TURUN YLIOPISTO

Zero Trust -arkkitehtuuri kyberturvallisuuden ratkaisuna: hyödyt ja haasteet

Luk-tutkielma
Tietojenkäsittelytiede
Tietotekniikan laitos, Teknillinen tiedekunta
Ville Suutari
Kesäkuu 2025

LuK-tutkielma
Tietotekniikan laitos, Teknillinen tiedekunta
Turun yliopisto

Tutkinto-ohjelma: Tietojenkäsittelytiede
Tekijä: Ville Topias Suutari
Otsikko: Zero Trust -arkkitehtuuri kyberturvallisuuden ratkaisuna: hyödyt ja haasteet
Sivumäärä: 22 sivua
Päivämäärä: Kesäkuu 2025

Zero Trust -arkkitehtuuri (ZTA) on tietoturvamalli, jossa luottamus ei perustu verkon fyysiseen sijaintiin. ZTA:ssa jokainen tehty pyyntö edellyttää autentikoinnin ja valtuutuksen, jonka jälkeen pyyntö joko hyväksytään tai hylätään. Tämä tutkielma tarkastelee ZTA:n teknologioita ja menetelmiä sekä vertailee niitä perinteiseen raja-alueisiin perustuvaan tietoturvamalliin. Lisäksi tutkielmassa arvioidaan ZTA:n käyttöönottoon liittyviä haasteita ja tutkitaan sen vaikutusta etätyöskentelyssä. Tutkielma on toteutettu kirjallisuuskatsauksena ja pohjautuu useisiin ajankohtaisiin tutkimusartikkeleihin ja alan asiantuntijalähteisiin.

ZTA eroaa merkittävästi perinteisestä tietoturvamallista erityisesti pääsynvalvonnan, luottamuksen hallinnan ja jatkuvan seurannan näkökulmista. ZTA:n käyttöönottoon liittyy teknisiä, organisatorisia ja kulttuurillisia haasteita, joita voidaan hallita vaiheittaisen implementoinnin ja tehokkaan suunnittelun avulla. Etäympäristöissä ZTA:n hyödyt korostuvat entisestään, koska se mahdollistaa turvallisen työskentelyn sijainnista ja laitteista riippumatta.

ZTA voi parantaa organisaation yleisen kyberturvallisuuden tasoa, mutta sen onnistunut käyttöönotto vaatii kokonaisvaltaista lähestymistä sekä taktisesti että hallinnollisesti.

Asiasanat: Zero Trust -arkkitehtuuri, tietoturva, kyberturvallisuus, autentikointi, segmentointi, käyttöönotto, käyttäjäkokemus, etätyöskentely

Sisällysluettelo

1 Johdanto 1

1.1 Tutkielman tavoite ja tutkimuskysymykset 2

1.2 Tutkimusmenetelmät ja tiedonhaku 3

1.3 Tutkielman rakenne 4

2 Zero Trust -arkkitehtuuri 5

2.1 Zero trust -arkkitehtuurin keskeiset teknologiat ja menetelmät 6

2.1.1 Autentikointi ja jatkuva autentikointi 6

2.1.2 Vähimpien oikeuksien periaate 7

2.1.3 Segmentointi 7

2.1.4 Käytäntöjen hallinta 7

2.1.5 Ohjelmiston määrittelemä piiri 8

2.1.6 Verkkoliikenteen seuranta 8

2.2 Käyttö nykyään 9

3 Zero Trust -arkkitehtuurin erot perinteiseen tietoturvamalliin 11

3.1 Perinteinen tietoturva 12

3.1.1 Zero Trust- arkkitehtuurin ominaisuuksien arviointi 12

3.1.2 Perinteisen tietoturvan ominaisuuksien arviointi 13

3.2 Keskeisimmät erot 13

3.2.1 Luottamuksen sijainti 13

3.2.2 Käyttäjien ja laitteiden hallinta 14

3.2.3 Suojausstrategiat 14

3.2.4 Reagointikyky ja valvonta 14

3.2.5 Skaalautuvuus ja nykyaikaisuus 15

4 Zero trust -arkkitehtuurin käyttöönotto ja siihen liittyvät haasteet 17

5 Vaikutus etätyöskentelyyn 20

6 Yhteenveto ja johtopäätökset 22

Lähteet 23

1 Johdanto

Erilaiset kyberuhkat kehittyvät ja yleistyvät, minkä takia yritysten on jatkuvasti arvioitava ja muokattava käytettävien verkkoympäristöjen turvallisuutta suojellakseen arvokkaita resursseja ja kriittistä infrastruktuuria. Nopeasti etenevä yritysten digitaalinen transformaatio ja monimutkaisemmat IT-ympäristöt luovat uusia haavoittuvaisuuksia, joita perinteiset tietoturvaratkaisut eivät välttämättä enää kykene ratkaisemaan. [1] Zero Trust (ZT) -käsitteen ja Zero Trust -arkkitehtuurin esittelivät ensimmäistä kertaa John Kindervag ja Forrester Market Research organization vuonna 2010. Kyseessä on verkkoarkkitehtuuri, jossa mikään verkko ei ole oletuksena turvallinen, vaan kaikkia verkkoja ja päätelaitteita kohdellaan mahdollisena uhkana. Zero Trust -arkkitehtuurissa kaikki yhteyspyynnöt autentikoidaan ja valtuutetaan ja samalla sellaiset yhteydet katkaistaan välittömästi, joita ei erikseen ole sallittu. [2]

Tällainen malli haastaa perinteisen oletuksen siitä, että yrityksen sisäinen verkko olisi lähtökohtaisesti turvallinen ja luotettava. Tämän paradigman myötä luottamus ei enää perustu sijaintiin verkossa, vaan tarkasti määriteltyihin käyttöoikeuksiin ja jatkuvaan tarkasteluun. Ydinajatuksena mallissa on periaate ”älä ikinä luota, varmista aina”, eli mihinkään yhdistettyihin laitteisiin tai käyttäjiin ei luoteta oletusarvoisesti [3]. Tämä lähestymistapa tuo mukanaan suuremman kontrollin ja näkyvyyden, mutta edellyttää myös huolellista suunnittelua ja toimintamallien päivittämistä. Esimerkiksi identiteetin- ja pääsynhallinnan merkitys korostuu merkittävästi, koska juuri näiden avulla varmistetaan, että vain oikeat käyttäjät pääsevät käsiksi oikeisiin resursseihin oikeaan aikaan.

ZT-paradigmalla on kaksi keskeistä oletusta:

- Ulkoiset ja sisäiset uhkat ovat verkossa läsnä jatkuvasti. Verkon tulee siis olla valmiina torjumaan hyökkäyksiä reaaliajassa.
- Luotettavuuden kannalta ei ole merkitystä onko yhteys paikallinen tai sisäinen. Verkkoon tunkeutuminen sivuttaisella liikkeellä (lateral movement) on yleinen hyökkääjien käyttämä strategia, missä tunkeudutaan aluksi ulompaan järjestelmään ja sen avulla syvemmälle verkkoon. Luottamus verkkoon saavutetaan varmistamalla, että pääsy tämän verkon eri resursseihin on tehokkaasti hallittua. [4]

Zero Trust -arkkitehtuuri ei ole yksittäinen ratkaisu tai tuote, vaan koko organisaation toimintatapaa ja tietoturvakulttuuria muovaava lähestymistapa. Se pakottaa organisaation miettimään kriittisesti, kehen ja mihin voidaan todella luottaa ja ennen kaikkea, miten tämä luottamus rakennetaan teknologisesti kestävällä tavalla. Zero Trust -arkkitehtuuri tarjoaa konkreettisen vastauksen jatkuvasti muuttuvan uhkaympäristön haasteisiin. Se ei pelkästään suojaa organisaatiota ja tämän resursseja, vaan vaatii

myös prosessien, käyttäjien toiminnan ja koko organisaatiokulttuurin tarkastelua. Tämä tekee siitä paitsi teknisesti vaikuttavan, myös strategisesti tärkeän lähestymistavan nykyaikaisessa kyberturvallisuudessa.

Statistan [5] kyselyssä tarkastellaan keskeisimpiä syitä, jotka johtavat arkaluontoisen tiedon vuotamiseen organisaatioiden sisällä. Kyselyn mukaan yleisimmät syyt tietovuodoille ovat huolimaton käyttäjä (70.6 %), vaarantunut järjestelmä (48.1 %), huonosti määritelty järjestelmä (45.3 %) ja tahallisesti haittaa aiheuttava työntekijä tai urakoitsija (20 %). Näistä arvoista nähdään se, että järjestelmän käyttäjä ja itse järjestelmän toteutus ovat kriittisiä tekijöitä tiedon eheyden säilyttämisessä. Zero Trust -arkkitehtuuri ja Zero Trust -menetelmien harjoittaminen organisaatioiden sisällä antaa mahdollisuuden vaikuttaa näihin edellä mainittuihin riskitekijöihin ja näin parantamaan yleistä tietoturvan tasoa sekä vähentämään tietovuotojen määrää.

1.1 Tutkielman tavoite ja tutkimuskysymykset

Tutkielman päätavoitteena on analysoida Zero Trust -arkkitehtuurin roolia nykyaikaisen kyberturvallisuuden ratkaisuna ja selvittää sen käytännön merkitystä erityisesti organisaatioiden tietoturvakäytännöissä. Tarkoituksena on tarkastella Zero Trust -arkkitehtuurin keskeisiä periaatteita, tunnistaa sen ominaisia menetelmiä ja teknologioita sekä vertailla niitä perinteiseen tietoturvamalliin. Näin pyritään luomaan selkeä käsitys siitä, millaisia etuja ja mahdollisia heikkouksia kumpikin malli pitää sisällään, ja miten ne eroavat toisistaan rakenteellisesti ja toiminnallisesti.

Tutkimuksessa tarkastellaan myös Zero Trust -arkkitehtuurin käyttöönottoon liittyviä käytännön haasteita. Näitä voivat olla esimerkiksi teknologiset rajoitteet, organisatoriset muutosprosessit sekä henkilöstön koulutustarpeet. Tavoitteena on tuoda esiin konkreettisia tapoja, joilla Zero Trust -arkkitehtuuria voidaan soveltaa ja kuinka se voidaan ottaa käyttöön osana organisaation infrastruktuuria.

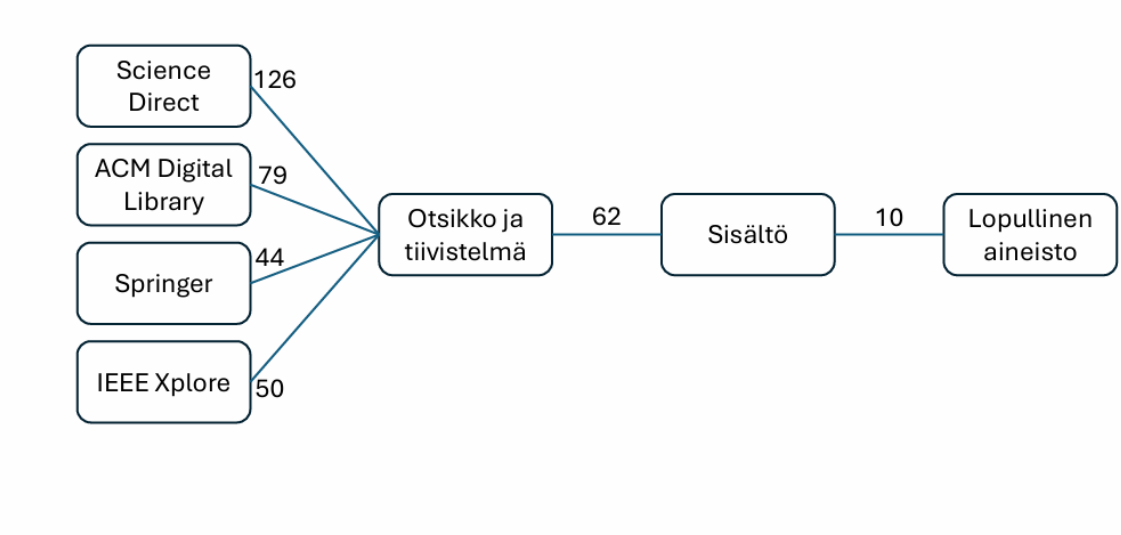
Lisäksi tutkielmassa pohditaan, miten Zero Trust -arkkitehtuuri vaikuttaa etätyöskentelyyn, joka on viime vuosina yleistynyt merkittävästi. Erityisesti tarkastellaan, kuinka Zero Trust -arkkitehtuuri voi tukea turvallista etätyötä ja suojautumista mahdollisia kyberuhkia vastaan hajautetussa työympäristössä.

Tämän tutkielman tavoitteena on muodostaa kattava kokonaiskuva siitä, mikä Zero Trust -arkkitehtuuri on, miten se voi auttaa organisaatioita parantamaan tietoturvansa tasoa ja millaisia haasteita sen käytännön soveltaminen voi tuoda mukanaan. Työn lähtökohtana toimivat seuraavat kolme tutkimuskysymystä, joiden avulla aihetta lähestytään systemaattisesti:

TK1: Mitä eroja on Zero Trust -arkkitehtuurilla ja perinteisellä tietoturvalla?
TK2: Mitä haasteita Zero Trust -arkkitehtuurin käyttöönotossa on?
TK3: Kuinka Zero Trust -arkkitehtuuri vaikuttaa etätyöskentelyyn?

1.2 Tutkimusmenetelmät ja tiedonhaku

Tutkielma on suoritettu kirjallisuuskatsauksena. Aiheeseen liittyvää tietoa haettiin seuraavista tietokannoista: Springer, ACM Digital Library, ScienceDirect ja IEEE Xplore. Tietoa haettiin pääosin kahdella vakiintuneella hakulausekkeella ("Zero trust architecture" OR "Zero trust network access" OR ZTNA) AND ("network security" OR "cloud security") ja ("Zero trust architecture" OR "Zero trust network access" OR ”ZTNA”) AND ("network security” OR "cloud security") AND ("identity management" OR "access control") AND ("threat detection" OR "insider threat"). Hakulausekkeita on muokattu myös sisältämään termejä, kuten ”remote work”, ”cybersecurity”, ”implement” ja ”segmentation”. Näillä lausekkeilla löydettyjä hakutuloksia karsittiin ensin otsikon, sitten tiivistelmän ja lopulta kokonaisuuden ja sisällön perusteella osaksi lopullista aineistoa. Hakujen tulosten määrä saatiin rajattua sopivaksi käyttämällä täsmällisiä hakulausekkeita, joita oli muokattu edellä mainitulla tavalla. Kuvassa 1.1 on havainnollistava kuva hakutulosten määrästä ja valikoitumisesta varsinaiseen aineistoon.



Kuva 1.1: Tutkielman aineiston tiedonhakuprosessi.

1.3 Tutkielman rakenne

Tutkielman toisessa luvussa perehdytään tarkemmin Zero Trust -arkkitehtuuriin sen käsitteen, periaatteiden sekä keskeisimpien menetelmien ja käyttötarkoitusten kautta. Tämä luku toimii teoreettisena taustoituksena ja tarjoaa lukijalle tarvittavan perustan myöhemmissä luvuissa esitettyjen havaintojen ja pohdintojen ymmärtämiseksi. Toisen luvun jälkeen siirrytään tutkielman varsinaisiin käsittelylukuihin, joissa aihetta lähestytään tutkimuskysymysten näkökulmasta. Näissä luvuissa pyritään tarjoamaan jokaiseen tutkimuskysymykseen selkeä ja perusteltu vastaus olemassa olevan kirjallisuuden ja muiden lähteiden avulla.

Kolmannessa luvussa tarkastellaan perinteisen tietoturvamallin ja Zero Trust -arkkitehtuurin välisiä eroja. Luvussa vertaillaan molempien mallien vahvuuksia ja heikkouksia muun muassa luottamuksen hallinnan, verkon suojaamisen ja käyttäjien tunnistamisen näkökulmista. Tämän vertailun tarkoituksena on havainnollistaa, millaisia konkreettisia muutoksia Zero Trust -arkkitehtuuri tuo mukanaan verrattuna aiempiin malleihin.

Neljännessä luvussa keskitytään Zero Trust -arkkitehtuurin käyttöönottoon liittyviin haasteisiin, erityisesti organisaatioiden näkökulmasta. Luvussa tarkastellaan, millaisia teknisiä, hallinnollisia ja kulttuurisia esteitä käyttöönoton tiellä voi esiintyä, ja miten niitä voidaan mahdollisesti ratkaista. Lisäksi käsitellään erilaisia käytännön keinoja ja strategioita, joilla Zero Trust -periaatteita voidaan implementoida osaksi organisaation tietoturvatoimintaa.

Viidennessä luvussa tutkitaan Zero Trust -arkkitehtuurin vaikutusta etätyöskentelyyn. Luvussa arvioidaan, kuinka Zero Trust -arkkitehtuuri voi tukea turvallista työskentelyä hajautetuissa ympäristöissä ja millä tavoin etätyön yleistyminen on vaikuttanut tietoturvan kokonaistasoon. Tarkastelun kohteena ovat muun muassa pääsynhallinta, käyttäjien autentikointi ja laitteiden luotettavuuden arviointi etätyökontekstissa.

2 Zero Trust -arkkitehtuuri

Zero Trust -arkkitehtuuri (ZTA) on yksi uusimmista organisaatioiden lähestymistavoista kyberuhkien torjumiseksi. Se on nopeasti syrjäyttämässä perinteisen raja-alueisiin perustuvan tietoturvamallin, koska tyypillisen yrityksen operatiivisten palveluiden kuten sisäisten verkkojen, etätoimistojen, paikallisen infrastruktuurin, pilvipalveluiden ja liikkuvan käyttäjäkunnan monimutkaisuus on merkittävästi lisääntynyt. Tällaisessa ympäristössä ei ole olemassa yhtä selkeästi määriteltyä menetelmää, joka riittäisi suojaamaan koko infrastruktuuria erilaisilta uhkilta. [6] Perinteiset mallit, jotka luottavat vahvasti verkon määritettyihin rajoihin ja olettavat verkkoon yhdistettyjen käyttäjien olevan automaattisesti luotettavia eivät enää vastaa nykyisiä uhkakuvia ja kykene turvaamaan koko verkkoympäristöä tehokkaasti. Hyökkäykset voivat lähteä liikkeelle järjestelmän sisältä joko tahattomasti tai tarkoituksellisesti.

Zero Trust -periaatteisiin perustuva ZTA on suunniteltu estämään tietovuotoja ja rajoittamaan järjestelmän sisäistä sivuttaista liikettä. Lähestymistavan pääasiallisena tavoitteena on tietojen ja palveluiden suojaaminen, mutta sitä on laajennettu kattamaan myös yrityksen varoja, laitteita, infrastruktuuria, virtuaalisia- ja pilvikomponentteja sekä loppukäyttäjiä ja sovelluksia, jotka pyytävät tietoa yrityksen resursseista. Zero Trust -periaatteiden oletus on se, että ympäristö on hyökkäyksen kohteena ja että yrityksen muut omat tai ulkopuoliset ympäristöt eivät ole luotettavia [6]. Tämä lähestymistapa on erityisen tärkeä nykypäivän hybridiorganisaatioissa, joissa palvelut ovat hajautettuja ja käyttäjät liikkuvia. Luottamuksen siirtäminen yksittäisitä verkoista tai sijainneista yksittäisiin käyttäjiin ja laitteisiin mahdollistaa tarkemman ja tehokkaamman riskienhallinnan.

Zero Trust on kyberturvallisuuden paradigma, joka keskittyy resurssien turvaamiseen ja oletukseen siitä, että luottamusta ei saada suoraan, vaan sen ylläpitäminen vaatii jatkuvaa arviointia. Lähtökohtana on rajoittaa pääsyä resursseihin ja antaa vain vähäisimmät tarvittavat käyttöoikeudet tehtävän suorittamiseen. [7] Näin voidaan välttyä tilanteilta, joissa käyttäjällä on pääsyoikeudet sellaisiin mahdollisesti kriittisiin resursseihin, joita tämä ei itse missään vaiheessa tarvitse. Tällaiset liialliset ja rajaamattomat käyttöoikeudet voivat johtaa yleiseen tietoturvan heikentymiseen, koska erityisesti tiedon luottamuksellisuus kärsii. Tämä on ollut konkreettinen ongelma tietomurroissa, joissa hyökkääjä on saanut haltuunsa yhden käyttäjätilin ja päässyt käsiksi sellaiseen tietomassaan, johon alkuperäisen käyttäjän ei edes olisi tarvinnut päästä.

Liian laajat tai huonosti hallitut pääsyoikeudet ovat usein merkittävä riski, erityisesti tilanteissa, joissa käyttäjillä on pääsy järjestelmiin tai dataan, jota he eivät työtehtävissään tarvitse. Näissä tapauksissa Zero Trust -arkkitehtuuri tuo konkreettista hyötyä estämällä esimerkiksi tietojen vuotamisen tai

järjestelmien manipuloinnin sisäisten uhkien seurauksena. Tämä on tärkeää erityisesti hajautetuissa työympäristöissä, joissa työntekijät voivat käyttää organisaation järjestelmiä eri paikoista, eri päätelaitteilla ja eri yhteyksillä. Zero Trust -arkkitehtuuri tukee modernia tapaa työskennellä mahdollistaen turvallisen etätyön, mutta samalla se asettaa selkeät menetelmät ja teknologiat, jotka estävät mahdolliset väärinkäytökset.

2.1 Zero Trust -arkkitehtuurin keskeiset teknologiat ja menetelmät

National Institute of Standards and Technology (NIST) määrittelee, että ZTA ei ole yksiselitteinen verkkoarkkitehtuuri, joka voitaisiin saavuttaa käyttämällä vain yhtä tiettyä teknologiaa. ZTA koostuu monista ohjeellisista periaatteista, jotka tulee strategisesti implementoida osaksi organisaatiota suojaamaan tämän resursseja kuten dataa, laitteita, käyttäjiä ja muita infrastruktuurin osia. [8] Tämä korostaa sitä, että ZTA ei ole pelkkä tekninen ratkaisu, vaan koko organisaation kattava lähestymistapa, jonka käyttöönotto edellyttää muutoksia organisaation teknologisessa arkkitehtuurissa ja toimintatavoissa.

2.1.1 Autentikointi ja jatkuva autentikointi

Identiteetin ja pääsynhallinta (Identity and access management, IAM) on keskeinen osa ZTA:ta, jonka tarkoituksena on varmistaa, että vain oikeilla henkilöillä on pääsy oikeisiin resursseihin oikeaan aikaan [9].

Autentikointi (Authentication) on prosessi, jolla pyritään varmistamaan väitetty henkilöllisyys. Autentikoinnin tarkoituksena on siis saada varmistus siitä, että esimerkiksi rajoitettuihin resursseihin pääsevät käsiksi vain tietyt henkilöt tai tietyn tason henkilöstö [8]. Erilaisia autentikointitapoja voivat olla esimerkiksi perinteinen käyttäjätunnus–salasana yhdistelmä, monivaiheinen tunnistautuminen (Multi Factor Authentication, MFA), biometrinen tunnistautuminen tai erilaiset laitekohtaiset varmenteet. Nykyisin yhä useammat organisaatiot hyödyntävät MFA:ta, sillä se tuo lisäkerroksen suojaa erityisesti tapauksissa, joissa käyttäjän salasana vuotaa tai tämä joutuu tietojenkalastelun kohteeksi.

Autentikointilla voidaan varmistaa henkilöllisyys vain käyttäjän kirjautumishetkellä. **Jatkuvalla autentikoinnilla** (Continuous authentication) on tarkoitus saada varmuus siitä, että kerran tunnistettu käyttäjä pysyy samana koko istunnon tai kirjautumisen ajan. Jatkuvan autentikoinnin menetelmien tulee pystyä tunnistamaan ja erottamaan käyttäjät toisistaan seuraamalla käyttäjän toimintoja ja ominaisuuksia [10]. Erilaisia jatkuvan autentikoinnin menetelmiä ovat esimerkiksi jatkuva kasvontunnistus, näppäimistön ja hiiren liikkeen seuranta sekä käyttäjän käytöksen seuranta. Näiden menetelmien avulla voidaan havaita poikkeavaisuuksia käyttäjän toiminnassa ja näin havaita

mahdollinen tietomurto reaaliajassa. Tämän perusteella järjestelmä voi automaattisesti rajoittaa käyttöoikeuksia tai vaatia uudelleenkirjautumista.

2.1.2 Vähimpien oikeuksien periaate

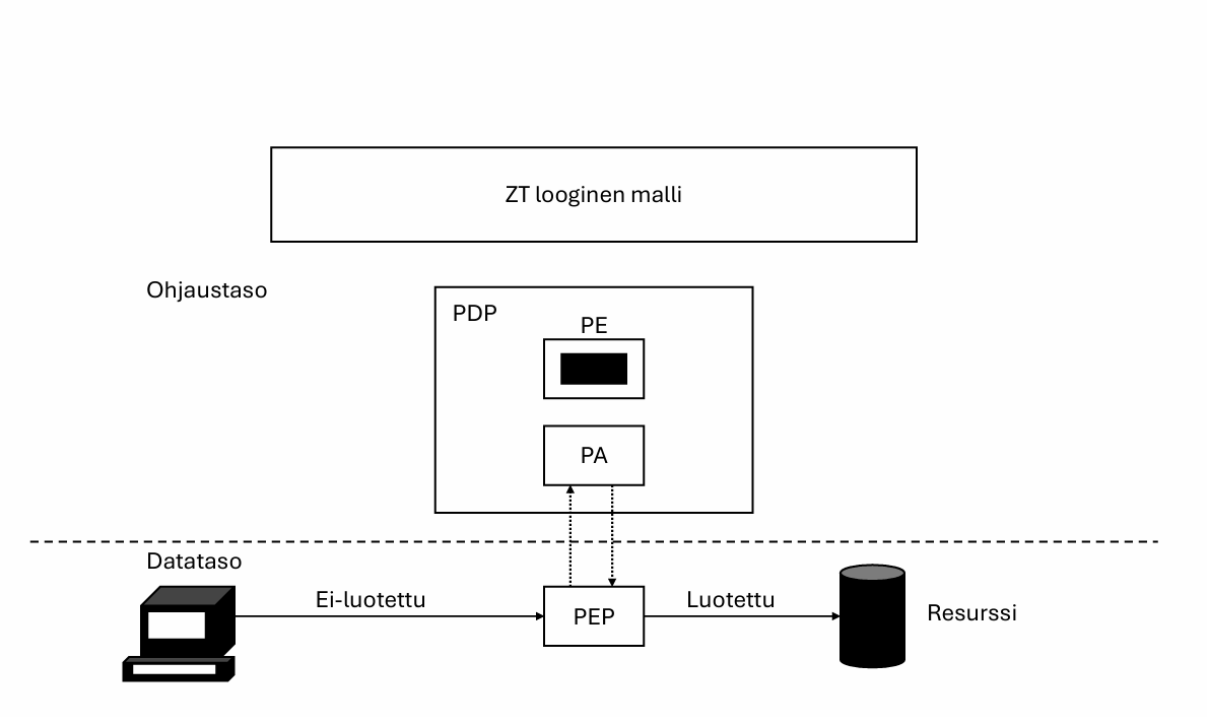
Vähimpien oikeuksien periaate (Least privilege) perustuu ajatukseen, että käyttäjälle annetaan vain pienimmät mahdolliset käyttöoikeudet järjestelmään ja sen eri osiin tehtävän suorittamiseksi [11]. Tällä periaatteella pyritään siihen, että tietomurron tapahtuessa hyökkääjän pääsy järjestelmän sisällä saadaan pidettyä mahdollisimman pienenä ja näin vähentämään vahingon määrää. Käytännössä tämä tarkoittaa sitä, että tavallinen työntekijä ei saa järjestelmänvalvojan oikeuksia, vaikka hän sitä tilapäisesti voisi tarvita päästäkseen käsiksi tiettyyn resurssiin. Lisäksi käyttöoikeuksia tulee muuttaa jatkuvasti tarpeen vaatiessa ja erityisesti silloin, kun työntekijän rooli tai tehtävät muuttuvat.

2.1.3 Segmentointi

Verkon **segmentoinnilla** (Segmentation) tarkoitetaan sen jakamista pienempiin ja paremmin turvattuihin vyöhykkeisiin. Jokainen vyöhyke erotetaan toisistaan käyttämällä erilaisia turvallisuusmenetelmiä ja tällä tavoin estetään niiden välillä tapahtuvaa liikettä. [12] Segmentoinnilla voidaan rajoittaa sivuttaista liikettä ja estää hyökkääjän pääsyä syvemmälle järjestelmässä. Tällainen rakenne ei ainoastaan paranna yleistä tietoturvan tasoa, vaan auttaa myös uhkien havaitsemisessa ja niihin reagoimisessa. Poikkeava tietoliikenne voidaan kohdentaa tarkasti tietylle vyöhykkeelle ja ryhtyä tarvittaviin vastatoimiin.

2.1.4 Käytäntöjen hallinta

Käytäntöjen toimeenpanopiste (Policy enforcement point, PEP) vastaa pääsynvalvonnasta, salauksesta ja käyttäjien jatkuvasta monitoroinnista. Käyttäjä lähettää pyynnön PEP:lle aina kun tämä haluaa päästä käsiksi joihinkin organisaation resursseihin. PEP varmistaa käyttäjän henkilöllisyyden ja pyyntö lähetetään eteenpäin käytäntöjen päätöspisteelle (Policy decision point, PDP). PDP taas puolestaan tekee päätöksen siitä, annetaanko käyttäjälle pääsy pyydettyyn resurssiin. [13] PDP koostuu käytäntöjen moottorista (Policy engine, PE) ja käytäntöjen valvojasta (Policy administrator, PA). PE tekee päätöksen järjestelmään pääsystä yrityksen ennalta määritettyjen käytäntöjen perusteella syöttämällä ulkoiset syötteet luottamusalgoritmille (Trust algorithm), joka toimii koko järjestelmän ”aivoina”. PA toimii tiiviisti yhdessä PE:n kanssa ja joko hyväksyy tai hylkää pääsyn PE:n päätöksen mukaan. [8] Kuvassa 2.1 on havainnollistettu käytäntöjen hallinnan toimintaa ja järjestelmän eri osia.



Kuva 2.1: Käytäntöjen hallintaa kuvaava malli [8]

2.1.5 Ohjelmiston määrittelemä piiri

Ohjelmiston määrittelemä piiri (Software defined perimeter, SDP) käyttää ohjainta varmistaakseen, että asiakassovellukset tai laitteet valtuutetaan ja todennetaan ennen salatun yhteyden luomista reaaliajassa pyydettyihin palvelimiin. SDP:llä on useita etuja, kuten sovellusten piilottaminen luvattomilta käyttäjiltä sekä täysi näkymättömyys ja yhteyden esto kaikille paitsi valtuutetuille käyttäjille ja laitteille. Lisäksi se mahdollistaa operaattorien dynaamisen verkon raja-alueiden määrittämisen ja se toimii yhdessä käyttäjien todentamisjärjestelmien kanssa. [14]

2.1.6 Verkkoliikenteen seuranta

Nykypäivän verkkoympäristöt ovat monimutkaisia ja koostuvat erilaisista laitteista, verkoista, sovelluksista ja verkkoliikenteestä. Jatkuvalla verkkoliikenteen seuraamisella kerätään ja analysoidaan valtavia määriä dataa monista eri lähteistä kuten lokeista, käyttäjien laitteista, käyttäytymiskuvioista ja käyttöjärjestelmän tapahtumista [12]. Epäilyttävät yhteydet ja normaalista poikkeava liikenne voidaan tunnistaa verkkoliikennettä seuraamalla ja ryhtyä välittömästi vastatoimiin.

2.2 Käyttö nykyään

Pilvilaskennan (Cloud computing) kasvu tarkoittaa sitä, että yritykset tallentavat kriittisiä yritysresurssejaan sekä pilveen että paikallisesti. Tämän seurauksena perinteinen verkon rajoihin perustuva tietoturvamalli ei enää riitä suojaamaan näitä resursseja [15].

Vaikka ZTA on suhteellisen uusi turvallisuusmalli, niin se on saanut huomattavaa suosiota eri organisaatioissa. Microsoftin vuoden 2021 kyselyssä vastanneista organisaatioista 76 % ilmoitti jo implementoivansa ZTA-ratkaisuja tai olevansa kiinnostuneita tekemään niin [10]. Suosion kasvua selittää osin juuri se, että perinteiset tietoturvamallit eivät enää riitä suojaamaan nykyaikaisia hajautuneita IT-ympäristöjä. Myös etätyön yleistyminen, pilvipalveluiden käyttö ja hienostuneemmat kyberhyökkäykset ovat pakottaneet organisaatioita ottamaan käyttöön vahvempia ja joustavampia suojausmalleja kuten ZTA. Maailmanlaajuinen Zero Trust -turvallisuusmarkkinan arvo on vuonna 2023 ollut noin 31.6 miljardia Yhdysvaltain dollaria ja luvun on odotettu nousevan 133:een miljardiin vuoteen 2032 mennessä [16]. Tämä heijastaa organisaatioiden halua panostaa omaan kyberturvallisuuteensa sekä sitä, kuinka tärkeänä ZTA-ratkaisuja pidetään organisaatoissa.

Lisäksi kyberrikoksista aiheutuneet kustannukset ovat maailmanlaajuisesti tasaisessa nousussa. Statistan [17] mukaan maailmanlaajuiset kustannukset ovat vuonna 2018 olleet 0.86 biljoonaa Yhdysvaltain dollaria ja luvun on ennustettu nousevan 15.63:een vuoteen 2029 mennessä. Kuvassa 2.2 on esitettynä kuvaaja Statistan sivuilta, josta voidaan havaita lähes lineaarinen kasvu kyberrikoksista aiheutuneista kustannuksista. Näistä luvuista voidaan päätellä, että Zero Trust -arkkitehtuurin ja Zero Trust-ratkaisujen noudattaminen ja niihin investoiminen on entistä tärkeämmässä roolissa nykypäivän IT-ympäristöissä ja moderneissa organisaatioissa. Forrester Researchin [18] tutkimuksessa on havaittu, että Zero Trustin avulla tietoturvatapahtumat voidaan havaita, ja niihin voidaan reagoida jopa 50% nopeammin.

Kuva 2.2: Kyberrikoksista aiheutuneet kustannukset maailmanlaajuisesti, data kerätty Statistan verkkosivuilta. [17]

Zero Trust -arkkitehtuurin yleistymistä selittävät myös erilaiset yhteiskunnalliset ja poliittiset ilmiöt. Toukokuussa 2021 Yhdysvaltain presidentti Joe Biden antoi toimeenpanomääräyksen (Executive Order 14028) valtion yleisen kyberturvallisuuden parantamiseksi. Sen keskeisenä tavoitteena on vahvistaa perustason tietoturvakäytäntöjä ja edistää siirtymistä Zero Trust- arkkitehtuuriin liittovaltion hallinnossa. Tavoitteena on hyödyntää pilvipohjaisen infrastruktuurin turvallisuusetuja ja samalla vähentää riskejä pitkällä aikavälillä. [19] Samankaltaisia määräyksiä on laadittu jo aikaisemminkin. Helmikuussa vuonna 2013 Yhdysvaltain presidentti Barack Obama antoi toimeenpanomääräyksen, joka keskittyi erityisesti valtion kriittisen infrastruktuurin kyberturvallisuuden parantamiseksi. Tämä toteutettiin siten, että eri toimijat jakavat valtion kanssa tietoa uusista kyberuhkista ja luovat yhdessä viitekehyksen kriittisen infrastruktuurin suojelemiseksi [20] [21].

3 Zero Trust -arkkitehtuurin erot perinteiseen tietoturvamalliin

Tässä luvussa keskitytään tunnistamaan keskeisimmät erot ZTA:n ja perinteisen tietoturvamallin välillä. Lisäksi molemmista malleista pyritään erottelemaan hyviä ja huonoja puolia sekä vertailemaan, kumpi ratkaisu on kokonaisvaltaisesti turvallisempi. Tutkielmassa käytetyssä aineistossa käsitellään laajasti eri teknologioita ja menetelmiä, joista ZTA ja perinteinen tietoturvamalli koostuvat. Taulukossa 3.1 on esiteltynä kaikkien valittujen tutkimuskysymysten kannalta keskeisiä lähteitä ja niitä käsitteleviä aiheita myös tulevia käsittelylukuja ajatellen.

Taulukko 3.1: Tutkielmassa käytetyt keskeisimmät aineistot, jotka käsittelevät valittujen tutkimuskysymysten aiheita.

	Zero Trust -arkkitehtuurin määritelmä	Perinteisen tietoturvamallin määritelmä	ZTA:n käyttöönotto	ZTA:n vaikutus etätyöskentelyssä
Q.Shen, Y. Shen, “Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach” (2024)		x		x
Y. Ren ym., “Zero Trust Networks: Evolution and Application from Concept to Practice” (2025)	x	x		
M. A. Azad ym., “Verify and trust: A multidimensional survey of zero-trust security in the age of IoT” (2024)	x	x		
C. Uwaoma, “The Challenges and Processes of Achieving Optimal Implementation of Zero Trust Architecture in Workplace” (2023)	x		x	x
I. Matiushin ja V. Korkhov, “Continuous Authentication Methods for Zero-Trust Cybersecurity Architecture” (2023)	x			
M. J. R. Cuyugan ja W. P. Rey, “Beyond the Firewall: Strategies in Securing Remote Work Environment” (2024)	x			x
N. F. Syed ym., “Zero Trust Architecture (ZTA): A Comprehensive Survey” (2022)	x	x	x	
P. Phiayura ja S. Teerakanok, “A Comprehensive Framework for Migrating to Zero Trust Architecture” (2023)			x	

3.1 Perinteinen tietoturva

Zero Trustin yksi keskeisin periaate on ”älä ikinä luota, varmista aina”. Tähän verrattuna perinteisen tietoturvamallin voitaisiin sanoa noudattavan periaatetta ”Varmista kerran, ylläpidä luottamus”. Perinteisestä tietoturvamallista käytetään myös nimikettä linnake ja vallihautamalli (Castle and moat), eli kaikki linnan ulkopuolella olevat ovat vihollisia ja sisäpuolella olevat ovat ystäviä. Käytännössä tämä tarkoittaa sitä, että käyttäjän päästyä verkon tai järjestelmän sisälle, tämän oletetaan automaattisesti olevan turvallinen ja valtuutettu käyttäjä. Tällainen malli perustuu vahvoihin verkon ja järjestelmän määritettyihin rajoihin, jotka ovat toteutettu käyttäen esimerkiksi perinteistä palomuuria.

Tällainen rajaturvallisuusmalli perustuu fyysisiin ja loogisiin rajoihin, kuten sisäisten ja ulkoisten verkkojen eristämiseen arkaluontoisten resurssien suojaamiseksi [9]. Rajaturvallisuusmalli käyttää suojaustoimenpiteinä palomuureja (Firewall), tunkeutumisen havaitsemisjärjestelmiä (Intrusion detection system), tietojen menetyksen estämistä (Data loss prevention) ja virtuaalisia yksityisverkkoja (Virtual private network, VPN) [12]. Tällä tavalla saadaan luotua verkkoympäristö, jonka rajat ovat selkeästi määritellyt ja turvatut eri menetelmillä ja teknologioilla.

3.1.1 Zero Trust -arkkitehtuurin ominaisuuksien arviointi

Zero Trust -arkkitehtuurissa käyttäjän tunnistaminen on keskeisessä roolissa turvallisen verkkoympäristön luomiseksi. Pelkän tunnistautumisen lisäksi mallissa oleellista on myös jatkuva oletus siitä, että järjestelmä on hyökkäyksen kohteena ja että mitkään käyttäjät tai laitteet eivät ole luotettuja riippumatta laitteesta, muodostetusta yhteydestä tai sijainnista. Luvussa kaksi lueteltiin Zero Trust -arkkitehtuurin keskeisiä teknologioita ja menetelmiä, jotka yhdessä luovat turvallisen ja modernin verkkoympäristön Zero Trust -periaatteita noudattaen. Näihin liittyy kuitenkin myös omia haasteita, joita on syytä tarkastella saadaksemme kokonaiskuvan siitä, mitä eroja näillä malleilla todellisuudessa on.

Zero Trust -arkkitehtuurille tyypillisessä menetelmässä SDP:ssä on järjestelmälle monia etuja, kuten valtuutus, todennus ja salaus. Eduista huolimatta SDP:llä on myös useita avoimia haasteita, kuten ongelmat ohjaimen haavoittuvuudessa ja lisääntyneessä viiveessä ohjaustasolla, joka tarjoaa todennuksen, pääsyn ja salauksen ominaisuuksia [14].

ZTA:ssa käytäntöjen hallinnassa käytetyt PE ja PA hallitsevat kaikkea liikennettä, mitä verkon välityksellä liikkuu. Tämä tarkoittaa sitä, että näitä osia järjestelmässä tulee päivittää ja tarkastaa säännöllisesti. Kaikki, joilla on pääsy muokkaamaan näiden osien käytäntöjä ja toimintaa voivat

suorittaa hyväksymättömiä muutoksia tai tehdä virheitä, jotka voivat haitata koko organisaation toimintaa. [7]

3.1.2 Perinteisen tietoturvan ominaisuuksien arviointi

Vaikka perinteisellä tietoturvamallilla on suhteellisen korkea turvallisuustaso kokonaisuudessaan, siihen liittyy ongelmia esimerkiksi ennalta tuntemattomien haavoittuvuuksien tunnistamisessa. Verkon käyttöoikeuskäytännöt perustuvat pitkälti vain tunnettuihin haavoittuvuuksiin ja uhkiin, jolloin uhkiin reagointi on hitaampaa ja se vaatii manuaalista työtä, joka edelleen lisää hallinnan vaikeutta ja tästä koituvia kustannuksia. [22] Zero Trust -arkkitehtuurissa samanlaista ongelmaa ei esiinny, sillä suojaus ei perustu tunnettuihin tai ei-tunnettuihin uhkiin, vaan kaikki yhteydet ja laitteet nähdään mahdollisena uhkana.

Riippuvuus kerroksellisesta internet arkkitehtuurista ja alueellisista jaoista johtaa sisäänrakennettujen turvatoimien puuttumiseen jokaisella tasolla, jolloin turvallisuus on pitkälti riippuvainen suunnittelijan tai käyttäjän omasta tietoisuudesta ja kyvyistä [9]. Rajaturvallisuusmallissa oletetaan, että pääsynvalvonta ja valtuutus tulisi tehdä käyttäjän sijainnin, laitteen tyypin ja laitteen auktorisoinnin mukaan. Kuitenkin IoT- ja pilvipohjaisissa verkoissa sekä verkoissa, joissa käytetään omia henkilökohtaisia laitteita (Bring your own device, BYOD) ei pääsyä verkkoon voida valtuuttaa pelkästään käyttäjän sijainnin perusteella [12].

3.2 Keskeisimmät erot

Zero Trust -arkkitehtuurin ja perinteisen tietoturvamallin toteutuksissa on huomattavia teknisiä ja periaatteellisia eroja. Aineistojen pohjalta voidaan todeta, että Zero Trust -arkkitehtuuri nähdään yleisesti parempana ja modernimpana tapana toteuttaa turvallinen verkkoympäristö. Nyt kun olemme perehtyneet perinteiseen tietoturvaan ja Zero Trust -arkitehtuuriin, voimme luetella niiden keskeisimmät eroavaisuudet ja pohtia niiden vaikutusta verkkoympäristön ja järjestelmän turvallisuuteen. Taulukossa 3.2 on esiteltynä eroja perinteisen tietoturvan ja Zero Trust -arkkitehtuurin välillä tiivistetyssä muodossa.

3.2.1 Luottamuksen sijainti

Perinteinen tietoturvamalli luo luottamuksen vyöhykkeen, jossa kerran sisälle päässyt käyttäjä oletetaan turvalliseksi. Tämä epäsuora luottamus on kuitenkin suuri heikkous, sillä määrätietoiset hyökkääjät voivat murtautua verkkoon käyttäen erilaisia keinoja, kuten tietojen kalastelua (phishing),

toimitusketjuhyökkäyksiä (supply chain attack) ja pahantahtoisen sisäpiiriläisen (malicious insider) hyväksikäyttöä [23].

Zero Trust -arkkitehtuurissa luottamus ei perustu verkon sijaintiin, vaan pääsy järjestelmän sisällä sen eri osiin määräytyy monien tekijöiden kuten käytäntöjen hallinnan, verkkoliikenteen seurannan ja jatkuvan autentikoinnin perusteella. Zero Trust -arkkitehtuurissa luottamus on siis vaikeammin ansaittu ja sitä täytyy ylläpitää jatkuvasti.

3.2.2 Käyttäjien ja laitteiden hallinta

Perinteisessä tietoturvamallissa käyttäjien ja laitteiden hallinta keskittyy pääasiassa verkon reuna-alueisiin. Kun käyttäjä tai laite on kerran todennettu ja päästetty järjestelmään sisään, tämän valtuutusta ei tarkasteta enää uudestaan. Myös perinteisen kertaluontoisen autentikoinnin on todettu olevan riskialtis tapa tunnistautumiselle. [8]

Zero Trust -arkkitehtuurissa käyttäjien ja laitteiden hallinta ja seuranta on jatkuvaa. Jokainen pyyntö arvioidaan erikseen ja pääsy myönnetään vain, jos kaikki määritellyt ehdot täyttyvät. Tämä pitää sisällään käyttäjän tunnistautumisen, laitteen tilan tarkastamisen, sijainnin huomioimisen ja käyttökontekstin arvioinnin [12]. Näin mahdollistetaan paljon tiukempi käyttäjien ja laitteiden seuranta, joka pienentää tietovuodon ja väärinkäytöksen riskiä. Lisäksi Zero Trust -arkkitehtuuri tukee nykyaikaista työympäristöä, jossa käyttäjät ja laitteet toimivat useista eri sijainneista ja verkkoyhteyksistä, mukaan lukien BYOD-työskentely ja pilvipalvelut.

3.2.3 Suojausstrategiat

Perinteisessä tietoturvamallissa merkittävä haavoittuvuus liittyy siihen, miten palomuuri toimii internetin ja sisäverkon rajalla. Ongelma ei ole itse palomuurissa, vaan siinä, että palomuurin läpäisseelle annetaan automaattisesti luottamus ja valtuutus. Kun hyökkääjä onnistuu murtautumaan palomuurin läpi, hän saa saman luottamustason kuin verkon muut käyttäjät ja pääsee samalla käsiksi sisäverkon suojattuihin resursseihin. Tällaista sisäistä uhkaa ei enää valvota erikseen toisin kuin Zero Trust -arkkitehtuurissa, jossa jokainen pääsy resursseihin edellyttää jatkuvaa todennusta ja valvontaa riippumatta käyttäjästä tai laitteesta.

3.2.4 Reagointikyky ja valvonta

Perinteinen tietoturvamalli perustuu suurelta osin ennalta asetettuihin suojausmekanismeihin ja sääntöihin, mikä voi johtaa hitaampaan reagointiin etenkin uudenlaisiin uhkiin. Reagointi perustuu usein jälkikäteen tehtyihin havaintoihin, kuten lokitietojen analysointiin tai itse järjestelmän käyttäjien ilmoituksiin epäilyttävästä toiminnasta.

Zero Trust -arkkitehtuurissa valvonta on jatkuvaa ja automaattista. Käyttäjien ja laitteiden toimintaa seurataan reaaliajassa ja poikkeavuuksiin pystytään reagoimaan välittömästi [12]. Esimerkiksi epätavalliset kirjautumiset tai poikkeuksellinen tiedonsiirto verkossa voidaan havaita nopeasti ja hyökkäykset voidaan estää ennen kuin vahinkoa on ehtinyt vielä tapahtua.

3.2.5 Skaalautuvuus ja nykyaikaisuus

Perinteinen tietoturvamalli ei ole suunniteltu nykyajan hajautettuja ja pilvipohjaisia järjestelmiä varten. Tämän sijasta se perustuu oletukseen siitä, että verkon sisällä olevat resurssit ja käyttäjät ovat kaikki luotettavia [9]. Tämä rajoittaa järjestelmän joustavuutta ja tekee sen skaalaamisesta haastavaa erityisesti etätyön ja uudenlaisten järjestelmien lisääntyessä. Lisäksi myös uusien teknologioiden, kuten IoT-laitteiden liittäminen turvallisesti voi osoittautua haastavaksi.

Zero Trust -arkkitehtuuri on suunniteltu skaalautumaan vaativiin ja monimuotoisiin nykyaikaisiin IT-ympäristöihin. Se mahdollistaa turvallisen pääsyn pilvipalveluihin, mobiililaitteisiin ja etätyöresursseihin riippumatta siitä, mistä käyttäjä luo yhteyden. [12] Järjestelmä voidaan laajentaa joustavasti uusille käyttäjille, sovelluksille ja laitteille, koska suojaus perustuu jatkuvaan arviointiin eikä pelkästään verkon sijaintiin.

Taulukko 3.2: Keskeisiä eroja Zero Trust -arkkitehtuurin ja perinteisen tietoturvamallin välillä.

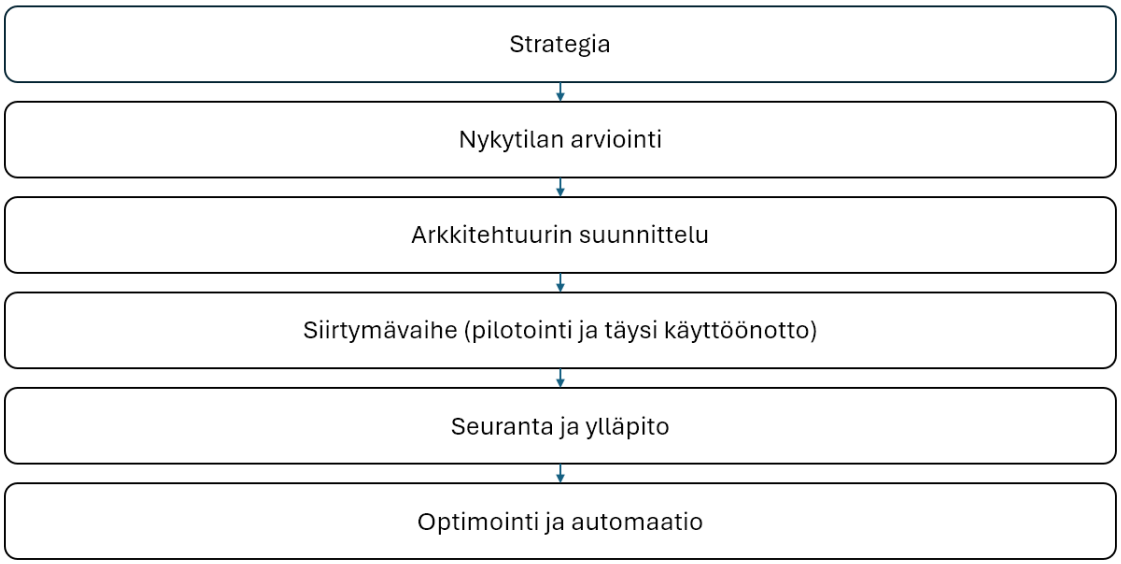
Ominaisuus/suojausmenetelmä	**Perinteinen tietoturvamalli**	**Zero trust -arkkitehtuuri**	**Lähteet**
Luottamuksen perusta	Perustuu verkon rajoihin: sisäverkko on luotettu	Luottamus ansaitaan, ei oleteta	[9], [12], [23]
Pääsynhallinta	Tapahtuu yleensä kertaluontoisesti	Jokainen pyyntö valtuutetaan erikseen	[12], [22]
Autentikointi	Käyttäjätunnus ja salasana riittävät	Monivaiheinen, jatkuva autentikointi	[12], [22]
Käyttöoikeudet	Roolipohjaisia, harvoin uudelleen tarkastetaan	Vähimpien oikeuksien periaate	[9], [12], [22]
Verkon suojaus	Palomuurit, VPN:t ja fyysiset rajat	Segemntointi, SDP ja käytäntöjen hallinta	[9], [22]
Laitteiden hallinta	Laitteen kuntoa tai luotettavuutta arvioidaan harvoin	Laite arvioidaan aina ennen pääsyä (tila, sijainti, sertifikaatit)	[9], [22]

Reagointi uhkiin	Usein manuaalista ja hidasta	Automaattinen ja reaaliaikainen uhkien seuranta	[12], [22]
Verkkoliikenteen seuranta	Rajallinen ja pistemäinen (palomuurit)	Jatkuva monitorointi ja käyttäytymisanalyysi	[9], [12]
Suojaus hajautetussa ympäristössä	Heikko BYOD- ja etätyöympäristöissä	Suunniteltu skaalautumaan pilveen, mobiilisovelluksiin ja etätyöhön	[9], [12]
Skaalautuvuus ja joustavuus	Rajallinen, vaikeuksia erityisesti IoT ja pilviympäristöissä	Hyvin skaalautuva ja suunniteltu nykyaikaisiin IT-ympäristöihin	[9], [12], [22]

4 Zero Trust -arkkitehtuurin käyttöönotto ja siihen liittyvät haasteet

ZTA:n käyttöönotto vaatii organisaatiolta monia muutoksia kuten organisaation resurssien tunnistamista, pääsynhallinnan uudelleenmäärittelyä sekä jatkuvaa arviointia ja valvontaa. Lisäksi onnistunut siirtymä edellyttää henkilöstön kouluttamista uusiin prosesseihin ja turvallisuuskäytäntöihin. ZTA:ssa oletuksena on, että verkon sisällä mikään ei ole automaattisesti luotettavaa, mikä tarkoittaa entistä yksityiskohtaisempaa tarkastelua niin käyttäjien kuin laitteidenkin osalta. Esineiden internetin (Internet of Things, IoT), reunalaskennan (Edge computing) ja muiden uusien teknologioiden käyttöönotto työpaikoilla on luonut uuden haasteen organisaatioissa turvallisen verkkoympäristön luomisessa käyttäen perinteistä tietoturvamallia [6]. Näissä ympäristöissä laitteet saattavat sijaita perinteisten verkon rajojen ulkopuolella tai siirtyä dynaamisesti eri sijaintien välillä, mikä tekee staattisista suojausmalleista riittämättömiä. On hyvä huomata, että hybridiympäristöjen yleistyminen johtaa suoraan siihen, että tietoturvakäytäntöjä ja toimintaperiaatteita tulee muuttaa Zero Trust -arkkitehtuurin periaatteiden mukaisesti organisaatioiden ylläpitääkseen vaadittavaa tietoturvan tasoa. Kriittisten resurssien tallentaminen hybridimuotoiseen pilvialustaan kasvattaa mahdollista hyökkäyspinta-alaa [24], jolloin siirtyminen Zero Trust -arkkitehtuuriin on yleisesti kannattavaa.

ZTA:n suunnittelu ja toteutus myös vaihtelevat organisaation tarpeiden, olemassa olevien teknologiatoteutuksien ja yleisen tietoturvan tason mukaan [6]. Kaikki yritykset eivät siis voi implementoida ZTA:ta osaksi yritystoimintaansa samalla tavalla, eikä mitään tiettyä oikeaa käyttöönoton mallia ole olemassa. Zero Trust -arkkitehtuuriin siirtyminen voikin olla kuormittavaa erityisesti pienille ja keskikokoisille organisaatioille [6]. Zero Trust -arkkitehtuurin käyttöönotto ei kuitenkaan edellytä kertaluontoista suurta järjestelmänmuutosta. Kerralla koko järjestelmän ja infrastruktuurin vaihtamisen sijaan ZTA voidaan vaiheittain osaksi perinteistä rajoihin perustuvaa tietoturvamallia [25]. On myös suositeltua valmistella pilotointiohjelma, jossa implementoinnin kriittisimmät kohteet huomioidaan ensin ja vasta sitten laajennetaan osaksi koko järjestelmää [26]. Vaiheittainen käyttöönotto mahdollistaa paremmin riskien hallinnan ja resurssien tehokkaan kohdentamisen. Kuvassa 4.1 on esitettynä yksinkertaistettu prosessikaavio ZTA:n käyttöönotosta. Kuva pohjautuu Phiayuran ja Teerakanokin [26] käyttöönoton malliin, joka on suunniteltu tukemaan onnistunutta ZTA:han siirtymistä kuudessa eri vaiheessa.



Kuva 4.1: Yksinkertaistettu kuvaus Zero Trust -arkkitehtuuriin siirtymisen vaiheista. [26]

Alun perin ZTA on tarkoitettu sellaisille organisaatioille, jotka ovat laajalti hajautettuja tai joilla on etäpainottunut ja liikkuva henkilöstö ja työvoima [6]. Pilvipalveluiden, mobiililaitteiden ja BYOD-käytäntöjen lisääntyminen on johtanut siihen, että yhä useammat yritykset täyttävät nämä vaatimukset ja tarvitsevat uudenlaisia ratkaisuja osaksi IT-infrastruktuuriaan juuri hyökkäyspinta-alan kasvun takia. ZTA:han siirtyvät organisaatiot aloittavat ensin perusteellisen inventaarion luomisella ja resurssien arvioimisella. Tärkeää on tunnistaa merkityksellisimmät turvatoimenpiteet ja keskittyä niihin. [6] Olemassa olevien resurssien tarkka kartoitus mahdollistaa sen, että mikään osa järjestelmästä ei jää uuden toimintamallin ulkopuolelle. Organisaation siirtyminen ZTA:han vaatii erityisen tarkkaa huomiota ZTA:n teknologioiden ja menetelmien määrittelyyn.

Ennen käyttöoikeuskäytäntöjen määrittelyä on tunnistettava verkon toiminnan sekä käyttäjien ja järjestelmien odotettujen tietovirtojen perustaso [15]. Tämä tarkoittaa sitä, että uuden järjestelmän käyttöoikeudet tulee toteuttaa noudattaen ZTA:lle tyypillistä vähimpien oikeuksien periaatetta. Tässä vaiheessa on myös oleellista rajata käyttöoikeudet riittävän tarkasti, että vältytään myöhemmin liian laajojen käyttöoikeuksien takia. Ongelmia voi ilmetä myös itse toteutusvaiheessa, kun määritetään käyttöoikeuksia ja asetetaan tietoturvavasteita. Virheellinen tai väärin toteutettu määrittely voi johtaa siihen, että verkon osia jää suojauksen ulkopuolelle. [24] Käyttöönotossa tulee myös kiinnittää huomiota muiden ZTA:n teknologioiden konfiguroinnissa. Esimerkiksi ZTA:ssa käytettävät PE ja PA ovat keskeisessä roolissa arkkitehtuuria ja näiden virheellinen konfigurointi ja valvonta voi aiheuttaa riskin hyökkäyksille [6].

Forresterin vuonna 2018 tehdyssä tutkimuksessa [18] on myös huomattu erityisesti verkon segmentoinnin tuottavan suuria haasteita. Tutkimuksen mukaan verkon mikrosegmenttien luominen ja ylläpito on haastavaa, kun halutaan varmistaa vain valtuutettujen laitteiden ja käyttäjien pääsy verkon eri osiin. Samalla huolenaiheeksi on myös nostettu jatkuvan autentikoinnin tuomat haasteet ympäristössä, jossa käyttäjiä ja laitteita on valtavia määriä.

Tämä osoittaa sen, että huomiota tulee kiinnittää monenlaisiin seikkoihin koko käyttöönottoprosessin aikana, että lopputuloksena saadaan onnistuneesti implementoitu Zero Trust -arkkitehtuuri. On myös todettu, että siirtymäprosessissa voi ilmetä monia organisaation kulttuurillisia haasteita, kuten tuen tai kiinnostuksen puute eri tason henkilöstöltä [24].

Vanha järjestelmä (Legacy system) on sellainen järjestelmä, jonka toiminta perustuu vanhoihin teknologioihin, standardeihin ja ohjelmointikieliin aikaisemmilta sukupolvilta. Vanhat järjestelmät eivät myöskään täysin kykene päivittymään uusimpiin teknologioihin, mutta suorittavat vielä sille määritellyt tehtävät. [27] Vanhat järjestelmät eivät kuitenkaan kykene suojaamaan verkkoympäristöä pitkään uusien kyberuhkien kehittyessä. Näiden järjestelmien yleisiä haavoittuvuuksia ovat vanhentuneet salausprotokollat, päivittämättömät ohjelmistot ja luontaisten turvaominaisuuksien puute. Nämä ovat haavoittuvuuksia, joita kyberrikolliset hyödyntävät käyttämällä esimerkiksi helposti ennustettavia toimintamalleja läpäisemään suojaus. [28] Lisäksi vanhoilla järjestelmillä ei usein ole tarpeeksi laskentatehoa ja muistia edistyneiden turvatoimenpiteiden tukemiseksi [29].

Siirtyminen Zero Trust -arkkitehtuuriin voi aiheuttaa ongelmia vanhoissa järjestelmissä, sovelluksissa ja muissa IT-infrastruktuureissa. Tämä seurauksena voidaan päätyä tilanteeseen, jossa alkuperäisten hallinnoitujen resurssien määrä kasvaa odotettua suuremmaksi. Lisäksi vanhojen järjestelmien uudelleensuunnittelu ja muokkaaminen ZTA:n tukemiseksi voi aiheuttaa suurempia kuluja ja vaatia enemmän aikaa [26].

5 Vaikutus etätyöskentelyyn

ZTA:n keskeiset teknologiat ja menetelmät tukevat turvallisen verkkorakenteen ylläpitämistä ja ottavat huomioon paikkatieteelliset ja laitekohtaiset haasteet. Samalla ne mahdollistavat organisaatioiden IT-infrastruktuurien kasvun ja kehityksen. Zero Trust -arkkitehtuurissa jokainen yhteyspyyntö validoidaan riippumatta siitä, tuleeko se sisä- vai ulkoverkosta. Tämä on erityisen tärkeää, kun käyttäjät toimivat erilaisissa verkoissa ja eri sijainneista. Etätyöskentelyn laajamittainen yleistyminen on johtanut siihen, että perinteinen rajaturvallisuuteen perustuva tietoturvamalli ei välttämättä ole enää riittävän turvallinen suojaamaan kaikkia organisaation kriittisiä resursseja.

Statistan mukaan sellaisten työntekijöiden määrä on noussut huomattavasti, jotka työskentelevät etänä joko täyspäiväisesti tai suurimman osan ajasta. Vuonna 2015 tällaisten työntekijöiden määrä maailmanlaajuisesti on ollut 7 %. Vuonna 2019 arvo on ollut 10 %, jonka jälkeen etätyöntekijöiden määrä on noussut voimakkaasti aina 28 %:iin asti vuoteen 2023 mennessä. [30] Tämän muutoksen selittää vuonna 2020 alkanut maailmanlaajuinen pandemia.

Laajamittainen siirtyminen etätyöskentelyyn pitkälti COVID-19-pandemian vaikutuksesta on muuttanut monien järjestelmien fyysistä rakennetta, eivätkä järjestelmien osat ole enää välttämättä keskittyneet yhteen tiettyyn paikkaan, rakennukseen, kaupunkiin tai edes valtioon. Tämän seurauksena on tarpeellista löytää kyberturvallisuuden parantamiseksi uusia ratkaisuja, jotka kykenevät suojaamaan järjestelmiä uhkilta ottaen huomioon jatkuvasti muuttuvan verkkoympäristön. [10] ZTA-ratkaisujen implementoinnilla organisaatiossa voidaan vastata juuri tähän tarpeeseen ja mahdollistaa turvallinen etätyöskentely-ympäristö.

Käyttäjien omien laitteiden turvaaminen on usein haastavaa, koska ne voivat altistua erilaisille kyberuhkille pienestäkin tahattomasta virheestä tai huolimattomuudesta [31]. On siis organisaation kannalta tärkeää pitää huoli siitä, että työntekijät noudattavat sovittuja tietoturvakäytänteitä ja pitävät työssä käytettävät laitteet ajan tasalla esimerkiksi päivitysten osalta. Organisaatiot myös panostavat koulutuksiin ja ohjelmiin, joissa painotetaan ihmisen roolin tärkeyttä kyberuhkien kannalta. Näiden koulutusten tarkoituksena on opettaa työntekijöitä mahdollisista uhkista ja samalla muokata koko työskentelykulttuuria turvallisemmaksi [32]. Etätyöskentelyssä tietoturvan taso saattaa olla alhaisempi kuin toimistolta käsin työskennellessä, jolloin työntekijän henkilökohtainen vastuu myös kasvaa uhkien välttämisessä. Ihmisen rooli on keskeinen osa etätyöympäristöjen turvallisuutta ja uusien turvallisuuskäytäntöjen noudattaminen etätyöskentelijöiden keskuudessa vaihtelee huomattavasti [32]. Esimerkiksi toimistolla työskennellessä käytetään usein organisaation omaa ja turvattua verkkoyhteyttä, kun taas etätyötä tehdessä samaa mahdollisuutta ei suoraan ole. Monissa

organisaatioissa etätyöskentelyssä hyödynnetään VPN-yhteyttä [33], jonka avulla pystytään luomaan verkkoyhteys etänä käyttämällä organisaation omaa verkkoa. Etänä työskennellessä on mahdollista, että työntekijä unohtaa hyödyntää VPN-yhteyttä, joka altistaa työntekijän ja laitteen erilaisille uhkille verkossa. Tämä oli vain yksi esimerkki siitä, kuinka työntekijä pystyy omilla teoillaan vaikuttamaan yleiseen kyberturvallisuuden tasoon.

On kuitenkin hyvä huomata, että digitaalinen transformaatio ja uudet käytännöt etätyöskentelyssä ovat mahdollistaneet uuden työympäristön syntymisen, jossa yhteistyökumppanit ja työntekijät pystyvät hyödyntämään ja käsittelemään organisaation resursseja tehokkaammin kuin aikaisemmin [6]. Kuten olemme aikaisemmin todenneet, Zero Trust -arkkitehtuuri ja sen teknologiat tukevat erityisesti etätyöskentely-ympäristöjä turvaten yhteydet ja käyttäjät.

Jatkuvasta autentikoinnista on tuotu esille näkökulma siitä, aiheuttaako ZTA mahdollisesti tarpeettomia tarkastuksia järjestelmää käyttäessä. Fernandez ja Brazhuk [11] ehdottavat, että kaikkien järjestelmän osien tasavertainen hallinnointi voi osoittautua turhaksi aiheuttaen tarpeettomia tarkastuksia. He myös painottavat sitä, että kyse ei ole riittävän tietoturvan tasosta vaan nimenomaan käyttäjäkokemuksessa. ZTA:ssa kuitenkin otetaan huomioon tarkastuksien tarpeellisuus määrittämällä resurssit ja järjestelmän osat niiden tärkeyden mukaan. Yleisiin ja ei-kriittisiin tietoihin pääsy ei ole yhtä rajattua kuin pääsy kriittisiin resursseihin. ZTA:ssa tämä toteutetaan esimerkiksi noudattamalla vähimpien oikeuksien periaatetta [11]. ZTA:n käyttöönotossa ja teknologioiden määrityksessä on siis hyvä ottaa huomioon etenkin se, kuinka määritellyt käyttöoikeudet ja roolit tulevat vaikuttamaan järjestelmän käyttäjien työskentelyyn.

6 Yhteenveto ja johtopäätökset

Tässä tutkielmassa tarkasteltiin Zero Trust -arkkitehtuuria nykyaikaisen kyberturvallisuuden ratkaisuna. Tutkimuksen päätavoitteena oli vertailla ZTA:ta perinteiseen tietoturvamalliin, selvittää sen käyttöönottoon liittyviä haasteita ja arvioida sen vaikutusta etätyöskentelyssä. Näihin kysymyksiin pyrittiin vastaamaan kirjallisuuskatsauksena käyttäen apuna kolmea tutkimuskysymystä ja hyödyntäen ajankohtaisia tutkimuksia ja vertaisarvioituja lähteitä.

Ensimmäinen tutkimuskysymys käsitteli Zero Trust -arkkitehtuurin ja perinteisen tietoturvamallin välisiä eroja. Tutkielman perusteella voidaan todeta, että keskeisimmät erot näiden välillä liittyvät luottamuksen hallintaan, pääsynvalvontaan ja valvonnan jatkuvuuteen. Perinteinen tietoturvamalli perustuu verkon reuna-alueiden suojaamiseen ja kertaluontoiseen autentikointiin, kun taas ZTA:ssa hyödynnetään jatkuvaa tarkastelua, verkon segmentointia ja käyttäjien sekä laitteiden jatkuvaan arviointiin. Tämä tekee ZTA:sta paremman ratkaisun vastaamaan nykyaikaisiin ja kehittyviin uhkiin, erityisesti hajautetuissa hybridiympäristöissä.

Toinen tutkimuskysymys keskittyi ZTA:n käyttöönoton haasteisiin. Tutkimuksessa havaittiin, että suurimmat haasteet liittyvät teknologiseen infrastruktuuriin, vanhojen järjestelmien yhteensopivuuteen, käyttöönoton vaiheistukseen ja organisaation sisäiseen muutosjohtamiseen. ZTA:n käyttöönotto edellyttää tarkkaa resurssien kartoittamista, käyttöoikeuksien uudelleenmäärittelyä sekä henkilöstön kouluttamista. ZTA:n käyttöönotto ei siis ole pelkästään tekninen projekti, vaan myös koko organisaation kulttuuria muuttava prosessi.

Kolmannessa tutkimuskysymyksessä tarkasteltiin ZTA:n vaikutusta etätyöskentelyyn. Löydösten perusteella voidaan todeta, että ZTA soveltuu erityisen hyvin tukemaan turvallista etätyötä. ZTA:n eri teknologiat ja menetelmät kuten laitteisto- ja sijaintiriippumattomuus, jatkuva autentikointi ja resurssikohtainen pääsynvalvonta mahdollistavat järjestelmän käyttäjien turvallisen työskentelyn. Samalla työntekijän oma rooli osana turvallista työskentely-ympäristöä korostuu, minkä vuoksi myös organisaation kulttuuri ja työntekijöiden koulutus nousevat keskeisiksi aiheiksi.

Zero Trust -arkkitehtuuri tarjoaa tehokkaan, turvallisen ja tulevaisuuteen suuntaavan lähestymistavan kyberturvallisuuden ratkaisuna. Sen käyttöönotto organisaatiossa edellyttää kuitenkin huolellista suunnittelua ja resurssien tunnistamista. Jatkotutkimuksissa voitaisiin tarkastella vielä tarkemmin organisaatiokohtaisia ZTA-toteutuksia ja vertailla eri implementointistrategioiden tehokkuutta ja kannattavuutta käytännön tasolla.

Lähteet

[1] A. Darshane, “Advanced network security concepts: network segmentation and zero trust architecture," *International Journal of Engineering and Technology Research (IJETR)*, vol. 9, no. 2, pp. 379–386, Sep. 2024, doi: 10.5281/zenodo.13851178.

[2] J. Heino, C. Jalio, A. Hakkala, and S. Virtanen, “JAPPI: An unsupervised endpoint application identification methodology for improved Zero Trust models, risk score calculations and threat detection,” *Computer Networks*, vol. 250, p. 110606, Aug. 2024, doi: 10.1016/j.comnet.2024.110606.

[3] W. Yeoh, M. Liu, M. Shore, and F. Jiang, “Zero trust cybersecurity: Critical success factors and A maturity assessment framework,” *Computers & Security*, vol. 133, p. 103412, Oct. 2023, doi: 10.1016/j.cose.2023.103412.

[4] M. Shore, S. Zeadally, and A. Keshariya, “Zero Trust: The What, How, Why, and When,” *Computer*, vol. 54, no. 11, pp. 26–35, Nov. 2021, doi: 10.1109/MC.2021.3090018.

[5] “Global causes of sensitive information loss 2023,” Statista. Accessed: May 19, 2025. [Online]. Available: https://www.statista.com/statistics/1387393/loss-sensitive-information-organizations-cause-worldwide/

[6] C. Uwaoma, “The Challenges and Processes of Achieving Optimal Implementation of Zero Trust Architecture in Workplace,” in *Proceedings of the 2023 Computers and People Research Conference*, in SIGMIS-CPR ’23. New York, NY, USA: Association for Computing Machinery, Aug. 2024, pp. 1–9. doi: 10.1145/3579168.3632735.

[7] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[8] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, “Zero Trust Architecture (ZTA): A Comprehensive Survey,” *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.

[9] Y. Ren, Z. Wang, P. K. Sharma, F. Alqahtani, A. Tolba, and J. Wang, “Zero Trust Networks: Evolution and Application from Concept to Practice,” *CMC*, vol. 82, no. 2, pp. 1593–1613, 2025, doi: 10.32604/cmc.2025.059170.

[10] I. Matiushin and V. Korkhov, “Continuous Authentication Methods for Zero-Trust Cybersecurity Architecture,” in *Computational Science and Its Applications – ICCSA 2023 Workshops*, O. Gervasi, B. Murgante, A. M. A. C. Rocha, C. Garau, F. Scorza, Y. Karaca, and C. M. Torre, Eds., Cham: Springer Nature Switzerland, 2023, pp. 334–351. doi: 10.1007/978-3-031-37120-2_22.

[11] E. B. Fernandez and A. Brazhuk, “A critical analysis of Zero Trust Architecture (ZTA),” *Computer Standards & Interfaces*, vol. 89, p. 103832, Apr. 2024, doi: 10.1016/j.csi.2024.103832.

[12] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, “Verify and trust: A multidimensional survey of zero-trust security in the age of IoT,” *Internet of Things*, vol. 27, p. 101227, Oct. 2024, doi: 10.1016/j.iot.2024.101227.

[13] J. Rana, P. K. Meher, and R. Priyadarshini, “Detection of Malicious and Abnormal Users for Policy Enforcement in a Zero Trust Network,” in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, Feb. 2025, pp. 179–184. doi: 10.1109/ESIC64052.2025.10962588.

[14] S. Rodigari, D. O’Shea, P. McCarthy, M. McCarry, and S. McSweeney, “Performance Analysis of Zero-Trust multi-cloud,” in *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, Sep. 2021, pp. 730–732. doi: 10.1109/CLOUD53861.2021.00097.

[15] A. Kerman, O. Borchert, S. Rose, E. Division, and A. Tan, “Implementing a Zero Trust Architecture,” Oct. 2020, doi: 10/21/implementing-a-zero-trust-architecture/final.

[16] “Global Zero Trust security market value 2032,” Statista. Accessed: May 20, 2025. [Online]. Available: https://www.statista.com/statistics/1299061/global-zero-trust-security-market-value/

[17] “Global cybercrime estimated cost 2029,” Statista. Accessed: May 21, 2025. [Online]. Available: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

[18] P. Mutabazi, E. Ndashimye, and J. D. Ndibwile, “Investigating the Challenges Companies in Rwanda Face when Implementing Zero-Trust Network,” in *2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2023, pp. 382–392. doi: 10.1109/FiCloud58648.2023.00062.

[19] S. Knittl, “Zero Trust: Die letzte Bastion für die IT-Sicherheit deutscher Behörden,” *Datenschutz Datensich*, vol. 47, no. 10, pp. 617–622, Oct. 2023, doi: 10.1007/s11623-023-1831-8.

[20] N. Kshetri, “Recent US Cybersecurity Policy Initiatives: Challenges and Implications,” *Computer*, vol. 48, no. 7, pp. 64–69, Jul. 2015, doi: 10.1109/MC.2015.188.

[21] R. L. Trope and S. J. Humes, “By Executive Order: Delivery of Cyber Intelligence Imparts Cyber Responsibilities,” *IEEE Security & Privacy*, vol. 11, no. 2, pp. 63–67, Mar. 2013, doi: 10.1109/MSP.2013.29.

[22] Q. Shen and Y. Shen, “Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach,” *Computers & Security*, vol. 136, p. 103537, Jan. 2024, doi: 10.1016/j.cose.2023.103537.

[23] “The Evolution of Zero Trust Architecture (ZTA) from Concept to Implementation | IEEE Conference Publication | IEEE Xplore.” Accessed: May 20, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10930254

[24] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, “Security of Zero Trust Networks in Cloud Computing: A Comparative Review,” *Sustainability*, vol. 14, no. 18, Art. no. 18, Jan. 2022, doi: 10.3390/su141811213.

[25] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, “A Survey on Zero Trust Architecture: Challenges and Future Trends,” *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 6476274, 2022, doi: 10.1155/2022/6476274.

[26] P. Phiayura and S. Teerakanok, “A Comprehensive Framework for Migrating to Zero Trust Architecture,” *IEEE Access*, vol. 11, pp. 19487–19511, 2023, doi: 10.1109/ACCESS.2023.3248622.

[27] H. K. A. Bakar, R. Razali, and D. I. Jambari, “Implementation Phases in Modernisation of Legacy Systems,” in *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*, Dec. 2019, pp. 1–6. doi: 10.1109/ICRIIS48246.2019.9073628.

[28] A. J. Bello, M. Diyan, and I. Asghar, “Zero Trust Implementation for Legacy Systems using Dynamic Microsegmentation, Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC),” in *2025 4th International Conference on Computing and Information Technology (ICCIT)*, Apr. 2025, pp. 181–189. doi: 10.1109/ICCIT63348.2025.10989392.

[29] A. Alshehri, B. Tufekci, and C. Tunc, “Identification Management for Zero Trust Through Network Analysis,” in *2024 IEEE/ACS 21st International Conference on Computer Systems and Applications (AICCSA)*, Oct. 2024, pp. 1–6. doi: 10.1109/AICCSA63423.2024.10912537.

[30] “Employees working primarily remotely worldwide 2015-2023,” Statista. Accessed: Apr. 14, 2025. [Online]. Available: https://www.statista.com/statistics/1450450/employees-remote-work-share/

[31] M. Tsai, S. Lee, and S. W. Shieh, “Strategy for Implementing of Zero Trust Architecture,” *IEEE Transactions on Reliability*, vol. 73, no. 1, pp. 93–100, Mar. 2024, doi: 10.1109/TR.2023.3345665.

[32] M. J. R. Cuyugan and W. P. Rey, “Beyond the Firewall: Strategies in Securing Remote Work Environment,” in *2024 14th International Conference on Software Technology and Engineering (ICSTE)*, Aug. 2024, pp. 94–101. doi: 10.1109/ICSTE63875.2024.00024.

[33] K. Ishide, S. Okada, M. Fujimoto, and T. Mitsunaga, “ML Detection Method for Malicious Operation in Hybrid Zero Trust Architecture,” in *2022 IEEE International Conference on Computing (ICOCO)*, Nov. 2022, pp. 264–269. doi: 10.1109/ICOCO56118.2022.10031702.