TURUN YLIOPISTO
Kauppakorkeakoulu

Zero Trust -mallin käyttö organisaation tietoturvaratkaisuna

Tietojärjestelmätieteen kandidaatintutkielma

Laatija:
Sofia Korkkinen

Ohjaaja:
FT Kai Kimppa

10.12.2025
Turku

Opiskelijan lausunto tekoälyn käytöstä tähän tutkielmaan liittyen:

☐ **En ole käyttänyt tekoälyä hyödyntäviä työkaluja** tätä tutkielmaa kirjoittaessani.

☒ **Olen käyttänyt tekoälyä hyödyntäviä työkaluja** tätä tutkielmaa kirjoittaessani. Tämä käyttö on dokumentoitu tutkielman liitteessä. Vakuutan, että tekoälyä käytettiin yliopiston ohjeistuksen mukaisella tavalla.

Kandidaatintutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä: Sofia Korkkinen
Otsikko: Zero Trust -mallin käyttö organisaation tietoturvaratkaisuna
Ohjaaja: FT Kai Kimppa
Sivumäärä: 40 sivua
Päivämäärä: 10.12.2025

Tiivistelmä

Zero Trust -tietoturvamalli on noussut keskeiseksi ratkaisuksi organisaatioiden kyberturvallisuuden hallinnassa erityisesti hajautetuissa ja pilvipohjaisissa ympäristöissä. Mallin perusperiaate "Älä luota, varmista aina" perustuu jatkuvaan todentamiseen, käyttöoikeuksien minimointiin, mikrosegmentaatioon, jatkuvaan valvontaan sekä uhkien tunnistamiseen ja torjuntaan. Zero Trust tarjoaa kokonaisvaltaisen lähestymistavan, joka parantaa järjestelmien näkyvyyttä, hallittavuutta ja reagointikykyä kyberuhkiin.

Tutkimuksessa hyödynnettiin kirjallisuuskatsausta ja tieteellisiä lähteitä, joiden avulla analysoitiin Zero Trustin hyötyjä, haasteita ja taloudellisia vaikutuksia eri järjestelmäympäristöissä. Erityistä huomiota kiinnitettiin pilvi-, IoT- ja hajautettuihin ympäristöihin, joissa käyttäjät, laitteet ja palvelut toimivat samanaikaisesti eri sijainneissa. Aineiston avulla arvioitiin mallin vaikutuksia tietoturvaan, toimintakäytäntöihin ja organisaatioiden taloudelliseen kestävyyteen.

Tulokset osoittavat, että Zero Trust vahvistaa merkittävästi tietoturvaa estämällä hyökkäysten etenemisen, lisäämällä autentikoinnin tarkkuutta ja parantamalla sisäpiiriuhkien torjuntaa. Lisäksi malli tukee liiketoiminnan ketteryyttä, resurssien tehokasta käyttöä ja strategista päätöksentekoa sekä vähentää tietomurroista aiheutuvia kustannuksia. Hyötyjä voidaan erityisesti soveltaa hajautetuissa ja pilvipohjaisissa ympäristöissä, joissa dynaaminen pääsynhallinta ja jatkuva valvonta ovat keskeisiä.

Tutkimus esittää myös Zero Trustin käyttöönoton haasteet, kuten autentikointiväsymyksen, infrastruktuurin monimutkaisuuden ja käyttäjien vastarinnan. Mallin tehokas hyödyntäminen edellyttää järjestelmällistä muutoksenhallintaa, henkilöstön koulutusta ja jatkuvaa ylläpitoa. Kokonaisuutena Zero Trust tarjoaa skaalautuvan, strategisen ja taloudellisesti perustellun ratkaisun nykyaikaisen kyberuhkaympäristön haasteisiin, mutta sen hyödyt realisoituvat vain, jos mallin vaatimukset otetaan systemaattisesti huomioon organisaation toiminnassa.

Avainsanat: Zero Trust -malli, kyberturvallisuus, hajautetut työympäristöt, mikrosegmentaatio, autentikointi

SISÄLLYS

KUVIOT

TAULUKOT

1 Johdanto

Organisaatioiden tietoturva on murroksessa. Aiemmin luotettavina pidetyt suojausmallit eivät enää vastaa nykyaikaisen, hajautetun ja jatkuvasti muuttuvan digitaalisen ympäristön tarpeita. Yritykset hyödyntävät yhä enemmän pilvipalveluita, monikanavaisia sovellusarkkitehtuureja ja etätyötä, mikä on hämärtänyt perinteisiä verkon rajoja ja lisännyt hyökkäyspinta-alaa. Tässä ympäristössä perinteinen perimetrisuojaukseen perustuva ajattelu, jossa verkon sisällä oletetaan olevan turvallista, ei enää riitä vastaamaan monimuotoisiin ja nopeasti muuttuviin kyberuhkiin. (Kim ym., 2024; Yeoh ym., 2023.) Kyberhyökkäysten seuraukset voivat olla yrityksille paitsi teknisesti vakavia, myös taloudellisesti ja maineellisesti tuhoisia. Tämän vuoksi ennakoivat, tehokkaat ja kohdistetut tietoturvaratkaisut ovat nykyisin yhä tärkeämmässä roolissa. (Azad ym., 2024.)

Yksi viime vuosina esiin nousseista ratkaisuista on Zero Trust -malli. Zero Trust on lähestymistapa, jossa verkossa toimiviin käyttäjiin, laitteisiin ja palveluihin ei oletusarvoisesti luoteta, vaan kaikki toiminnot vaativat jatkuvaa tunnistautumista ja valvontaa. Toisin kuin perinteisessä mallissa, suojaus ei kohdistu pelkästään verkon rajoihin, vaan suoraan niihin resursseihin, joita halutaan suojata. Näin pyritään estämään hyökkäysten leviäminen verkon sisällä ja vähentämään riskejä tilanteissa, joissa hyökkääjä onnistuu ohittamaan perinteisen suojauksen. Zero Trust on noussut erityisen kiinnostavaksi vaihtoehdoksi sen joustavuuden, skaalautuvuuden ja resurssikeskeisyyden vuoksi. (Rose ym., 2020; Simpson, 2022)

Zero Trust -mallin perusajatus, "älä koskaan luota, varmista aina", tuo mukanaan sekä hyötyjä että haasteita. Yhtäältä se mahdollistaa tarkemman pääsynhallinnan, tehokkaamman reagoinnin ja paremman suojan sisäisiä uhkia vastaan. Toisaalta jatkuva epäluottamus käyttäjiä ja laitteita kohtaan voi herättää vastustusta ja aiheuttaa käyttökokemukseen liittyviä haasteita. Siksi on tärkeää, että mallin käyttöönotto suunnitellaan huolellisesti sekä teknisestä että organisatorisesta näkökulmasta. (Azad ym., 2024; Lee ym., 2025)

Zero Trust -mallin keskeisiä osa-alueita ovat jatkuva todennus, käyttöoikeuksien minimointi, mikrosegmentaatio, käyttäytymisen ja tapahtumien analysointi sekä uhkien tunnistaminen ja torjunta (Rose ym., 2020). Nämä elementit muodostavat yhdessä joustavan ja skaalautuvan turvallisuusmallin, joka pyrkii estämään sekä ulkoisia hyökkäyksiä että sisäisiä uhkia. Lisäksi Zero Trust -periaatteet soveltuvat erityisesti tilanteisiin, joissa edellytetään nopeaa reagointia ja kykyä palautua hyökkäyksistä tehokkaasti. (Kim ym., 2024; Yeoh ym., 2023)

Tässä tutkielmassa esitetään mistä Zero Trust -malli koostuu ja minkälaisiin tietojärjestelmäympäristöihin se soveltuu. Työssä analysoidaan mallin keskeisiä periaatteita, sen tuomia hyötyjä ja haasteita sekä vertaillaan sen toimivuutta nykyaikaisissa tietojärjestelmäympäristöissä. Tarkastelun kohteena ovat erityisesti nykyaikaiset käyttöympäristöt, kuten pilvi- ja monipilviarkkitehtuurit, esineiden internet (engl. internet of things, IoT) sekä etätyö ja hajautetut työympäristöt. Työssä tarjotaan kokonaiskuva siitä, miten Zero Trust voi parantaa organisaatioiden valmiuksia torjua ja hallita kyberuhkia entistä tehokkaammin. Tutkielman tutkimuskysymykset ovat seuraavat:

1. *Miten Zero Trust -malli on kehittynyt vastauksena muuttuneeseen kyberuhkaympäristöön, ja mitä sen keskeiset periaatteet tarkoittavat käytännössä?*
2. *Millaisiin tietojärjestelmäympäristöihin Zero Trust -periaate soveltuu?*
3. *Millaisia kokonaisvaikutuksia Zero Trustin käyttöönotolla on organisaatioissa?*

Toisessa luvussa käsitellään ensimmäistä tutkimuskysymystä tarkastelemalla Zero Trustin ydinperiaatteita ja niiden suhdetta perimetripohjaiseen suojaan. Vaikka Zero Trust ei ole ainoa ratkaisu nykypäivän tietoturvahaasteisiin, sen suosio on kasvanut merkittävästi viime vuosien aikana. Luvussa käydään läpi nykyistä tietoturvaympäristöä ja kuvataan, miksi Zero Trust on noussut kannattavaksi vaihtoehdoksi erityisesti hajautetuissa ja dynaamisissa toimintaympäristöissä.

Kolmas luku vastaa toiseen tutkimuskysymykseen käsittelemällä Zero Trust -periaatteen soveltuvuutta erilaisiin tietojärjestelmäympäristöihin. Tarkastelu rajautuu erityisesti käyttöympäristöihin, joissa Zero Trust -mallin käyttöönotolla voidaan saavuttaa merkittäviä hyötyjä. Näitä ovat pilvipohjaiset ja monipilviympäristöt, IoT-järjestelmäympäristöt sekä hajautetut työympäristöt.

Neljännessä luvussa tarkastellaan Zero Trust -mallin hyötyjä ja haasteita sekä mallin taloudellista vaikuttavuutta. Tämä auttaa ymmärtämään, millaisia vaikutuksia ja resurssitarpeita liittyy mallin käyttöönottoon, ja missä tilanteissa Zero Trust tarjoaa selkeää lisäarvoa verrattuna muihin ratkaisuihin.

2 Zero Trust ja sen keskeiset periaatteet

2.1 Kyberturvallisuuden nykytilanne ja kehitys

Tutkielman sisällön ymmärtämiseksi on alkuun hahmotettava kyberturvallisuuden merkitys nykyaikaisissa toimintaympäristöissä. Rose ym. (2020) määrittelevät kyberturvallisuuden järjestelmälliseksi ja strategiseksi kokonaisuudeksi, jonka tehtävä on suojata organisaation järjestelmiä sisäisiltä sekä ulkoisilta uhilta. Laajentaaksemme määritelmää yhä entisestään, Dave ym. (2023) korostavat omassa tutkimuksessaan edellisten lisäksi myös henkilökohtaisten tietojen suojelun merkitystä. Heidän mukaansa nykyisessä digitaalisessa yhteiskunnassa, jossa lähes kaikilla on digitaalinen jalanjälki, henkilökohtaisten tietojen suojaaminen on kyberturvallisuuden perusta. Näiden näkökulmien avulla voidaan todeta, ettei organisaation tietoturva ole enää vain tekninen kysymys, vaan myös sosiaalinen, organisatorinen ja yksilöllinen haaste.

Organisaatioiden kyberturvallisuus on monikerroksinen kokonaisuus, joka pyrkii luotettavaan yhteyteen käyttäjän ja järjestelmän välille. Tämä kerroksellisuus sisältää myös datan ja järjestelmien saatavuuden sekä eheyden. (Dave ym., 2023; Rose ym., 2020.) Erityisesti tutkimuksessaan Dave ym. (2023) korostavat sisäisten uhkatilanteiden (engl. insider threat) vakavuutta. Nämä sisäiset uhkatilanteet liittyvät luottamuksellisten tietojen hallitsemattomaan käyttöön. Ne eroavat tyypillisemmistä ulkoisista uhista siten, että tekijöitä ovat yritysten omat käyttäjät, joko tahallisesti tai tahattomasti. Heidän mukaansa monissa ympäristöissä tietoturvariskejä lisää se, ettei pääsyoikeuksia ole rajattu käyttäjän roolin tai tarpeen mukaan. (Dave ym., 2023.)

Juuri tähän näkökulmaan tarttuvat Bast ja Yeh (2024), joiden mukaan Zero Trust -ajattelun ydin on nimenomaan jatkuva ja kontekstipohjainen pääsynhallinta. He osoittavat, että mallin vahvuus ei ole vain ulkoisten uhkien torjumisessa, vaan erityisesti sisäisten riskien hallinnassa. Kun jokainen käyttöpyyntö todennetaan erikseen ja käyttöoikeudet perustuvat yksilölliseen tarpeeseen, mahdollisuus vahingolliseen toimintaan, tahalliseen tai tahattomaan, vähenee merkittävästi (Bast & Yeh, 2024). Näin Zero Trust ei ainoastaan ratkaise Daven ym. (2023) esiin nostamia ongelmakuvia, vaan tarjoaa monikerroksisen ratkaisumallin, joka nojaa jatkuvaan epäluottamukseen (Rose ym., 2020).

Zero Trust -mallin ajankohtaisuus korostuu entisestään, kun tarkastellaan viime vuosien kehitystä erilaisten kyberuhkien määrässä. Eri hyökkäystyyppien tilastollinen kasvu viittaa siihen, että niin sisäiset kuin ulkoisetkin uhat eivät esiinny poikkeuksina vaan yhä useammin toistuvina ilmiöinä

(Dave ym., 2023). Tätä kehitystä havainnollistetaan taulukossa 1, joka kokoaa yhteen keskeisimpien hyökkäystyyppien kasvun vuosina 2015–2022.

Taulukko 1. Hyökkäysten määrän kasvu vuosina 2015-2022, tapaukset miljoonissa esitettynä (Dave ym., 2023)

Tapaukset	2015	2016	2017	2018	2019	2020	2021	2022	kasvu (%)
Petos	3,4	3,5	3,7	3,9	4,2	4,5	4,7	5,2	**50%**
Palvelunestohyökkäys	0,4	0,5	0,7	0,8	0,9	1,3	1,4	1,6	**327%**
Kyberhäirintä	0,3	0,5	0,7	0,8	0,8	1,2	1,3	1,5	**328%**
Haitallinen koodi	0,4	0,5	0,8	1,0	1,2	1,2	1,4	1,6	**285%**
Murtoyritykset	0,3	0,4	0,6	0,7	0,8	1,2	1,3	1,4	**438%**
Yhteensä	**4,8**	**5,4**	**6,5**	**7,0**	**7,9**	**9,4**	**10,1**	**11,3**	

Taulukosta 1 voidaan havaita, että lähes kaikki näistä keskeisistä kyberhyökkäystyypeistä ovat yleistyneet merkittävästi vuosien 2015-2022 aikana. Erityisesti palvelunestohyökkäykset (+327 %), kyberhäirintä (+328 %) ja murtoyritykset (+438 %) ovat nousseet esiin uhkina, joiden määrällinen kasvu heijastaa hyökkäysten lisääntyvää monipuolisuutta ja kohdentuvuutta. Taulukon sisältöä tukee myös AL-Hawamlehin (2023) tekemä ennakoiva tutkimus tulevaisuuden kyberhyökkäyksistä, jossa todetaan, että hyökkäysten tiheys on jatkuvassa kasvussa. Siinä missä vuonna 2019 hyökkäys tapahtui keskimäärin 19 sekunnin välein, vuonna 2022 arvioitiin, että uusi hyökkäys tapahtuu jo 11 sekunnin välein (AL-Hawamleh, 2023). Taulukon ja tutkimuksen kehityssuunnat osoittavat, että kyse ei ole yksittäisistä poikkeustapauksista, vaan systemaattisesta kasvutrendistä. Yhä useampi organisaatio, toimialasta tai koostaan riippumatta, voi joutua hyökkäyksen kohteeksi (Ministr & Pinter, 2024).

Vaikka kyberuhkien määrällinen kasvu on hyvin dokumentoitu, yksittäiset tapaukset osoittavat, miten syvälle organisaatioihin hyökkäykset voivat ulottua, jos suojaus perustuu oletettuun luottamukseen (CSIS, 2025). Yhdysvaltalainen Center for Strategic and International Studies (2025) on koonnut aikajanan merkittävistä kyberhyökkäyksistä, jotka kohdistuivat hallituksiin, suuriin teknologiayrityksiin tai joihin liittyi huomattavia taloudellisia menetyksiä. Näistä tapauksista Microsoftin tietomurto maaliskuussa 2024 on erityisen kuvaava. CSIS:n (2025) mukaan valtiollinen kybertoimija käytti väsytyshyökkäysmenetelmää (engl. brute-force attack) murtautuakseen Microsoftin sisäisiin sähköposteihin sekä lähdekoodiin. Kyseessä oleva väsytyshyökkäys sisälsi kaikkien mahdollisten merkkijonoyhdistelmien läpikäynnin päästäkseen käsiksi organisaation järjestelmään ja dataan (Kanta ym., 2022). Microsoft Security Response Centerin (2024) mukaan

hyökkäys jäi huomaamatta useiksi kuukausiksi ja hyökkäysvolyymi kasvoi lähes kymmenkertaiseksi alkuvuoden aikana.

Microsoftin tapaus osoittaa, kuinka kertaluonteinen todennus ja oletettu sisäinen turvallisuus voivat altistaa pitkäkestoiselle hyökkäykselle erityisesti ympäristöissä, joissa Zero Trust -periaatteita ei ole toteutettu täysimääräisesti. Zero Trust -arkkitehtuuri, jossa pääsyä arvioidaan jatkuvasti kontekstin ja käyttäjäkohtaisen riskin perusteella, olisi voinut rajoittaa hyökkääjän liikkumista ja minimoida vahingot järjestelmän pienempään osaan. (Yeoh ym., 2023.) Tapaus havainnollistaa sekä Zero Trustin periaatteiden ennaltaehkäisevää merkitystä että tarvetta luopua vanhentuneista turvallisuusolettamuksista. Tämä ja muut samankaltaiset tapaukset muodostavat tarpeen tälle John Kindervagin toimesta vuonna 2010 kehittämälle mallille (Gambo & Almulhem, 2026; Kim ym., 2024).

Malli luotiin haastamaan aikaisemmat turvallisuusparadigmat, kun Kindervag yhdessä muiden Forresterin tutkimuslaitoksen tutkijoiden kanssa havaitsi, etteivät silloin käytössä olleet mallit enää riittäneet nykyisten uhkien torjumiseen (Gambo & Almulhem, 2026; Kim ym., 2024; Tyler & Viana, 2021; Yeoh ym., 2023). Nämä perinteiset tietoturvamallit, kuten palomuureihin tai VPN-ratkaisuihin perustuvat perimetrisuojaukset, tukeutuvat oletukseen, että verkon sisällä olevat käyttäjät ovat luotettavia eikä niitä siten tarvitse valvoa jatkuvasti (Gambo & Almulhem, 2026; Yeoh ym., 2023). Golden ym. (2021) hahmottavat tätä lähestymistapaa linnoitusmallina. Linnoitusmallissa verkon ulkopuolisia uhkia pyritään torjumaan vahvalla perimetrisuojauksella, mutta sisäverkossa käyttäjien ja järjestelmien välistä pääsyä ei valvota tai rajoiteta yhtä tiukasti (Golden ym., 2021).

Kuten Microsoftin tapauksessa esitettiin, perinteiset perimetrisuojausmallit osoittautuvat haavoittuviksi (CSIS, 2025). Jos hyökkääjä onnistuu murtautumaan sisäverkkoon esimerkiksi varastetuilla tunnistetiedoilla tai hyödyntämällä järjestelmähaavoittuvuuksia, hänellä on laajat käyttöoikeudet organisaation kriittisiin tietoihin ja resursseihin (Dave ym., 2023). Tällaisia heikkouksia vastaan kehitettiin tutkielmassa käsiteltävä Zero Trust -malli, jonka pohjana toimii joukko keskeisiä ydinperiaatteita. Nämä seuraavaksi käsiteltävät ydinperiaatteet määrittelevät, kuinka organisaatioiden tulisi hallita tietoturvaa dynaamisessa ja jatkuvasti muuttuvassa uhkaympäristössä (Jimmy, 2024).

2.2 Ydinperiaatteet

2.2.1 Lähtökohdat käyttöönottoon

Zero Trust -mallin käyttöönotto edellyttää organisaatioilta keskeisten tietoturvaperiaatteiden omaksumista. Tutkielmassa käsiteltävät ydinperiaatteet muodostavat Zero Trust -ajattelun käytännön perustan, joiden toteutus määrittää suojauksen tehokkuuden. (Kang ym., 2023.) Ydinperiaatteiden käyttöönotto edellyttää organisaatioilta yhtenäistä ja järjestelmällistä lähestymistapaa, sillä yksittäiset tietoturvaratkaisut, kuten pelkkä monivaiheinen tunnistus, eivät yksin riitä muodostamaan luotettavaa suojauskokonaisuutta (Tyler & Viana, 2021; Yeoh ym., 2023).

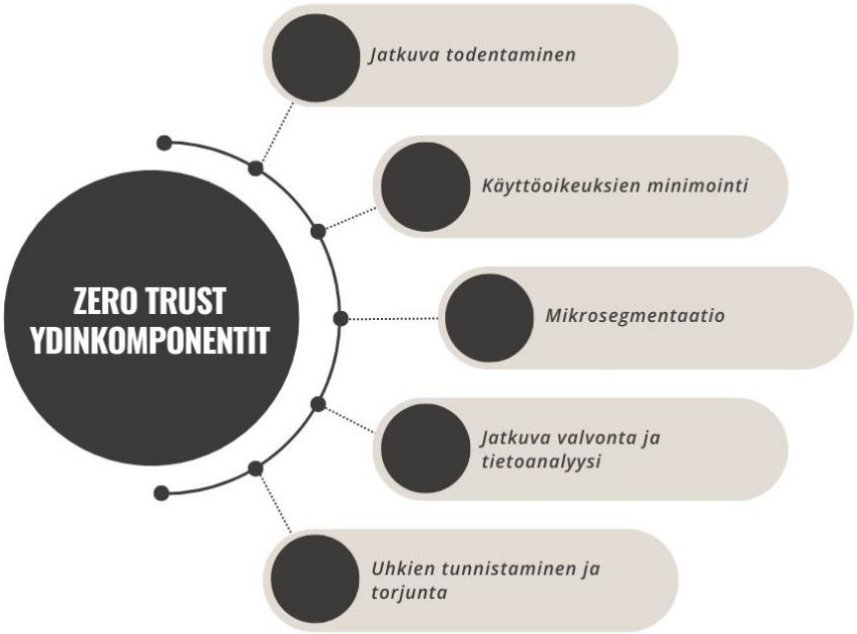
Periaatteiden käyttöönotto voi vaihdella suuresti organisaation koosta, resursseista ja lähtötilanteesta riippuen (Ren ym., 2025). Useat akateemiset lähteet korostavat, että erityisesti pienissä ja keskisuurissa organisaatioissa resurssien rajallisuus johtaa usein vaiheittaiseen käyttöönottoon. Tällöin osa järjestelmän alueista voi jäädä väliaikaisesti suojaamatta. (Jimmy, 2024; Ren ym., 2025.) Sen sijaan periaatteiden kattava ja koordinoitu käyttöönotto on todettu tehokkaaksi keinoksi vähentää sisäverkon haavoittuvuutta ja ehkäistä hyökkääjän liikkumista järjestelmästä toiseen (Golden ym., 2021). Seuraavaksi käydään läpi keskeisimmät periaatteet, joiden avulla Zero Trust -mallia voidaan toteuttaa käytännössä.

Zero Trust -arkkitehtuurin ydinperiaatteiden määrittely vaihtelee jonkin verran eri lähteissä, ja alan kirjallisuudessa esiintyy samankaltaisia, osittain päällekkäisiä kuvauksia niiden sisällöstä ja painotuksista. Jimmy (2024) nostaa esiin monivaiheisen todennuksen (engl. multi-factor authentication, MFA), mikrosegmentaation (engl. microsegmentation), identiteetin- ja pääsynhallinnan (engl. identity and access management, IAM) sekä vähimmän etuoikeuden periaatteen (engl. principle of least privilege) keskeisinä teknisinä osina. Ren ym. (2025) puolestaan painottavat neljää hieman eri tavalla jäsennettyä elementtiä: sisäänrakennettua epäluottamusta, dynaamista käyttöoikeuksien hallintaa, hienojakoista autentikointia sekä kontekstipohjaista politiikkaa. Viitekehys, jonka Rose ym. (2020) esittävät, tuo mukaan käyttäytymisanalyysin ja uhkien tunnistamisen osaksi jatkuvaa arviointia.

Koska Zero Trust on ennen kaikkea ajattelumalli, eivätkä sen käytännön toteutukset ole täysin standardoituja, tässä tutkimuksessa ydinkomponenttien tarkastelu perustuu ensisijaisesti viitekehykseen, jonka Rose ym. (2020) esittävät, ja jota on täydennetty Jimmy (2024) ja Ren ym.

(2025) näkemyksillä. Ydinkomponenttien rajauksessa on lisäksi huomioitu Kang ym. (2023) tiivistelmät laajalti eri tutkimuksissa havaituista yhtenevistä Zero Trust -komponenteista.

Kuvio 1 hahmottaa Zero Trust -periaatteet jäsenneltyinä viiteen peruspilariin. Nämä kyseiset osa-alueet ovat jatkuva todentaminen (engl. continuous authentication, CA), käyttöoikeuksien minimointi, mikrosegmentaatio, jatkuva valvonta ja tietoanalyysi sekä uhkien tunnistaminen ja torjunta. Kuvio havainnollistaa Zero Trustin olevan systemaattinen lähestymistapa, jonka osa-alueet yhdessä toimiessaan rakentavat kokonaisvaltaisen suojauksen (Kang ym., 2023).



Kuvio 1. Zero Trustin viisi käsiteltävää ydinkomponenttia

2.2.2 Jatkuva todentaminen

Jatkuvan todentamisen periaate on kehittynyt reaktio siihen, että kertaluonteinen tunnistautuminen ei riitä suojaamaan istunnon aikaisia käyttöoikeuksia (Junquera-Sánchez ym., 2021). He ym. (2022) määrittelevät jatkuvan todentamisen prosessiksi, joka tarkistaa käyttäjän identiteetin ja pääsyoikeudet toistuvasti yhden istunnon aikana. Junquera-Sánchez ym. (2021) tarkentavat määritelmää toteamalla, että jatkuva autentikointi koostuu joukosta teknologioita, jotka arvioivat käyttäjän identiteetin säilymistä reaaliaikaisesti. Tätä toteutetaan esimerkiksi hyödyntämällä vahvempia tunnistautumismenetelmiä, kuten monivaiheista tunnistautumista tai käyttäytymiseen perustuvia analytiikkamenetelmiä (He ym., 2022).

Yksi kertakirjautumista kehittyneempi ja jatkuvan todentamisen kanssa laajasti käytetty ratkaisu on monivaiheinen tunnistautuminen. MFA yhdistää useita toisistaan riippumattomia tunnistustekijöitä, kuten salasanan, biometrisen tunnisteen tai fyysisen laitteen, ja siten tarjoaa vahvemman suojan kuin pelkkä kertaluonteinen kirjautuminen. (He ym., 2022; Lee ym., 2025.) Tarkoituksena on vaatia käyttäjältä kahta tai useampaa kirjautumisen elementtiä päästäkseen käsiksi resursseihin. Elementit on jaettu kirjautumisen yhteydessä esimerkiksi seuraavasti: salasanavarmenne, puhelimitse avattava kertaluonteinen koodi sekä sormenjälkitunniste tai kasvojentunnistus. Kun kahta tai useampaa elementtiä yhdistetään, vähennetään riskiä varastetuista tunnistetiedoista merkittävästi. (Jimmy, 2022.)

Käyttöystävällisyyden varmistamiseksi useassa lähteessä todetaan MFA:n ja kertakirjautumisratkaisun (engl. single sign-on, SSO) yhteiskäytön vähentävän käyttäjän kokemaa rasitusta monivaiheisesta tunnistautumisprosessista. SSO:n hyödyt ovat laajat, sillä sen implementointi poistaa yksittäiseltä käyttäjältä tarpeen ylläpitää useita eri käyttäjätunnuksia. Kirjautuminen keskitetään yhteen paikkaan, jolloin yhdellä monivaiheisella kirjautumisella pääsee käsiksi useampaan sovellukseen. (Lee ym., 2025; Yeoh ym., 2023.)

Teknologiayritys Ciscon vuonna 2022 kokema tietomurto havainnollistaa konkreettisesti MFA-järjestelmien tunnettuja haavoittuvuuksia. Hyökkääjät ohittivat monivaiheisen tunnistautumisen hyödyntämällä käyttäjän väsymystä toistuviin varmennuspyyntöihin. He lähettivät väärennettyjä MFA-linkkejä, joiden avulla saivat haltuunsa käyttäjätunnuksia ja pääsivät sisäisiin järjestelmiin. (Lee ym., 2025.) Tapaus on linjassa aiempien tutkimusten kanssa, sillä MFA varmistaa identiteetin vain kirjautumishetkellä, joten väärentämisen riski säilyy (Junquera-Sánchez ym., 2021; Lee ym., 2025). Tästä syystä jatkuva identiteetin varmentaminen istunnon aikana on keskeinen osa järjestelmien suojaamista nykyaikaisia uhkia vastaan. Jatkuva todentaminen tarjoaa mekanismeja, jotka täydentävät MFA:ta tilanteissa, joissa pelkkä kirjautumishetken todennus ei riitä. (Junquera-Sánchez ym., 2021; Lee ym., 2025.)

2.2.3 Käyttöoikeuksien minimointi

Pelkästään kirjautuminen ja autentikaatiometodit eivät kuitenkaan pysty torjumaan nykyaikaisia hyökkäyksiä yksinään. Tästä syystä toinen Zero Trust -arkkitehtuurin keskeisistä periaatteista on käyttöoikeuksien rajaus, hallinnointi ja minimointi. Kun käyttäjät, laitteet tai prosessit on todennettu, määritellään tunnistetietojen perusteella käyttäjälle kuuluvat käyttöoikeudet ja noudatettavat politiikat. Työntekijällä ei tule siis olla pääsyä kriittisiin järjestelmiin tai arkaluontoisiin tietoihin, ellei se ole hänen roolinsa kannalta välttämätöntä. Tällä tavoin rajataan

hyökkäyspinta-alaa ja vähennetään riskiä siitä, että luvattomat käyttäjät tai haittaohjelmat voisivat väärinkäyttää pääsyoikeuksia. (Azad ym., 2024)

Zero Trust -mallissa pääsyoikeudet eivät ole pysyviä, vaan ne mukautuvat dynaamisesti käyttötilanteen ja riskiperusteisen arvioinnin mukaan. Tässä hyödynnetään niin sanottua tarpeellisuusperiaatetta (engl. need-to-know principle), jonka mukaan pääsy resursseihin myönnetään vain silloin, kun se on työtehtävän suorittamisen kannalta tarpeellista. Tämä estää ylimääräisten oikeuksien kertymisen ja rajoittaa väärinkäytösten mahdollisuutta, vaikka käyttäjä olisikin alun perin tunnistautunut oikein. (Azad ym., 2024)

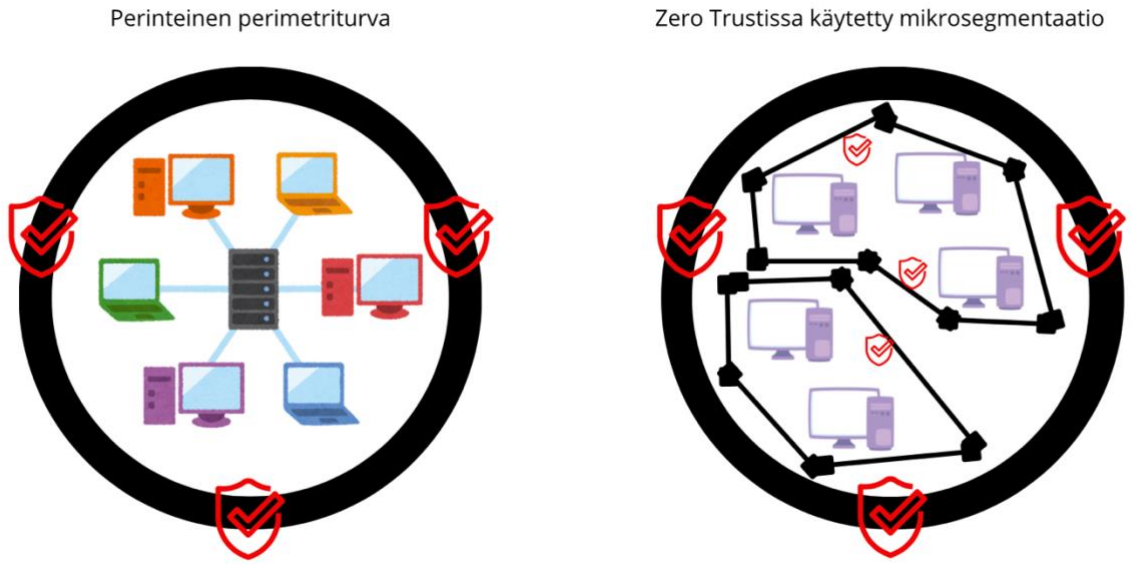
Dynaamisen käyttöoikeuden hallinnoinnin ytimessä on vähimmän etuoikeuden periaate (Azad ym., 2024). Azad ym. (2024) perustavat sen toiminnallisuuden jatkuvaan käyttöoikeuksien verifiointiin, jolloin oikeuksia annetaan vain niihin tietoihin, mitä pidetään välttämättöminä. Lisäksi heidän mukaansa periaate sisällyttää mahdollisuuden muutoksiin, kuten istunnon keskeytykseen, mikäli tilanne sitä vaatii. Yksittäisen käyttäjän oikeudet määritellään esimerkiksi käyttäjän roolin, sijainnin tai käytettävän välineistön perusteella (Azad ym., 2024). Verma ym. (2024) laajentavat mahdollisten käytettävissä olevien attribuuttien listaa toteamalla, että käyttöoikeuksien antamiseen vaikuttaa myös data aiemmasta käyttäytymisestä, vuorovaikutuksista sekä käyttäjäarvioista. Lisäksi algoritmi voi huomioida myös kontekstuaalisia tekijöitä, kuten aikaa sekä käyttäjän ympäristöä (Verma ym., 2024).

Zero Trustin käyttöoikeuksien hallinnoinnin ytimessä toimivat etenkin kaksi komponenttia, joiden vastuualueita ovat oikeuksien myöntäminen sekä päätöksenteko. Ensimmäinen vastaantuleva komponentti on päätöksentekopiste (engl. Policy Decision Point, PDP). (Azad ym., 2024.) Tässä vaiheessa analysoidaan käyttäjän pyyntö ja verrataan sitä ennalta määriteltyihin sääntöihin, joiden perusteella päätetään, voidaanko pääsy myöntää (Bernabé Murcia ym., 2025). Azad ym. (2024) korostavat, että PDP-vaiheessa määritellään oikeustaso käyttäjälle, jonka jälkeen tehty päätös välitetään pääsynvalvontapisteelle (engl. Policy Enforcement Point, PEP). PEP suorittaa PDP:n antaman päätöksen perusteella komentoja aina yhteyksien mahdollistamisesta niiden katkaisemiseen käyttäjän sekä resurssin välillä (Bernabé Murcia ym., 2025).

Käyttöoikeuksien minimointi parantaa organisaation tietoturvaa merkittävästi, sillä se vähentää niin ulkoisten hyökkäysten vaikutusaluetta kuin sisäisten uhkien mahdollisuuksia. Oikein toteutettuna periaate parantaa myös järjestelmän joustavuutta, sillä dynaamiset oikeudet mukautuvat turvallisuustilanteeseen ilman pysyvien laajojen oikeuksien tarvetta. (Azad ym., 2024; Bernabé Murcia ym., 2025; Verma ym., 2024)

2.2.4 Mikrosegmentaatio

Mikrosegmentaatio on olennainen elementti Zero Trust -arkkitehtuurissa, jonka keskeisenä tavoitteena on rajata hyökkäyspinta-alaa ja estää luvattoman pääsyn leviäminen verkon sisällä (Azad ym., 2024; Verma ym., 2024). Sen perusidea on jakaa organisaation verkko pienempiin ja paremmin suojattuihin alueisiin eli mikrosegmentteihin. Jokainen väline tai sovellus sijoitetaan omaan segmenttiinsä, ja segmenttien välistä liikennettä hallitaan dynaamisilla turvatoimilla. (Azad ym., 2024; Poirrier ym., 2025.) Zanasi ym. (2024) korostavat kuitenkin, että mikrosegmentointi edellyttää jatkuvaa luottamusrajojen mukauttamista, jotta suojaus pysyy tehokkaana myös muuttuvissa verkko-olosuhteissa. Kuvio 2 havainnollistaa, miten mikrosegmentointi eroaa perinteisestä perimetripohjaisesta verkkosegmentoinnista. Se mahdollistaa segmenttikohtaisen itsenäisen hallinnan ja valtuutuksen.



Kuvio 2. Perinteisen perimetripohjaisen segmentoinnin ja mikrosegmentoinnin ero

Jokainen verkon osa voi määrittää omat suojauskäytäntönsä riippumatta muista segmenteistä, mikä tukee Zero Trust -periaatteen mukaista epäluottamukseen perustuvaa arkkitehtuuria. Näiden periaatteiden toteuttamiseksi mikrosegmentaation on tarjottava kyky määritellä segmenttien välinen vuorovaikutus, säilyttäen samalla alkuperäiset turvallisuusvaatimukset. Pienempien segmenttien avulla mikrosegmentointi toteuttaa Zero Trust -arkkitehtuuria mahdollistaen yksityiskohtaisemman kontrollin ja korkeammat turvallisuustasot. (Li ym., 2024; Zanasi ym., 2024)

Mikrosegmentaatio tarjoaa erityistä lisäarvoa pilvipohjaisissa järjestelmissä, joissa perinteiset suojausmekanismit eivät ulotu verkon sisäiseen liikenteeseen. Sen avulla voidaan tarkastella

liikennettä sovelluskerroksen yläpuolella, mikä mahdollistaa poikkeavuuksien havaitsemisen ja nopean reagoinnin mahdollisiin uhkiin. Lisäksi mikrosegmentaatio mahdollistaa pääsynhallinnan soveltamisen entistä tarkemmalla tasolla, jonka takia käyttöoikeudet voidaan rajata tiettyihin segmentteihin, palveluihin tai jopa yksittäisiin resursseihin. (Li ym., 2024)

Kokonaisuudessaan mikrosegmentaatio toimii osana Zero Trust -ajattelun perusperiaatetta, jossa oletettu luottamus järjestelmän sisällä korvataan kontekstipohjaisella ja jatkuvasti valvotulla pääsynhallinnalla. Sen avulla organisaatiot voivat eristää järjestelmän osia toisistaan ja estää hyökkäysten leviämisen, mikä tekee siitä kriittisen osan nykyaikaista tietoturva-arkkitehtuuria. (Verma ym., 2024).

2.2.5 Jatkuva valvonta ja tietoanalyysi

Toisin kuin perinteiset tietoturvamallit, Zero Trust toimii dynaamisesti ja mukautuvasti, analysoiden käyttäjiä, laitteita ja järjestelmätapahtumia reaaliaikaisesti. Tämä jatkuva tarkkailu mahdollistaa uhkien havaitsemisen jo ennen kuin ne ehtivät aiheuttaa vahinkoa, mikä tekee mallista proaktiivisen toisin kuin perinteiset reaktiiviset järjestelmät. (Mickie & Jiefeng Weng, 2025.) Yeoh ym. (2023) korostavat tutkimuksessaan valvonnan ja datankeruun merkitystä tuomalla esiin, että ilman tällaista monitorointia ei voida olla varmoja toimiiko Zero Trust -malli niin kuin on tarkoitettu.

Jotta Zero Trust -malliin kuuluvaa jatkuvaa valvontaa ja datankeruuta voidaan toteuttaa, on tärkeää mahdollistaa aluksi koko infrastruktuurin kattava näkyvyys. Näkyvyys ja analytiikka toimivat yhteistyössä kattaen käyttäjien toiminnan verkostoissa, verkon liikenteen, laitteiden kunnon sekä esimerkiksi järjestelmä- ja lokitiedot analysointia varten. Yeoh ym. (2023) tarkentavat näkyvyyden ja analytiikan käytäntöä edelleen todeten, että organisaatiot käyttävät erilaisia analyysityökaluja pystyäkseen turvata järjestelmiä reaaliaikaisesti. Analyysityökalut paljastavat esimerkiksi hyökkääjien sijainnin verkossa ja tukevat päätöksentekoa tehokkaiden tietoturvaratkaisujen suunnittelussa. (Yeoh ym., 2023)

Azad ym. (2024) nostavat esiin verkkomonitoroinnin merkityksen nykyisissä monimutkaisissa ja hajautetuissa ympäristöissä. Zero Trust -mallissa analysoidaan suuria tietomääriä tekoälyä, koneoppimista ja tapahtumakorrelaatiota hyödyntäen. Näiden keinojen avulla voidaan tunnistaa epänormaalia toimintaa, havaita poikkeamia käyttäytymisessä sekä arvioida riskejä dynaamisesti (Verma ym., 2024; Azad ym., 2024). Tällaiset analyysit tukevat myös jatkuvaa pääsyoikeuksien säätelyä ja resurssien hallintaa tilanteen muuttuessa.

Organisaatiot hyödyntävät valvonnan ja monitoroinnin tehostamisessa muun muassa tunkeutumisen havaitsemisjärjestelmiä (engl. intrusion detection systems, IDS) ja estojärjestelmiä (engl. intrusion prevention systems, IPS). Nämä teknologiat soveltuvat hyvin Zero Trust -arkkitehtuuriin, sillä ne ovat monipuolisia ja voidaan sijoittaa arkkitehtuurin eri tasoille. IDS- ja IPS-ratkaisujen laaja käyttö perustuu niiden kykyyn havaita poikkeamia ja estää haitallista toimintaa tavalla, joka tukee Zero Trust -mallin jatkuvaa valvontaa ja epäluottamukseen perustuvaa toimintalogiikkaa. (Azad ym., 2024)

2.2.6 Uhkien tunnistaminen ja torjunta

Viimeisenä käsiteltävänä Zero Trust -ydinperiaatteena on uhkien tunnistaminen ja torjunta sekä niihin liittyvät toimenpiteet. Jos hyökkääjä onnistuu ohittamaan proaktiiviset suojausmenetelmät ja etenee järjestelmän sisällä, käytetään Zero Trustin menetelmiä hyökkäyksen tunnistamiseen ja torjuntaan (Mickie & Jiefeng Weng, 2025).

Uhkien tunnistaminen alkaa päätelaitteista, jotka ovat usein hyökkäysten ensisijaisia kohteita. Päätelaiteturvallisuus tarkoittaa suojausratkaisuja, jolla estetään ja tunnistetaan haitallinen toiminta ennen kuin se pääsee leviämään verkossa. (Verma ym., 2024.) Rose ym. (2020) määrittelevät päätelaitesuojauksen koostuvan teknologioista, jotka auttavat havaitsemaan poikkeavuuksia päätelaitteen toiminnassa. Rose ym. (2020) nostavat esimerkkeinä esiin kaksi teknologiaa: päätelaitesuojausjärjestelmän (engl. endpoint protection platform, EPP) sekä päätelaitteiden havainto- ja reagointijärjestelmän (engl. endpoint detection and response, EDR). Nämä järjestelmät toimivat ratkaisuina, joilla tuetaan Zero Trust -mallin tavoitetta keskeyttää haitallinen toiminta mahdollisimman aikaisessa vaiheessa (Verma ym., 2024).

Zero Trust -ympäristöissä uhkien tunnistamista voidaan tehostaa hyödyntämällä tietoturvatietojen hallinta- ja valvontajärjestelmiä (engl. security information and event management, SIEM), jotka keräävät ja analysoivat tietoa koko verkon tapahtumista reaaliaikaisesti. Kun SIEM yhdistetään Zero Trust -mallin muihin turvajärjestelmiin, saadaan aikaan kokonaisuus, joka paitsi havaitsee uhkia nopeasti, myös reagoi niihin ennalta määritettyjen turvallisuuskäytäntöjen mukaisesti. SIEM-järjestelmät oppivat aiemmasta datasta ja käyttävät sitä rakentamaan tehokkaamman turvajärjestelmän, minkä seurauksena myös hyökkäyksiin reagoiminen nopeutuu huomattavasti. (Ahuja ym., 2025)

Hyökkäystilanteessa on tärkeä toimia nopeasti, jotta vältytään vakavilta seurauksilta (Sharma ym., 2024). Tämän takia Sharma ym. (2024) painottavat tutkimuksessaan tekoälyn ja koneoppimisen

käyttöä analytiikan tukena sekä reaaliaikaisen uhkien tunnistamisen että niihin reagoimisen mahdollistamiseksi. Rose ym. (2020) korostavat myös näiden työkalujen hyödyntämistä Zero Trust -ympäristössä erityisesti siksi, että niiden käyttö mahdollistaa verkkoliikenteen luokittelun turvalliseksi tai haitalliseksi.

Mallin periaatteiden mukaisesti hyökkäyksiä pyritään estämään sekä ennen tunkeutumista että sen jälkeen, mikäli hyökkääjä onnistuu pääsemään järjestelmään käsiksi. Tällöin Zero Trust hyödyntää useita, jo aiemminkin tutkielmassa käsiteltyjä kontrollikerroksia ja niiden välisiä esteitä, kuten monivaiheista tunnistautumista ja liikkumista rajoittavia mekanismeja. Nämä kerrokset kaventavat hyökkääjän toimintamahdollisuuksia ja estävät etenemisen verkon sisällä. (Simpson, 2022)

Alevizos ym. (2022) ovat tarjonneet kehittyneen ratkaisun etenkin pitkäkestoisten ja edistyneiden uhkien torjumiseksi. Heidän lohkoketjuteknologiaan perustuva järjestelmänsä tallentaa kaikki tapahtumat muuttumattomasti, mikä tekee hyökkäyksen etenemisen havaitsemisesta ja estämisestä tehokkaampaa. Järjestelmä tarkistaa, että vain sen sallimat toiminnot ja ohjelmat voivat käynnistyä, ja estää muun epäilyttävän toiminnan. Tämä katkaisee hyökkäysketjun jo varhaisessa vaiheessa ja tukee Zero Trust -periaatetta, jossa pääsyä resursseihin tarkistetaan jatkuvasti eikä luottamusta anneta automaattisesti. (Alevizos ym., 2022)

Zero Trust -mallissa uhkien tunnistaminen ja torjunta perustuvat useiden eri teknologioiden ja periaatteiden yhteistoimintaan. Tärkeintä on, että mahdolliset uhat havaitaan riittävän aikaisin ja niihin pystytään reagoimaan nopeasti, usein automaattisesti. Näin estetään hyökkäysten eteneminen ja minimoidaan niiden vaikutukset. Tällainen toimintamalli tukee Zero Trust -periaatteen tavoitetta luoda tietoturvaa, joka ei perustu oletettuun luottamukseen vaan jatkuvaan valvontaan ja varmistamiseen. (Rose ym., 2020)

3 Zero Trust -mallin sovellettavuus

3.1 Pilvi- ja monipilviympäristöt

Pilvipalveluilla tarkoitetaan tietoteknistä infrastruktuuria, joka mahdollistaa datan tallentamisen, käsittelyn ja jakamisen internetin kautta. Organisaatiot voivat hyödyntää pilvipalveluita esimerkiksi etätyössä, tietojen varmuuskopioinnissa ja ohjelmistojen käytössä ilman, että palvelut ovat fyysisesti omilla palvelimillaan. (Petri ym., 2017.) Pilvipalvelut tarjoavat joustavuutta, sillä resursseja voidaan helposti lisätä tai vähentää tarpeen mukaan. Lisäksi ne tukevat tietoturvallista viestintää sekä sujuvaa pääsynhallintaa, kuten kertakirjautumista. (Petri ym., 2017; Wang ym., 2025.) Pilvipalveluita voidaan toteuttaa yksityisinä pilvinä, joita hallitaan organisaation sisällä, tai hyödyntää julkisia pilvialustoja, kuten Amazon AWS:ää tai Microsoft Azurea (Azad ym., 2024; Petri ym., 2017).

Monipilviympäristö viittaa tilanteeseen, jossa organisaatio käyttää useita eri pilvipalvelualustoja samanaikaisesti ilman, että kaikki keskitetään yhteen pilveen. Tämä mahdollistaa sen, että kukin yksikkö tai projekti voi valita juuri sen infrastruktuurin, joka parhaiten vastaa omia tarpeitaan. Monipilvimalli tukee tehokasta yhteistyötä, kun useat organisaatiot työskentelevät yhdessä säilyttäen kuitenkin hallinnan omiin järjestelmiinsä ja dataansa. (Petri ym., 2017; Rose ym., 2020)

Pilvipalveluiden yleistyminen on tehostanut tiedon jakamista ja resurssien käyttöä, mutta samalla se on tuonut mukanaan uusia ja kasvavia tietoturvariskejä, joihin perinteiset verkon rajapohjaiset suojaukset eivät vastaa tehokkaasti (Kang ym., 2023; Rose ym., 2020). Pilviympäristöt eroavat perinteisistä järjestelmäympäristöistä erityisesti hajautetun rakenteen, monikäyttäjäisyyden ja jatkuvan skaalautuvuuden vuoksi. Useat eri käyttäjät ja organisaatiot jakavat saman infrastruktuurin, mikä lisää riskiä muun muassa tietovuotoihin ja valtuuksien ylittämiseen. (Wang ym., 2025.) Pilvessä käyttäjä- ja resurssikokonaisuudet muuttuvat dynaamisesti, ja palveluita voidaan käyttää eri sijainneista ja eri laitteilla ilman perinteisiä verkon rajoja (Junquera-Sánchez ym., 2021).

Zero Trust -periaatteelle tyypillisesti myös yrityksen itse omistaman pilvijärjestelmän ja hallinnoiman verkon luottotason tulee olla yhtä alhainen kuin ulkopuolisen palveluntarjoajan ylläpitämän verkon luottotaso (Rose ym., 2020). Pilviturvallisuutta käsittelevissä tutkimuksissa nostetaan esiin useita keskeisiä osa-alueita, joiden avulla Zero Trustia pyritään toimeenpanemaan. Sharma ym. (2024) korostavat aiemmin käsitellyistä ydinkomponenteista erityisesti vahvoja salausmenetelmiä, turvallista pääsynhallintaa sekä säännöllisiä haavoittuvuustarkastuksia. Kang ym.

(2023) puolestaan painottavat pilviympäristöissä turvallista kommunikointia palvelukokonaisuuksien välillä, dynaamisen verkkoarkkitehtuurin luomista ja selkeiden luottamussuhteiden rakentamista. Yhtä oikeaa ratkaisua pilviympäristön täydelliseen turvaamiseen ei ole, mutta useiden ydinkomponenttien yhdistäminen luo yhtenäisen puolustusmallin, joka vahvistaa kokonaisvaltaista suojausta (Kang ym., 2023).

Pilvipohjaisessa Zero Trust -mallissa keskeistä on, että hajautettua infrastruktuuria hallitaan yhtenäisesti riippumatta käytössä olevista palvelumalleista tai kuormituksista. Jokainen yhteys todennetaan erikseen ennen pääsyn myöntämistä, ja pääsypolitiikat määritellään sekä toimeenpannaan keskitetysti. Pilvipohjainen toteutus tukee tätä erityisen hyvin, sillä alustapalvelut (engl. platform as a service, PaaS), sovelluspalvelut (engl. software as a service, SaaS) ja pilvialustojen valmiit työkalut mahdollistavat politiikkojen automaation, skaalautuvan valvonnan ja yhtenäisen Zero Trust -arkkitehtuurin. (Azad ym., 2024; Kang ym., 2023)

Monipilviympäristöissä tietoturvan hallinta on entistä vaativampaa, koska organisaation data ja sovellukset ovat hajautettuina useille eri pilvialustoille. Jokaisella alustalla voi olla omat pääsynhallintakäytäntönsä ja turvallisuusstandardinsa, mikä vaikeuttaa yhtenäisten ja johdonmukaisten Zero Trust -periaatteiden soveltamista. (Petri ym., 2017.) Erityisiä haasteita aiheuttavat myös yhteistoiminta ja valvonnan sirpaleisuus. Pääsynhallinnan, tietoliikenteen valvonnan ja uhkien torjunnan toteuttaminen kaikilla alustoilla edellyttää huolellista integraatiota ja selkeitä turvallisuuspolitiikkoja. Lisäksi riski väärinkäytöksille kasvaa, kun käyttäjät ja sovellukset liikkuvat vapaasti eri alustojen välillä ilman tehokasta näkyvyyttä ja kontrollia. Pilvipohjaiset järjestelmät ovat yleistyvä hyökkäyskohde, jonka takia niihin on pystyttävä implementoimaan Zero Trust -toimenpiteitä mahdollisimman monipuolisesti ja kattavasti. (Azad ym., 2024.)

3.2 Esineiden internetin ympäristöt

Esineiden internet tarkoittaa fyysisten laitteiden verkkoa. Laitteet, kuten kodinkoneet ja ajoneuvot, on varustettu älykkäillä ominaisuuksilla, kuten sensoreilla ja langattomalla yhteydellä, mikä mahdollistaa datan keruun ja reaaliaikaisen vaihtamisen. (Nag ym., 2024; Rabl ym., 2015.) Pilviympäristöihin verrattuna Zero Trust -ratkaisujen keskeinen painopiste IoT-ympäristöissä on lohkoketjuteknologian hyödyntäminen ja erilaisten käytännön toimintaympäristöjen tarpeiden huomioiminen. Zero Trust tarjoaa toimivan tietoturva-arkkitehtuurin IoT:lle, sillä laitteiden suuri määrä ja jatkuva vaihtuvuus vaativat dynaamisia ratkaisuja. (Kang ym., 2023.)

IoT-ympäristöjen rooli kriittisten infrastruktuurien, kuten terveydenhuollon, älyliikenteen ja energiaverkkojen, hallinnassa on kasvanut merkittävästi (Rabl ym., 2015; Szymanski, 2022). Näissä sovelluksissa tietoturva ei ole ainoastaan järjestelmän eheyden kysymys, vaan suoraan ihmisten turvallisuuteen ja yhteiskunnan toimintavarmuuteen liittyvä tekijä. Reaaliaikainen tiedonkeruu ja päätöksenteko ovat avainasemassa esimerkiksi liikenteenohjauksessa ja terveydenhuollon etämonitoroinnissa. (Nag ym., 2024; Wu ym., 2022.) Zero Trust -malli mahdollistaa luotettavan datan käytön ja estää haitallisen toiminnan leviämisen verkossa, varmistaen siten kriittisten prosessien turvallisen ja häiriöttömän toiminnan. Reaaliaikaisen uhkien havainnoinnin ja jatkuvan autentikoinnin avulla voidaan merkittävästi parantaa järjestelmien resilienssiä. Tämä pätee myös odottamattomia hyökkäyksiä vastaan. (Azad ym., 2024; Dhanaraj ym., 2024.)

IoT-laitteiden määrä kasvaa nopeasti, ja vuonna 2024 niiden arvioitiin ylittäneen 41 miljardia (Azad ym., 2024). Tämä kasvu tuo mukanaan merkittäviä kyberturvallisuusriskejä, sillä monet IoT-laitteet ovat resurssirajoitteisia ja niissä hyödynnetään puutteellisia suojausratkaisuja (Nag ym., 2024; Wu ym., 2022). Lisäksi laitteiden monimuotoisuus, kuten erilaiset mallit, viestintätavat ja tiedonsiirtomenetelmät, tekee turvallisuusarkkitehtuurien käyttöönotosta haastavaa. IoT-laitteiden hallintaa tukevat arkkitehtuurit ja toimintamallit, kuten lohkoketjupohjaiset ratkaisut ja keskitetyt hallintajärjestelmät, helpottavat kuitenkin merkittävästi Zero Trust -periaatteiden soveltamista tällaisissa ympäristöissä. (Kang ym., 2023.)

Yksi yleisimmistä teknisistä lähestymistavoista Zero Trustin toteuttamisessa IoT-ympäristöissä on lohkoketjuteknologia. Sen hajautettu rakenne tukee monitasoista luottamuksen hallintaa ja varmistaa, että laitteiden tunnistautuminen perustuu tiedon eheyttä ja yhdenmukaisuutta koskeviin tarkistuksiin. (Kang ym., 2023.) Lisäksi koneoppimiseen perustuvat järjestelmät voivat arvioida laitteiden ja käyttäjien aiempaa käyttäytymistä ja sijaintia pääsyoikeuksia myönnettäessä. Riskitietoiset ratkaisut mukauttavat myös pääsynhallintaa reaaliajassa havaittujen uhkien perusteella. (Routray & Bera, 2024.)

Vaikka Zero Trust tuo merkittäviä hyötyjä, sen soveltaminen IoT-ympäristöihin kohtaa omat haasteensa. Laitteiden rajoitettu laskenta- ja energiateho vaikeuttavat raskaita todennusprosesseja (Nag ym., 2024). Lisäksi dynaamiset verkot, joissa laitteet liittyvät ja poistuvat jatkuvasti, edellyttävät jatkuvaa autentikointia ja pääsynhallintaa, mikä voi lisätä viiveitä ja kuormittaa verkon suorituskykyä (Routray & Bera, 2024). Myös monimutkaiset tietoturvauhat, kuten palvelunestohyökkäykset, vaativat edistyneitä suojausmekanismeja, joita perinteiset IoT-laitteet eivät aina tue (Szymanski, 2022). Vaikka nykyiset Zero Trust -ratkaisut IoT- ja

lohkoketjuympäristöissä tarjoavat osan tarvittavista toiminnallisuuksista, IoT-laitteiden luontaiset rajoitukset asettavat edelleen haasteita arkkitehtuurin suunnittelulle ja toteutukselle. (Kang ym., 2023).

Zero Trust -mallin omaksuminen IoT-ympäristöihin tarjoaa välttämättömän turvakehyksen alati kasvavan ja kehittyvän laiteverkoston suojaamiseksi. Soveltamalla jatkuvaa autentikointia, kontekstuaalista riskienhallintaa ja hajautettuja suojausteknologioita voidaan parantaa järjestelmien turvallisuutta, yksityisyyttä ja toimintavarmuutta merkittävästi. (Azad ym., 2024; Dhanaraj ym., 2024; Routray & Bera, 2024.) Tulevaisuuden kehitystyön kannalta keskeistä on kehittää kevyempiä ja tehokkaampia Zero Trust -ratkaisuja, jotka soveltuvat myös vähäresurssisille IoT-laitteille (Kang ym., 2023).

3.3 Etätyö ja hajautetut työympäristöt

Etätyön ja hajautettujen työympäristöjen nopea yleistyminen, erityisesti COVID-19-pandemian seurauksena, on tuonut organisaatioille merkittäviä uusia tietoturvahaasteita. Siirtyminen toimistoympäristön suojatusta verkosta kotitoimistojen julkisiin verkkoihin on lisännyt hyökkäyspinta-alaa ja tehnyt perinteisestä tietoturvamallista vanhentuneen. Useissa organisaatioissa etätyö tarkoittaa, että käyttäjät toimivat täysin yritysverkon ulkopuolella tilassa, jossa rajapohjaiset suojaukset, kuten palomuurit, eivät enää yksin riitä. (Nag ym., 2024)

AT&T:n vuonna 2021 toteuttaman kyselyn mukaan noin 70% yli 5000 työntekijän yrityksistä katsoi etätyön lisänneen haavoittuvuutta kyberhyökkäyksille (Nwankpa & Datta, 2023). Tämä haavoittuvuus johtuu siitä, että käyttäjät siirtyvät käsittelemään yrityksen sisäisiä resursseja suojaamattomasta ympäristöstä, jolloin perinteiset suojausmekanismit eivät pysty estämään tai tunnistamaan uhkia riittävän tehokkaasti (Tsai ym., 2024). Zero Trust -malli vastaa haasteeseen poistamalla oletetun luottamuksen ja vaatimalla jatkuvaa todennusta, vahvaa identiteetinhallintaa ja kontekstipohjaista pääsynvalvontaa jokaisessa yhteyspyynnössä.

Yksi erityinen ongelma etätyössä on henkilökohtaisten laitteiden käytön (engl. bring your own device, BYOD) yleistyminen. Nämä laitteet eivät kuulu organisaation hallintaan ja voivat siten sisältää haavoittuvuuksia. Zero Trust -mallissa tämä otetaan huomioon jatkuvalla laitearvioinnilla, joka arvioi muun muassa laitteen ohjelmistoversion, suojaustilan ja sijainnin ennen pääsyn sallimista. Anderson ym. (2022) esittelevät BYOZ-arkkitehtuurin (engl. bring your own zero trust, BYOZ), joka on suunniteltu mahdollistamaan Zero Trust -periaatteiden soveltaminen BYOD-käyttöön jatkuvan autentikoinnin ja kontekstitiedon avulla. Tällainen lähestymistapa on erityisen

tärkeä mobiilissa ja hajautetussa työympäristössä, jossa käyttäjien sijainti ja laitetaso voivat vaihdella merkittävästi. (Anderson ym., 2022)

Zero Trust mahdollistaa myös siirtymisen pois perinteisestä VPN-riippuvuudesta kohti käyttäjä- ja sovelluskohtaista pääsynhallintaa. Vaikka VPN-teknologia tarjoaa salatun yhteyden julkisista verkoista yritysverkkoihin, se perustuu edelleen oletukseen luotettavasta sisäverkosta, mikä tekee siitä haavoittuvan. Zohaib ym. (2024) tarjoavat ratkaisuna ZT-VPN -mallin, joka yhdistää Zero Trust -periaatteet ja mahdollistaa huomattavasti tiukemman ja joustavamman hallinnan kuin perinteinen VPN. Tämä tarjoaa organisaatiolle paremman näkyvyyden käyttäjien toimintaan ja mahdollistaa nopean reagoinnin poikkeavuuksiin. (Zohaib ym., 2024)

Zero Trust -mallin tehokkuus korostuu myös reaaliaikaisessa uhkien havainnoinnissa, mikä on välttämätöntä etätyöympäristöissä. Etäkäyttäjien suuri määrä ja moninaiset käyttökuviot tekevät perinteisestä sääntöpohjaisesta tunnistuksesta riittämätöntä. Koneoppimista hyödyntävät järjestelmät voivat analysoida käyttäjien käyttäytymishistoriaa, kuten kirjautumisten sijaintia, aikaa ja toimintamallia, ja erottaa poikkeavat toiminnot normaalista käyttäytymisestä. Tällainen käyttäytymisanalytiikka mahdollistaa esimerkiksi kirjautumisen estämisen, jos käyttäjä yrittää kirjautua tuntemattomalta laitteelta tai yllättävästä maasta. (Parkhomenko ym., 2024)

Lisäksi Zero Trust -malli tukee tietoturvakulttuurin kehitystä. Vaikka etätyö voi lisätä käyttäjän altistumista huijauksille ja sosiaaliselle manipuloinnille, se voi myös vahvistaa yksilön tietoisuutta tietoturvasta. Etätyöntekijät tiedostavat usein, että heidän käytössään ei ole toimiston tarjoamaa suojaa, mikä kasvattaa heidän vastuuntuntoaan ja valmiuttaan noudattaa turvallisuuskäytäntöjä. (Nwankpa & Datta, 2023)

Tämän lisäksi Zero Trust -lähestymistapa vahvistaa organisaation vastuullisuutta ja läpinäkyvyyttä tietosuojaan liittyvissä kysymyksissä. Zhangin (2023) mukaan yksityisyyden suoja ei ole vain sääntelyn täyttämistä, vaan olennainen osa luottamuksen rakentamista eri sidosryhmien kanssa. Zero Trust edistää tätä asettamalla käyttöoikeudet tiukasti määriteltyjen tarkoitusten ja vähimmän oikeuden periaatteen mukaisesti. Näin rajoitetaan mahdollisia vahinkoja ja vahvistetaan järjestelmien resilienssiä, mikä on ratkaisevaa etätyöympäristöissä, joissa data liikkuu laajasti organisaation ulkopuolella. (Zhang, 2023)

4 Zero Trust -mallin vaikutukset organisaatioissa

4.1 Tietoturvahyödyt

Zero Trust tarjoaa organisaatiolle kokonaisvaltaisen tietoturvan, joka mukautuu nykyaikaisiin työ- ja teknologiaympäristöihin. Se mahdollistaa paremman näkyvyyden, tarkemman pääsynhallinnan ja riskien vähentämisen sekä tukee liiketoimintaa ilman, että sitä rajoitetaan. Tämän vuoksi se nousee vahvaksi vaihtoehdoksi perinteisten suojausmallien tilalle etenkin organisaatioissa, jotka etsivät pitkän aikavälin kyberturvallisuusstrategiaa. (Nwankpa & Datta, 2023.) Kuvioon 3 on tiivistetty useiden eri tieteellisten lähteiden mainitsemat Zero Trustin hyödyt organisaatiolle, jaoteltuna kolmeen kategoriaan: tietoturvavaikutukset, liiketoiminnalliset vaikutukset sekä vaikutukset organisaation näkyvyyteen ja hallittavuuteen.

Kuvio 3. Mallin hyödyt jaoteltuna kolmeen pääosioon (Cunningham ym., 2019)

Kuvion tietoturvaosio sisältää suurimman hyötyosuuden Zero Trustin vaikutuksista. Koska Zero Trust -arkkitehtuurissa kaikki informaatio tarkistetaan ja käsitellään asianmukaisesti, poikkeamat sisällöissä havaitaan nopeammin ja niihin pystytään reagoimaan ajoissa (Cunningham ym., 2019). Vahvaa tietoturvaa mahdollistaa myös lukuisat autentikaatiomenetelmät, joiden avulla varmistutaan arkaluonteisten tietojen suojaamisesta sekä pienennetään datavuotojen riskejä (Nisha T N ym., 2023). Zero Trust -malli on erikoistunut sisäpiiriuhkien torjumiseen, ja siksi se tuo organisaatioille hyötyjä käyttämällä jatkuvaa todennusta näiden uhkien välttämiseksi. Lisäksi yksi huomattavimmista eduista organisaation tietoturvan varmistamiseksi piilee Zero Trustin

käytännöissä estää hyökkäyksen eteneminen mikäli sellainen on tapahtunut. (Cunningham ym., 2019.)

Toisena käsiteltävänä hyötyosiona kuviossa on organisaation liiketoimintaan vaikuttavat tekijät. Koska Zero Trust -arkkitehtuuri on luotu vastaamaan nykyaikaisia uhkia, on se myös todistetusti ketterämpi ja skaalautuvampi tietoturvaratkaisu kuin perinteiset tietoturva-arkkitehtuurit (Rose ym., 2020). Tukien tätä Nisha T N ym. (2023) tuovat esiin etenkin Zero Trustin käyttömahdollisuudet moderneissa ympäristöissä, kuten pilvipohjaisissa organisaatiorakenteissa sekä yhdessä etätyöratkaisujen kanssa. Lisäksi he korostavat parannettua työntekijäkokemusta implementoimalla sujuvia MFA sekä SSO ratkaisuja. Zero Trust -malli vahvistaa myös organisaation sisäistä yhteistyötä. Järjestelmien lisääntynyt läpinäkyvyys vähentää epäselkeitä toimintatapoja ja mahdollistaa nopeamman ongelmanratkaisun sekä kokonaisvaltaisemman teknologiajohtamisen (Cunningham ym., 2019).

Kuvion viimeisessä kohdassa käsitellään Zero Trustin hyötyvaikutuksia organisaation näkyvyydessä sekä hallittavuudessa. Zero Trust tarjoaa organisaatiolle merkittäviä etuja parantamalla verkon ja järjestelmien läpinäkyvyyttä, sillä kaiken liikenteen jatkuva tarkastelu antaa aiempaa tarkemman kokonaiskuvan ympäristön toiminnasta ja mahdollisista poikkeamista. Malli edellyttää myös kriittisen datan inventointia ja luokittelua, mikä vahvistaa organisaation tietoisuutta omista resursseistaan ja auttaa niiden suojaamisessa. Verkkojen segmentointi ja selkeä pääsynhallinta tukevat tietoturvavaatimusten täyttymistä, mikä vähentää auditointien työmäärää ja niihin liittyviä riskejä. Näiden ominaisuuksien ansiosta Zero Trust tekee kokonaisuudesta helpommin hallittavan ja joustavan, jolloin arkkitehtuuria voidaan sovittaa organisaation tarpeiden ja käyttötapausten mukaan. (Buck ym., 2021; Cunningham ym., 2019)

4.2 Haasteet ja rajoitteet

Zero Trust -mallin käyttöönottoon liittyy monia haasteita, jotka voivat hidastaa sen laajamittaista soveltamista organisaatioissa. Yksi merkittävä tekninen haaste liittyy suorituskykyyn. Koska jokainen pääsypyynnön vaihe edellyttää vahvistusta ja riskinarviota, Zero Trust -ratkaisut voivat lisätä verkon viivettä ja järjestelmän kuormitusta. (Buck ym., 2021; Kang ym., 2023.) Erityisesti hajautetut pilvipalvelut ja resurssirajoitteiset laitteet, kuten IoT-yksiköt, voivat kärsiä suorituskykyongelmista, mikäli autentikointi- ja pääsynhallintaratkaisut eivät skaalaudu riittävän tehokkaasti (Azad ym., 2024).

Haasteet eivät rajoitu vain teknisiin osa-alueisiin, vaan myös käyttäjät ja organisaatiokulttuuri voivat muodostaa esteen onnistuneelle käyttöönotolle. Zero Trust -malli edellyttää jatkuvaa valvontaa ja tunnistautumista, mikä saattaa herättää vastarintaa työntekijöissä ja aiheuttaa kokemuksen lisääntyneestä valvonnasta tai turhasta byrokratiasta. (Sarkar ym., 2022.) Lisäksi mallin käyttämä tietojen keruu käyttäjien toiminnasta ja järjestelmien tapahtumista voi synnyttää yksityisyyteen liittyviä huolia etenkin pilvipohjaisissa ympäristöissä (Kang ym., 2023).

Lee ym. (2025) tuovat esiin autentikointiväsymyksen riskin erityisesti ympäristöissä, joissa monivaiheinen tunnistautuminen edellyttää käyttäjiltä toistuvia kirjautumisia salasanan ja kertakäyttökoodin avulla. Tällainen toistuvuus voi johtaa turhautumiseen, heikentyneeseen käyttökokemukseen ja välinpitämättömyyteen tietoturvakäytäntöjä kohtaan (He ym., 2022; Lee ym., 2025). Tämän vuoksi onnistunut siirtymä Zero Trust -malliin vaatii myös onnistunutta muutoksenhallintaa, koulutusta ja avoimuutta, jotta työntekijät ymmärtävät toimenpiteiden merkityksen ja kokevat ne mielekkäiksi (Mickie & Jiefeng Weng, 2025).

Junquera-Sánchez ym. (2021) korostavat, että liiallinen todennustiheys ei ainoastaan kuormita käyttäjiä, vaan se voi myös heikentää tuottavuutta ja lisää inhimillisten virheiden todennäköisyyttä. Tämän vuoksi heidän mukaansa Zero Trust -ympäristössä tulisi pyrkiä ratkaisuihin, jotka yhdistävät turvallisuuden ja käytettävyyden. Yhtenä mahdollisena ratkaisuna Junquera-Sánchez ym. (2021) esittävät käyttäytymiseen perustuvia biometrisiä menetelmiä, kuten näppäilyn rytmin tai hiiren liikkeen analyysiä. Heidän mukaansa näiden avulla jatkuva tunnistaminen voidaan toteuttaa passiivisesti ja huomaamattomasti ilman, että käyttäjän työskentely keskeytyy.

Mallin kompleksisuus näkyy teknisen toteutuksen lisäksi myös organisaation toimintatapojen uudelleenjärjestelyissä. Zero Trust edellyttää hienojakoista pääsynhallintaa, jatkuvaa käyttäjä- ja laiteverifiointia sekä monien käyttöpolitiikkojen määrittämistä ja hallintaa. Tämä tekee mallin rakentamisesta ja ylläpidosta huomattavan vaativaa erityisesti suurissa tai monimutkaisissa järjestelmäympäristöissä. Monissa organisaatioissa siirtymä perinteisestä arkkitehtuurista Zero Trust -malliin vaatii huomattavia investointeja, muutoksia infrastruktuuriin sekä asteittaista käyttöönottoa, mikä voi johtaa siihen, että Zero Trust toimii vain osittain. (Bertino, 2021)

Zero Trust -malli nojaa politiikkapohjaiseen pääsynhallintaan, jossa käyttöoikeudet myönnetään tarkasti määriteltyjen ehtojen perusteella. Tämä tekee mallista herkästi riippuvaisen politiikoiden oikeellisuudesta. Mikäli ennalta määritetty politiikka puuttuu tai sisältää virheitä, pääsy voidaan estää myös niiltä käyttäjiltä, joilla olisi siihen oikeus. Seurauksena voi olla tarpeettomia käyttökatkoksia ja tarve järjestelmänvalvojan manuaalisille korjaustoimille, mikä lisää sekä

kustannuksia että viiveitä. Lisäksi mallin keskeiset komponentit, kuten PDP ja PEP, voivat muodostaa kriittisiä haavoittuvuuksia. Jos nämä komponentit vaarantuvat, seurauksena voi olla koko organisaation toiminnan häiriintyminen. (Azad ym., 2024; Bertino, 2021)

Zero Trust ei myöskään ole täysin tunnettu tai ymmärretty lähestymistapa. Vaikka sen edut verrattuna perinteisiin ratkaisuihin ovat merkittäviä, monille organisaatioille mallin konkreettiset hyödyt ja rajoitteet ovat yhä epäselviä. Tämä epävarmuus voi estää päätöksentekoa ja hidastaa laajempaa käyttöönottoa. (Buck ym., 2021.) Haasteita lisää se, että onnistunut toteutus vaatii henkilöstön vahvaa sitoutumista ja periaatteiden ymmärtämistä. Jos ylläpitäjillä tai käyttäjillä ei ole riittävää osaamista, tai jos turvakäytäntöjä kierretään, järjestelmän turvallisuus heikkenee. Lisäksi Zero Trustin käyttöönotto voi olla teknisesti vaativa, koska se edellyttää jatkuvaa ylläpitoa ja päivityksiä. Ilman aktiivista hallintaa arkkitehtuurin tehokkuus voi ajan myötä heikentyä. (Zhang, 2023.)

Zero Trust -mallin tehokas toteuttaminen edellyttää turvallisuutta myös monilla muilla tasoilla. Käyttäjätunnusten väärinkäyttö, IoT-laitteiden heikko suojaus, kolmansien osapuolien haavoittuvuudet sekä fyysisen turvallisuuden puutteet voivat kaikki muodostaa merkittäviä riskejä (Azad ym., 2024). Näiden riskien hallinta vaatii kattavaa näkökulmaa ja jatkuvaa arviointia, jotta Zero Trust -mallin täysi potentiaali saadaan hyödynnettyä ilman, että sen aiheuttamat kuormitukset muodostuvat esteeksi sen käytölle.

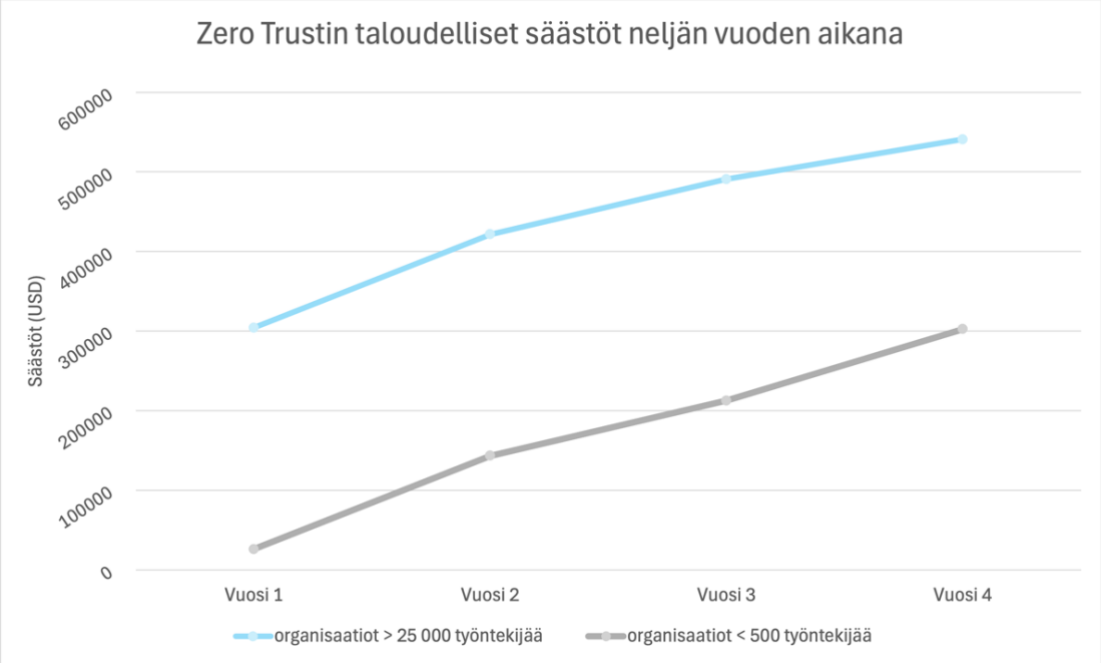
4.3 Taloudelliset vaikutukset

Etenkin organisaatiolle tärkeäksi aspektiksi nousevat kustannus- ja resurssihyödyt. Zero Trust vähentää tietoturvavahinkojen aiheuttamia kustannuksia, koska uhkiin voidaan reagoida aikaisemmin ja estää niiden leviäminen kriittisiin järjestelmiin. Cunningham (2019) toteaa tämän olevan erityisen merkittävää tilanteissa, joissa suojataan organisaation immateriaalioikeuksia ja muuta strategisesti arvokasta tietoa, sillä niiden menettäminen voi näkyä suoraan yrityksen tulevissa tuotoissa. Zero Trust myös yksinkertaistaa teknistä ympäristöä yhdistämällä erillisiä suojausratkaisuja keskitetysti hallittaviksi kokonaisuuksiksi. Tämä vähentää päällekkäisiä työkaluja ja pienentää hallinta-, ylläpito- ja koulutuskustannuksia, kun tietoturvaa ei tarvitse ohjata useiden eri järjestelmien kautta. (Cunningham ym., 2019)

Zero Trust -arkkitehtuurin taloudellinen kannattavuus rakentuu ennen kaikkea sen kyvystä vähentää merkittävästi kyberhyökkäyksistä aiheutuvia riskejä ja niistä seuraavia kustannuksia. Yhdysvaltojen tilastot osoittavat, että kyberhyökkäysten aiheuttamat taloudelliset menetykset ovat kasvaneet

jyrkästi viime vuosikymmeninä, sillä pelkästään vuosien 2016 ja 2023 välillä tappiot kasvoivat 861% (Lee ym., 2025). Tämän kasvavan uhan edessä Zero Trust tarjoaa konkreettisen keinon pienentää liiketoimintariskejä ja sitä kautta parantaa organisaatioiden taloudellista kestävyyttä. Adahman ym. (2022) tuovat myös tutkimuksessaan esiin, että tietomurtojen maailmanlaajuinen keskimääräinen kustannus nousi pelkästään vuonna 2021 3,86 miljoonasta dollarista 4,24 miljoonaan dollariin, mikä korostaa turvallisuusratkaisujen taloudellista merkitystä.

Kuvio 4 havainnollistaa tietomurroista aiheutuneita kustannuksia sekä pienissä että suurissa organisaatioissa. Kuvion säästöt ovat dollareissa ja tarkastelun aikavälinä on neljä vuotta. Pienten organisaatioiden rajauksessa on käytetty alle 500 työntekijän organisaatioita ja suurissa yli 25 000 työntekijän organisaatioita.



Kuvio 4. Zero Trust -arkkitehtuurin käyttöönoton vaikutus tietomurtokustannuksiin pienissä ja suurissa organisaatioissa neljän vuoden aikana, määrät dollareissa esitettyinä (Adahman ym., 2022)

Pienissä organisaatioissa tietomurroista aiheutuva kustannusten riski voi vähentyä jopa 302 000 dollarilla neljän vuoden aikana, ja suurissa organisaatioissa noin 540 000 dollarilla. Vieläkin suuremmissa organisaatioissa säästövaikutus korostuu entisestään: ensimmäisenä vuonna keskimäärin yli 300 000 dollaria ja neljän vuoden aikana jopa yli 2,1 miljoonaa dollaria. Kuvio havainnollistaa myös, että kustannussäästöt kertautuvat tasaisesti ajan myötä. Vaikutus on suhteellisesti merkittävä kaikenkokoisissa organisaatioissa, mikä korostaa Zero Trust -arkkitehtuurin taloudellista hyötyä pitkällä aikavälillä. (Adahman ym., 2022)

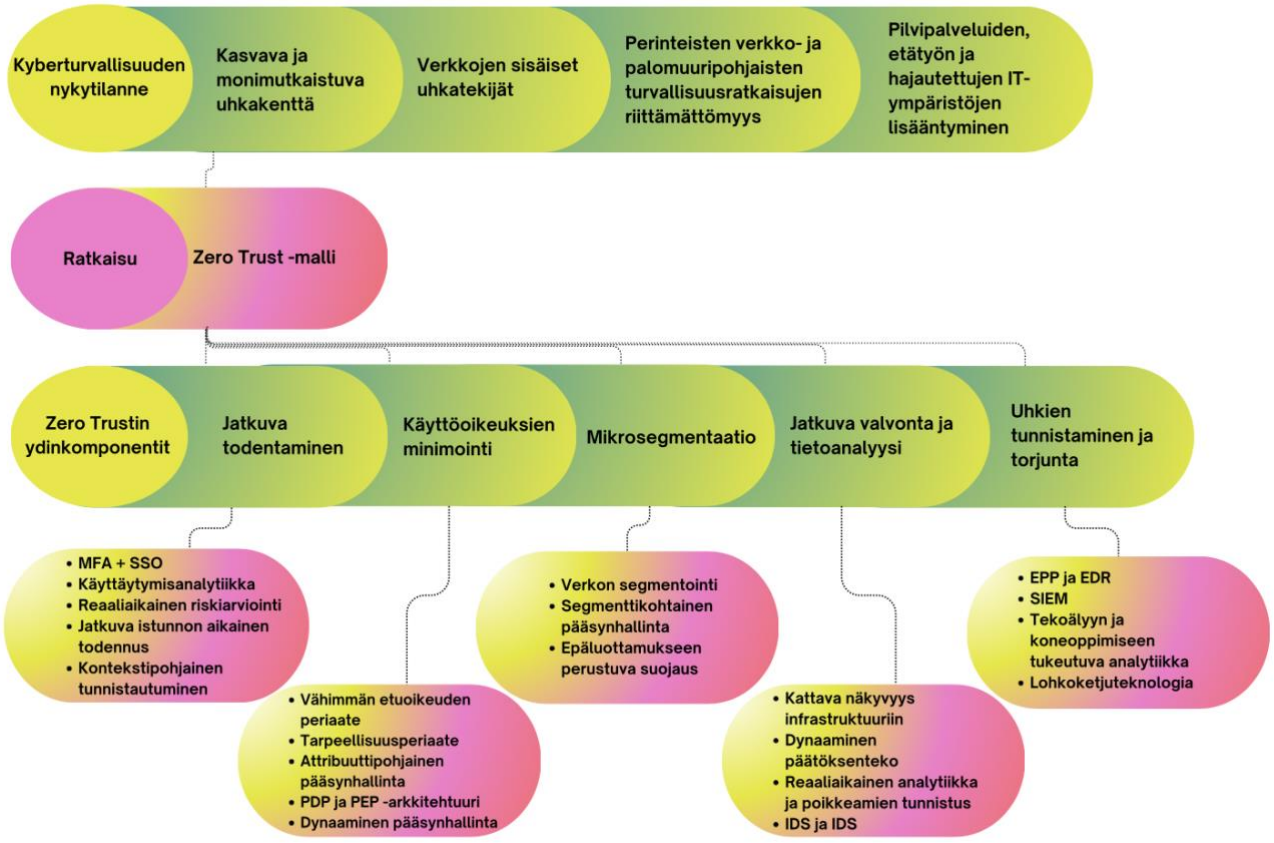
Vaikka Zero Trustin käyttöönotto voi vaatia alkuun merkittäviä investointeja teknologioihin ja muutosjohtamiseen, sen pitkän aikavälin hyödyt näkyvät erityisesti kyberturvallisuuden kehityksenä ja liiketoimintariskiä pienentävänä vaikutuksena. Organisaatioissa, jotka ovat ottaneet Zero Trust -mallin laajalti käyttöön, tietomurroista aiheutuvat keskimääräiset kustannukset ovat jopa 1,76 miljoonaa dollaria pienemmät kuin organisaatioissa, joissa malli ei ole käytössä. (Adahman ym., 2022.) Kyseessä ei siis ole pelkästään tietoturvatekninen ratkaisu, vaan myös strateginen investointi, joka voi tuottaa huomattavaa taloudellista lisäarvoa organisaatiolle (Bartakke & Kashyap, 2024).

5 Yhteenveto ja johtopäätökset

Tässä tutkielmassa tarkasteltiin Zero Trust -periaatteen käyttöä organisaatioiden tietoturvassa ja sen soveltuvuutta erilaisiin järjestelmäympäristöihin. Zero Trust on suhteellisen uusi tietoturvamalli, joka on noussut keskeiseksi tavaksi hallita muuttuvia kyberuhkia. Tutkielman tavoitteena oli jäsentää mallin keskeiset periaatteet ja komponentit ymmärrettävästi sekä havainnollistaa sen tuomat tietoturvamahdollisuudet organisaatioiden kokonaisrakenteessa. Lisäksi tutkimuksessa arvioitiin Zero Trustin käyttöönoton vaikutuksia organisaatioiden tietoturvaan ja toimintakäytäntöihin sekä sen kykyä vastata nykyaikaisen kyberuhkaympäristön haasteisiin. Kyberuhkien monimutkaistuessa organisaatioiden on entistä tärkeämpää siirtyä kokonaisvaltaisempaan ja dynaamisempaan tietoturvaratkaisuun.

Tutkielmassa todettiin, että Zero Trust ei ole pelkkä tekninen ratkaisu, vaan kokonaisvaltainen ajattelumalli, jonka tavoitteena on vahvistaa organisaation kyberturvallisuutta, riskienhallintaa ja toimintavarmuutta. Vaikka Zero Trustia ei ole standardoitu yhtenäiseksi malliksi, sen keskeiset periaatteet toistuvat johdonmukaisesti akateemisessa kirjallisuudessa. Tässä tutkielmassa periaatteet rajattiin viiteen ydinalueeseen: jatkuva todentaminen, käyttöoikeuksien minimointi, mikrosegmentaatio, jatkuva valvonta ja tietoanalyysi sekä uhkien tunnistaminen ja torjunta. Näiden toteuttaminen edellyttää erityisesti identiteetin- ja pääsynhallintaa, verkon segmentointia, datan analysointia ja automaattisia suojausmekanismeja.

Kuvio 5 havainnollistaa tutkielmassa todettuja kyberturvallisuuden nykytilanteen heikkouksia ja esittää, miten Zero Trust -malli vastaa niihin. Lisäksi se kokoaa yhteen mallin ydinkomponentit sekä niiden käytännön toimeenpanoon tarvittavat keinot, jolloin se vastaa myös ensimmäiseen tutkimuskysymykseen. Tämä tutkimuskysymys tarkasteli mallia kokonaisuutena, ja siihen vastattaessa tiivistettiin kunkin ydinperiaatteen toteutustavat. Tutkielmassa havaittiin, että organisaatiot voivat itse sovittaa ydinperiaatteet omiin lähtökohtiin ja tietoturvatavoitteisiinsa. Mallin keskeinen periaate on ”Älä luota, varmista aina”, mitä voidaan toteuttaa esimerkiksi vähimmän etuoikeuden periaatteella, dynaamisella päätöksenteolla, verkkosegmentoinnilla, jatkuvalla valvonnalla sekä MFA- ja SSO-järjestelmien avulla.



Kuvio 5. Zero Trustin kehitykseen johtanut kyberturvallisuuden nykytila sekä keskeiset periaatteet ja niitä tukevat tekniset ratkaisut

Koska Zero Trust -malli on skaalautuva, dynaaminen ja soveltuu erityisen hyvin monipuolisiin työympäristöihin, tutkielmassa tarkasteltiin sen käyttöä pilvi- ja monipilviympäristöissä, IoT-ympäristöissä, etätyöympäristöissä ja hajautetuissa ympäristöissä. Taulukko 2 kokoaa yhteen tutkielman keskeiset havainnot kunkin ympäristön Zero Trust -toimintamahdollisuuksista ja rajoitteista. Mallin ja näiden ympäristöjen yhteensopivuus korostuu erityisesti kasvaneen datamäärän ja hallintatarpeiden seurauksena. Zero Trustin helppo skaalautuvuus tekee siitä kilpailukykyisen ratkaisun moderneille ja kasvaville organisaatioille.

Taulukko 2. Zero Trustin vaikutukset pilvi-, IoT- ja hajautetuissa ympäristöissä

	Zero Trustin hyödyt	Rajoitukset / haasteet
Pilvi- ja monipilviympäristöt	Keskitetty pääsynhallinta, automaattinen valvonta, dynaaminen riskienhallinta	Integraatiohaasteet, suorituskykykuormitus, alkuinvestointi

IoT-ympäristöt	Laitteiden jatkuva tunnistus, mikrosegmentaatio, haitallisen toiminnan esto	Laitteiden rajoitettu tuki, ylläpidon kuormittavuus, resurssirajoitteet
Etätyö ja hajautetut ympäristöt	Käyttäjä- ja laitekohtainen pääsynvalvonta, kontekstuaalinen riskien arviointi	Käyttäjäkokemus, hallinnollinen kuormitus, jatkuvan valvonnan tarve
Yhteiset vaikutukset	Parempi näkyvyys, vahva tietoturva, jatkuva todennus, sisäpiiriuhkien torjunta, skaalautuva ja ketterä, parannettu työntekijäkokemus, hallittavuus ja joustavuus, taloudelliset säästöt	Autentikointiväsymys, monimutkainen hallinta, politiikkariippuvuus, järjestelmän haavoittuvuudet

Tutkielman mukaan Zero Trust -malli on erityisen tehokas hajautetuissa ja pilvipohjaisissa ympäristöissä, joissa käyttäjät, laitteet ja palvelut toimivat samanaikaisesti eri sijainneissa. Pilvi- ja monipilviympäristöissä malli mahdollistaa keskitetyllä pääsynhallinnalla ja automatisoidulla valvonnalla jokaisen yhteyden yksilöllisen todentamisen. IoT-ympäristöissä se tukee laitteiden jatkuvaa tunnistusta, riskipohjaista pääsynhallintaa ja haitallisen toiminnan proaktiivista estoa. Etätyö- ja BYOD-ympäristöissä Zero Trust mahdollistaa käyttäjä- ja laitekohtaisen pääsynvalvonnan, kontekstuaalisen riskinarvioinnin ja poikkeavuuksien reaaliaikaisen havaitsemisen, mikä vähentää tietovuotojen ja väärinkäytösten riskiä. Malli ei siis ainoastaan vahvista turvallisuutta, vaan tarjoaa organisaatioille joustavan ja keskitetyn tavan hallita monimuotoisia ja dynaamisia tietojärjestelmäympäristöjä.

Zero Trustin kokonaisvaikutuksia organisaatioon tarkasteltiin kolmannen tutkimuskysymyksen avulla. Tutkimukset korostavat sen pitkäaikaisia taloudellisia, organisatorisia ja teknisiä hyötyjä: malli parantaa organisaation resilienssiä, vähentää tietoturvaloukkauksista aiheutuvia kustannuksia ja mahdollistaa nopeamman reagoinnin uhkatilanteissa. Lisäksi se lisää läpinäkyvyyttä ja hallittavuutta, mikä tukee strategista päätöksentekoa ja vähentää riippuvuutta yksittäisistä

järjestelmistä. Hyötyjen maksimoimiseksi käyttöönotto edellyttää kuitenkin suunnitelmallista muutoksenhallintaa, henkilöstön koulutusta ja jatkuvaa ylläpitoa.

Tutkielma osoitti, että Zero Trustin käyttöönottoon liittyy merkittäviä haasteita ja rajoituksia, jotka voivat vaikuttaa hyötyjen toteutumiseen. Keskeisiä haasteita ovat järjestelmän suorituskyvyn kuormittuminen, autentikointiväsymys ja monimutkaisen infrastruktuurin hallinnan vaativuus. Myös organisaatiokulttuuri ja käyttäjien hyväksyntä voivat muodostaa esteitä, sillä jatkuva valvonta ja todennus voivat aiheuttaa turhautumista tai epäluottamusta. Taloudellisesti alkuinvestoinnit ja ylläpitokustannukset voivat olla merkittäviä, mutta pitkällä aikavälillä Zero Trust vähentää tietomurroista aiheutuvia kustannuksia, tehostaa resurssien käyttöä ja yhdistää hajautetut suojausratkaisut hallittaviksi kokonaisuuksiksi. Kokonaisuutena Zero Trust tarjoaa merkittäviä hyötyjä, mutta käyttöönotossa on huomioitava myös sen rajoitukset ja riskit.

Tutkielman havaintojen mukaan Zero Trust -periaatteen käyttö tarjoaa organisaatioille kokonaisvaltaisen ratkaisun tietoturvan parantamiseen. Mallin avulla voidaan lisätä järjestelmien näkyvyyttä ja hallittavuutta, vahvistaa käyttäjien ja laitteiden autentikointia, estää hyökkäysten etenemistä sekä vähentää tietomurroista aiheutuvia taloudellisia riskejä. Samalla tutkimuksessa havaittiin, että Zero Trustin tehokas implementointi edellyttää huomattavia teknisiä, organisatorisia ja kulttuurisia resursseja, jatkuvaa valvontaa sekä politiikkojen ja prosessien huolellista hallintaa. Kokonaisuutena malli tarjoaa strategisen ja skaalautuvan ratkaisun nykyaikaisen kyberuhkaympäristön haasteisiin. Hyödyt realisoituvat kuitenkin vain, jos sen vaatimukset otetaan systemaattisesti huomioon ja organisaation toimintamallit mukautetaan tukemaan jatkuvaa turvallisuutta. Näin Zero Trust tarjoaa merkittävän välineen yrityksen tietoturvan vahvistamiseen nykyaikaisissa hajautetuissa järjestelmissä.

Lähteet

Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security*, *122*, 102911. https://doi.org/10.1016/j.cose.2022.102911

Ahuja, L., Vashisth, S., & Thakur, A. (2025). Integrating SIEM with Zero Trust Architecture. *2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, 1–6. https://doi.org/10.1109/IITCEE64140.2025.10915422

Alevizos, L., Eiza, M. H., Ta, V. T., Shi, Q., & Read, J. (2022). Blockchain-Enabled Intrusion Detection and Prevention System of APTs Within Zero Trust Architecture. *IEEE Access*, *10*, 89270–89288. https://doi.org/10.1109/ACCESS.2022.3200165

AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications*, *14*(2). https://doi.org/10.14569/IJACSA.2023.0140292

Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, *27*, 101227. https://doi.org/10.1016/j.iot.2024.101227

Bast, C., & Yeh, K.-H. (2024). Emerging Authentication Technologies for Zero Trust on the Internet of Things. *Symmetry*, *16*(8), 993. https://doi.org/10.3390/sym16080993

Bernabé Murcia, J. M., Cánovas, E., García-Rodríguez, J., M. Zarca, A., & Skarmeta, A. (2025). Decentralised Identity Management solution for zero-trust multi-domain Computing Continuum frameworks. *Future Generation Computer Systems*, *162*, 107479. https://doi.org/10.1016/j.future.2024.08.003

Bertino, E. (2021). Zero Trust Architecture: Does It Help? *IEEE Security & Privacy*, *19*(5), 95–96. https://doi.org/10.1109/MSEC.2021.3091195

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*, 102436. https://doi.org/10.1016/j.cose.2021.102436

CSIS. (2024). *Significant Cyber Incidents Since 2006*. Center for Strategic and International Studies. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cunningham, C., Holmes, D., & Pollard, J. (2019). *The Eight Business And Security Benefits Of Zero Trust*.

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The New Frontier of Cybersecurity: Emerging Threats and Innovations. *2023 29th International Conference on Telecommunications (ICT)*, 1–6. https://doi.org/10.1109/ICT60153.2023.10374044

Dhanaraj, R. K., Singh, A., & Nayyar, A. (2024). Matyas–Meyer Oseas based device profiling for anomaly detection via deep reinforcement learning (MMODPAD-DRL) in zero trust security network. *Computing*, *106*(6), 1933–1962. https://doi.org/10.1007/s00607-024-01269-y

Gambo, M. L., & Almulhem, A. (2026). Zero Trust Architecture: A Systematic Literature Review. *Journal of Network and Systems Management*, *34*(1), 25. https://doi.org/10.1007/s10922-025-09998-x

Golden, D., Perinkolam, A., Nicholson, M., Rafla, A., & Norton, K. (2021). *Zero trust: Never trust, always verify*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2021/zero-trust-security-framework.html

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing*, *2022*, 1–13. https://doi.org/10.1155/2022/6476274

Jimmy, F. (2022). Zero Trust Security: Reimagining Cyber Defense for Modern Organizations. *International Journal of Scientific Research and Management (IJSRM)*, *10*(04), 887–905. https://doi.org/10.18535/ijsrm/v10i4.ec11

Jimmy, F. (2024). Zero Trust Security: Reimagining Cyber Defense for Modern Organizations. *International Journal of Scientific Research and Management (IJSRM)*, *10*, 887–905. https://doi.org/10.18535/ijsrm/v10i4.ec11

Junquera-Sánchez, J., Cilleruelo, C., De-Marcos, L., & Martinez-Herráiz, J.-J. (2021). Access Control beyond Authentication. *Security and Communication Networks*, *2021*, 1–11. https://doi.org/10.1155/2021/8146553

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy*, *25*(12), 1595. https://doi.org/10.3390/e25121595

Kanta, A., Coisel, I., & Scanlon, M. (2022). A Novel Dictionary Generation Methodology for Contextual-Based Password Cracking. *IEEE Access*, *10*, 59178–59188. https://doi.org/10.1109/ACCESS.2022.3179701

Kim, Y., Sohn, S.-G., Kim, K. T., Jeon, H. S., Lee, S.-M., Lee, Y., & Kim, J. (2024). Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. *KSII Transactions on Internet and Information Systems*, *18*(9). https://doi.org/10.3837/tiis.2024.09.011

Lee, J.-S., Chen, T.-H., Chew, C.-J., Wang, P.-Y., & Fan, Y.-Y. (2025). Unconsciously Continuous Authentication Protocol in Zero-Trust Architecture Based on Behavioral Biometrics. *IEEE Transactions on Reliability*, 1–14. https://doi.org/10.1109/TR.2025.3541224

Li, D., Yang, Z., Yu, S., Duan, M., & Yang, S. (2024). A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology. *Future Internet*, *16*(9), 320. https://doi.org/10.3390/fi16090320

Mickie, J. & Jiefeng Weng. (2025). *Zero Trust Security: A Proactive Cybersecurity Model for Risk Management*. Unpublished. https://doi.org/10.13140/RG.2.2.20335.55201

Microsoft Security Response Center. (2024). *Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*. Microsoft. https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

Ministr, J., & Pinter, T. (2024). Cyberattacks on critical infrastructure—A changing landscape. *IDIMT-2024 : Changes to ICT*, *Management*, Czech Republic (2024). https://doi.org/10.35011/IDIMT-2024-103

Nag, A., Hassan, Md. M., Das, A., Sinha, A., Chand, N., Kar, A., Sharma, V., & Alkhayyat, A. (2024). Exploring the applications and security threats of Internet of Thing in the cloud computing paradigm: A comprehensive study on the cloud of things. *Transactions on Emerging Telecommunications Technologies*, *35*(4), e4897. https://doi.org/10.1002/ett.4897

Nisha T N, Pramod, D., & Singh, R. (2023). Zero trust security model: Defining new boundaries to organizational network. *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing*, 603–609. https://doi.org/10.1145/3607947.3608067

Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*, *130*, 103266. https://doi.org/10.1016/j.cose.2023.103266

Parkhomenko, I., Myrutenko, L., Ohiievych, R., & Savonik, M. (2024). *Using Zero Trust Principles for Detecting Authorization Attacks in Cloud Environments*. *2024*.

Petri, I., Rana, O. F., Beach, T., & Rezgui, Y. (2017). Performance analysis of multi-institutional data sharing in the Clouds4Coordination system. *Computers & Electrical Engineering*, *58*, 227–240. https://doi.org/10.1016/j.compeleceng.2017.02.015

Poirrier, A., Cailleux, L., & Heide Clausen, T. (2025). Is Trust Misplaced? A Zero-Trust Survey. *Proceedings of the IEEE*, *113*(1), 5–39. https://doi.org/10.1109/JPROC.2025.3555131

Rabl, T., Sachs, K., Poess, M., Baru, C., & Jacobson, H.-A. (Toim.). (2015). *Big Data Benchmarking: 5th International Workshop, WBDB 2014, Potsdam, Germany, August 5-6- 2014, Revised Selected Papers* (Vol. 8991). Springer International Publishing. https://doi.org/10.1007/978-3-319-20233-4

Ren, Y., Wang, Z., Sharma, P. K., Alqahtani, F., Tolba, A., & Wang, J. (2025). Zero Trust Networks: Evolution and Application from Concept to Practice. *Computers, Materials & Continua*, *82*(2), 1593–1613. https://doi.org/10.32604/cmc.2025.059170

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Routray, K., & Bera, P. (2024). Risk-Aware Lightweight Data Access Control for Cloud-Assisted IIoT: A Zero-Trust Approach. *Proceedings of the SIGCOMM Workshop on Zero Trust Architecture for Next Generation Communications*, 40–42. https://doi.org/10.1145/3672200.3673880

Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability*, *14*(18), 11213. https://doi.org/10.3390/su141811213

Sharma, S., Agrawal, S. S., & Kumar, S. A. (2024). Unlocking Cybersecurity Horizons: Exploring Cutting-Edge Technologies, Strategies, and Trends in the Dynamic Cyber Threat Landscape. *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*, 1–6. https://doi.org/10.1109/ICEC59683.2024.10837210

Simpson, Dr. W. R. (2022). Toward a zero trust metric. *Procedia Computer Science*, *204*, 123–130. https://doi.org/10.1016/j.procs.2022.08.015

Szymanski, T. H. (2022). The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). *IEEE Access*, *10*, 45893–45930. https://doi.org/10.1109/ACCESS.2022.3169137

Tsai, M., Lee, S., & Shieh, S. W. (2024). Strategy for Implementing of Zero Trust Architecture. *IEEE Transactions on Reliability*, *73*(1), 93–100. https://doi.org/10.1109/TR.2023.3345665

Tyler, D., & Viana, T. (2021). Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture. *Applied Sciences*, *11*(16), 7499. https://doi.org/10.3390/app11167499

Verma, P. K., Singh, B., Shubham, P., Sharma, K., & Prasad Joshi, R. (2024). Evaluating the Effectiveness of Zero Trust Architecture in Protecting Against Advanced Persistent Threats. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, *13*, e31611. https://doi.org/10.14201/adcaij.31611

Wang, R., Li, C., Zhang, K., & Tu, B. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity*, *8*(1), 12. https://doi.org/10.1186/s42400-024-00320-x

Wu, H., Zhou, B., & Zhang, C. (2022). Secure Distributed Estimation Against Data Integrity Attacks in Internet-of-Things Systems. *IEEE Transactions on Automation Science and Engineering*, *19*(3), 2552–2565. https://doi.org/10.1109/TASE.2021.3090416

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers & Security*, *133*, 103412. https://doi.org/10.1016/j.cose.2023.103412

Zanasi, C., Marchetti, M., & Colajanni, M. (2024). Cybersecurity Domains: A design pattern for creating Zero Trust Architectures through microsegmentation. *2024 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC)*, 15–22. https://doi.org/10.1109/DASC64200.2024.00009

Zhang, Y. (2023). Privacy-Preserving with Zero Trust Computational Intelligent Hybrid Technique to English Education Model. *Applied Artificial Intelligence*, *37*(1), 2219560. https://doi.org/10.1080/08839514.2023.2219560

Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work. *Information*, *15*(11), 734. https://doi.org/10.3390/info15110734

Liitteet

Liite 1 Selvitys tekoälyn käytöstä

Tutkielman laatimisessa on hyödynnetty tekoälyä aiheiden ja tutkimuskysymysten ideointiin, tekstin kieliasun tarkistamiseen, visuaalisten kuvioiden ideointiin, muistiinpanojen jäsentämiseen ja teknisten kokonaisuuksien hahmottamiseen. Tekoäly toimi tukivälineenä tiedon hallinnassa, esitystavan selkeyttämisessä ja monimutkaisten konseptien ymmärtämisessä. Lisäksi Scopus AI:tä hyödynnettiin artikkeleiden etsinnässä.