Haaga-Helia
ammattikorkeakoulu Oy

Tietoturvan ylläpitäminen julkisissa pilvialustoissa

Miko Lähdesmäki

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2020

Tiivistelmä

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä
Miko Lähdesmäki

Koulutusohjelma
Tietojenkäsittely koulutusohjelma

Raportin/Opinnäytetyön nimi
Tietoturvan ylläpitäminen julkisissa pilvialustoissa

Sivu- ja liitesivumäärä
28

Julkisten pilvialustojen käyttö kasvaa jatkuvasti, ja niihin kohdistuvat uhat ja vaatimukset sen myötä. Yksi yleisimmistä tietomurtojen aiheuttajista ovat julkisia pilvialustoja hyödyntävän yrityksen tekemät puutteelliset tai virheelliset konfiguraatiot. Monilla yrityksillä hidasteena julkiseen pilveen siirtymiselle on epävarmuus vaatimustenmukaisuudesta ja riittävästä tietoturvasta.

Tämän opinnäytetyön aiheena on tietoturvan ylläpitäminen julkisissa pilvialustoissa. Opinnäytetyön tavoitteena on selvittää ajankohtaisia tietoturvakontrolleja ja käytäntöjä julkisten pilvialusten suojaamiseen. Tutkimuksessa keskitytään suurimpien pilvipalvelutarjoajien (AWS, Azure, GCP) IaaS-alustojen tietoturvallisuuteen. Työssä käydään läpi yleistasolla pilvipalveluiden eri palvelu- ja käyttömallit, sekä asiakkaan ja pilvipalveluntarjoajan kesken jaettu vastuumalli ja sen vaikutukset tietoturvan toteuttamiseen.

Työssä selvitetään, minkälaisia uhkia ja tietoturvavaatimuksia julkisiin pilvialustoihin kohdistuu ja miten ne eroavat perinteisiin paikallisiin ympäristöihin nähden. Lisäksi käydään läpi erilaisia tietoturvaratkaisuja, joita pilven tietoturvaan on saatavilla. Työssä syvennytään CSPM (Cloud Security Posture Management) ratkaisuihin, joiden tarkoituksena on auttaa organisaatioita kartoittamaan käytettyjen pilvipalveluiden tietoturvallisuuden tasoa konfiguraatioiden ja vaatimustenmukaisuuden kannalta.

Tuloksena työssä on käyty läpi erilaisia CSPM-teknologioita, joita on saatavilla sekä julkisista pilvialustoista että kolmansilta osapuolilta. Selvityksessä käy ilmi erilaisiin käyttötapauksiin soveltuvia ratkaisuja, sekä suosituksia niiden harkintaan. CSPM-teknologiat ovat suhteellisen uusia teknologioita tietoturvamarkkinoilla, ja kehitystä niissä on odotettavissa vielä pitkään.

Ongelmat, joita CSPM-teknologioilla pyritään ratkaisemaan ovat erittäin kriittisiä ja koskevat kaikkia julkisten pilvipalveluiden käyttäjiä. Julkisten pilvipalveluiden käytön kasvaessa tarve riskien lieventämiselle korostuu, ja riskien lieventämiseen CSPM-teknologiat tai niiden kaltaiset kontrollit ovat suositeltavia.

Asiasanat
pilvipalvelut, tietoturva, vaatimustenmukaisuus

Sisällys

1 Johdanto

Julkiseen pilvialustaan siirtyminen on erittäin houkutteleva vaihtoehto monelle yritykselle, ja joillakin aloilla se on jopa liiketoiminnan kehittämisen edellytys. Pilvipohjaisen infrastruktuurin skaalautuvuus, kustannustehokkuus, käyttöönottojen nopeus sekä fyysisen tietoturvavastuun siirtäminen palvelun tarjoajalle ovat sellaisia etuja, joihin perinteinen paikallinen konesali ei pysty vastaamaan. Julkisten pilvialustojen tarjoamat ominaisuudet kehittyvät ja laajenevat nopeasti, jonka myötä houkuttelevia käyttötapauksia ilmenee jatkuvasti enemmän. Julkisiin pilviympäristöihin siirtyminen, ja niissä tarjottujen ominaisuuksien hyödyntäminen on lähtökohtaisesti helppoa ja nopeaa, eikä edellytä käyttäjältä suuria investointeja.

Pilviympäristöön siirryttäessä ilmenee ristiriitoja sen myötä, kun yritykset haluavat hyödyntää useampia tarjottuja ominaisuuksia, mutta riittäviä resursseja ei välttämättä löydy niiden tietoturvalliseen operoimiseen ja valvontaan. Kokonaiskuva pilvi-infrastruktuurista monimutkaistuu, eikä enää pystytä noudattamaan parhaita käytäntöjä tietoturvan kannalta. Näkyvyyden ja tietoturvan hallinnan puute pilviympäristöissä aiheuttaa huomattavia riskejä liiketoiminnalle, ja niistä voi pahimmillaan aiheutua erittäin suurta tai jopa korvaamatonta vahinkoa.

Pilvipalvelumarkkinoiden kasvun odotetaan kasvavan eksponentiaalisesti vuoteen 2022, ja nopeimmin kasvava pilvipalvelumarkkinoiden osa-alue on ollut selvästi IaaS, eli Infrastructure as a Service-pilvipalvelumalli. Vuonna 2018 IaaS-pilvipalveluntarjoajien tuotot olivat 30,5 miljardia dollaria, josta se kasvoi vuonna 2019 noin 39 miljardiin. Vuodelle 2020 on arvioitu, että tuotot nousevat 49,1 miljardiin. Gartnerin arvioiden mukaan yli kolmannes yrityksistä pitää investointeja pilveen tärkeimpinä. (Costello 2019.) Tietomurtojen aiheuttamat kustannukset voivat kuitenkin olla moninkertaisia pilvi-investointeihin nähden, ja siitä syystä on erityisen tärkeää, että pilven tietoturvaa pidettäisiin myös korkean prioriteetin investointina.

Tämä opinnäytetyö käsittelee niitä tietoturvan osa-alueita, joilla voidaan vähentää pilvialustojen konfiguraatiovirheistä aiheutuvia tietomurtoja, tai vähintäänkin lieventää niiden vaikutuksia. Työssä analysoidaan aiheeseen liittyviä raportteja, teknologioita, standardeja ja vaatimuksia.

1.1 Tutkimuksen tavoite

Tutkimuksen tavoitteena on kartoittaa tietoturvallisuuden osa-alueita, joita tulisi ottaa huomioon pilvialustoihin siirryttäessä. Tutkimustyyppi on suurimmilta osin sisällönanalyysia, ja lähteinä käytetään tietoturvayhteisöjen aineistoja, markkinakohtaisia analyyseja, toimialoja koskevia vaatimuksia ja regulaatioita sekä suurimpien pilvialustojen tuottamia dokumentaatioita. Tietoturvaratkaisujen osalta tarkastellaan pilvialustojen omia työkaluja, sekä joitakin kolmannen osapuolen teknologioita ja niiden ominaisuuksia.

Lopputuloksena on tuotettu tiivis selvitys teknologioista ja prosesseista, joita voidaan hyödyntää pilvialustan tietoturvan parantamisessa.

Tavoitteena on vastata seuraaviin tutkimuskysymyksiin:

- Mitä riskejä julkisiin pilvialustoihin siirtyminen sisältää, ja miten niitä voidaan lieventää?
- Minkälaisia vaatimuksia ja vastuita asiakkaan näkökulmasta julkisiin pilvialustoihin siirtymisessä on?
- Millaisia teknologioita voidaan käyttää pilvialustaa koskevien tietoturvavaatimusten noudattamiseksi?

Tutkimus rajoittuu tämän hetken suurimpiin julkipilvitarjoajiin, jotka ovat Amazon Web Services, Microsoft Azure sekä Google Cloud Platform. Pilven tietoturva on hyvin laaja aihe, eikä tässä työssä syvennytä konseptitasoa pidemmälle teknologoihin, jotka ei suoranaisesti liity itse pilvialustan konfiguraatioiden ja vaatimustenmukaisuuksien ylläpitämiseen.

1.2 Käsitteet

AWS	Amazon Web Services, Amazonin tarjoama pilvialusta
Azure	Microsoft Azure, Microsoftin tarjoama pilvialusta
GCP	Google Cloud Platform, Googlen tarjoama pilvialusta
SaaS	Software as a Service, sovellus tarjottuna internetin yli palveluna
PaaS	Platform as a Service, sovelluskehitys-alusta palveluna
IaaS	Infrastructure as a Service, IT-infrastruktuuri tarjottuna palveluna
CSPM	Cloud Security Posture Management, prosessi pilvialustan tietoturvallisuuden hallintaan
CWPP	Cloud Workload Protection Platform, teknologia työkuormien suojaamiseen
CASB	Cloud Access Security Broker, laaja ratkaisu pilven tietoturvan eri osa-alueisiin
IAM	Identity and Access Management, identiteetin- ja pääsynhallinta
DevOps	Toimintamalli, jossa yhdistyy sovelluskehitys ja operointi
DevSecOps	Sovelluskehitysprosessi, jonka osaksi on sulautettu tietoturvallisuuden hallinta
DLP	Data Loss Prevention, tietovuotojen ehkäisyyn tarkoitettu teknologia
NIST	National Institute of Standards and Technology, yhdysvaltalainen standardointivirasto
PCI-DSS	Payment Card Industry Data Security Standard, korttimaksamisen turvallisuuden tekniset vaatimukset
GDPR	General Data Protection Regulation, yleinen tietosuoja-asetus
CIS	Center for Internet Security, tietoturvayhteisö, joka tarjoaa muun muassa kyberturvallisuuden parhaita käytäntöjä

2 Pilvipalveluiden taustaa

Yhdysvaltalainen standardisointivirasto NIST on määritellyt pilvipalvelut toimintamalliksi, joka mahdollistaa pääsyn internetin ylitse käytettäviin IT-resursseihin tarpeen mukaisesti mistä tahansa. Pilvestä voidaan tarjota erilaisia resursseja kuten verkkoja, palvelimia, tallennustilaa, sovelluksia ja muita palveluita. Pilviresurssien käyttöönotto on helppoa ja nopeaa, eikä edellytä asiakkaan ja palveluntarjoajan välillä ylimääräistä vuorovaikutusta. Viraston määrittelemä toimintamalli rakentuu viidestä olennaisesta ominaisuudesta, kolmesta palvelumallista ja neljästä käyttömallista (Mell & Grance 2011).

Pilvipalveluiden viisi olennaista ominaisuutta:

- Palveluiden käyttäjä voi ottaa itsenäisesti käyttöön resursseja tarpeidensa mukaisesti, ilman vuorovaikutusta palvelun tarjoajien kanssa.

- Palveluita pystyy käyttämään internet-yhteyden välityksellä tyypillisillä päätelaitteilla, kuten kannettavat työasemat, mobiililaitteet ja tabletit.

- Palvelut käyttävät yhteisesti eri käyttäjien välillä jaettua fyysistä alustaa, joissa käyttäjien resurssit ovat loogisesti eroteltu toisistaan. Käyttäjällä ei ole mahdollisuutta hallita tai tietää tarkasti käyttämiensä resurssien alustaa, mutta voi määritellä esimerkiksi käytettävän konesalin maantieteellisen sijainnin.

- Resursseja voidaan ottaa käyttöön ja pois käytöstä välittömästi tarpeen mukaan, ja usein niiden skaalautuvuutta voidaan ohjata automaattisesti.

- Palveluiden käyttämiä resursseja optimoidaan tarpeen ja kuormituksen mukaan, joka mahdollistaa tarkan monitorointikyvyn sekä käyttäjälle että palvelun tarjoajalle.

(Mell & Grance 2011.)

2.1 Palvelumallit

Pilvipalvelumallit eroavat toisistaan pääosin niiden käyttötarkoituksen perusteella, ja vaikka yleisesti puhutaan kolmesta palvelumallista, niin on niiden välimaastossa palveluita, jotka eivät suoraan sovi ominaisuuksiltaan yksittäiseen yleiseen palvelumalliin. Käyttäjän ja pilvipalveluntarjoajan välillä myös vastuunjako vaihtelee sen mukaisesti, mitä palvelumallia hyödynnetään.

Seuraavissa kappaleissa käydään läpi lyhyesti kolmea yleisesti tunnettua palvelumallia, ja niihin liittyviä tyypillisiä käyttötapauksia. Lisäksi kuvaillaan kahta vähemmän tunnettua, mutta suosiotaan kasvattavaa palvelumallia.

2.1.1 Software as a Service (SaaS)

SaaS-mallissa käyttäjälle tarjotaan sovellus palveluna verkon ylitse. Käyttäjän ei tarvitse asentaa tai ylläpitää sovellukseen liittyviä komponentteja itse, sillä palvelun tarjoaja vastaa sovelluksen käyttämästä infrastruktuurista, kuten verkosta, palvelimista, käyttöjärjestelmistä ja päivityksistä. SaaS-palveluita käytetään tyypillisesti internet-yhteyden yli joko selaimella, mobiilisovelluksena tai kevyen asiakasohjelmiston kautta. Riippuen SaaS-sovelluksesta, on käyttäjillä yleensä mahdollisuus muokata sovelluksen sisäisiä asetuksia joissain määrin (Mell & Grance 2011). SaaS-palveluissa asiakkaan vastuulle jää tyypillisesti vain palvelun rajapinta, käyttäjätilit ja palvelussa sijaitseva asiakasdata.

SaaS-sovelluksia on saatavilla moniin käyttötarpeisiin sekä kuluttajille että yrityksille. Monet yritykset ovat siirtyneet käyttämään esimerkiksi Microsoft Office 365 tarjoamia pilvisovelluksia, jotka sisältävät tyypillisesti kaikki perinteiset Microsoftin tuottavuusohjelmistot kuten Word, Excel, Powerpoint, Outlook. SaaS-sovellukset ovat usein tilauspohjaisia.

2.1.2 Platform as a Service (PaaS)

PaaS-mallissa käyttäjälle tarjotaan palveluna sovelluskehitysympäristö. Palvelun tarjoaja ylläpitää sovelluskehitykseen tarvittavia fyysisiä järjestelmiä ja ohjelmistoja, joihin tyypillisesti sisältyy palvelimet, tietokannat, käyttöjärjestelmät, verkkolaitteet, väliohjelmistot ja tallennustilat. Usein palvelun mukana tarjotaan erilaisia lisäresursseja, kuten hallintaohjelmistoja tietokantoihin, ohjelmointikieliä ja -kirjastoja sekä sovelluskehitykseen käytettäviä työkaluja. PaaS mahdollistaa käyttäjille nopean ja kustannustehokkaan kehitysalustan, jota voidaan käyttää internetin ylitse esimerkiksi selaimen kautta. Käyttäjän vastuulle jää alustan päällä käytetyt sovellukset ja tietyiltä osin PaaS-ympäristössä käytettyjen resurssien konfiguraatiot (Rouse s.a.).

Suosittuja PaaS-palveluita ovat esimerkiksi AWS Elastic Beanstalk, Heroku, Force.com ja Google App Engine.

2.1.3 Infrastructure as a Service (IaaS)

IaaS-mallissa tarjotaan IT-infrastruktuurikapasiteettia palveluna. Käyttäjällä on mahdollisuus perustaa IaaS-ympäristöön erilaisia resursseja, kuten palvelimia, tallennustilaa ja verkkoyhteyksiä. IaaS-mallissa palvelun tarjoajan vastuulla on ainoastaan alustan fyysiset resurssit, joista kapasiteettia tarjotaan. Käyttäjän vastuulle jää IaaS-ympäristössä käytettävät resurssit, konfiguraatiot ja ohjelmistot. IaaS-palveluita käytetään usein paikallisten järjestelmien ulkoistamiseen, jolloin niiden saatavuus ja skaalautuvuus paranee, ja käyttäjän ylläpidollinen vastuu poistuu fyysisten resurssien osalta (Mell & Grance 2011).

Suosituimpia IaaS-palveluita ovat Amazon Web Services (AWS), Microsoft Azure ja Google Cloud Platform (GCP).

2.1.4 Containers as a Service (CaaS)

Konttiteknologiat ovat kasvattaneet suosiotaan huomattavasti viime vuosina, ja myös niille soveltuvia alustoja tarjotaan palveluna pilvestä. Kontteja käytetään pääosin mikropalveluarkkitehtuuriin perustuvaan sovelluskehitykseen, jossa virtualisointia tehdään laitteiston sijaan sovellustasolla. Kontit ovat perinteisiin virtuaalikoneisiin verrattuna kevyempiä, laiteriippumattomia ja joustavampia. CaaS-palvelumalli on ominaisuuksiltaan ja jaetuista vastuualueista lähimpänä IaaS-palvelumallia (Sumo Logic s.a.).

Google Container Engine (GKE), Amazon EC2 Container Service (ECS), Azure Container Service (ACS) ovat suosituimpien IaaS-palveluntarjoajien konttialustoja.

2.1.5 Function as a Service (FaaS)

Pilvialustoissa ajettavia funktiota on ollut tarjolla jo vuodesta 2014, kun Amazon julkaisi AWS Lambda-toiminnot. Microsoft julkaisi omat palvelupohjaiset funktiot Azure Function nimellä vuonna 2016. Käytännössä tämän tyyppisillä palveluilla luodaan pilvessä ajettavia loogisia toimintoja, joita perinteisesti ajettaisiin omalta palvelimelta. Nämä palvelut kuuluvat niin sanottuun serverless, eli palvelittomaan arkkitehtuuriin, jossa koodilogiikan suorittava alusta on abstraktoitu käyttäjän näkökulmasta. Käyttäjän vastuulle jää ainoastaan suoritettavan toiminnon rakenne ja sisältö.

FaaS-palveluilla voidaan rakentaa tarpeen mukaan käytettäviä loogisia toimintoja, joita voidaan skaalata käytön perusteella.

2.2 Pilven käyttömallit

Pilvipalveluiden käyttömallit on yleisesti määritelty neljään kategoriaan, joissa pilviympäristön omistajuuden taso ja käyttöoikeudet määrittelevät käyttömallin tyypin. Tässä opinnäytetyössä keskitytään julkisiin pilvipalveluihin, mutta on syytä huomioida myös muut käyttömallit, sillä edellytykset niiden tietoturvaan ovat monelta osin samanlaisia kuin julkisissa pilvipalveluissa.

Yhdysvaltalainen standardointivirasto NIST on määritellyt pilven eri käyttömallit seuraavasti:

Julkinen pilvi. Pilvi-infrastruktuuri on yleisesti käytettävissä ja julkisesti saatavilla. Palvelua tarjoava organisaatio omistaa pilviympäristön.

Yksityinen pilvi. Pilvi-infrastruktuuri on yksittäisen organisaation käytössä. Yksityistä pilveä voi ylläpitää organisaatio itse tai kolmas osapuoli. Infrastruktuuri voi sijaita joko organisaation paikallisessa konesalissa tai ulkopuolisessa tilassa.

Yhteisöpilvi. Pilvi-infrastruktuuri on jaettu useamman organisaation kesken, joilla on yhteisiä tavoitteita tai vaatimuksia pilviympäristössä. Yhteisöpilveä voi hallinnoida organisaatiot itse tai kolmas osapuoli. Yhteisöpilven infrastruktuuri voi sijaita paikallisessa tai ulkoisessa konesalissa.

Hybridipilvi. Pilvi-infrastruktuuri koostuu kahdesta tai useammasta edellä mainituista käyttömalleista, ja ne ovat sidoksissa toisiinsa siirrettävyyden tai saatavuuden saavuttamiseksi. Hybridipilveksi kutsutaan myös tapauksia, joissa perinteinen konesali on yhdistetty suoraan pilviympäristöön.

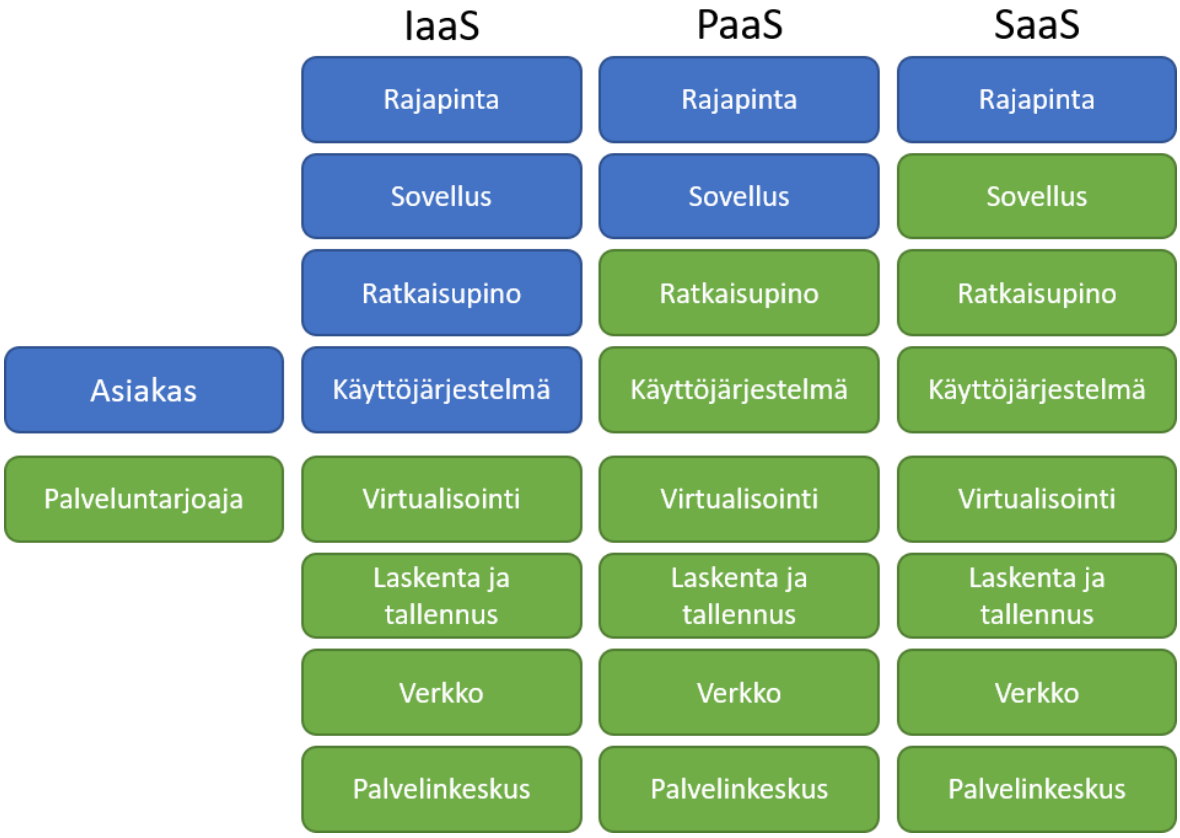
(Mogull 2017, 11-12).

Tietoturvan kannalta hybridipilvi on käyttömalleista haastavin, sillä tietoturvakontrollit ja vaatimustenmukaisuus on toteutettava kaikkien käytettyjen ympäristöjen osalta. Kääntöpuolella on taas huomioitava mahdolliset edut, joita hybridipilvellä voidaan saavuttaa. Palveluiden levittäminen julkisiin pilvialustoihin vahvistaa niiden saatavuutta ja skaalautuvuutta poikkeustilanteissa, ja ne ovat kustannustehokkaita. Suurimmilta julkipilvitarjoajilta

on saatavilla myös yksityisiä ympäristöjä, joissa kuluttajalle tarjotaan heidän käyttöönsä omistettuja fyysisiä resursseja, jotka eivät ole jaettuja muiden käyttäjien kesken. (Newcombe 2020, luku 2.)

2.3 Pilvipalveluiden vastuujakomalli

Pilvipalvelun käyttäjän ja toimittajan väliset vastuualueet määräytyvät palvelumallin perusteella, sekä kyseessä olevan palvelutoteutuksen yksityiskohdista. Palvelumallien vastuut saattavat erota toisistaan huomattavasti eri pilvipalveluntarjoajien välillä, ja sen vuoksi tärkeimpänä seikkana tietoturvan kannalta on selvittää tarkasti vastuut ja roolit käytettävässä pilvipalvelussa.

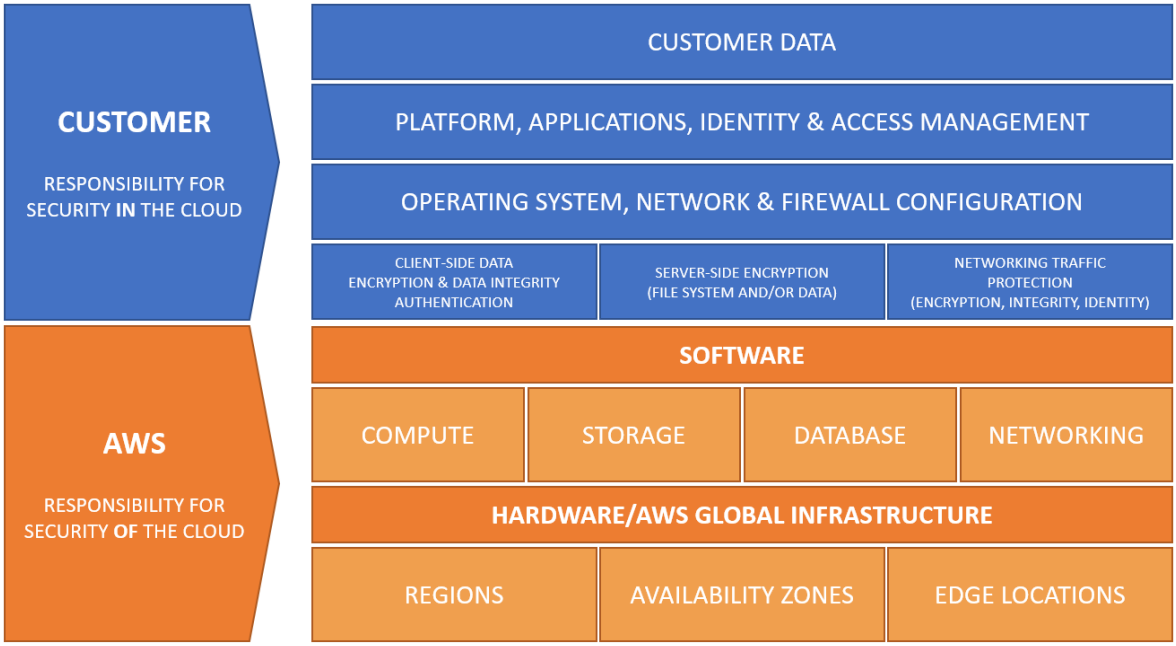


Kuva 1. Tyypillinen vastuujakomalli (mukaillen Traficom 2020.)

Julkisten pilvialustojen vastuujakomallit ovat pääpiirteittäin samanlaisia, ja etenkin suurimpien pilvipalveluntarjoajien osalta vastuualueiden jaottelu on tarkasti määritelty.

Amazon Web Services käyttää vastuualueiden kuvaamiseen jaettua vastuumallia (Shared Responsibility Model), jossa Amazonin vastuualueena on pilven tietoturva (Security ”of” the Cloud), ja asiakkaan vastuuna on tietoturva pilvessä (Security ”in” the Cloud). Sen sijaan, että vastuita kuvattaisi edellä kuvatun pilvipalvelumallin perusteella, niin AWS suosii

enemmän palveluiden abstraktiotasoa vastuualueen rajaamisen havainnollistamisessa. AWS:n vastuualueella on käytännössä kaikki pilvipalvelun osa-alueet, jotka ovat asiakkaan hallinnan ulkopuolella. Amazonin käyttämä jaettu vastuumalli havainnollistettuna kuvassa 2.



Kuva 2. AWS:n jaettu vastuumalli (mukaillen Amazon 2020a.)

AWS pitää huolen taustalla toimivasta infrastruktuurista ja fyysisestä turvasta. Asiakkaan tulee konfiguroida käyttämänsä resurssit asianmukaisesti ja varmistaa että alustassa käytetyt työkuormat pysyvät päivitettyinä. Asiakas määrittelee pääsynhallinnan, palomuurisäännöt ja tietojen salauskäytännöt. AWS tarjoaa alustallaan ohjeistuksia ja parhaita käytäntöjä, mutta asiakkaan vastuulla on kouluttaa itsensä ja muut alustalla toimivat tahot ympäristön käytöstä. (Amazon 2020a.)

Microsoft Azure ja Google Cloud Platform noudattavat saman tyyppisiä vastuujakomalleja, ja on hyvin oleellista tietoturvan kartoittamisen kannalta ymmärtää nämä vastuualueet. Centrifyn laatiman kyselyn mukaan jopa 60 % vastanneista oletti, että AWS on vastuussa käyttäjien pääsynhallinnan suojaamisesta, joka todellisuudessa on täysin asiakkaan vastuulla (Centrify 2019, 8). Veritasin laatimasta tutkimuksesta ilmeni, että jopa 83 % organisaatioista uskoo pilvialustan suojaavan asiakkaan dataa, ja 69 % uskoi voivansa asettaa kaiken vastuun tiedon suojauksesta, salaamisesta ja vaatimustenmukaisuudesta pilvipalvelun tarjoajalle (Veritas 2017).

3 Tietoturva julkisissa pilvialustoissa

Tässä kappaleessa käydään läpi yleistasolla julkisten pilvialustojen tietoturvaan liittyviä osa-alueita ja eroja fyysisen infrastruktuurin tietoturvan hallintaan. Alaotsikoissa syvennytään pilvialustoihin kohdistuviin uhkiin, tietoturvavaatimuksiin ja julkisten pilvialustojen tietoturvaan keskittyviin teknologioihin.

Tietoturvan keskeinen tavoite on varmistaa tietojen käytettävyys, eheys ja saatavuus. Tavoitteen saavuttamiseksi on olemassa IT-infrastruktuurin eri osa-alueisiin kohdistuvia tietoturvakäytäntöjä, jotka monelta osin pätee myös pilven tietoturvaan. Yritysten sisäisten palveluiden ja IT-infrastruktuurin siirtäminen kolmannen osapuolen pilvialustoihin edellyttää kuitenkin tietyillä osa-alueilla erilaisia lähestymistapoja tietoturvan tavoitteiden saavuttamiseksi. Pilvialustaan siirryttäessä luovutetaan vastuu fyysisistä tiloista ja laitteista palveluntarjoajalle, eikä näin ollen paikallisilla palomuureilla, verkkoympäristöillä tai muilla fyysiseen sijaintiin sidotuilla kontrolleilla ole tietoturvallisuuden kannalta samaa vaikuttavuutta. Vaikka perinteiset, paikallisen tietoturvallisuuden alueet koskevat monelta osin myös pilven tietoturvaa, on ymmärrettävä muuttuneet riskit, roolit ja vastuut, jotka koskevat pilviympäristöjä (Newcombe 2020, luku 3).

Perinteisessä IT-hallintomallissa tavoitteena on kontrolloida ja ylläpitää organisaation käytäntöjä, proseduureja ja standardeja, jotka kohdistuvat IT-järjestelmiin ja niiden hankintoihin. Pilvipalveluiden saatavuus, kustannustehokkuus ja käyttöönoton nopeus aiheuttaa hallinnollisia haasteita, sillä näkyvyyttä ja kontrolleja näihin palveluihin ei pystytä perinteisin tavoin toteuttamaan. Yksittäinen henkilö tai osasto pystyy ohittamaan organisaation perinteisen IT-hallinnon ottamalla pilvipalveluita käyttöön itsenäisesti, jonka seurauksena palveluiden vaatimustenmukaisuutta ja tietoturvallisuutta ei pystytä aina varmistamaan (Grance & Jansen 2011, 14).

3.1 Julkisiin pilvialustoihin kohdistuvat uhat

Yhtenä suurena erona paikallisen konesalin ja julkisen pilvi-infrastruktuurin välillä on se, miten resurssien verkkoympäristö ja siinä tapahtuvat toiminnallisuudet toteutetaan. Paikallisessa konesalissa pysytään tyypillisesti suurimmilta osin sisäverkossa, eikä julkisen internet-yhteyden kautta päästä hallinnoimaan resursseja tai käyttämään yrityksen sisäiseen käyttöön tarkoitettuja järjestelmiä. Julkiseen pilveen siirryttäessä paikallinen sisäverkko ei ole resurssien suojakerroksena, sillä palveluita voidaan käyttää tyypillisesti internet-yhteyden välityksellä. Tämän takia pilvipalveluihin oikeutetut identiteetit ja liittymäkohdat ovat kriittisiä tietoturvallisuuden kannalta (Dotson 2019, luku 4).

Pilvialustojen hallintaan liittyvät toimet toteutetaan laajalti API-rajapinnoilla, eli sovellusliittymillä. API-rajapinnat sallivat kommunikoinnin useiden sovellusten välillä, ja niitä hyödyntämällä pilvipalveluiden modulaarisuus ja rakenne yleisesti toteutetaan. Tyypillisesti pilvialustoissa tehdyt toimet tapahtuvat API-rajapintoja hyödyntäen, riippumatta siitä käytetäänkö pilvialustan tarjoamaa käyttö- tai komentoliittymää (Mogull 2017, 69-70).

Käyttäjien ja sovellusten käyttämät identiteetit pilvialustoissa omaavat rooleihinsa perustuvat käyttöoikeudet pilvialustan API-rajapintoihin, ja tästä syystä yksi houkuttelevimpia ja yleisimpiä hyökkäyskohteita ovat nämä identiteetit (Dotson 2019, luku 4).

Cloud Security Alliance-tietoturvayhteisön teettämässä, vuosittaisessa Top Threats-raportissa katselmoidaan yleisimpiä pilveen kohdistuva uhkia. Tuoreimman, vuonna 2020 julkaistun kyselyn tuloksena merkityksellisyydeltään suurimpina uhkina pidettiin seuraavia tekijöitä:

1. Tietomurrot
2. Konfiguraatiovirheet ja riittämätön muutostenhallinta
3. Pilvitietoturva-arkkitehtuurin ja strategian puute
4. Puutteellinen identiteetin- ja pääsynhallinta
5. Käyttäjätilien kaappaaminen
6. Sisäinen uhka
7. Turvattomat käyttöliittymät ja API-rajapinnat
8. Heikot käyttöliittymät hallintaan
9. Palvelun rakenteelliset puutteet
10. Näkyvyyden puute pilvikäyttöön
11. Pilvipalveluiden väärinkäyttö

(Cloud Security Alliance 2020).

Raportin yhteenvedossa mainitaan, että pilven tietoturvaa pitäisi useammin lähestyä konfiguraatioiden ja identiteetinhallinnan kannalta, eikä pelkästään perinteisten haavoittuvuuksien ja haittaohjelmien havaitsemisen pohjalta (Cloud Security Alliance 2020). Yksinomaan konfiguraatiovirheet voivat olla juurisyy monelle listatulle uhkatyypille, sillä useammat uhat ovat vältettävissä asianmukaisilla konfiguraatioilla, ja oikein käytetyillä kontrolleilla.

3.2 Tietoturvavaatimukset pilvialustoissa

Tietoturvavaatimuksilla määritellään kriteerit, joiden pohjalta tietoturvallisuutta tulisi hallinnoida ja toteuttaa. Yleisesti, erilaisten tietoturvavaatimuksien suojaustavoitteet eivät varsinaisesti eroa pilvipalveluiden ja paikallisten palveluiden välillä, mutta niiden soveltamisessa on eroavaisuuksia, johtuen jaetuista rooleista ja vastuista pilvipalveluntarjoajan ja asiakkaan välillä (Mogull 2017, 20). Organisaatioihin kohdistuvia tietoturvavaatimuksia on monenlaisia, ja ne voivat olla esimerkiksi toimialakohtaisia, ympäristöllisiä tai sääntelyiden mukaisia. Organisaatiossa saatetaan soveltaa erilaisia kriteeristöjä tai parhaita käytäntöjä, tai liiketoiminnan edellytyksenä vaaditaan tiettyjen standardien noudattamista.

Yleisiä vaatimuksia ovat esimerkiksi korttimaksamisen turvallisuuden tekniset vaatimukset PCI-DSS-standardi, tietoturvallisuuden hallintajärjestelmät ISO 27001 ja yleinen tietosuoja-asetus GDPR. Pilvialustoilla on myös usein omia parhaita käytäntöjään niissä käytettävien resurssien konfigurointiin, kuten Amazonin AWS Well-Architected-viitekehys. Yrityksissä saatetaan soveltaa erilaisia kriteeristöjä kuten pilvipalveluiden turvallisuuden arviointikriteeristöä (PiTuKri), Cloud Security Alliance-pilviturvayhteisön kriteeristöjä tai vastaavia suosituksia ja ohjeistuksia.

Paikallisten palveluiden toteutuksissa erona julkisiin pilvialustoihin on se, että lähes kaikista vaatimusten alaisista alueista vastaa organisaatio itse, eikä vastuuta jaeta kolmansien osapuolien kesken. Erityisen tärkeää pilvialustoihin siirtyessä on siis se, että varmistetaan myös pilvipalveluntarjoajan vaatimustenmukaisuus kaikilla organisaatioon kohdistuvien tietoturvavaatimusten edellyttämillä osa-alueilla. Joissakin tapauksissa julkisiin pilvialustoihin siirtyminen voi myös helpottaa tiettyihin vaatimuksiin vastaamista. Suuremmille julkisille pilvipalveluntarjoajille on usein myönnetty kattavia sertifiointeja, jotka täyttävät vaatimusten mukaisen kriteeristön. Näin ollen kaikki pilvialustan kautta tarjotut palvelut perivät pilvipalveluntarjoajan toteuttamat tietoturvakontrollit heidän vastuualueeltaan. (Amazon 2020b.)

Pilvialustoja käyttävän asiakkaan on itse toteutettava vaatimusten edellyttämät tietoturvakontrollit vastuualueillaan, johon tyypillisesti kuuluu kaikki pilvialustassa käytetyt resurssit ja niiden konfiguraatiot. Tyypillisesti pilvialustoissa on erikseen käyttöön otettavia palveluita, joilla tietoturvakontrolleja voidaan toteuttaa. Tarvittaessa on myös mahdollista käyttää kolmannen osapuolen tietoturvaratkaisuja, jotka ovat usein kattavasti liitettävissä pilvialustoihin.

3.3 Tietoturvaratkaisut julkisiin pilvialustoihin

Paikallisten palveluiden siirtäminen pilvialustoihin tarkoittaa sitä, että myös niissä käytetyt tietoturvakontrollit on toteutettava vastaavilla teknologioilla pilvialustassa. Julkisissa pilvialustoissa on tyypillisesti pilvipalveluntarjoajan omia ratkaisuja, joilla voidaan toteuttaa samoja kontrolleja kuin paikallisessa konesalissa. Tietoturvaratkaisuissa saattaa ilmetä pilvipalveluntarjoajien välillä huomattavia eroja toiminnallisuudessa, saatavuudessa ja hinnoittelussa.

Vaihtelevien ominaisuuksien lisäksi pilvipalveluntarjoajat käyttävät omia termistöjään tietoturvaratkaisuissa, ja osalla tietoturvaratkaisuista on keskenään ristiin meneviä ominaisuuksia. Tämän myötä palveluiden välisen yhdenmukaisuuden puute voi aiheuttaa huomattavia haasteita pilviympäristöjen tietoturvan hallinnassa ja kokonaiskuvan ymmärtämisessä (Grigorof 2019). Ote Adrian Grigorofin ja Marius Mocanun (EventID 2019) ylläpitämästä matriisista pilvipalveluntarjoajien tietoturvaratkaisujen eroavaisuuksista taulukossa 1.

Teknologia	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Data Loss Preventation	*Amazon Macie*	*Azure Information Protection*	*Cloud Data Loss Preventation API*
Firewall & ACLs	*Security Groups* - *AWS Network ACLs*	*Network Security Groups* - *Azure Firewall*	*Cloud Armor* - *VPC Firewall*
Web Application Firewall	*AWS WAF* - *AWS Firewall Manager*	*Application Gateway*	*Cloud Armor*
SIEM & Log Analytics	*AWS Security Hub* - *Amazon GuardDuty*	*Azure Sentinel* - *Azure Monitor*	*Chronicle Backstory* - *Event Threat Detection*

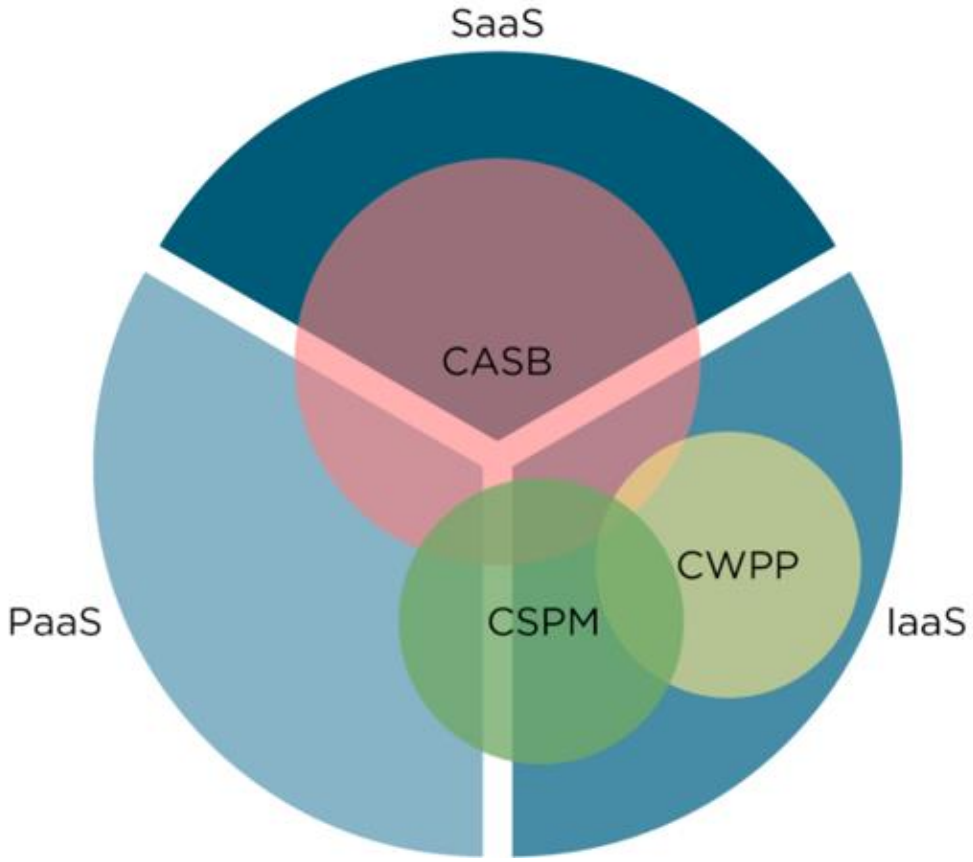
Taulukko 1. Eroavaisuuksia teknologioiden nimeämisissä pilvipalveluntarjoajien välillä

Suurimmilla julkisilla pilvialustoilla on omia, laajasti eri tarpeisiin soveltuvia tietoturvaratkaisuja, mutta joillakin puutteellisilla osa-alueilla on turvauduttava kolmannen osapuolen teknologioihin. Tarve pilvialustojen ulkoisille tietoturvaratkaisuille korostuu etenkin silloin, kun siirrytään käyttämään useampaa julkista pilvialustaa, tai pilvipalveluiden käyttö yleisesti laajenee organisaatiossa.

Pilven tietoturva on laaja ja jatkuvasti kehittyvä alue, ja tähän monimutkaisuuteen rakennetta on tuonut kansainvälinen ICT-alan tutkimus- ja konsultointiyritys Gartner määrittämällä erilaisiin pilvitietoturvan käyttötapauksiin kolme oleellista teknologiakonseptia, jotka ovat:

- Cloud Access Security Broker (CASB)
- Cloud Workload Protection Platform (CWPP)
- Cloud Security Posture Management (CSPM)

Määritellyistä teknologioista CSPM on oleellisin tässä tutkimuksessa käsiteltävän aihealueen kannalta, ja sen sisältämiin prosesseihin syvennytään tarkemmin seuraavassa pääotsikossa. CASB ja CWPP ovat oleellisia teknologioita tutkimuksen aihealueeseen liittyen, sillä teknologioiden välillä on toisiinsa vahvasti liittyviä ominaisuuksia, ja on useita tuotteita, joista löytyy kaikkia mainittuja teknologioita. Yleisesti, CASB keskittyy eniten SaaS-palveluihin, ja vaihtelevalla laajuudella muihin palvelumalleihin. CWPP keskittyy ainoastaan IaaS-alustalla käytettyjen työkuormien, kuten virtuaalikoneiden sisäiseen suojaamiseen. CSPM-ominaisuuksilla varmistetaan, että kaikki pilvialustassa hyödynnettävät resurssit ovat asianmukaisesti konfiguroitu (Loureiro 2019).



Kuva 4. CASB, CWPP ja CSPM alueet eri pilvipalvelumallien välillä. (mukaillen Loureiro 2019.)

Cloud Access Security Broker (CASB) on Gartnerin määrittelemistä teknologioista laajin ominaisuuksiltaan, ja myös asemansa markkinoilla vahvasti vakiinnuttanut pilven tietoturvaratkaisu. CASB-teknologiat perustuvat neljään ydintoiminnallisuuteen:

1. **Näkyvyys**

   CASB tarjoaa kattavan näkyvyyden organisaation pilvipalveluiden käytöstä keräämällä yksityiskohtaisia tietoja käyttäjien toimista pilvipalveluissa, riippumatta loppukäyttäjän sijainnista tai laitteesta, josta palveluita on käytetty. Joillakin CASB-tuotteilla on myös omia tietokantoja eri pilvipalveluiden luotettavuudesta, joiden avulla palveluiden käyttöön liittyviä riskejä voidaan kartoittaa (Riley & Lawson 2019, 2).

2. **Tietojen suojaus**

   CASB-ratkaisuilla voidaan havaita pilvipalveluissa käsiteltäviä arkaluonteisia tietoja. Havaintoihin perustuen voidaan asettaa käytäntöjä, joilla estetään potentiaalisia tietovuotoja ja kiellettyjä tietojen käsittelytapoja. CASB-tuotteilla voidaan esimerkiksi automaattisesti kontrolloida pilvipalvelussa sijaitsevien tiedostojen käyttöoikeuksia määriteltyihin käytäntöihin perustuen (Riley & Lawson 2019, 2).

3. **Uhilta suojautuminen**

   CASB pystyy havaitsemaan sisäisiä ja ulkoisia uhkia, kuten vääriin käsiin joutuneet käyttäjätilit ja poikkeukselliset käyttäjätoimet. Toiminnallisuus perustuu CASB-tuotteilla tyypillisesti niin sanottuun User and Entity Behavior Analytics, eli UEBA-prosesseihin, joiden avulla analysoidaan käyttäjien ja resurssien toimia poikkeavaisuuksien havaitsemiseksi. Usein CASB-tuotteisiin voidaan myös integroida ulkoisia tietoturvaratkaisuja, ja luoda säännöstöjä niiden uhkatietoihin perustuen (Riley & Lawson 2019, 2).

4. **Vaatimustenmukaisuus**

   Tyypillisesti CASB-ratkaisuissa on kyvykkyyksiä arkaluonteisen tiedon ja sen sijainnin havainnointiin sekä luokitteluun. Näiden perusteella voidaan määritellä tietojen käsittelylle käytäntöjä, joilla varmistetaan, että käsittely tapahtuu vaatimusten mukaisesti. CASB-ratkaisut keskittyvät ensisijaisesti SaaS-palveluissa käsiteltäviin tietoihin, mutta yhä useampi CASB-tuote sisältää toiminnallisuuksia, jotka ulottuvat myös IaaS ja PaaS-palveluihin (Riley & Lawson 2019, 2-3).

CASB-markkinat ovat saavuttaneet suhteellisen vakauden, ja erottuakseen markkinassa, valmistajat lisäävät CASB-tuotteisiinsa laajempia toiminnallisuuksia. Monipuoliset CASB-ratkaisut tarjoavat enemmän kyvykkyyksiä useammalle pilvipalvelulle ja vastaa erilaisiin käyttötapauksiin laajemmin. Ominaisuuksiltaan laajenevien CASB-ratkaisujen myötä yhä useampi ominaisuuksiltaan kapeampia tuotteita valmistavia yrityksiä ostetaan suoraan osaksi laajempia CASB-tuotteita (Riley & Lawson 2019, 21). Tässä työssä tutkittavat CSPM-ominaisuudet yhä useammin sisältyvät CASB-ratkaisuihin.

Cloud Workload Protection Platform (CWPP) on Gartnerin määrittelemä termi ratkaisuista, joita käytetään työkuormien suojaamiseen. CWPP-ratkaisuilla voidaan suojata hybridiympäristöissä sijaitsevia työkuormia, jotka voivat olla fyysisiä palvelimia, virtuaalikoneita, kontteja (CaaS) tai serverless-funktioita (FaaS). CWPP koostuu kahdeksasta kontrollitasosta:

1. Kovennus, konfiguraatioiden- ja haavoittuvuuksien hallinta
2. Verkon palomuuraukset, näkyvyys ja mikrosegmentointi
3. Järjestelmän eheyden varmistaminen
4. Sovellusten hallinta
5. Muistin suojaus
6. Päätelaitteen suojaus, monitorointi ja uhkien havaitseminen
7. Laitekohtainen tunkeutumisen havaitsemisjärjestelmä
8. Haittaohjelmien skannaus

CWPP-ratkaisut ovat monelta osin rinnastettavissa CSPM-ratkaisuihin, sillä molemmilla teknologioilla on tarkoitus suojata pilviresursseja. CWPP suojaa työkuormia niiden sisältä, ja CSPM suojaa niiden ulkopuolella olevia osa-alueita, kuten työkuormien käyttämien resurssien vaatimustenmukaisia konfiguraatioita. Pilvialustan kokonaisturvallisuutta ajatellen molemmat teknologiat ovat hyvin oleellisia. Yhä useampi suuremmista CASB-tuotteista sisältää molempia teknologioita (MacDonald 2019a).

4 Cloud Security Posture Management

Tässä kappaleessa syvennytään prosesseihin, joilla julkisten pilvialustojen vaatimustenmukaisuutta ja konfiguraatioiden tilaa voidaan käytännössä valvoa. Gartner on määritellyt tähän tarpeeseen Cloud Security Posture Management, eli CSPM-prosessin. Määritelmän mukaan CSPM-prosesseilla valvotaan pilviympäristöjä jatkuvasti niissä esiintyvien riskien varalta tarkastelemalla resursseja ja vertaamalla niiden konfiguraatioita yleisiin viitekehyksiin, parhaisiin käytäntöihin, regulaatiovaatimuksiin ja organisaation omiin tietoturvavaatimuksiin. CSPM ydintoimintona on siis estää, havaita ja reagoida pilviympäristöissä esiintyviin vaatimustenmukaisuuden poikkeamiin sekä konfiguraatiovirheisiin automaattisesti. (MacDonald 2019b, 1).

Kuten aikaisemmissa kappaleissa on käyty läpi, ovat pilvessä esiintyvien tietomurtojen ja -vuotojen juurisyynä usein konfiguraatiovirheet tai puutteellinen näkyvyys omaan pilviympäristöön. Julkiseen pilvialustaan siirryttäessä on ymmärrettävä jaetut vastuut, ja hyödynnettävä pilvialustan tarjoamia välineitä ympäristössä käytettävien resurssien suojaamiseen. Gartner on arvioinut, että vuoteen 2021 mennessä lähes puolilla pilvipalveluita käyttävillä yrityksillä on tietämättään puutteita pilviympäristönsä konfiguraatioissa, ja lähes kaikki pilviympäristöissä tapahtuvista virheistä tulevat tapahtumaan asiakkaan toimesta (MacDonald 2019b, 2). Cybersecurity Insiders-tietoturvayhteisön teettämän kyselyn mukaan haastavimpia asioita pilviympäristön suojaamiseen liittyen ovat vaatimustenumukaisuuden ylläpitäminen, näkyvyys pilviympäristöön ja osaavan työvoiman puute (Cybersecurity Insiders 2019, 7). Kyselyn mukaan suurimpina uhkina julkisissa pilvialustoissa pidettiin luvattomia pääsyjä pilviresursseihin, suojaamattomia API-rajapintoja ja konfiguraatiovirheitä (Cybersecurity Insiders 2019, 8).

Julkiset pilvialustat kehittyvät erittäin nopeasti, ja monet organisaatiot ovat siirtyneet käyttämään useampaa palvelun tarjoajaa. Pilviympäristöjen hallinta muuttuu jatkuvasti haastavammaksi, kun uusia palveluita lisätään alustoihin, eikä näkyvyyttä tai resursseja niiden asianmukaiseen ylläpitämiseen välttämättä ole riittävästi. Julkiset pilvialustat kuten Amazon Web Services, Google Cloud Platform ja Microsoft Azure ymmärtävät niiden monirakentuneisuuden aiheuttamat haasteet, ja tarjoavat alustoissaan erilaisia työkaluja, joilla CSPM-prosessin mukaisia toimintoja voidaan toteuttaa. Haittapuolena on se, että työkalut ovat tarkoitettu käytettäväksi vain omilla alustoillaan, jolloin ylläpidollinen kuormitus on moninkertainen verrattuna tilanteeseen, jossa käytettäisiin yksittäistä CSPM-ratkaisua kaikkiin käytössä oleviin pilvialustoihin.

Kuten useammat pilvialustoihin tarkoitetut työkalut, myös suurin osa tarjolla olevista kolmannen osapuolen CSPM-ratkaisuista hyödyntää pilvialustojen API-rajapintoja toiminnallisuuksissaan. Tästä syystä kynnys ratkaisujen kehittämiselle on lähtökohtaisesti matala, ja se näkyy myös markkinassa laajana ja ominaisuuksiltaan vaihtelevana tarjontana. Gartner on arvioinut, että CSPM-tuotteet eivät todennäköisesti tulisi pysymään itsenäisinä ratkaisuina, vaan ne tulevat sulautetuksi osaksi laajempia pilven tietoturvaratkaisuja. Useita, pelkästään CSPM-teknologioihin keskittyneitä yrityksiä on ostettu osaksi suurempia tunnettuja tietoturvayrityksiä. CSPM-ominaisuuksia yritysostoksilla ovat hankkineet yritykset, kuten Palo Alto Networks, Check Point Software, Trend Micro ja Sophos. (MacDonald 2019b, 15.)

Tässä kappaleessa tarkastellaan tarkemmin, mitä CSPM-prosesseihin käytännössä sisältyy, ja miten prosesseja suositellaan sovellettavan. Lisäksi tarkastellaan suosituimpien julkisten pilvipalveluntarjoajien työkaluja, sekä kolmannen osapuolen tuotteita joilla CSPM-prosesseja voidaan toteuttaa. Tässä tutkimuksessa ei syvennytä yksityiskohtaisiin arviointeihin tai vertailuihin työkalujen osalta, vaan tavoitteena on kartoittaa tämänhetkistä tarjontaa ja tuoda esiin erilaisiin käyttötapauksiin soveltuvia suosituksia.

4.1 CSPM-prosessit käytännössä

Ensisijaisesti CSPM-ratkaisuilla pyritään välttämään pilvialustoissa tapahtuvia virheellisiä konfiguraatioita. Virheelliset konfiguraatiot voivat kohdistua esimerkiksi käyttäjätileihin, virtuaalikoneisiin, tietokantoihin, verkkoasetuksiin ja pilvitallennustiloihin. CSPM-ratkaisuissa on tyypillisesti sääntökokoelmia, joita vasten pilvialustan resurssien konfiguraatioita tarkastellaan. Säännöt ovat yleensä koottuja parhaita käytäntöjä, regulaatiovaatimuksia tai standardeja. Monesti yrityksillä on myös omia vaatimuksia pilvialustan turvaamiseen, ja siihen tarpeeseen monilla CSPM-ratkaisuilla on mahdollisuus luoda omia sääntöjä. CSPM-ratkaisuilla valvotaan pilvialustan sisältämiä konfiguraatioita jatkuvasti, ja kaikki tiedot kerätään keskitettyyn näkymään, josta kokonaiskuva pilvialustan riskeistä ja korjausehdotuksista löytyvät. Joissakin CSPM-ratkaisuissa on myös mahdollisuus automaattisiin korjaustoimenpiteisiin sääntöjen pohjalta.

Esimerkkinä CSPM-käyttötapaukseen kuvitellaan yhdysvaltalainen yritys, jonka liiketoiminta perustuu vahvasti verkkokaupankäyntiin. Yritys on laajentamassa tarjontaansa EU-alueelle, jonka seurauksena on noudatettava GDPR-regulaatiovaatimuksia. Tämän laajennuksen lisäksi verkkokauppa halutaan siirtää kokonaan yksityisestä hybridipilvestä julkiselle pilvialustalle, ja tätä varten yritys on hankkinut kolmannen osapuolen rakentamaan uuden verkkokauppaympäristön. Haasteena yrityksellä on varmistaa, että verkkokauppa

rakentuu asetettujen vaatimusten rajoissa, ja että sitä tullaan jatkossa myös ylläpitämään vaatimusten mukaisesti.

Haasteita varten yritys on ottanut käyttöönsä CSPM-ratkaisun, jolla saadaan keskitetysti jatkuva näkyvyys uuteen pilvialustaan ja siinä käytettyihin resursseihin. CSPM-ratkaisussa otetaan käyttöön vaatimusten mukaiset säännöt ja parhaat käytännöt, joiden rajoissa uutta ympäristöä tullaan rakentamaan. CSPM-ratkaisulla valvotaan, ettei pilvialustassa käynnistetyt resurssit ja niiden konfiguraatiot tuota yritykselle ylimääräisiä riskejä, ja yritykseen kohdistuvia vaatimuksia noudatetaan. Ratkaisu helpottaa myös kolmannen osapuolen toimittajan työtä siten, että heidän kehitystyönsä tulee tapahtumaan CSPM-ratkaisussa asetettujen rajojen puitteissa. Lopputuloksena CSPM-ratkaisuilla lievennetään huomattavasti laajaan migraatioprojektiin liittyviä riskejä, ja kaikilla osapuolilla on keskitetty ja dynaaminen näkymä pilvialustan sisällöstä ja tapahtumista.

CSPM-prosessit tulisi nähdä osana julkisiin pilvialustoihin sovellettavaa tietoturvastrategiaa. CSPM-ratkaisujen sisältämillä ominaisuuksilla mahdollistetaan pilvialustojen jatkuva tietoturvallisuustason tarkastelu tietoturvavaatimuksiin ja parhaisiin käytäntöihin verraten. CSPM-prosessit soveltuvat esimerkiksi hyvin osaksi laajasti käytettyä DevOps-toimintamallia, jossa palveluiden kehitys tapahtuu nopealla ja jatkuvalla julkaisusyklillä. DevOps-toimintamallia sovellettaessa pilvialustoissa on tyypillistä, että kehittäjät luovat, muokkaavat ja poistavat alustassa käytettyjä resursseja jatkuvasti. Tästä syntyy myös tarve sille, että käytettyjen resurssien konfiguraatiot pysyisivät tietoturvallisina ja tavoitteiden mukaisina. Kehittäjien päätehtäviin ei tyypillisesti sisälly tietoturvasta huolehtiminen kaikilla eri osa-alueilla, ja tämän seurauksena tietoturvan toteutuksessa saattaa esiintyä puutteita, ja kokonaiskuva pilvialustan tietoturvasta jää epäselväksi. (MacDonald 2019b, 4-5.)

DevOps-toimintamalliin voidaan sisällyttää tietoturva omaksi osa-alueeksi, jolloin puhutaan niin sanotusta DevSecOps-toimintamallista, jossa tietoturvallisuuden toteuttamiseen otetaan osaksi tietoturva-asiantuntijoita ja -teknologioita. Tällä toimintamallilla vähennetään tietoturvavastuualueita kehittäjiltä, ja varmistetaan tietoturvallisuuden asianmukainen toteutus kaikilla osa-alueilla. CSPM-prosesseilla voidaan toteuttaa jatkuvaa ja automaattista tietoturvallisuuden kartoitusta ja asettaa kehittäjille ohjaavia rajoitteita. (Cornell University 2017.) CSPM-prosessien myötä kehittäjien vastuulle jää vähemmän tietoturvapäätöksiä, ja asetettuja rajoja voidaan määritellä joustavasti sekä kehitys että tuotantovaiheissa.

CSPM-prosesseja voidaan luonnollisesti soveltaa myös tapauksiin, joissa ei varsinaista DevOps-toimintamallia hyödynnetä. Pilvialustojen tietoturvaa tulisi tarkastella mahdollisimman kattavasti riippumatta siitä, miten ja mihin tarkoitukseen alustoja käytetään, sillä lähes kaikki onnistuneet hyökkäykset pilvipalveluihin johtuvat puutteellisista konfiguraatioista tai hallinnallisista virheistä. CSPM-prosessit kohdistuvat näihin ongelmakohtiin. (MacDonald 2019b, 3.)

4.2 CSPM-ratkaisut julkisissa pilvialustoissa

Julkiset pilvialustat tarjoavat erilaisia ratkaisuja CSPM-prosessien toteuttamiseksi. Tässä kappaleessa käydään läpi Amazonin, Googlen ja Microsoftin tarjoamia ratkaisuja, jotka soveltuvat CSPM-prosessien toteuttamiseen.

4.2.1 Amazon Web Services

AWS Config

AWS Config-palvelu soveltuu käyttötapauksiin, joissa tarvitaan näkyvyyttä käytettyjen resurssien konfiguraatioihin ja niihin tehtyihin muutoksiin. Palvelussa voidaan asettaa resurssikohtaisia konfiguraatiovaatimuksia, joita määritellään konfiguraatiosäännöillä. Konfiguraatiosääntöinä voidaan käyttää valmiiksi koottuja sääntöpohjia (Conformance Pack), joita on mahdollista käyttää pohjana omien sääntöjen asettamiseen.

Palvelussa voidaan valvoa keskitetysti useamman AWS-tilin konfiguraatioiden vaatimustenmukaisuutta ja muokkaushistoriaa. Konfiguraatioissa ilmenneistä poikkeamista voidaan luoda automaattisia hälytyksiä sekä korjaustoimenpiteitä, jotka vaativat toiminnallisuuksissaan muita AWS-palveluita. (Amazon 2020c.)

AWS Trusted Advisor

AWS Trusted Advisor-palvelulla saadaan yleisemmän tason suosituksia ja parhaita käytäntöjä AWS-ympäristön osa-alueisiin. Suosituksia tarjotaan viiteen eri osa-alueeseen, jotka ovat kulujen optimointi, suorituskyky, turvallisuus, vikasietoisuus ja palvelurajat.

AWS Trusted Advisor ei ole kattavin palvelu CSPM-prosesseja ajatellen, eikä sitä voi juurikaan laajentaa tekemällä esimerkiksi omia säännöstöjä tai määritelmiä. Palvelu on kuitenkin hyödyllinen ja käytettäväksi suositeltava, mikäli palvelun kattamiin osa-alueisiin ei muuten ole seurantaa käytössä. (Amazon 2020d.)

AWS Control Tower

AWS Control Tower palvelulla voidaan hallinnoida useammasta AWS-tilistä koostuvaa AWS-ympäristöä. Palvelun kautta voidaan luoda tilejä ympäristöön, joihin koskevat automaattisesti yhteiset asetetut säännöt ja rajoitteet. Tilien luontia varten voidaan tehdä mallipohjia, joihin perustuen uudet AWS-tilit luodaan ympäristöön. Palvelun toiminnallisuus koostuu useammasta AWS-palvelusta, joihin lukeutuu myös aikaisemmin läpikäyty AWS Config-palvelu.

AWS Control Tower yhdistää pilviympäristön hallinnollisia toimia ja yksinkertaistaa ylläpidollista työtä. Ympäristön vaatimustenmukaisuutta voidaan valvoa ja hallinnoida keskitetystä käyttöliittymästä. (Amazon 2020e.)

AWS Security Hub

AWS Security Hub-palveluun voidaan keskittää AWS-ympäristöstä löytyviä tietoturvahavaintoja toisista AWS-palveluista tai kolmannen osapuolen tietoturvatuotteista. Palvelun kautta voidaan kerätyn aineiston perusteella tarkastella resurssien vaatimustenmukaisuutta ja parhaiden käytäntöjen noudattamista. (Amazon 2020f.)

4.2.2 Microsoft Azure

Azure Policy

Azure Policy-palvelulla voidaan määritellä ja valvoa organisaation edellyttämiä tietoturvavaatimuksia Azure-ympäristössä käytetyissä resursseissa. Palvelun kautta voidaan tarkastella keskitetysti resurssien vaatimustenmukaisuutta ja asettaa automaattisia korjaavia toimenpiteitä säännöistä poikkeaville resursseille. (Microsoft 2020a.)

Azure Blueprints

Azure Blueprints on palvelu, jolla voidaan määritellä standardit ja vaatimukset, joita sovelletaan Azure-ympäristöjen luontiin ja hallinnointiin. Palvelussa tehtyjä määritelmiä voidaan luoda useampia ja niitä voidaan käyttää uudelleen, mahdollistaen kattavan ja jatkuvan johdonmukaisuuden Azure-ympäristöjen luontiin. Azure Blueprints-pohjilla voidaan tehostaa ympäristöjen luontia ja varmistaa samalla niiden vaatimustenmukaisuus. Azure Blueprints-pohjat koostuvat erinäisistä resurssimalleista ja artefakteista, joita yhdistämällä voidaan luoda haluttu mallipohja ympäristöjen luomiseen. Palvelussa on myös saatavilla valmiita mallipohjia yleisiin standardeihin ja regulaatiovaatimuksiin. (Microsoft 2020b.)

Azure Management Groups

Azure Management Groups on hallinnollinen palvelu Azuressa, joka mahdollistaa määritettyjen käytäntöjen, pääsynhallintasääntöjen sekä vaatimustenmukaisuuden valvonnan kohdentamisen valituille ryhmille. Management Groups käyttää hyödykseen Azure-ympäristön tilauksia, joita ryhmittämällä voidaan hallinnoinnista tehdä joustavampaa ja nopeampaa. Management Groups muodostaa hierarkkisen kokonaisuuden, jolloin haluttuja sääntöjä ja määräyksiä voidaan kohdentaa käyttäjille matalalta tai korkealta tasolta, tarpeen mukaisesti. (Microsoft 2020c.)

Azure Security Center

Azure Security Center on Azuren sisäisten ja ulkoisten resurssien suojaamiseen kehitetty työkalu, joka tarjoaa näkyvyyttä, suosituksia ja parhaiden suojauskäytäntöjen mukaisia toiminnallisuuksia resurssien suojaamiseen. Security Center mahdollistaa ympäristöjen jatkuvan valvonnan ja arvioinnin, joka avustaa tietoturvapuutosten paikantamisessa ja töiden priorisoinnissa. Security Centerin toiminnallisuus on kohdennettavissa IaaS-, PaaS-, ja SaaS-tyyppisiin resursseihin, mutta osa alustan avustavista toiminnoista vaatii maksullisen version hyödyntämistä. (Microsoft 2020d.)

4.2.3 Google Cloud Platform

Google Cloud Platform-pilvialustassa on käytettävissä Security Command Center-palvelu, joka on keskitetty hallintapaneeli GCP-ympäristön tietoturvaan ja riskienhallintaan. Palvelun avulla voidaan monitoroida pilviympäristössä käytettyjä resursseja ja niiden konfiguraatioiden vaatimustenmukaisuutta. Security Command Center ulottuu myös resurssien tarkempaan monitorointiin, kuten arkaluontoisten tietojen ja haavoittuvuuksien havainnointiin. Osa palvelun toiminnallisuuksista edellyttää muiden palveluiden liittämistä Security Command Centeriin. (Google 2020.)

4.3 Kolmannen osapuolen CSPM-ratkaisut

Kuten edellisistä kappaleista kävi ilmi, on julkisissa pilvialustoissa kattavasti tarjolla erilaisia työkaluja CSPM-prosessien toteuttamiseen, ja ne saattavat monissa käyttötapauksissa olla riittäviä, etenkin jos käytetään vain yhtä pilvialustaa. Monelle organisaatiolle on kuitenkin todennäköistä, että pilvialustojen käyttö laajenee useampaan tarjoajaan, ja nii-

den ylläpitämiseen tarvitaan huomattavasti enemmän resursseja. Tilanteissa, joissa pilvialustojen tarjoamat työkalut eivät riitä kattamaan tarpeita, on suositeltavaa harkita keskitettyä, kolmannen osapuolen CSPM-työkalua.

Useammat CSPM-työkalut rakennetaan julkisten pilvialustojen API-rajapintoja hyödyntäen, joka tarkoittaa sitä, että CSPM-ratkaisujen toteuttamiselle on suhteellisen matala kynnys. Tästä syystä markkinoilla on paljon tarjolla eri tasoisia ja ominaisuuksiltaan vaihtelevia tuotteita, jotka rajoittuvat monilta osin pilvialustojen tarjoamiin API-rajapintoihin. 2019–2020 välisenä aikana monet johtavat tietoturvayritykset ovat laajentaneet pilvitietoturvatarjontaansa hankkimalla CSPM-ominaisuuksia yritysostoin. Tässä kappaleessa tarkastellaan joidenkin suurimpien yritysten tarjoamia CSPM-ratkaisuja.

4.3.1 Trend Micro Cloud Conformity

Trend Micro on 1988 perustettu japanilainen tietoturvayritys, joka erikoistuu hybridipilvien, päätelaitteiden ja tietoverkkojen tietoturvaratkaisuihin. Yrityksen tarjoamat pilven tietoturvaratkaisut on koottu Cloud One-palvelukokonaisuuden alle, josta on mahdollista ottaa käyttöön yksittäisiä teknologioita erilaisiin käyttötapauksiin. Teknologioita on tarjolla sovellusten, työkuormien, konttien, verkkojen ja pilvitallennustilojen suojaamiseksi. Osaksi Cloud One kokonaisuutta Trend Micro osti vuoden 2019 lopulla Cloud Conformityn, joka on 2016 perustettu CSPM-teknologiaa kehittävä yritys. (Trend Micro 2020a.)

Conformity on alun perin AWS-ympäristöihin keskittynyt CSPM-ratkaisu, ja edelleen suurin osa toiminnallisuuksista on saatavilla ainoastaan niihin. Conformity on laajentanut toiminnallisuuksia joiltain osin myös Microsoft Azureen, ja Google Cloud Platform on tulossa osaksi tuettuja alustoja tulevaisuudessa. Azure- ja AWS-ympäristöihin on molempiin saatavilla sääntöpohjaisia tarkistuksia ja korjausohjeistuksia, jotka perustuvat pilvialustojen parhaisiin käytäntöihin sekä yleisiin regulaatiovaatimuksiin ja standardeihin, kuten GDPR, NIST, CIS, PCI-DSS. Sääntöjä on myös mahdollista luoda itse, mutta ne ovat käytettävissä tällä hetkellä ainoastaan AWS-ympäristöissä integroimalla Conformity AWS Config-palveluun. (Trend Micro 2020b.)

Conformity on liitettävissä tehtävienhallintaratkaisuihin kuten Jira, Slack, Zendesk ja ServiceNow. Conformity-alustaan on myös mahdollista liittää vahvoja kertakirjautumisratkaisuja, kuten Okta, Microsoft ADFS tai Azure AD. Conformity-alustaa voidaan hallinnoida myös API-rajapintojen avulla, joka lisää palvelun käytön joustavuutta ja integraatiomahdollisuuksia. (Trend Micro 2020b.)

Edellisten ominaisuuksien lisäksi AWS-ympäristöihin on saatavilla CloudFormation-pohjien skannaukset, konfiguraatioiden automaattiset korjaukset sekä reaaliaikainen uhkien monitorointi. Conformity on saatavilla kahdessa tuotepaketissa, josta edullisempi sisältää kaikki ominaisuudet, paitsi reaaliaikaisen uhkien monitoroinnin. Tuote on kuukausihinnoiteltu AWS/Azure-tilien määrän mukaan, ja tuotteesta on mahdollista saada määräalennusta. (Trend Micro 2020c.)

Conformity on listattu Amazonin virallisena teknologiakumppanina, ja se on tästä syystä hyvin kypsä CSPM-tuote AWS-ympäristöihin. Conformity ei vielä sovellu hyvin käyttötapauksiin, joissa on runsaasti Azure tai Google Cloud Platform-ympäristöjä. Tuote soveltuu parhaiten tapauksiin, joissa pääosin käytetään AWS-ympäristöjä, eikä ympäristöt rakennu monesta erillisestä AWS-tilistä. Conformityn rinnalle on myös saatavilla muita Cloud One-tuoteperheen teknologioita, joista esimerkiksi työkuormien suojausratkaisu Deep Security on Trend Microlla yksi markkinoiden parhaimmista (Trend Micro 2020d).

4.3.2 Netskope Public Cloud Security

Netskope on vuonna 2012 perustettu yhdysvaltalainen tietoturvayritys, joka tunnetaan parhaiten markkinoita johtavasta CASB-ratkaisustaan. Netskopen tarjonta keskittyy puhtaasti pilven tietoturvaan, ja kaikki Netskopen tarjoamat tietoturvaratkaisut löytyvät yhdestä alustasta keskitetysti. Netskopen tarjontaan kuuluu muun muassa SaaS-palveluiden suojaus ja kontrollointi, tietovuotojen estäminen, haittaohjelmien havainnointi ja estäminen sekä verkkoliikenteen valvonta. Netskope osti vuonna 2018 julkisten pilvialustojen tarkistuksiin keskittyneen Sift Securityn, josta on muodostunut Netskopen nykyinen CSPM-tarjonta. (Netskope 2020a.)

Netskope käyttää kyseisestä CSPM-tuotteesta nimeä Public Cloud Security, ja se on käytettävissä AWS, Azure ja GCP pilvialustoissa. Palvelussa tulee mukana useita valmiita sääntöjä, kuten alustakohtaisia parhaita käytäntöjä sekä yleisempiä regulaatiovaatimuksia ja standardeja. Netskopen CSPM-ratkaisussa on mahdollista luoda omia sääntöjä, ja myös automaattiset korjaustoimenpiteet ovat joissakin tapauksissa mahdollisia. Säännöt kohdistuvat pilviympäristöistä löytyviin resursseihin, joihin kuuluu virtuaalikoneet, tallennustilat, tietokannat, virtuaaliverkot, ryhmät, roolit sekä käyttäjät. Palvelu hinnoitellaan tarkasteltujen resurssien määrän mukaan vuosittain. (Netskope 2020b.)

CSPM-tuote itsessään ei ole mainittuja toimintoja kattavampi, ja tyypillisesti julkisten pilvialustojen tietoturvaa varten otetaan käyttöön myös muita Netskopen toiminnallisuuksia,

kuten tietovuotojen estäminen (DLP) ja haittaohjelmien havainnointi ja estäminen, jotka hinnoitellaan datamäärän perusteella.

Netskopen CSPM-ratkaisu ei ole markkinoilla oleviin tuotteisiin nähden kattavimpia, mutta yhdistettynä alustan muihin ominaisuuksiin siitä saa laajan näkyvyyden ja suojan julkisiin pilvialustoihin. Suurena etuna on se, että ratkaisu on käytettävissä kolmessa suurimmassa pilvialustassa, ja muut Netskopen toiminnallisuudet edesauttavat niiden suojaamisessa. Hinnoittelumalli sopii parhaiten käyttötapauksiin, joissa on useita tilejä, mutta resursseja ei käytetä määrällisesti paljon. Mikäli etusijalla on kokonaisvaltaisempi pilvitietoturvahanke, kuten CASB, niin Netskope markkinajohtajana on luonnollisesti järkevä vaihtoehto. Pilven työkuormien suojaamiseen on syytä kuitenkin etsiä muita ratkaisuja, sillä Netskopella ei ole siihen alueeseen mitään tarjolla.

Kaikki Netskopen tarjoamat tuotteet sisältyvät yhteen keskitettyyn alustaan, joka yksinkertaistaa kyseisen tuotekokonaisuuden hallintaa. Lisäksi alustaan on mahdollista liittää useita kolmannen osapuolen tuotteita esimerkiksi identiteetin hallintaan, päätelaitteiden suojaan tai monitorointiin.

4.3.3 Palo Alto Prisma Public Cloud

Palo Alto Networks on 2005 perustettu yhdysvaltalainen tietoturvayritys, joka on tunnettu erityisesti seuraavan sukupolven palomuureistaan ja nykyisin myös laajasta pilvitietoturvatarjonnasta. Palo Alto Networks on laajentanut tarjontaansa huomattavasti yritysostoin, hankkien osaksi yritystä vuodesta 2018 lähtien yhdeksän erilaista tietoturvayritystä (Crunchbase 2020). Palo Alto Networks jakaa tuotteensa kolmeen tuoteryhmään, Prisma, Cortex ja Strata. Palo Alton CSPM-ratkaisu on saatavilla osana laajempaa Prisma Cloud tuotetta, johon voi sisällyttää lisenssimallin mukaan myös pilven työkuormien suojausteknologioita.

Prisma Cloud CSPM-ominaisuuksiin sisältyy verkkoliikenteen analytiikka, resurssien ja konfiguraatioiden monitorointi, vaatimustenmukaisuuden hallinta ja raportointi, valmiita regulaatioiden ja standardien mukaisia sääntöjä sekä mahdollisuus luoda omia sääntöjä. Myös automaattisia korjauksia voidaan toteuttaa, riippuen pilvialustasta ja korjauksen tyypistä. Prisma Cloud on saatavilla kolmeen suurimpaan julkipilvitarjoajaan, ja niiden lisäksi tuettuna on myös esimerkiksi IBM Cloud sekä Alibaba Cloud. Tuote on integroitavissa kolmannen osapuolen järjestelmiin. (Palo Alto 2020a.)

Prisma Cloud hinnoittelu perustuu laskutettavien resurssien mukaisesti, joita ovat virtuaalikoneet, tietokannat, kuormantasaajat ja virtuaaliverkot. Laskutus perustuu keskimääräiseen resurssien käyttöön, eli hetkellisistä kasvuista ei näin ollen muodostu huomattavia kuluja. (Palo Alto 2020b.)

Prisma Cloud on saatavilla kolmessa lisenssimallissa, joista kaksi soveltuu pelkästään julkisiin pilvialustoihin. CSPM-ominaisuus sisältyy Business Edition-lisenssiin, ja CWPP-ominaisuudet saa lisättyä ottamalla Enterprise Edition-lisenssin. Prisma Cloud CWPP-ratkaisulla voidaan suojata virtuaalikoneita, kontteja sekä skannata tekstipohjaisia funktioita ja konfiguraatioita. (Palo Alto 2020b.)

Yhteenvetona Palo Alto Networks tarjoaa kattavaa suojaa julkisiin pilvialustoihin, ja etenkin jos tarkoituksena on myös suojata pilven työkuormia, on Palo Alto Networks hyvin suositeltava vaihtoehto. Lisenssimalli sopii parhaiten käyttötapauksiin, joissa käytetään laajasti eri pilvialustoja, ja valvottavien työkuormien määrä saattaa ajoittain vaihdella huomattavasti.

5 Yhteenveto ja pohdinta

Tämän työn tavoitteena oli selvittää mitä riskejä julkisiin pilvialustoihin siirtyminen sisältää, ja minkälaisia työkaluja voidaan käyttää riskien lieventämiseksi. Työssä tarkasteltiin myös pilvipalveluntarjoajan ja asiakkaan välistä vastuun jakautumista, ja siitä seuraavia erilaisia tietoturvavaatimuksia, joita asiakkaan tulisi ottaa huomioon. Julkisten pilvialustojen tietoturvavaatimusten noudattamiseen ja riskien hallintaan on olemassa erilaisia teknologioita, työkaluja ja prosesseja, joista tämän työn aiheeseen soveltuvin kokonaisuus oli CSPM-teknologiat.

Julkisten pilvialustojen suojaamiseen on selvästi kasvava tarve, ja se on havaittavissa lukuisista tietovuodoista ja murroista, joita tapahtuu maailmalla jatkuvasti. Suuri osa ongelmista syntyy pilvialustojen puutteellisista konfiguraatioista ja siitä, ettei riittävää näkyvyyttä ympäristöihin ole, eikä resurssit välttämättä riitä niiden tietoturvalliseen ylläpitämiseen. Useat tietoturvayritykset ovat investoineet huomattavasti pilvialustojen suojausteknologioihin, ja viime vuosina suurin osa suurimmista tietoturvayrityksistä ovat yritysostoin lähteneet rakentamaan kyvykkyyksiä pilven turvaamiseksi.

Pilvialustoihin siirtyminen on monelta osin kannattavaa ja tehokasta, mutta siihen liittyviä riskejä on myös huomattavan paljon. Julkiset pilvialustat eivät ota vastuulleen asiakkaiden tekemiä virheitä tai puutteita käyttöönotossa, ja usein pilvialustoissa saattaa toimia useita kolmansia osapuolia, jolloin tietoturvasta ei välttämättä ole keskitettyä kokonaisvastuuta tai näkyvyyttä. Riskinä on myös tietoturvavaatimusten noudattamattomuus, kun ei välttämättä huomata asioita, joita julkisissa pilvialustoissa tulisi ottaa huomioon. Usein saatetaan myös ymmärtää väärin jaetut vastuut, ja olettaa pilvialustan ottavan vastuuta laajemmin mitä todellisuudessa ottavat.

Pilvialustoja käyttävän asiakkaan on siis ymmärrettävä jaetut vastuut ja yritykseensä kohdistuvat tietoturvavaatimukset. Riskejä voidaan lieventää siten, että julkisten pilvialustojen käyttöön sovelletaan yhtenäistä tietoturvapolitiikkaa, ja kokonaiskuva ja näkyvyys ympäristöön on jatkuva ja valvottu. Asiakkaan on kartoitettava yritystään koskevat vaatimukset, ja asettaa asianmukaiset kontrollit niiden noudattamiseksi pilvialustoissa. Kontrollien tulisi olla myös pilviympäristön kanssa skaalautuvia, ja ylläpidollisesti keskitettyä. Erilaisiin käyttötapauksiin soveltuvia teknologioita on jo laajasti tarjolla, ja niitä on saatavilla sekä pilvialustoista itsestään sekä kolmansilta osapuolilta. Suurimmasta osasta tähän tarpeeseen soveltuvista teknologioista käytetään termiä CSPM.

Useat kolmannen osapuolen teknologiat sisältävät CSPM-ratkaisujen lisäksi hyvin usein myös muita pilvitietoturvateknologioita, kuten työkuormien suojaamiseen tarkoitettuja CWPP-ratkaisuja tai laajempaan pilven tietoturvaan keskittyviä CASB-alustoja. Etenkin CSPM ja CWPP ovat julkisten pilvialustojen kannalta loogisia yhdessä, sillä ensimmäisellä varmistetaan, että pilvialustaan sovelletaan parhaita käytäntöjä ja varmistetaan käytettyjen resurssien vaatimustenmukaisuus, ja toisella suojataan suoraan yksittäisiä työkuormia, kuten virtuaalikoneita. Lisenssimallit vaihtelevat teknologioiden välillä huomattavasti, ja onkin tärkeää selvittää omaan käyttötapaukseen sopivin vaihtoehto. Pilven tietoturvaa on syytä katsoa myös laajempana kokonaisuutena, ja valita teknologia mielellään siten, että se sisältää myös muita tarvittavia kontrolleja.

Pilven tietoturva on kokonaisuutena hyvin laaja alue, ja se eroaa monelta osin huomattavastikin perinteisistä tietoturvakonsepteista. Alue on myös jatkuvassa muutoksen tilassa, ja useat teknologiat ovat vielä varhaisessa vaiheessa kehityksessä. Tässä työssä käytetyt lähteet toivat esiin sen, että julkisten pilvialustojen käyttö tulee kasvamaan entisestään, ja myös niihin kohdistuvat hyökkäykset sen mukana. Gartnerin teettämien analyysien mukaan erityisesti CSPM on tähän kasvuun tarvittava tietoturvateknologia. Suurin osa tässä työssä käsitellyistä CSPM-ratkaisuista ovat vielä kohtalaisen uusia, ja ominaisuudet niissä kehittyvät jatkuvasti. Analyyseissa suositellaankin, että CSPM-ratkaisuja otettaisiin käyttöön vain lyhyeksi määräajaksi kerralla, sillä teknologiamarkkina tulee vielä rakentumaan vakaammaksi tulevina vuosina.

Tässä työssä käytetyt lähteet olivat pääosin julkisia markkina-analyysejä, sekä riippumattomien tietoturvayhteisöjen dokumentteja sekä alan kirjallisuutta. CSPM-ratkaisuista pyrittiin löytämään tietoa neutraalista näkökulmasta testaamalla ratkaisuja itse ja perustamalla tiedot osittain omiin havaintoihin, ja loput tarjolla olleisiin teknisiin dokumentteihin. Tästä työstä ilmenneiden tulosten luotettavuutta voisi parantaa teettämällä tarkemman vertailun teknologioihin, joka edellyttäisi laajempaa yhteistyötä myös niitä tarjoavilta tahoilta. CSPM-markkinan ollessa vielä varhaisessa murroksessa, oli syvemmän analyysin tekeminen kirjoittamishetkellä hankalaa.

Oman oppimisen kannalta työn aiheisiin syventyminen oli hyvin edullista ammatillisesti, ja syy tämän aiheen valintaan oli työperusteinen. Sain työn tuloksena laajemman käsityksen julkisten pilvialustojen tietoturvasta, ja niihin kohdistuvista uhista ja vaatimuksista. Näinkin tuoreesta aiheesta kirjoittaminen oli paikoittain haastavaa harvojen lähteiden vuoksi, mutta olen tyytyväinen lopputuloksena kerättyihin tietoihin, ja pystyn jatkossa seuraamaan aihealuetta paremmin siihen syvennyttyäni tässä työssä.

Lähteet

Amazon 2020a. Shared Responsibility Model. Luettavissa: https://aws.amazon.com/compliance/shared-responsibility-model/. Luettu: 28.3.2020.

Amazon 2020b. Security and Compliance. Luettavissa: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html. Luettu: 1.5.2020.

Amazon 2020c. AWS Config. Luettavissa: https://aws.amazon.com/config/. Luettu: 6.5.2020.

Amazon 2020d. AWS Trusted Advisor. Luettavissa: https://aws.amazon.com/premiumsupport/technology/trusted-advisor/. Luettu: 6.5.2020.

Amazon 2020e. AWS Control Tower. Luettavissa: https://aws.amazon.com/controltower/. Luettu: 6.5.2020.

Amazon 2020f. AWS Security Hub. Luettavissa: https://aws.amazon.com/security-hub/. Luettu: 6.5.2020.

Centrify 2019. Reducing Risk in Cloud Migrations. Luettavissa: https://www.centrify.com/resources/reducing-risk-in-cloud-migrations/. Luettu 9.8.2020.

Cloud Security Alliance 2020. Top Threats to Cloud Computing The Egregious 11. Luettavissa: https://cloudsecurityalliance.org/download/artifacts/top-threats-to-cloud-computing-egregious-eleven/. Luettu: 17.4.2020.

Cornell University 2017. DevOps vs DevSecOps: What Is the Difference? Luettavissa: https://blogs.cornell.edu/react/devops-vs-devsecops-what-is-the-difference/. Luettu: 3.5.2020.

Costello, K. 2019. Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019. Luettavissa: https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g. Luettu: 28.3.2020.

Crunchbase 2020. List of Palo Alto Networks's 13 Acquisitions, including CloudGenix and Aporeto. Luettavissa: https://www.crunchbase.com/search/acquisitions/field/organizations/num_acquisitions/palo-alto-networks. Luettu: 9.7.2020.

Cybersecurity Insiders 2019. 2019 Cloud Security Report. Luettavissa: https://www.isc2.org/-/media/ISC2/Landing-Pages/2019-Cloud-Security-Report-ISC2.ashx?la=en&hash=06133FF277FCCFF720FC8B96DF505CA66A7CE565. Luettu: 5.5.2020.

Dotson, C. 2019. Practical Cloud Security. O'Reilly Media, Inc.

EventID 2019. Luettavissa: http://www.eventid.net/docs/onprem_to_cloud.asp. Luettu: 2.5.2020.

Google 2020. Security Command Center conceptual overview. Luettavissa: https://cloud.google.com/security-command-center/docs/concepts-security-command-center-overview. Luettu: 7.5.2020.

Grance, W. & Jansen, T. 2011. Guidelines on Security and Privacy in Public Cloud Computing. Luettavissa: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. Luettu: 28.3.2020.

Grigorof, A. 2019. Mapping of On-Premises Security Controls vs Major Cloud Providers — Version 4.0. Luettavissa: https://medium.com/@adriangrigorof/mapping-of-on-premises-security-controls-vs-major-cloud-providers-version-4-0-c5f703658bfd. Luettu: 28.4.2020.

Loureiro, S. 2019. Cloud security tools: Understanding the differences between CASB, CSPM and CWPP. Luettavissa: https://outpost24.com/blog/find-the-differences-between-CASB-CSPM-and-CWPP. Luettu: 15.4.2020.

MacDonald, N. 2019a. Market Guide for Cloud Workload Protection Platforms. Gartner, Inc.

MacDonald, N. 2019b. Innovation Insight for Cloud Security Posture Management. Gartner, Inc.

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing. Luettavissa: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Luettu: 27.3.2020.

Microsoft 2020a. What is Azure Policy? Luettavissa: https://docs.microsoft.com/en-us/azure/governance/policy/overview. Luettu: 7.5.2020.

Microsoft 2020b. What is Azure Blueprints? Luettavissa: https://docs.microsoft.com/en-us/azure/governance/blueprints/overview. Luettu: 7.5.2020.

Microsoft 2020c. What are Azure management groups? Luettavissa: https://docs.microsoft.com/en-us/azure/governance/management-groups/overview. Luettu: 7.5.2020.
Microsoft 2020d. What is Azure Security Center? Luettavissa: https://docs.microsoft.com/en-us/azure/security-center/security-center-intro. Luettu: 7.5.2020.

Mogull, R. 2017. Security Guidance For Critical Areas of Focus In Cloud Computing v4.0. Luettavissa: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf. Luettu: 4.4.2020.

Netskope 2020a. Market-Leading CASB. Luettavissa: https://www.netskope.com/products/casb. Luettu: 9.7.2020.

Netskope 2020b. Public Cloud Security. Luettavissa: https://www.netskope.com/products/public-cloud-security. Luettu: 9.7.2020.

Newcombe, L. 2020. Securing Cloud Services – A pragmatic approach, second edition. O'Reilly Media, Inc.

Palo Alto 2020a. Visibility, governance and compliance across cloud native environments. Luettavissa: https://www.paloaltonetworks.com/prisma/cloud/visibility-governance-compliance. Luettu: 10.7.2020.

Palo Alto 2020b. Prisma Cloud Licensing and Editions Guide. Luettavissa: https://www.paloaltonetworks.com/resources/guides/prisma-cloud-pricing-and-editions. Luettu: 10.7.2020.

Riley, S. & Lawson, C. 2019. Magic Quadrant for Cloud Access Security Brokers. Gartner, Inc.

Rouse, M. s.a. Platform as a Service (PaaS). Luettavissa: https://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS. Luettu: 27.3.2020.

Sumo Logic, s.a. What is CaaS? Luettavissa: https://www.sumologic.com/glossary/caas/. Luettu: 27.3.2020.

Traficom liikenne- ja viestintävirasto kyberturvallisuuskeskus 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Traficomin julkaisuja 13/2020 PiTuKri – versio 1.1 – maaliskuu 2020. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf. Luettu: 28.3.2020.

Trend Micro 2020a. Cloud Conformity. Luettavissa: https://www.trendmicro.com/en_us/business/products/hybrid-cloud/cloud-one-conformity.html. Luettu: 7.7.2020.

Trend Micro 2020b. Security and Compliance. Luettavissa: https://www.cloudconformity.com/solutions/aws/security-compliance.html. Luettu: 7.7.2020.

Trend Micro 2020c. Cloud One Conformity Pricing. Luettavissa: https://www.cloudconformity.com/pricing.html. Luettu: 7.7.2020.

Trend Micro 2020d. Trend Micro has been named a leader in
The Forrester Wave™: Cloud Workload Security, Q4 2019! Luettavissa: https://resources.trendmicro.com/Forrester-Cloud-Workload-Leadership-Report.html. Luettu. 7.7.2020.

Veritas, 2017. Veritas Study: Alarming Majority of Organizations (69%) Export Full Responsibility for Data Protection, Privacy and Compliance onto Cloud Service Providers. Luettavissa: https://www.veritas.com/en/uk/news-releases/2017-10-25-veritas-study-alarming-majority-of-organizations-export-full-responsibility-for-data-protection-privacy-and-compliance-onto-cloud-service-providers. Luettu: 9.8.2020.