttaa vakavia vahinkoja organisaation imagolle ja toiminnalle sekä myös yhteiskunnan turvallisuudelle. (Andreasson & Koivisto, 2013, s. 32)

Toimet liittyen tietoturvaan tulee kohdistaa tärkeimpien tietojen ja järjestelmien suojaamiseen, joiden käytettävyyden, eheyden tai luottamuksellisuuden mahdollinen vaarantuminen aiheuttaisi vakavaa haittaa yritykselle. Tämä ei tarkoita, etteikö myös muun tieto-omaisuuden turvallisuuteen pitäisi kiinnittää huomiota. Kyse on organisaatioiden ”kruununjalokiviin” keskittyvä toimiva ja tehokas riskiperusteinen tapa käsitellä tietoturvallisuutta. (Keskus-kauppakamari, 2020, s. 8)

### 3 Pilvipalvelut

Pilvipalvelut ovat tietojenkäsittely- ja tallennuspalveluita sekä tietoliikennepalveluita, jotka toimivat verkkoyhteyden välityksellä. Pilvipalveluista voidaan puhua palvelumalleina, jossa on useita tietoteknisiä resursseja tarjottuna tietoverkkojen yli usean käyttäjän kesken.

Pilvipalveluihin pääsy on tehty mutkattomaksi. Toiminnallisuuksia voidaan kytkeä päälle ja pois, sekä yhdistäminen toisiin palveluihin on tehty nopeaksi ja helpoksi käyttäjän tarpeiden mukaan. Myös palvelun käytön ja kuormituksen seuranta on tehty läpinäkyväksi ja helpoksi. Yhdistettynä helpon resurssien hallinnan kanssa, toiminnan ja kulujen optimointi on tehty helpoksi. (Kyberturvallisuuskeskus, 2014, s. 5)

Pilvipalvelut voidaan muun muassa luokitella sen mukaan, miten pilvipalvelua tarjotaan (palvelumallit) ja miten sen hankinta on mahdollistettu (hankintamallit). Täten pilvipalvelu voidaan tarjota minä tahansa palvelu- ja hankintamallien yhdistelmänä (Kyberturvallisuuskeskus, 2014, s. 5). Kuva 2 on esitetty yhteenveto palvelu- ja hankintamalleista. Yhteenveto pilvipalvelun palvelu- sekä hankintamalleista (Kyberturvallisuuskeskus, 2014, s. 6)

#### 3.1 Pilvipalveluiden ominaisuudet

Pilvipalvelun ominaisuudet voidaan yleisesti jakaa viiteen eri kohtaan: (Heino, 2010 s. 48)

##### 1. Pilvipalveluissa on elastinen provisiointi

Elastisella provisioinnilla tarkoitetaan sitä, että uudet asiakkaat sekä palveluiden tarjoaminen nykyisille asiakkaille ja palveluiden käytön lopettaminen on tehty joustavaksi, jopa automaattiseksi. (Heino, 2010, s. 40)

##### 2. Pilvipalvelut toteutetaan jaetusta teknisestä multitenant-ympäristöstä

Usein pilvipalveluiden määritelmässä edellytetään sitä, että palvelukoneisto on jaettu lähes kaikkien asiakkaiden kesken. Näin asiakas hyötyy, koska palvelun kohentamisen, ylläpitämisen ja lopettamisen kustannukset tasataan kaikkien asiakkaiden kesken. (Heino, 2010, s. 42)

### 3. Pilvipalvelut ovat yksinkertaistettuja bulkki- ja volyymipalveluita

Tarjonta pilvipalveluissa keskittyy usein tavanomaisiin tietojenkäsittelytarpeisiin, sillä pilvipalvelu on tasapäistetty tai typistetty aina jollain tavalla. Palvelut, jotka ovat yksittäisiä, on niiden räätälöintimahdollisuudet rajalliset. (Heino, 2010, s. 44)

### 4. Pilvipalvelut ovat riippumattomia käytettävästä käyttöpaikasta tai päätelaitteesta

Palveluiden resurssit, joita tarjotaan asiakkaalle ovat palveluntarjoajan tiloissa. Näihin resursseihin on automaattinen tietoliikenneyhteys, tai niihin järjestetään pääsy.

Tietoliikenneyhteys pystytään muodostamaan useasta eri paikasta. (Heino, 2010, s. 45)

### 5. Pilvipalveluiden toimintaa pystytään mittaamaan

Resurssien käyttöasteesta sekä toimivuudesta saadaan tarvittaessa tietoja niin palveluntarjoajalle kuin asiakkaallekin. Tiedot voivat koskea palvelimien keskusmuistin käyttöä, pilvikoneiston tallennuskapasiteettia tai erilaisia tietoliikenteen suorituskykytietoja. Saatuja tietoja voidaan käyttää ympäristön kehittämiseen, valvontaan ja hallintaan. (Heino, 2010, s. 48)

## 3.2 Pilvipalveluiden palvelumallit

Pilvipalveluiden pilvipalvelumallit voidaan jakaa perinteisesti kolmeen eri malliin. Näitä ovat Software as a Service (SaaS), Platform as a Service (PaaS) ja Infrastructure as a Service (IaaS). (Elonen, 2016)

Kaikissa palvelumalleissa turvallisuuteen liittyvät vastuut jakautuvat palveluntarjoajan ja asiakkaan välillä (Kyberturvallisuuskeskus, 2020, s. 10). Toteutustapa kertoo sen, minkälaisia tietojenkäsittelytehtäviä pilvipalvelusta saadaan ja miten kyseessä olevaan koneistoon liitytään (Heino, 2010). Kuva 1 on esitelty tarkemmin palvelumallien vastuujako.

### **3.2.1 Ohjelmistoresurssi-palvelumalli**

Ensimmäinen palvelumalli on Software as a Service (SaaS). Suomeksi ohjelmistoresurssi-palvelumalli. Tämä malli antaa käyttäjälle vähän mahdollisuuksia vaikuttaa palvelun toteutukseen ja tekniseen tietoturvaan, mutta on samalla yksinkertaisin ottaa käyttöön. Tässä palvelumallissa palvelun tuottaja antaa asiakkaidensa käyttöön tiettyjä valikoituja ohjelmistoja, joita käytetään verkon yli. Tyypillisiä esimerkkejä ovat erilaiset tallennussovellukset sekä verkkoselaimella käytettävät toimisto-ohjelmat. (Kyberturvallisuuskeskus, 2014, s. 5)

Tämä palvelumalli on kustannustehokas ja vaivaton tapa ostaa ohjelmistot valmiissa paketissa. Kustannussäästöt saadaan ylläpitotarpeen vähentyessä. Palveluntuottaja huolehtii näistä automaattisesti. (Eronen, 2016)

### **3.2.2 Alustaresurssipalvelu**

Seuraava palvelumalli on nimeltään alustaresurssipalvelu, eli Platform as a Service (PaaS). Tässä palvelumallissa palvelun tuottaja tarjoaa kokonaisuutta valitsemastaan apuohjelmista ja sovelluskehitysympäristöstä. Käyttäjä voi halutessaan toteuttaa omia ohjelmistoja ja niihin liittyviä tietoturvaratkaisuja. Fyysisiin- ja virtuaalisiin tietojärjestelmien käyttöjärjestelmiin käyttäjät eivät voi kuitenkaan vaikuttaa. (Kyberturvallisuuskeskus, 2014, s. 5)

Valmiiden alustojen käyttäminen poistaa tarvetta omalle ylläpidolle sekä tuo tehokkuutta. Se myös mahdollistaa ketterän kehityksen. (Eronen, 2016)

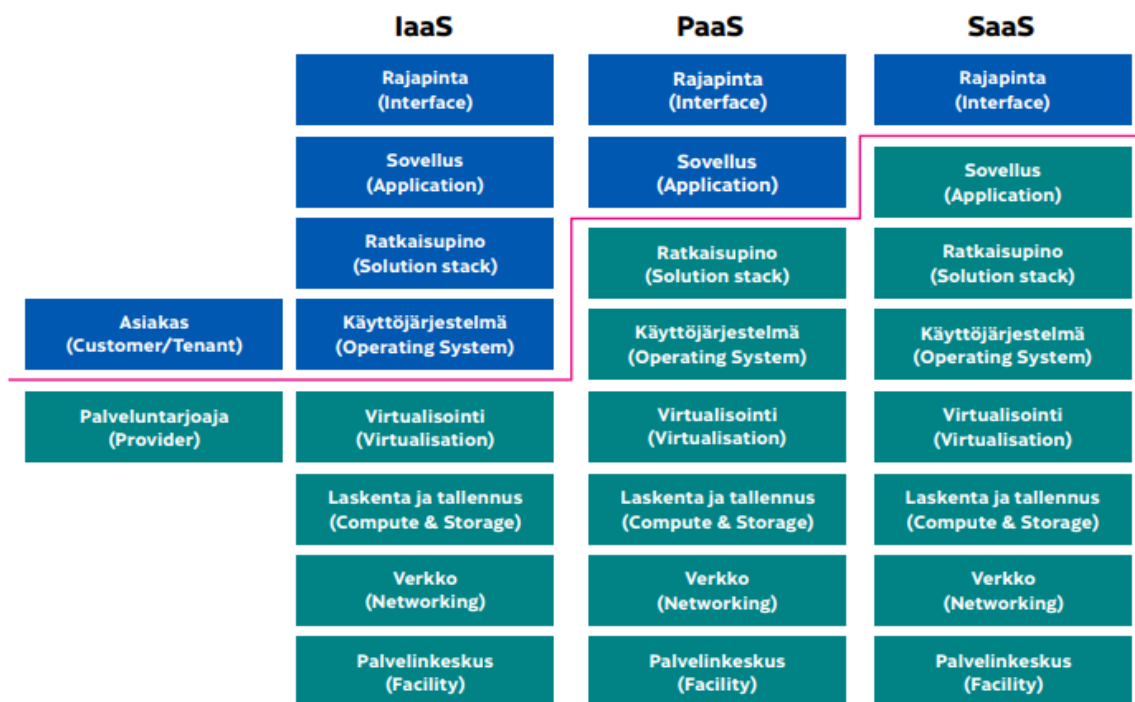
### **3.2.3 Infrastruktuuriresurssipalvelu**

Kolmas palvelumalli (Infrastructure as a Service, IaaS) eli infrastruktuuriresurssipalvelu tarjoaa käyttäjälle suurimman toimintavapauden mutta myös suurimman vastuun. Palvelumallissa palvelun tarjoaja antaa asiakkailleen tallennustilaa, tietokoneiden laskentatehoa sekä verkkoyhteyksiä. Pilvipalvelumalli mahdollistaa sen, että asiakas voi itse valita ja toteuttaa haluamansa ohjelmistot ja loogiset yhteydet. (Kyberturvallisuuskeskus, 2014, s. 5)



Palvelumalli sopii hyvin esimerkiksi organisaatiolle, jolla on IT-osasto yrityksessään tai tarvittavaa osaamista muuta kautta. Käyttäjä huolehtii itse palvelimien asennuksista, ohjelmistoista, palomuurauksesta sekä tietoturvasta. (Eronen, 2016)

Kuva 1 Pilvipalveluiden palvelumallien vastuujako (Kyberturvallisuuskeskus, 2020)



### 3.3 Pilvipalveluiden hankintamallit

Pilvipalveluiden hankintamallit voidaan jakaa neljään pääluokkaan: yksityinen, yhteisö, julkinen ja hybridi. (Kyberturvallisuuskeskus, 2014, s. 6)

#### 3.3.1 Yksityinen pilvipalvelu

Yksityinen pilvipalvelu on vain tietyn organisaation omiin tarpeisiinsa hankittu ja käytetty palvelu. Yksityinen pilvipalvelu voi olla myös käyttäjäorganisaation ulkopuolelta tuotettu ja hankittu. Tässä tapauksessa toinen osapuoli tuottaa palvelun organisaatiolle, joka sen on tilannut. (Kyberturvallisuuskeskus, 2014, s. 6)

Vahvuutena yksityisessä pilvipalvelussa voidaan pitää pilvipalveluinfrastruktuurin sekä siinä käsiteltyjen tietojen loogisen ja fyysisen tason luotettava erottelu. Tällä mallilla voidaan toteuttaa tyypillisemmin palveluita, joilla on korkeampi turvataso. (Kyberturvallisuuskeskus, 2020)

Parhaimmillaan malli mahdollistaa it-resurssien tehokkaan käytön ja siten paremman hyötysuhteen. Sen ajatellaan tarjoavan it-toiminnon käyttäjille parempaa palvelua, muun muassa uusien palveluiden käyttöönoton nopeutumisen myötä. (Heino, 2010, s. 55)

### **3.3.2 Yhteisöpilvipalvelu**

Yhteisöpilvipalvelu on rajatun organisaatiojoukon omiin tarpeisiinsa hankkima sekä käyttämä. Yhteisöllä on tyypillisesti yhteiset tavoitteet ja vaatimukset pilviratkaisulle. Pilvipalvelua voi tuottaa sekä yksi, että useampi yhteisön jäsen, kolmas osapuoli tai näiden yhdistelmä. (Kyberturvallisuuskeskus, 2014, s. 6)

Yhteisöpilvipalvelun avulla pilven omistamisen ja pystyttämisen kustannukset jakautuvat edullisemmin. Tällä tavoin julkinen valta voisi välttyä teknisen ympäristön rakentamisen jokaiseen laitokseen ja virastoon erikseen. (Heino, 2010, s. 56)

### **3.3.3 Julkinen pilvipalvelu**

Julkisen pilvipalvelun käyttäjiä ei ole rajattu ennalta. Palvelun tuottaja pyörittää palvelua omissa tiloissaan (Kyberturvallisuuskeskus, 2014, s. 6). Julkinen pilvipalvelu on mahdollistettu kaikkien saataville globaalisti sekä käyttöönotettavaksi itsepalveluna. (Virta, 2020)

Julkisessa pilvessä pilvipalveluinfrastruktuuriin sekä tietoihin, joita siellä käsitellään, kohdistuu laajempi hyökkäyspinta-ala kuin esimerkiksi yksityisessä pilvessä. Tämä tapahtuu palvelun käyttäjien kautta tai ulkoisten toimijoiden kautta. (Kyberturvallisuuskeskus, 2020)

Tietoliikenneyhteydelle ei tässä mallissa ole yleensä suuria vaatimuksia ja palveluntarjoaja järjestää asiakkaalle tarvittavat nimipalvelu- ja osoiteresurssit. Asiakkaan verkon ja pilvipalveluun kuljetaan yleensä salatun VPN-tyyppisen yhteyden avulla. (Heino, 2010, s. 55)

### 3.3.4 Hybridipilvipalvelu

Hybridipilvipalvelussa yhdistetään muilla edellä mainituilla hankintamalleilla tuotettuja pilvipalveluita käyttäen sovittuja rajapintoja. Esimerkki tästä voisi olla yksityinen pilvipalvelu, jonka käsittelykapasiteetin loppuessa, haettaisiin lisäkapasiteettia julkisesta pilvipalvelusta. (Kyberturvallisuuskeskus, 2014, s. 6)

Turvataso yhdistelmäpilvessä riippuu siitä, miten turvallisuus on järjestetty pilvien rajapinnoissa ja mitä tietoja on mahdollisuus siirtää julkisen pilvipalvelun puolelle. (Kyberturvallisuuskeskus, 2020)

Kuva 2 Yhteenveto pilvipalvelun palvelu- sekä hankintamalleista (Kyberturvallisuuskeskus, 2014, s. 6)

Palvelumallit	Ohjelmisto	Käyttäjällä on vähän vaikutusmahdollisuuksia tekniseen tietoturvaan			
	Alusta	Käyttäjällä on kohtalaisesti vaikutusmahdollisuuksia tekniseen tietoturvaan			
	Infrastruktuuri	Käyttäjällä on paljon vaikutusmahdollisuuksia tekniseen tietoturvaan			
		Yksityinen	Yhteisö	Julkinen	Hybridi
		Hankintamallit			

## 3.4 Pilvipalveluiden hyödyt

Merkittävämpiä hyötyjä pilviteknologiassa ovat kustannussäästöt, nopeus, skaalautuvuus, tietoturva, tehokkuus sekä toimintavarmuus. Kustannussäästöt eivät automaattisesti synny,

kun pilvipalveluita otetaan käyttöön. Säästöt usein syntyvät, kun asioita pystytään tehdä entistä fiksummin, sekä pilven resursseja voidaan käyttää juuri sen verran kuin tarvitaan. Samalla kun oman konesalin ylläpidosta pääsee eroon, vapauttaa se resursseja muiden tehtävien hoitamiseen. (Vento, 2021)

Pilviteknologioiden tärkeimmät ylläpitoon liittyvät tehtävät ovat kustannus- sekä kapasiteetinoptimointi. Tämä tarkoittaa säännöllistä resurssien käytön valvontaa ja toimenpiteiden tekoa, joiden avulla resurssien ja kapasiteetin käyttö pysyy sopivana. Puhutaan usein myös termistä *rightsizing*. Erityisesti SaaS-palvelumallien kohdalla säästöt syntyvät siitä, kun huolehditaan sopivasta lisenssistä, eli ei makseta turhista käyttöoikeuksista. (Vento, 2021)

Yksi merkittävämpiä etuja pilvipalveluissa on sen skaalautuvuus. Pilviteknologian käyttöä voi kasvattaa sen mukaan, kun tarpeet sekä liiketoiminta kasvavat. Toisin sanoen voidaan käyttää aina sen verran resursseja pilvestä, kun tarvitsee. (Vento, 2021)

Merkittävä etu on myös mahdollisuus ottaa käyttöön uusia teknologisia kyvykkyyksiä. Esimerkiksi koneoppimista tai tekoälyä on mahdollista vuokrata suoraan hyperskaalan pilvialustoista. Harva yritys omaa resursseja rakentaa itselleen tällaisia kyvykkyyksiä omiin konesaleihin eikä se olisi kustannustehokasta, sillä niitä on jo valmiiksi tarjolla. (Vento, 2021)

### 3.5 Pilvipalveluiden haasteet

Matalan pilvikypsyysyden omaaville organisaatioille suureksi esteeksi on muodostunut olemassa olevan IT-ympäristön monimutkainen integrointi. Myös organisaatioissa, joissa pilvipalvelut ovat arkipäivää integrointi nähdään esteenä. Olemassa olevat järjestelmät ovat haastavia integroida, kun siirrytään vanhoista järjestelmistä uusiin pilvipalveluihin. Ongelmaksi muodostuu varsinkin perinteisten palveluiden päälle rakennettu tietoturva, joka ei ole suunniteltu pilvipalveluiden päälle. (Tietoevry, 2020)

Pilvikypsät organisaatiot näkevät esteenä laajemmalle pilvipalveluiden käyttöönotolle tietoturvan. Myös epäkypsät organisaatiot tunnistavat tietoturvan haasteet, mutta näkevät

sen yhtenä ongelmana siirtymiskustannusten ja toimittajasidonnaisuuden rinnalla. (Tietoevry, 2020)

### 3.6 Tietoturvallisuus pilvipalveluissa

Pilven tietoturvalla voidaan tarkoittaa protokollia, teknologiaratkaisuja ja parhaita käytäntöjä, jolla suojataan pilvessä toimivia sovelluksia, pilvessä säilytettävää dataa sekä pilvipalveluympäristöjä (Kapersky, n.d). Asiakkaiden kannattaakin aina valita palveluntarjoaja, joka on tietoturvakeskeinen, sekä lisäksi keskittyä turvallisiin käyttötapoihin sekä asianmukaiseen määrittämiseen. Asiakkaan on hyvä myös varmistua, että loppukäyttäjän laitteisto sekä verkko on hyvin suojattu. (Kapersky, n.d)

Monta tekijää vaikuttaa pilvipalveluiden tietoturvallisuuteen. Itse palvelun turvallisuuteen vaikuttaa toteutuksen lisäksi sitä ympäröivä maailma. Esimerkkinä, palvelun ylläpidolla voi olla pääsy käyttäjän tietoihin. Turvallisuuteen vaikuttaa myös laitteistojen, ohjelmistojen ja koko fyysisen ympäristön toimittaja- ja huoltoketjut (Kyberturvallisuuskeskus, 2014, s. 12). Pilvipalveluiden tietoturvaan vaikuttaa myös ihmisen toiminta ja täten tulee ottaa huomioon pilvipalveluiden tietoturvassa. (Wallenius, 2020)

Pilvipalvelun turvallisuutta arvioidessa on hyvä arvioida itse toteutusta palvelulle, sekä palveluntarjoajan toimintaa. Nykyään palveluntarjoajat ymmärtävät käyttäjien tarpeen varmistaa tietoturallinen toiminta ja täten pyrkivät tekemään omasta toiminnastaan läpinäkyvää. (Kyberturvallisuuskeskus, 2014, s. 12)

Olemassa oleviin mahdollisiin kolmannen osapuolen tekemiin auditointeihin, sertifiointeihin sekä palveluntarjoajan dokumentteihin on hyvä tutustua käytännön toimien ja teknisten toteutuksien osalta. Palveluntarjoajat eivät voi paljastaa yksityiskohtia turvallisuuden ylläpitämiseksi ja kilpailukyvyyn säilyttämiseksi. (Kyberturvallisuuskeskus, 2014, s. 12)

Asiakkaalle tarjottu teknisen ympäristön osa suojataan yleensä palvelin- ja tietoliikennetekniikan menetelmillä. Pilvipalvelukoneisto itsessään suojataan palomuurin avulla. Pilvipalveluntarjoaja omistaa sekä ylläpitää palomuurijärjestystä pilvikoneiston ja internetin välillä. Koneisto suojataan lisäksi *tunkeilijan havaitsemisjärjestelmällä*. Voidaan

puhua termistä Intrusion Detection System (IDS) tai Intrusion Detection and Prevention System (IDPS). Tämä järjestelmä osaa reagoida mahdollisiin hyökkäystilanteisiin katkaisemalla hyökkääjän yhteydet. (Heino, 2010, s. 93)

Itse siirrettävät tiedot salataan *kryptauksen* avulla. Jos mahdollinen tunkeutuja saa pääsyn pilvipalvelussa olevaan tietoon, tieto on salattu eikä sitä saada luettavaan muotoon tunkeutujan saatavilla olevien resurssien avulla. Jotta kryptaus onnistuu, tarvitaan sen mahdollistava ohjelmisto ja menettely salausavaimien tallessa pitämiseen. (Heino, 2010, s. 93)

Jotta pilvipalvelun koneistossa olevia palvelimia saadaan mahdollisimman vastustuskykyisiksi hyökkäyksiä vastaan, täytyy palvelimia *koventaa*. Koventamisella tarkoitetaan sitä, että palvelimesta poistetaan järjestelmäpalveluita, joita ei välttämättä tarvita. Mahdollinen tunkeutuja voisi päästä näitä järjestelmäpalveluita pitkin käsiksi tietoihin tai käyttäjätunnuksiin. (Heino, 2010, s. 93)

### **3.7 Pilvipalveluiden turvallisuuden arviointi**

Pilvipalveluiden turvallisuuden arvioinnissa käytetään arviointikriteeristöä, PiTuKria. Sen on tarkoitus edistää salassa pidettävän tiedon turvallisuutta viranomaistasolla. PiTuKri on työkalu pilvipalveluiden turvallisuuden arvioinnissa. Se on Suomen kansallisten tarpeiden näkökulmasta laadittu. Kriteeristö tukee uusiutunutta lainsäädäntöä, joka tuli voimaan 2020. (Kyberturvallisuuskeskus, 2020)

PiTuKri on jaettu yhteentoista eri osa-alueeseen. Erityisasemassa olevat esiehdot ovat ensimmäisenä osa-alueena. Muita osa-alueita ovat: turvallisuusjohtaminen, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, identiteetin ja pääsyn hallinta, tietojärjestelmäturvallisuus, salaus, käyttöturvallisuus, siirrettävyys ja yhteensopivuus ja viimeisenä muutostenhallinta ja järjestelmäkehitys. Osa-alueet koostuvat erilaisista vaatimuskorteista. Kortteihin on muun muassa kuvattu teema, soveltamiskohteet, suojaustavoite ja konkreettinen vaatimus. (Kyberturvallisuuskeskus, 2020)

Vaikka kriteeristö on tarkoitettu pilvipalveluiden turvallisuuden käyttöön, voidaan sitä myös käyttää pilvipalveluntarjoajilla omaehtoisen turvallisuutta edistävän työn tukena. Kriteeristö tukee erilaisia käyttötapauksia ja pilvipalveluita. Kriteeristössä turvallisuusvaatimukset ovat mitoitettu siten, että tyypillisimmät riskit, jotka kohdistuvat salattaviin tietoihin saadaan pidettyä siedettävällä tasolla. (Kyberturvallisuuskeskus, 2020)

## **4 Vertailtavat alustat**

Opinnäytetyössä otetaan käyttöön ja vertaillaan kolmea eri julkista pilvialustaa, niiden käytettävyyttä ja tietoturvallisuutta kattavan tuloksen saamiseksi. Vertailuun on valittu pilvialustoiksi: Google Cloud Platform, Microsoft Azure sekä Amazon Web Services. Pilvipalvelut ovat valittu niiden suosion ja ajankohtaisuuden vuoksi. Tässä osiossa käydään läpi ohjelmistot yleisesti.

### **4.1 Google Cloud Platform**

Google Cloud Platform on julkinen pilvipalvelu, joka on tuotettu Googlen konesaleista. Sitä voidaan hyödyntää IaaS, sekä PaaS alustana (Valtti, n.d). Alustalla on saatavilla erilaisia hostattuja palveluita muun muassa tallennustilaan, laskentaan sekä ohjelmistokehitykseen. Palvelut ovat saatavilla ohjelmistokehittäjille, pilven ylläpitäjille sekä muille it-ammattilaisille julkisen verkon kautta. (Bigelow, 2017)

Google Cloud Platform tarjoaa palveluita laskentaan, säilöntään, verkkoon, big dataan, koneoppimiseen ja esineiden internettiin (IoT). Lisäksi palveluita on pilvihallintaan sekä turvallisuuteen. Google Cloud Platform tarjoaa myös työkaluja ohjelmistokehittäjille. (Bigelow, 2017)

### **4.2 Microsoft Azure**

Microsoft Azure on alustapalvelu, jonka tavoitteena on toimia alustana kaikenlaisille sovelluksille, palvelimille ja palveluille. Azure tarjoaa siis IaaS- että PaaS-tyyppistä palvelua alustaksi sovelluksille. (Bergius, 2014)

Lisäksi on vielä erilaisia lisäkomponentteja, mitä pystytään hyödyntämään, kun halutaan laajentaa Azuren hostattavien sovellusten toimintaa. Nämä komponentit voidaan karkeasti jakaa kolmeen eri ryhmään: varsinaiset alustapalvelut, lisäpalvelut ja tallennuspalvelut (Bergius, 2014)



### 4.3 Amazon Web Services

Amazon Web Services eli AWS on Amazonin tarjoama pilvialusta. AWS on tehty monista erilaisista pilvilaskentaan liittyvistä tuotteista ja palveluista. AWS tarjoaa muun muassa palvelimia, tallennustilaa ja verkkotyöskentelyyn liittyviä palveluita. AWS voidaan jakaa kolmeen eri päätuotteeseen. EC2, Amazonin virtuaalikoneet, Glacier, pilvitallennuspalvelu sekä S3, Amazonin tallennusjärjestelmä. (Page, 2021)

AWS tarjoaa monia eri ratkaisuja ja työkaluja yrityksille ja ohjelmistokehittäjille. Eri ryhmät, kuten koulut, yksityiset organisaatiot ja valtion virastot voivat käyttää AWS:ää. (Gillis, 2020)

## 5 Alustojen käyttöönotto

Opinnäytetyön käytännönsuudessa aluksi otetaan vertailtavat alustat käyttöön. Kaikki alustat tarjoavat ilmaista kokeiluversioita. Opinnäytetyössä käytetään ilmaisversioita tuotteista. Seuraavaksi käydään läpi vaiheet jokaisen pilvialustan käyttöönotolle.

### 5.1 Google Cloudin käyttöönotto


Ensimmäisenä otetaan käyttöön Google Cloud Platform. Käyttöönotto alkaa menemällä aluksi sivulle:

[https://console.cloud.google.com/freetrial/signup/tos?\\_ga=2.195456684.1880000705.1644226698-1663421130.1644226698&\\_gac=1.81446373.1644305441.CjwKCAiAo4OQBhBBEiwA5KWu\\_6gQy4LJ07mfQiymmcz4LplawzCU70F22MuEuO3DDBmJ8fcnv5ojRRoCxAkQAvD\\_BwE](https://console.cloud.google.com/freetrial/signup/tos?_ga=2.195456684.1880000705.1644226698-1663421130.1644226698&_gac=1.81446373.1644305441.CjwKCAiAo4OQBhBBEiwA5KWu_6gQy4LJ07mfQiymmcz4LplawzCU70F22MuEuO3DDBmJ8fcnv5ojRRoCxAkQAvD_BwE)



Sivustolle täytyy aluksi kirjautua Google-käyttäjätunnuksella.

Ensimmäisessä vaiheessa (Kuva 3) annetaan käyttäjän tiedot ja hyväksytään palvelun käyttöehdot.

Kuva 3 Tarvittavat tiedot käyttäjästä alustan käyttöön

 Try Google Cloud for free

### Step 1 of 3 Account Information

  [SWITCH ACCOUNT](#)

Country

Finland ▼

What best describes your organization or needs?

Please select ▼

**Terms of Service**


☐ I have read and agree to the [Google Cloud Platform Terms of Service](#), [Supplemental Free Trial Terms of Service](#), and the terms of service of [any applicable services and APIs](#).

Required to continue

[CONTINUE](#)

Käyttöönoton toisessa vaiheessa kysytään puhelinnumeroa (Kuva 4) tunnistautumisen vahvistukseksi.

Kuva 4 Alustan käyttöönoton toinen vaihe

 Try Google Cloud for free

## Step 2 of 3 Identity Verification and Contact Information

We'll send a text message with a 6-digit code to verify your identity and confirm where we can reach you about solutions to support your Cloud experience. Standard rates apply.



+358 Phone number

SEND CODE

Puhelinnumerolla tunnistautumisen jälkeen seuraa viimeinen vaihe, jossa annetaan maksutiedot. Tietojenannon jälkeen käyttäjän täytyy tunnistautua pankkiohjelman kautta. Tunnistautumisen jälkeen käyttäjä voi aloittaa alustan ilmaisen kokeilun.


## 5.2 Microsoft Azuren käyttöönotto


Seuraavana otetaan käyttöön Microsoft Azure -pilvialusta. Alustan käyttöönotto tapahtuu kirjautumalla aluksi Microsoft-tilille. Tämän jälkeen avataan sivusto:

<https://azure.microsoft.com/en-gb/free/> ja aloitetaan antamalla tarvittavat tiedot (Kuva 5)

Kuva 5 Näkymä osasta tarvittavista tiedoista

## Your profile

Country/Region 

Finland 

Choose the location that matches your billing address. **You cannot change this selection later.** If your country is not listed, the offer is not available in your region. [Learn More](#)


First name

This field is required


Middle name (Optional)

Last name

This field is required

Email address 

This field is required

Phone 

Example: 50 123 45 67

This field is required

☐ Use a different phone number to verify your identity.

Text me

Call me

Tietojen antamisen jälkeen Azure kysyy luotto- tai pankkikorttia tilapäiseen tunnistautumiseen. Annettujen tietojen jälkeen Azure tallentaa tiedot ja luo käyttäjälle asetukset. Näiden vaiheiden jälkeen Azure on valmis käytettäväksi.

### 5.3 Amazon Web Servicen käyttöönotto

Viimeisenä otetaan käyttöön Amazon Web Service. Käyttöönotto tapahtuu sivustolla

[https://aws.amazon.com/free/?trk=ps\\_a134p000003yHiLAAU&trkCampaign=acq\\_paid\\_search\\_brand&sc\\_channel=PS&sc\\_campaign=acquisition\\_ND&sc\\_publisher=Google&sc\\_category=Core-Main&sc\\_country=ND&sc\\_geo=EMEA&sc\\_outcome=acq&sc\\_detail=aws&sc\\_content=Brand\\_Core\\_aws\\_e&sc\\_segment=444204369308&sc\\_medium=ACQ-P|PS-GO|Brand|Desktop|SU|Core-Main|Core|ND|EN|Text&skwid=AL!4422!3!444204369308!e!!g!!aws&ef\\_id=EA!aIQobChMlrqvVvvnv9QIVg9KyCh0YsQ6REAAAYASAAEgJVhPD\\_BwE:G:s&skwid=AL!4422!3!444204369308!e!!g!!aws&all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=\\*all&awsf.Free%20Tier%20Categories=\\*all](https://aws.amazon.com/free/?trk=ps_a134p000003yHiLAAU&trkCampaign=acq_paid_search_brand&sc_channel=PS&sc_campaign=acquisition_ND&sc_publisher=Google&sc_category=Core-Main&sc_country=ND&sc_geo=EMEA&sc_outcome=acq&sc_detail=aws&sc_content=Brand_Core_aws_e&sc_segment=444204369308&sc_medium=ACQ-P|PS-GO|Brand|Desktop|SU|Core-Main|Core|ND|EN|Text&skwid=AL!4422!3!444204369308!e!!g!!aws&ef_id=EA!aIQobChMlrqvVvvnv9QIVg9KyCh0YsQ6REAAAYASAAEgJVhPD_BwE:G:s&skwid=AL!4422!3!444204369308!e!!g!!aws&all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=*all&awsf.Free%20Tier%20Categories=*all)

Ensimmäisessä vaiheessa palveluun täytyy luoda käyttäjä. Käyttäjän luonnin jälkeen, toisessa vaiheessa annetaan tarvittavat yhteystiedot (Kuva 6).

Kuva 6 AWS käyttöönoton toinen vaihe

### Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.



**Always free**  
Never expires



**12 months free**  
Start from initial sign-up date



**Trials**  
Start from service activation date

## Sign up for AWS

### Contact Information

How do you plan to use AWS?

- ☐ Business - for your work, school, or organization
- ☐ Personal - for your own projects

Who should we contact about this account?

Full Name

Phone Number

Enter your country code and your phone number.

Country or Region

Address



City

State, Province, or Region

Postal Code

☐ I have read and agree to the terms of the [AWS Customer Agreement](#).

**Continue (step 2 of 5)**

Kolmannessa vaiheessa annetaan maksutiedot. Maksutietojen annon jälkeen tunnistautuminen tapahtuu pankkiohjelman kautta. Onnistuneen tunnistautumisen jälkeen käyttäjän täytyy todentaa puhelinnumero joko tekstiviestillä tai puhelulla (Kuva 7).

Kuva 7 Näkymä neljännessä vaiheesta

## Sign up for AWS

### Confirm your identity

Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

How should we send you the verification code?

☒ Text message (SMS)




☐ Voice call

Country or region code

United States (+1) ▼

Mobile phone number

Security check

Type the characters as shown above

**Send SMS (step 4 of 5)**


Onnistuneen todentamisen jälkeen valitaan vielä tuen sopimusmuoto. Valitaan Basic support (Kuva 8). Näiden vaiheiden jälkeen painetaan "Complete sign up" ja AWS on valmis käytettäväksi.






Kuva 8 Näkymä tuen valitsemisesta

## Sign up for AWS


### Select a support plan

Choose a support plan for your business or personal account. [Compare plans and pricing examples](#)  
 You can change your plan anytime in the AWS Management Console.

<p><input checked="" type="radio"/> <b>Basic support - Free</b></p> <ul style="list-style-type: none"> <li>Recommended for new users just getting started with AWS</li> <li>24x7 self-service access to AWS resources</li> <li>For account and billing issues only</li> <li>Access to Personal Health Dashboard &amp; Trusted Advisor</li> </ul> 	<p><input type="radio"/> <b>Developer support - From \$29/month</b></p> <ul style="list-style-type: none"> <li>Recommended for developers experimenting with AWS</li> <li>Email access to AWS Support during business hours</li> <li>12 (business)-hour response times</li> </ul> 	<p><input type="radio"/> <b>Business support - From \$100/month</b></p> <ul style="list-style-type: none"> <li>Recommended for running production workloads on AWS</li> <li>24x7 tech support via email, phone, and chat</li> <li>1-hour response times</li> <li>Full set of Trusted Advisor best-practice recommendations</li> </ul> 
--	---	---



#### Need Enterprise level support?

From \$15,000 a month you will receive 15-minute response times and concierge-style experience with an assigned Technical Account Manager. [Learn more](#) 

**Complete sign up**

Opinnäytetyössä valittujen alustojen käyttöönotto on yksinkertainen prosessi. Alustojen vaiheet käyttöönotolle noudattavat pitkälti samaa kaavaa. Ainoa iso ero käyttöönotossa on, että Azure ei käytä tunnistautumisessa pankkiohjelmaa todentamiseen. Muut alustat kuin AWS, ei kysy millaisen sopimuksen haluaa tuen osalta.

## 6 Alustojen vertailu

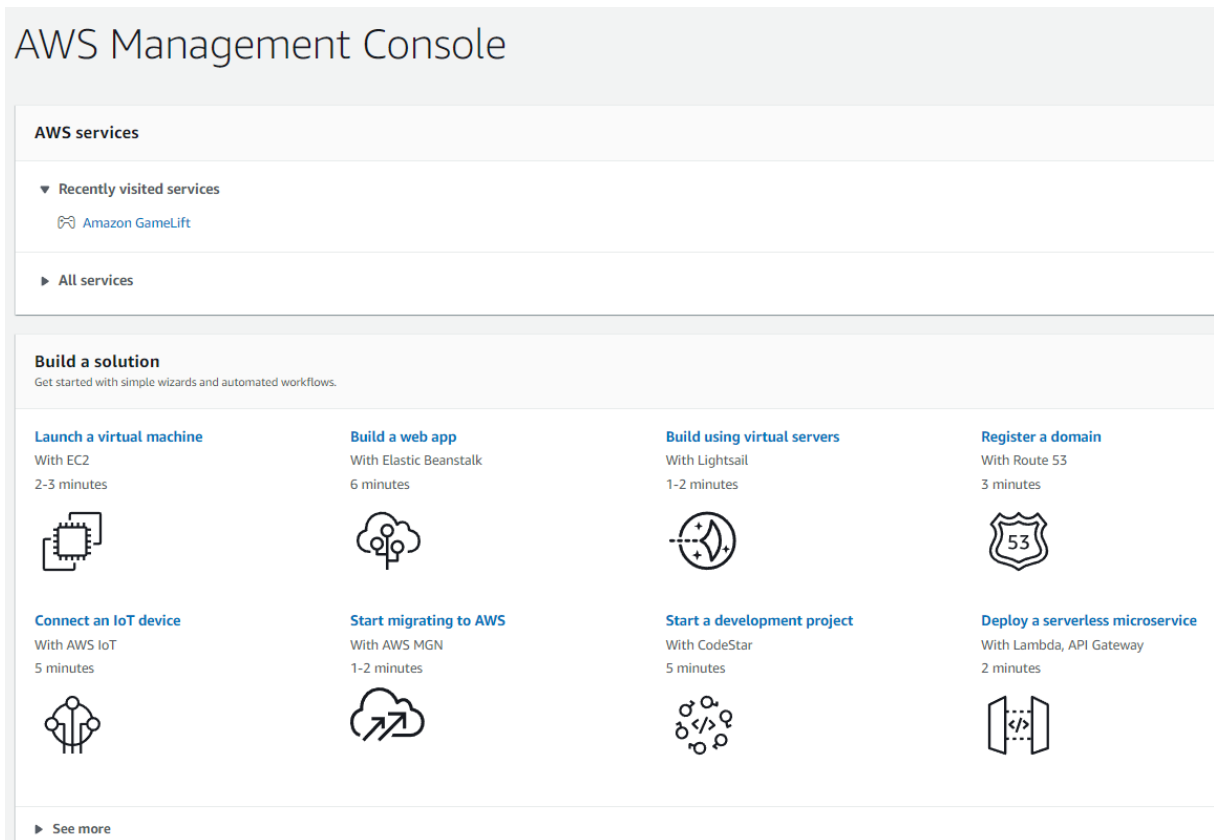
Opinnäytetyössä käytetään menetelmänä vertailua uuden tiedon saamiseksi. Vertailu on valittu menetelmäksi siksi, koska sen avulla kerättyä tietoa saadaan esitettyä selkeäksi ja ymmärrettäväksi. Alustojen käyttöönoton jälkeen opinnäytetyössä vertaillaan alustojen käytettävyyttä ja tietoturvaa.

Käytettävyydessä käydään läpi yleisilmettä sekä alustoja kokonaisuutena. Opinnäytetyön rajallisuuden vuoksi alustoja ei käydä läpi yksityiskohtaisesti. Tietoturvallisuuteen perehdytään sen sijaan kattavammin. Tietoturvan osalta käydään läpi tärkeimpiä tietoturvatoimia, joita alustojen turvallisuudessa käytetään.

### 6.1 Käytettävyys

Alustat tarjoavat jokainen erilaisen näkymän. Käytettävyyden osalta navigointi alustoilla on tehty selkeäksi, vaikka tarjontaa eri palveluista on paljon. Omalta osalta käyttökokemuksen kannalta, AWS on tehty käyttäjälle selkeimmäksi (Kuva 9). Azuren kohdalla käyttö on myös selkeää ja visuaalisuuteen on panostettu enemmän kuin muissa alustoissa (Kuva 10). Google Cloud Platform on mielestäni alustoista sekavin (Kuva 11). Google Cloud Platformin esillepano ei ole niin yksinkertaistettu kuin muut alustat ja saattaa täten vaikeuttaa käytön aloitusta. Kaikissa alustoissa on kattavasti tarjolla valmiita tutoriaaleja eri palveluiden käytöstä.

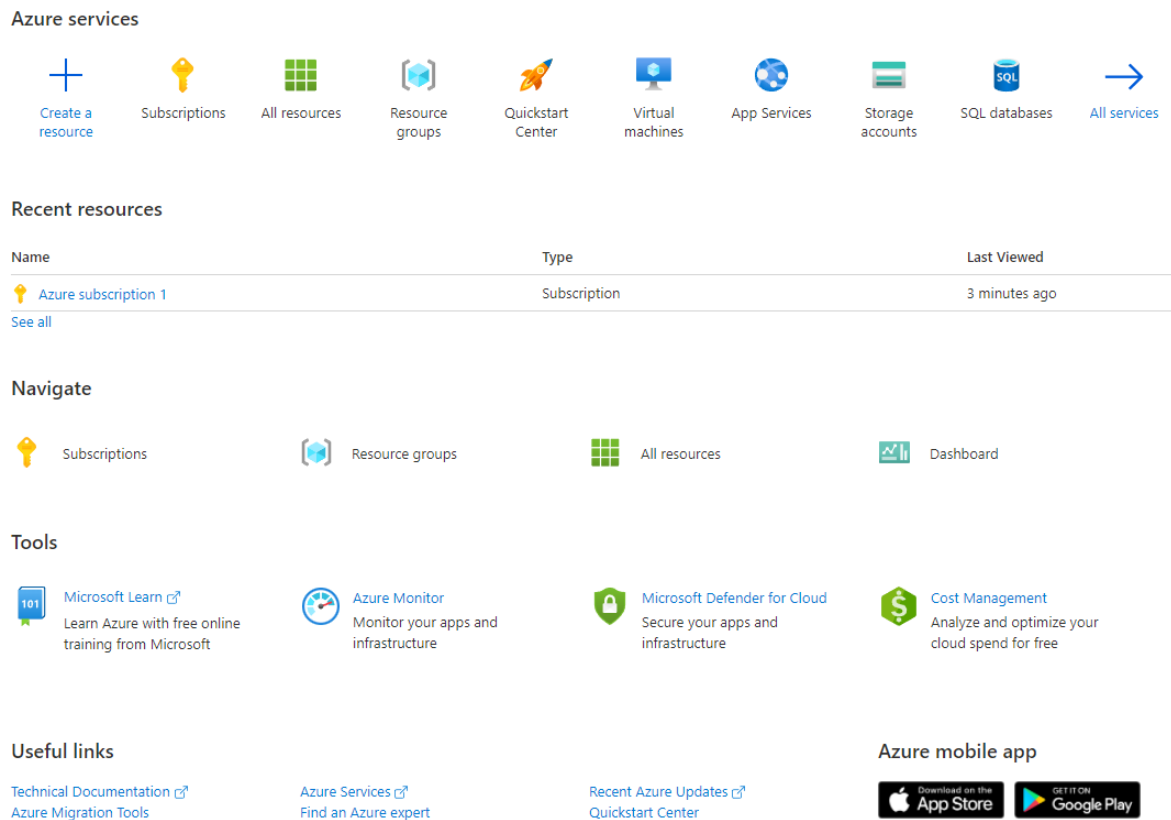
Kuva 9 Yleisnäkymä AWS:än pääikkunasta



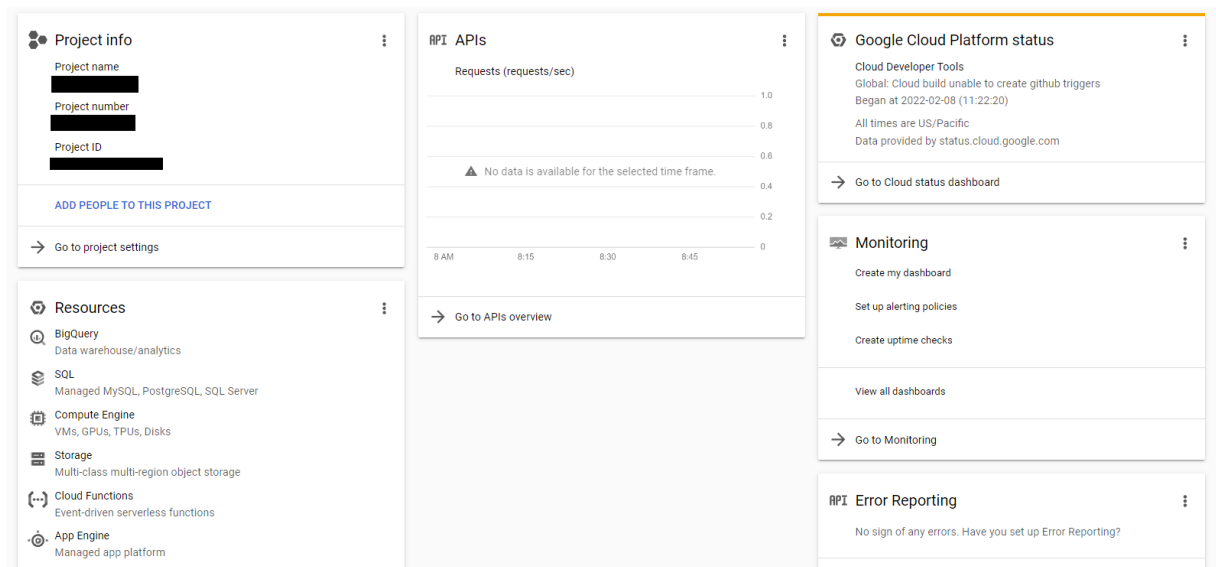
Alustojen palveluiden määrä vaihtelee. Google Cloud Platform tarjoaa yli 90 eri IT-palvelua (Acronis, n.d). Azuren pilvialustalla on noin. 200 tuotetta ja pilvipalvelua (Microsoft, n.d). AWS tarjoaa yli 200 palvelua. (Amazon, n.d)

Kaikkia alustoja voi myös käyttää mobiililaitteilla. Mobiilisovelluksen lataus on tehty helpoksi AWS:än ja Azuren kanssa. Google Cloud Platform ei suoraan omalta alustaltaan tarjoa mahdollisuutta ladata mobiilisovellusta. Mobiilisovellukset ovat ladattavissa Google Play -kaupasta ja App Storesta.

Kuva 10 Yleisnäkymä Azuren pääikkunasta



Kuva 11 Yleisnäkymä Google Cloud Platformin pääikkunasta



Käytettävyyden vertailun jälkeen eroa pilvalustojen välillä löytyy. Näistä kolmesta pilvalustasta Google Cloud Platform on käytettävyyden osalta muita jäljessä. Käyttöliittymä tuntuu sekavammalta kuin muissa alustoissa. Yritystoiminnan näkökulmasta katsottuna

yritys, joka on aloittamassa pilvipalveluiden käyttöönottoa, Microsoft Azure ja AWS on molemmat potentiaalisia vaihtoehtoja. Molemmat näistä tarjoavat kattavan tarjonnan palveluista ja tuotteista. Itse palvelujen käyttö on myös helpompaa kuin esimerkiksi Google Cloud Platformissa. Jos mietitään palveluiden näkökulmasta AWS tarjoaa kattavimman valikoiman tuotteita ja palveluita.

## 6.2 Tietoturva

Tietoturvallisuuden kannalta katsottuna kaikkien alustojen turvallisuuteen on panostettu merkittävästi. Tässä osioissa käydään läpi alustojen eri tietoturvatoimia. Taulukko 1 avaa tärkeimpiä toimia, joita alustojen tarjoajat käyttävät hyvän tietoturvan saavuttamiseksi. Taulukossa listattujen palveluiden lisäksi alustojen tarjoajilla on myös paljon muita erilaisia tietoturvapalveluita- ja tuotteita. Opinnäytetyössä käydään rajauksen vuoksi tärkeimpiä tietoturvatoimia. Taulukko on jaettu kahdeksaan eri kategoriaan: palomuuuri, kryptaus, tunnistautuminen, uhkien suojaus, protokollat, resurssienhallinta, tuki ja monitorointi.

Taulukko 1 Kooste alustojen tärkeimmistä tietoturvatoimista

	<b>Google Cloud Platform</b>	<b>Microsoft Azure</b>	<b>Amazon Web Services</b>
<b>Palomuuuri</b>	Google Cloud firewalls	Azure Firewall	AWS Firewall Manager
<b>Kryptaus</b>	AES	AES	AES
<b>Tunnistautuminen</b>	2-step verification, SSO	Azure AD Multi-Factor Authenticator	Multi-Factor Authenticator, SSO
<b>Uhkien suojaus</b>	VirusTotal	Microsoft Sentinel, Microsoft Defender for Cloud, Azure Security Center	AWS Shield
<b>Protokollat</b>	TLS	TLS	SSL/TLS
<b>Resurssienhallinta</b>	Identity and Access Management (IAM)	Azure Resource Manager (ARM)	AWS IAM
<b>Tuki</b>	Support	Microsoft Azure Support	AWS Support Center
<b>Monitorointi</b>	Cloud Monitoring	Microsoft Defender for Cloud	GuardDuty

Kaikki palveluntarjoajat tarjoavat tärkeimmät tietoturvaan liittyvät toimet alustoille. Kaikissa alustoissa on palomuuuri, joilla suojataan verkkoyhteyksiä. Kryptaus on toteutettu kaikissa AES-salausmenetelmällä. Tunnistautumiseen on saatavilla kaikissa alustoissa monivaiheinen tunnistautuminen kirjautumisen suojaamiseksi. Tunnistautuminen on helposti otettavissa käyttöön alustojen asetuksista. Mahdollisten uhkien suojaus on alustoissa tehty mahdolliseksi tarjoamalla eri palveluita. Kaikilla palveluntarjoajilla on käytössään yksi tai useampi palvelu uhkien suojaamiseen. Alustojen sisällä eri resurssinhallintatyökaluilla voidaan muun muassa muuttaa valtuuksia, rooleja ja tutustua tietoturvasäännöksiin. Jokainen alusta tarjoaa oman tuen mahdollisille vikatilanteille ja ongelmille. Käyttäjä pystyy monitoroimaan erilaisia tilastoja monitorointityökalujen avulla.

Tutkiessa alustojen tietoturvaa taulukon kautta, käy ilmi, että jokaisessa alustassa on kattavat palvelut tietoturvan turvaamiseksi. Mistään alustasta ei puutu tietoturvan kannalta tärkeitä palveluita.

### **6.2.1 Tietoturvamenetelmien tarkempi läpikäynti**

Tässä osiossa käydään läpi muutamia edellisessä kappaleissa mainittuja tietoturvamenetelmiä tarkemmin eri pilvialustoista. Osiossa katsotaan sitä, miten eri menetelmät näkyvät ja miten niiden käyttöönotto näkyy pääkäyttäjälle pilvialustojen käytön aikana.

### **6.2.2 Palomuurit**

Palomuurien säännöillä voidaan hallita ulkoa tulevaa ja sisältä menevää liikennettä. Kaikki alustat tarjoavat mahdollisuuden tehdä omia sääntöjä palomuuureihin. Ainakin Azuressa ja AWS:ssä voidaan tehdä omia palomuuureja. Google Cloud Platformissa tätä ei ole tehty yhtä helpoksi. Uudelle palomuurille tarvitsee antaa vain tarvittavat tiedot. Palomuuureja käytetään alustoissa virtuaalisten verkkojen turvaamiseen. Azure (Kuva 12) antaa pääkäyttäjän itse tehdä omia palomuuria vaivattomasti.

Kuva 12 Näkymä uuden palomuurin luomisesta Azuressa

[Home](#) > [Firewalls](#) >

## Create a firewall ...

[Basics](#) [Tags](#) [Review + create](#)

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more.](#)

### Project details

Subscription \*

(Disabled) Azure subscription 1

Resource group \*

[Create new](#)

### Instance details

Name \*

Region \*

East US

Availability zone ⓘ

None

Kuva 13 Uuden palomuurisäännön luominen Google Cloud Platformissa

**VPC network**

- VPC networks
- External IP addresses
- Bring your own IP
- Firewall**
- Routes
- VPC network peering
- Shared VPC
- Serverless VPC access
- Packet mirroring

**Create a firewall rule**

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name \*

Lowercase letters, numbers, hyphens allowed

Description

**Logs**

Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)

☐ On

☒ Off

Network \*

default

Priority \*

1000 [CHECK PRIORITY OF OTHER FIREWALL RULES](#)

Priority can be 0 - 65535

**Direction of traffic**

☒ Ingress

☐ Egress

**Action on match**

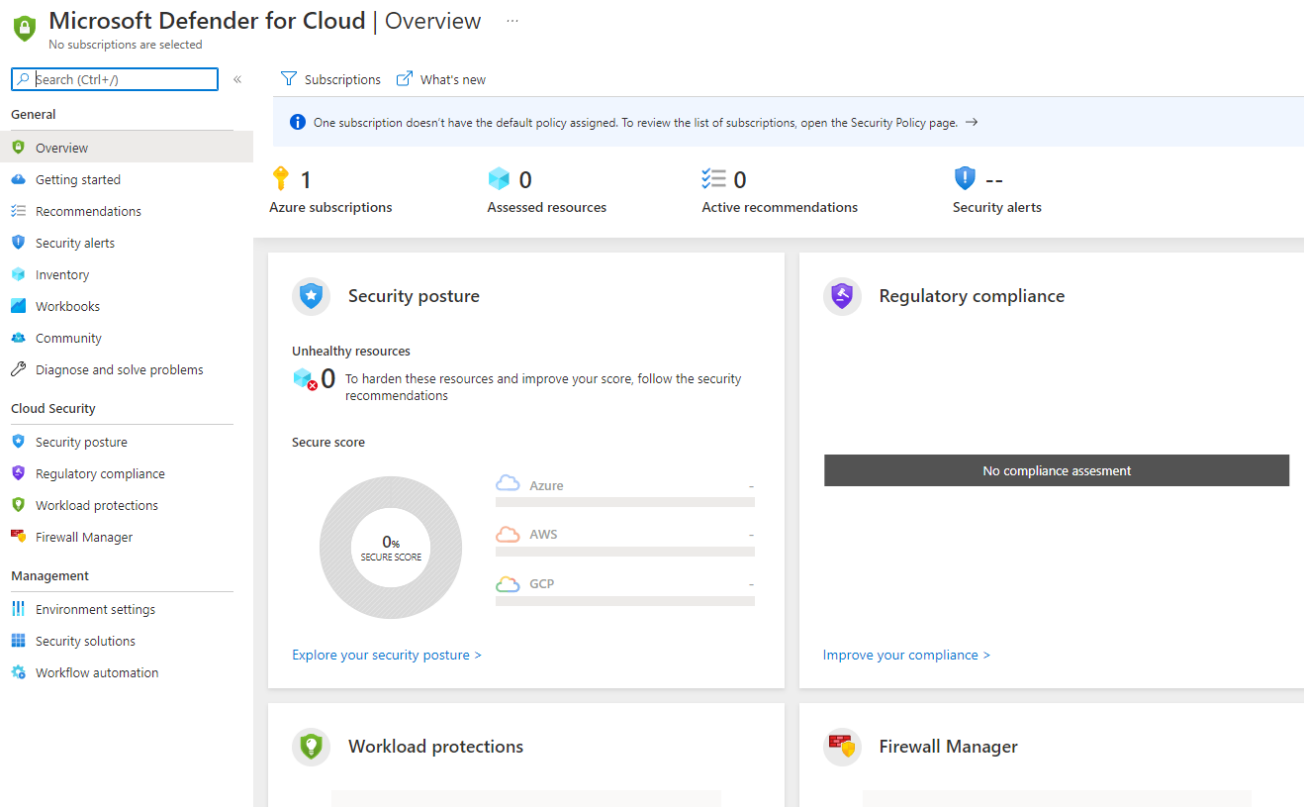
☒ Allow

### 6.2.3 Monitorointi

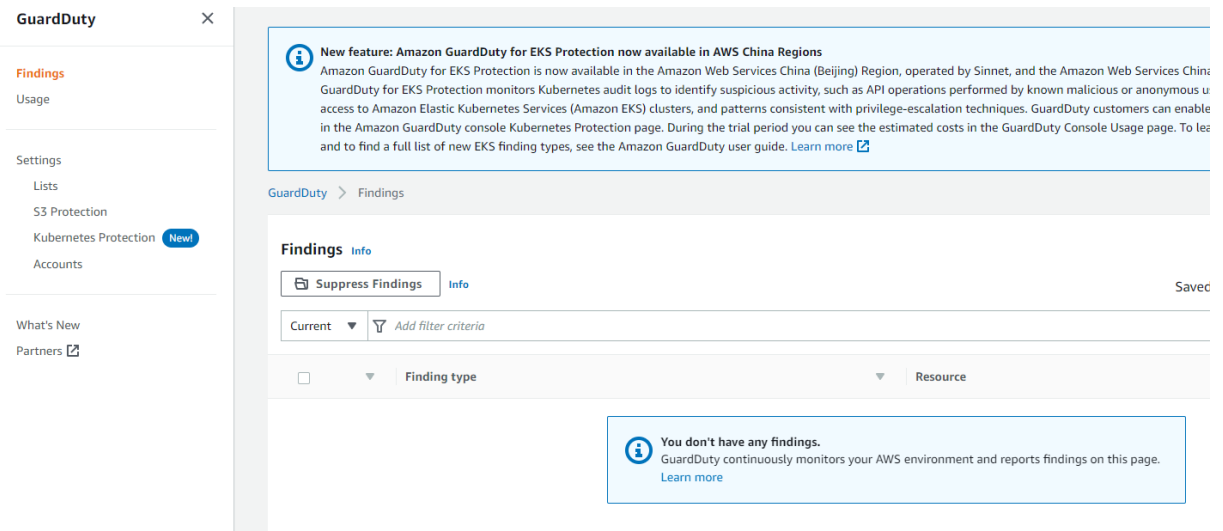
Monitoroinnilla voidaan reaaliaikaisesti katsoa ja mitata tämänhetkisiä tapahtumia pilvialustassa. Pääkäyttäjänä monitoroinnin osalta kaikki alustat tarjoavat mahdollisuuden rakentaa omia dashboardeja, joihin voi itse valita mitä kaikkea tietoja halutaan monitoroida. Dashboardeihin voi lisätä erilaisia kaavioita, pylväsdiagrammeja ja paneeleita. Monitoroiduille resursseille voidaan lisätä hälytyksiä, joiden avulla palvelu ilmoittaa, kun tietty resurssi menee yli asetetun rajan. Azuren Microsoft Defender for Cloud (Kuva 14) antaa selkeää tietoa mahdollisista uhista ja käyttäytymisestä. AWS:än oma GuardDuty (Kuva 15) monitoroi jatkuvasti AWS:än ympäristöä ja kertoo mahdollisista uhista.



Kuva 14 Näkymä Microsoft Defender for Cloud -palvelusta



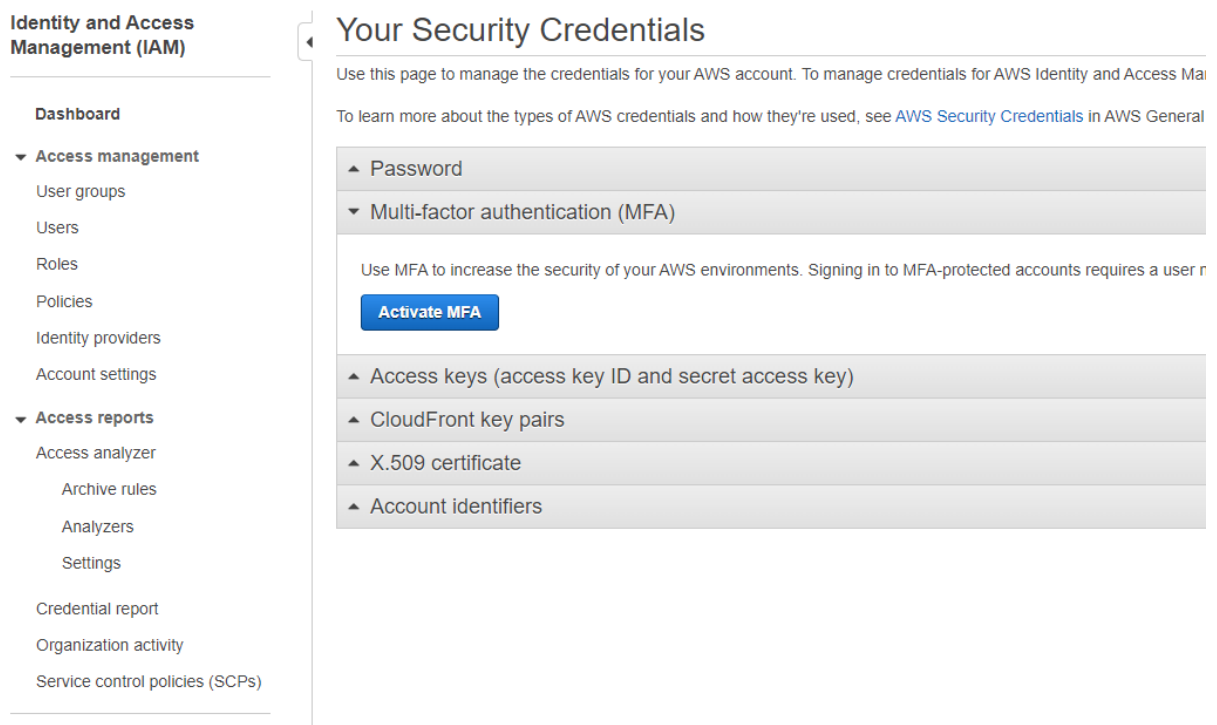
Kuva 15 AWS:än GuardDutyn näkymä



## 6.2.4 Tunnistautuminen

Tunnistautumisen eri työkaluilla voidaan pitää huoli, että asiattomat eivät pääse kirjautumaan sisään omille tunnuksille. AWS:än sisällä tunnistautuminen voidaan turvata ottamalla käyttöön MFA (Multi-Factor Authentication). Suomeksi kaksivaiheinen tunnistautuminen. Se onnistuu helposti AWS:än asetuksista (Kuva 16). Tunnistautumiseen voidaan muun muassa käyttää erillistä applikaatiota, joka voidaan ladata koneelle tai mobiililaitteille. Sisään kirjautuessa kysytään koodia, jolla päästään sisään tilille (Kuva 17). Azure ei tarjoa ilmaisessa perusversiossa mahdollisuutta käyttää kaksivaiheista tunnistautumista (Kuva 18). Google Cloud Platformissa tunnistautumisen aktivointi on tehty hankalammaksi kuin muissa alustoissa. AWS ja Google Cloud Platform tarjoaa myös Single Sign-on (SSO) eli kertakirjautumisen mahdollisuuden. Tämän avulla käyttäjien tarvitsee kirjautua vain kerran sisään ja he voivat käyttää eri palveluita ja sovelluksia.

Kuva 16 AWS:än kaksivaiheisen tunnistautumisen aktivointi



Kuva 17 Esimerkinäkymä AWS:än sisäänkirjautumisesta MFA päällä



## Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address XXXXXXXXXX@XXXXX.XXX

MFA code

**Submit**

Kuva 18 Azuren näkymä kaksivaiheisen tunnistautumisen aktivoinnista

[Home](#) >

### Multi-Factor Authentication | Overview

« [Get a free Premium trial to use this feature](#) →

**Overview**

Diagnose and solve problems

**Settings**


Block/unblock users

Providers


**Troubleshooting + Support**

New support request

## Multi-Factor Authentication

 Enhance the security and convenience of your data and applications. Microsoft Azure Multi-Factor Authentication reduces organizational risk: credentials, to secure employee, customer, and partner access. This Azure service can be used for both on-premises and cloud applications.


### Why use Azure Multi-Factor Authentication?



**SECURE APPLICATIONS AND DATA**

Require additional layer of security when accessing on-premises and cloud applications.

---



**SIMPLE TO USE**

Choose from call, text, or mobile app during registration. End users can change their method anytime.

### 6.2.5 Tuki

Tuella on tärkeä merkitys alustojen tietoturvallisuudessa. Mahdollisia ongelmatilanteisiin voidaan hakea ratkaisua alustojen asiantuntijoilta. Alustat tarjoavat erilaisia mahdollisuuksia ottaa yhteyttä tukeen. Google Cloud Platformissa voidaan ottaa yhteys joko viestillä tai puhelimitse. AWS antaa käyttäjän tehdä ”tapauksia” joihin laitetaan tiedot liittyen ongelmaan. Azuressa voidaan lähettää pyyntö, johon laitetaan vaaditut tiedot.

Vaihtoehtojen riippuvat tuen sopimuksesta. Jos tukeen haluaa ottaa yhteyttä puhelimitse, tarvitaan siihen maksullinen sopimus. Ilmaiseen tukeen sisältyy vain tilin ja laskutuksen tuki, kun taas maksulliseen sisältyy lisäksi tekninen tuki. Vastausajat riippuvat siitä, minkä sopimuksen tueksi on valinnut. Tuen sopimusta voidaan myös jälkikäteen muuttaa (Kuva 19).

Kuva 19 Google Cloud Platformin tuen hinnoittelu

Support	Support offerings			
Overview				
Cases				
Chat support				
Phone support				
Community support				
Settings				
	Basic	Standard	Enhanced	Premium
	\$0	\$29 per month + 3% of net spend	\$500 per month + 3% of net spend	\$12,500 per month + 4% of net spend (1 year minimum commitment)
	Current Plan	BUY NOW	BUY NOW	CONTACT SALES
Billing Support	✓	✓	✓	✓
Technical Support Target Initial Response Times		P2: 4 hours P3: 8 hours P4: 8 hours	P1: 1 hour P2: 4 hours P3: 8 hours P4: 8 hours	P1: 15 mins P2: 2 hours P3: 4 hours P4: 8 hours
Case Escalation			✓	✓
Technical Account Manager (TAM)				Named TAM
Technical Account Advisor Service			For Additional Purchase	
Recommenders		✓	✓	✓

### 6.2.6 Hyviä käytäntöjä alustojen tietoturvassa

Alustoja käytettäessä on hyvä ottaa huomioon eri asetusten ja käytäntöjen tärkeys tietoturvaan liittyen. Hyvillä käytännöillä voidaan edistää alustojen tietoturvaa ja tätä kautta parantamaan organisaation toimintaa.

Yhtenä hyvänä käytäntönä voidaan pitää vahvaa salasanaa. Vahva salasana sisältää joukon kirjaimia, numeroita ja erikoiskirjaimia. Kirjautumisessa on tärkeää ottaa käyttöön kaksivaiheinen tunnistautuminen, jolloin käyttäjätunnusten lisäksi kirjautuminen vaatii käyttäjän todennuksen.

Organisaation sisällä on tärkeää, että henkilöstö koulutetaan hyvin pilvipalveluihin ja tietoturvaan. Tällä voidaan varmistaa se, että henkilöstöllä on tarvittavat edellytykset tietoturvalliseen työskentelyyn organisaatiossa.

Turvallisuuden kannalta on tärkeää, että palomuri on konfiguroitu oikein ja turha ulkopuolinen pääsy on estetty. Palomuurin konfiguroinnilla voidaan estää turha ulkopuolisten pääsy verkkoon.

#### **6.2.7 Tietomurrot**

Vaikka alustat ovat mielletty turvallisiksi ja alustojen palveluntarjoajat panostavat tietoturvallisuuteen mittavilla toimilla, on alustojen tietoturvassa silti ongelmia. Isona ongelmana alustoissa ovat tietomurrot.

Viimeisin AWS:ään tapahtunut tietomurto oli joulukuussa 2021, jonka ansiosta hakkerit saivat dataa yli kolmelta miljoonalta FlexBooker käyttäjältä. Nämä tiedot altistuivat huonojen konfiguraatioiden takia. (Heiligenstein, 2022)

Azuren tietokanta Cosmos DB jäi hyökkäyksen kohteeksi vuonna 2019 haavoittuvuuden takia ja yli 3 300 Azuren käyttäjää altistui hyökkäykselle. Microsoft korjasi haavoittuneen tietokannan 48 tunnin kuluessa siitä, kun siitä ilmoitettiin. (Ricker, 2021)

Google Cloudin tietokantassa tapahtui massiivinen hakkerointi vuonna 2020. Hakkeri sai käsiin yli 200 miljoonan käyttäjän tietoja. Tietoihin kuului muun muassa henkilöiden nimet, osoitteet, puhelinnumerot, lainatiedot ja luottotiedot. (Paganini, 2020)

### 6.2.8 Pilvialustojen tietoturvan tulevaisuus

Tulevaisuudessa organisaatioiden vievän enemmän dataa ja sovelluksia pilveen, asiantuntijat ovat huolissaan tietoturvaan, säädäntöihin ja hallinointiin liittyvissä asioissa. Tärkeät tiedot organisaatioista saattavat altistua, kun kyberuhat ovat entistä hienostuneempia ja monimutkaisempia. Jatkuva monitorointi on viime vuosina kehittynyt ja tulee olemaan tärkeä osa myös tulevaisuudessa.

Haasteet ei niinkään liity itse turvallisuuteen, vaan käytäntöihin ja teknologioihin. Monet organisaatiot ovat tottuneet pilvipalveluihin. On silti epäselvää, mitä teknologiat voivat tarjota. Epävarmuuden liittyen pilvipalveluiden hyötyihin liittyy erilaisia kysymyksiä turvallisuuteen ja hallinnan malleihin liittyen. Koska turvallisuusvaatimukset lisääntyvät koko ajan, fyysinen pääsy datakeskuksiin on entistä rajatumpaa. Pääsy tulee tarvitsemaan elektronisen avaimen mutta myös mahdollinen biometrinen skannaus täytyy käydä läpi. (Seidu, 2018)

### 6.3 Alustojen tietosuoja

Tietoturvaan liittyy myös tietosuoja. Kaikkien alustojen tietosuojaan on panostettu ja sitä pidetäänkin tärkeänä osa-alueena alustojen toiminnassa. Kaikkien alustojen tietosuoja noudattaa pitkälti samoja kaavoja.

AWS haluaa turvata asiakkaiden tietoja tarjoamalla kattavan määrän palveluita ja tuotteita. AWS tarjoaa teknisiä, operatiivisia ja sopimuksenmukaisia toimenpiteitä tiedon suojaamiseen. Käyttäjä hallitsee omien tietojensa yksityisyyttä ja sitä kuka tietoihin pääsee käsiksi. Käyttäjä päättää myös, kuinka tieto kryptataan. (Amazon, n.d)

Azurea käyttäessä tiedot, jotka laitetaan säilöön tai hostaukseen ovat käyttäjän omistuksessa. Azure ei jaa käyttäjän tietoja mainontaan tai louhi tietoja mahdolliseen mainostamiseen. Azure prosessoi dataa vain käyttäjän suostumuksella ja tietoja käytetään vain asiakkaan valitsemiin palveluihin. Kun palvelun käyttö loppuu, Microsoft tuhoaa kaiken tiedon järjestelmistään. (Microsoft, n.d)

Google Cloudissa käyttäjä hallinnoi omia tietoja. Google Cloud prosessoi dataa vain sopimuksen mukaan. Google Cloud ei käytä käyttäjän dataa profiilien luomiseen tai tuotteiden kehitykseen. Google Cloud tekee toiminansa läpinäkyväksi datan keräämiseen liittyen ja ohjeiden mukaisesti noudattaa säännöksiä. Dataa ei koskaan myydä kolmannelle osapuolille ja tuotteiden kehityksessä tietoturva- ja suoja on pääosassa. (Google, n.d)

Tietosuojan osalta voidaan todeta, että kaikki ovat selvästi ottaneet tietoturvan huomioon palveluiden käytössä. Kaikilla alustan palveluntarjoajilla on selvät linjaukset, miten he käsittelevät tietoja yrityksissään.

GDPR:n noudattaminen on kaikkien palveluntarjoajien osalta otettu huomioon ja osaksi toimintaa. Tietoa GDPR:n soveltamisesta palveluntarjoajien alustoissa löytyy kattavasti palveluntarjoajien sivuilta.

## 7 Johtopäätökset

Alustojen käyttöönotto sujui ongelmitta ja oli itsessään yksinkertainen prosessi. Kaikkien alustojen käyttöönotto noudatti pitkälti samaa kaavaa. Käyttöönotoissa ei ollut suurempia eroja alustojen kesken. Ainoa suuri ero, jonka itse huomasin käyttöönotossa, oli se, että Azure ei käyttänyt tunnistautuessa pankkiohjelmaa. Opinnäytetyössä käytettiin ilmaisia versioita alustoista.

Käytettävyyden osalta käytiin läpi alustoja yleisesti ja päädyttiin johtopäätökseen, että Google Cloud Platform on näistä alustoista hankalakäyttöisin. Azure sekä AWS ovat molemmat hyvin potentiaalisia vaihtoehtoja yritystoimintaan käytettävyyden osalta. AWS tarjoaa näistä laajimman määrän palveluita ja tuo sen kannalta eniten hyötyä yritykselle.

Tietoturvan osalta opinnäytetyössä taulukoitiin tärkeimmät alustojen tietoturvatoimet. Tämän jälkeen taulukon sisältöä avattiin tarkemmin. Johtopäätöksenä voidaan todeta, että jokainen alusta sisälsi tärkeät palvelut tietoturvallisuuden kannalta. Yrityksen näkökulmasta tietoturvan osalta merkittävää eroa ei ole. Yritysten tuleekin tässä tapauksessa enemmän miettiä mahdollista valintaa omien tarpeiden mukaan. Hyvät käytännöt edesauttavat tietoturvallista pilvipalvelun käyttöä. Ongelmaksi pilvipalveluissa nousevat tietomurrot ja tulevaisuudessa kyberuhkien torjumisella on merkittävä vaikutus tietojen turvaamisessa.



## 8 Yhteenveto

Opinnäytetyön tavoitteena oli tarkastella tietoturvaa sekä tietosuojaa yleisellä tasolla. Tietoturvaa katsottiin myös yritystoiminnan näkökulmasta. Työssä käytiin myös läpi pilvipalveluita yleisesti, niiden palvelu- ja hankintamalleja sekä kokonaisuutta yritystoiminnan kannalta. Käytännönsuudessa otettiin käyttöön kolme eri pilvialustaa: Google Cloud Platform, Microsoft Azure ja Amazon Web Services, joiden käytettävyyttä ja tietoturvaa vertailtiin ja pohdiskeltiin. Asetettuihin tutkimuskysymyksiin pystyttiin vastamaan opinnäytetyötä tehdessä. Haasteita opinnäytetyölle asetti kokonaisuuden rajaaminen varsinkin käytännön osuudessa, sillä materiaalia löytyi paljon.

Opinnäytetyön prosessin myötä opin lisää tietoturvasta, pilvipalveluista, niiden ominaisuuksista ja malleista sekä tietoturvan merkityksestä pilvipalveluissa. Työssä opin myös pohtimaan näiden tärkeyttä yritystoiminnan näkökulmasta.

## Lähteet

- Acronis. (n.d). *Google Cloud Platform: What it is, how to use it, and how it compares*. Haettu 9. 2. 2022 osoitteesta <https://www.acronis.com/en-us/articles/google-cloud-platform/>
- Amazon. (2020). *Introduction to AWS Security*. Haettu 15. 2. 2022 osoitteesta [https://d1.awsstatic.com/whitepapers/Security/Intro\\_to\\_AWS\\_Security.pdf?did=wp\\_card&trk=wp\\_card](https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf?did=wp_card&trk=wp_card)
- Amazon. (n.d). *What is AWS*. Haettu 8. 2. 2022 osoitteesta <https://aws.amazon.com/what-is-aws/>
- Amazon. (n.d). *Data Protection at AWS*. Haettu 16. 2. 2022 osoitteesta <https://aws.amazon.com/compliance/data-protection/>
- Andreasson, A.;& Koivisto, J. (2013). *Tietoturvaa toteuttamassa*.
- Bergius, K. (2014). *Mikä se Azure oikein on?* Sulava. Haettu 7. 2. 2022 osoitteesta <https://sulava.com/pilvi-infrastrukturi/mika-se-azure-oikein/>
- Bigelow, S. (2017). *Google Cloud Platform (GCP)*. Haettu 7. 2. 2022 osoitteesta <https://www.techtarget.com/searchcloudcomputing/definition/Google-Cloud-Platform>
- Eronen, H. (15. 3. 2016). *IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi*. Planeetta. Haettu 7. 2. 2022 osoitteesta <https://www.planeetta.fi/2016/03/15/iaas-paas-saas-mika-pilvipalvelu-sopii-yrityksellesi/>
- Gillis, A. (2020). *Amazon Web Services (AWS)*. Haettu 8. 2. 2022 osoitteesta <https://searchaws.techtarget.com/definition/Amazon-Web-Services>
- Google. (n.d). *Privacy Resource Center*. Haettu 21. 2. 2022 osoitteesta <https://cloud.google.com/privacy>
- Hanninen, M. L. (2017). *Henkilötietojen käsittely*. Kauppakamari. Haettu 27. 1. 2022 osoitteesta [https://kauppakamaritieto-fi.ezproxy.hamk.fi/ammattikirjasto/teos/henkilotietojen\\_kasittely#kohta:Henkil\(\(f6\)ti etojen\(\(20\)k\(\(e4\)sittely](https://kauppakamaritieto-fi.ezproxy.hamk.fi/ammattikirjasto/teos/henkilotietojen_kasittely#kohta:Henkil((f6)ti etojen((20)k((e4)sittely)
- Heiligenstein, M. (4. 2 2022). *Amazon Web Services (AWS) Data Breaches: Full Timeline Through 2022*. Haettu 8. 4. 2022 osoitteesta <https://firewalltimes.com/amazon-web-services-data-breach-timeline/>
- Heino, P. (2010). *Pilvipalvelut*. Talentum Media Oy.

- Kaspersky. (n.d). *Mitä pilven tietoturvalla tarkoitetaan?* Haettu 27. 1. 2022 osoitteesta <https://www.kaspersky.fi/resource-center/definitions/what-is-cloud-security>
- Keskuskauppakamari. (2016). *Tietoturvaopas yrityksille*. Kansainvälinen keskuskauppakamari. Haettu 25. 1. 2022 osoitteesta <https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf>
- Kyberturvallisuuskeskus. (2014). *Pilvipalveluiden turvallisuus*. Viestintävirasto. Haettu 25. 1. 2022 osoitteesta [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden\\_tietoturva\\_organisaatioille.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf)
- Kyberturvallisuuskeskus. (2020). *Pilvipalveluiden turvallisuuden arviointikriteeristö*. [kuva]. Noudettu osoitteesta [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden\\_turvallisuuden\\_arviointikriteeristo\\_PiTuKri\\_v1\\_1.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf)
- Kyberturvallisuuskeskus. (2020). *Pilvipalveluiden turvallisuuden arviointikriteeristö*. Liikenne- ja viestintävirasto Traficom. Haettu 26. 1. 2022 osoitteesta [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden\\_turvallisuuden\\_arviointikriteeristo\\_PiTuKri\\_v1\\_1.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf)
- LLKY. (2019). *Tietoturva- ja tietosuojapolitiikka*. Suupohjan peruspalveluliikelaitoskuntayhtymä. Haettu 25. 1. 2022 osoitteesta [http://www.llky.fi/tiedostot/hallinto/Tietoturva\\_ ja\\_tietosuojapolitiikka2019.pdf](http://www.llky.fi/tiedostot/hallinto/Tietoturva_ ja_tietosuojapolitiikka2019.pdf)
- Microsoft. (n.d). *What is Azure?* Haettu 8. 2. 2022 osoitteesta <https://azure.microsoft.com/en-us/overview/what-is-azure/>
- Microsoft. (n.d). *Privacy in Azure*. Haettu 21. 2. 2022 osoitteesta <https://azure.microsoft.com/en-us/overview/trusted-cloud/privacy/>
- Paganini, P. (3. 4 2020). *Open Cloud Database Exposes 200 Million Americans*. Haettu 8. 4. 2022 osoitteesta <https://securityaffairs.co/wordpress/101015/data-breach/cloud-db-exposes-200m-americans.html>
- Page, V. (2021). *What Is Amazon Web Services and Why Is It So Successful?* Haettu 7. 2. 2022 osoitteesta <https://www.investopedia.com/articles/investing/011316/what-amazon-web-services-and-why-it-so-successful.asp>
- Ricker, T. (27. 8 2021). *Microsoft Azure cloud vulnerability is the ‘worst you can imagine’*. Haettu 8. 4. 2022 osoitteesta

<https://www.theverge.com/2021/8/27/22644161/microsoft-azure-database-vulnerability-chaosdb>

Seidu, R. (12. 2 2018). *Secure the Cloud: The Future of Cloud Computing & Security*. Haettu

11. 4. 2022 osoitteesta <https://content.dsp.co.uk/secure-cloud-future-cloud-computing-security>

Suomen Asiakastieto. (22. 5. 2018). *Kysymyksiä ja vastauksia GDPR:ään liittyen*. Haettu 1. 2.

2022 osoitteesta <https://www.asiakastieto.fi/web/fi/asiakastieto-media/kysymyksia-ja-vastauksia-gdpraan-liittyen.html>

Tietoevry. (2. 4. 2020). *Pilvipalvelujen haasteet – miten taklata ne pala palalta*. Haettu 28. 1.

2022 osoitteesta <https://www.tietoevry.com/fi/uutishuone/kaikki-uutiset-ja-tiedotteet/blogi/2020/pilvipalvelujen-haasteet--miten-taklata-ne-pala-palalta/>

Vento, J. (2. 4. 2021). *Mikä on pilvipalvelu?* Haettu 28. 1. 2022 osoitteesta

<https://onrego.fi/mika-on-pilvipalvelu/>

Virta, J. (2020). *Julkipilviterapiaa*. Haettu 28. 1. 2022 osoitteesta

<https://tahtogroup.fi/julkipilviterapiaa/>

Wallenius, N. (2020). *Miten pilvipalvelun tietoturva eroaa perinteisestä tietoturvasta*. Haettu

26. 1. 2022 osoitteesta <https://niklaswallenius.fi/pilvipalvelun-tietoturva-erilainen/>

## **Liite 1: Aineistohallintasuunnitelma**

Opinnäytetyöhön ei liity haastatteluita tai kyselyitä.

Aineiston kerääminen ja tallennus tapahtuu henkilökohtaiselle koneelle C-asemalle, jolle on turvattu pääsy vain opinnäytetyön tekijällä. Aineisto on varmuuskopioitu oppilaitoksen henkilökohtaiselle tilille OneDriveen. Tänne on pääsy turvattu vain sen käyttäjällä kaksivaiheisen tunnistautumisen avulla. OneDrivessä pidetään ainakin kahta viimeisintä versiota opinnäytetyöstä.