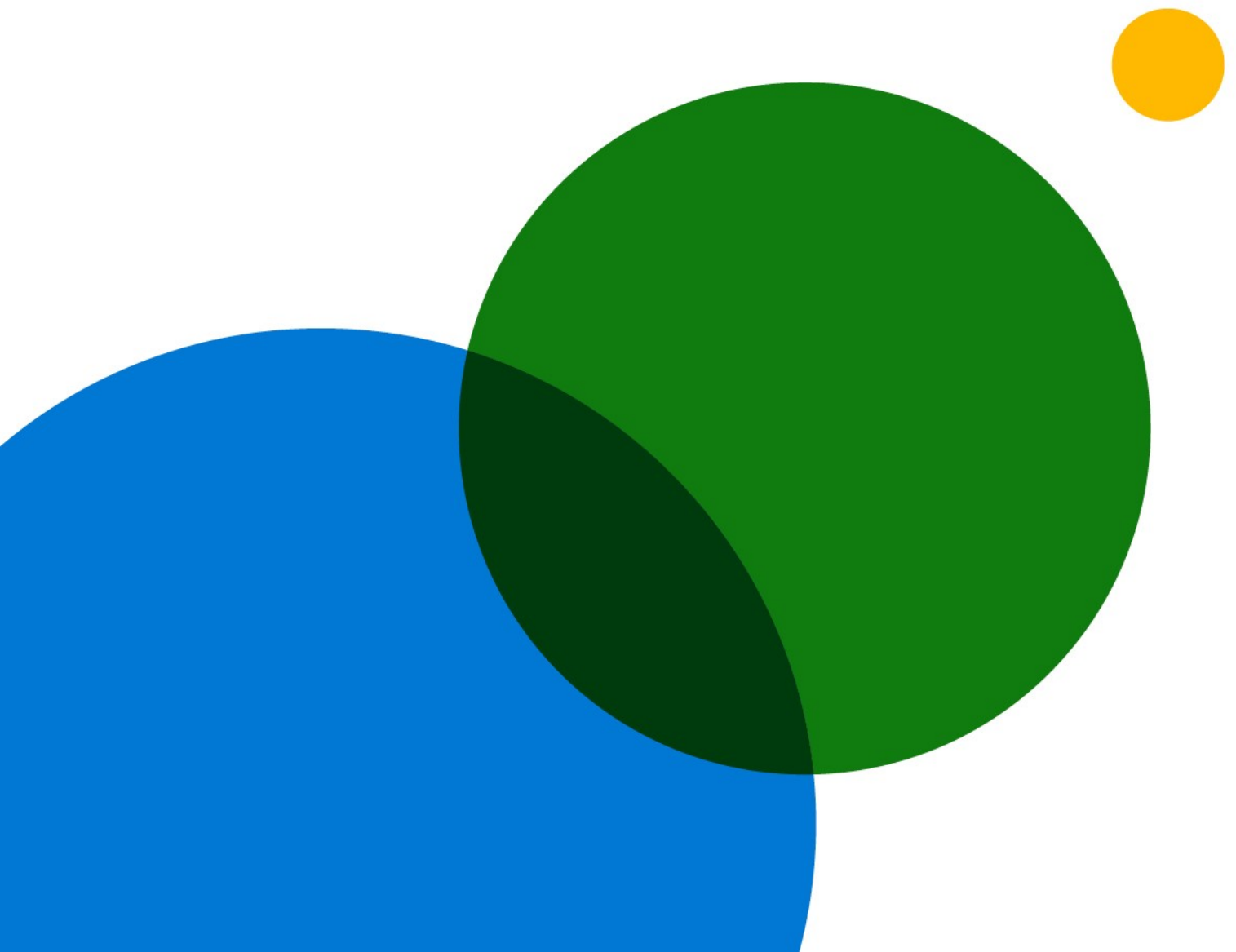


Zero Trust -strategian käyttöönottoraportti



Sisällysluettelo

03

Johdanto

06

Tutkimukseen osallistuneet

04

Menetelmät

07

Tutkimuksen yleiset opetukset

05

Tärkeitä faktoja Zero Trust
-strategian käyttöönotosta

24

Yksityiskohtaiset tutkimustavoitteet
ja kohderyhmän rekrytointi

Johdanto

Vasu Jakkal / varatoimitusjohtaja, Tietoturva, vaatimustenmukaisuus ja käyttäjätiedot

Kuluneena vuonna kyberturvallisuus on kehittynyt merkittävästi ja Zero Trust -strategiasta on tullut toimialamme ja ympäri maailmaa olevien organisaatioiden toimintaa ohjaava strategia.

Pandemian alkaessa organisaatioissa siirryttiin lähes kokonaan etätööhön yhdessä yössä. Tämä muutos pakotti organisaatiot mukautumaan nopeasti, jotta ne pystyivät tukemaan hankalassa tilanteessa olevia työntekijöitä, jotka käyttivät henkilökohtaisia laitteita, tekivät yhteistyötä pilvipalveluiden kautta ja jakoivat tietoja yritysverkon ulkopuolelle saadakseen töitä tehtyä. Organisaatioiden mukautuessa tähän muutokseen ne kohtasivat myös entistä taitavampia kyberrikollisia, joiden kohdentaminen, taktiikat ja resurssit kehittyvät jatkuvasti.

Hybridityöstä on tullut todellisuutta. Tässä nopeasti muuttuvassa tilanteessa kyselyymme osallistuneet kertoivat tukeutuvansa Zero Trust -strategiaan pystyäkseen parantamaan tietoturvaa ja vaatimustenmukaisuutta, havaitsemaan ja korjaamaan uhkia nopeammin sekä yksinkertaistamaan tietoturva-analytiikkaa ja parantamaan sen saatavuutta.

Kattava Zero Trust -arkkitehtuurin periaatteet ovat nimenomainen todennus, vähäisimpien käyttöoikeuksien antaminen ja ajattelutapa, jossa oletuksena on tietomurto. Näin pystytään turvaamaan käyttäjätiedot, päätepiisteet, sovellukset, infrastruktuurin, verkoston ja tiedot sekä parantamaan näkyvyyttä, automaatiota ja orkestrointia. Sen lisäksi, että suosittelemme tätä lähestymistapaa asiakkaillemme ja kumppaneillemme, olemme omaksuneet sen myös Microsoftin omaan globaalin tietoturvaan ja ohjelmistokehitykseen.

Tässä raportissa kerrotaan Zero Trust -strategian käyttöönotosta eri markkina-alueilla ja toimialoilla. Toivomme, että tässä tutkimuksessa tehdyt havainnot ja päätelmät nopeuttavat Zero Trust -strategian käyttöönottoa, antavat tietoa alan toimijoiden kollektiivisesta etenemisestä sekä auttavat ennakoimaan nopeasti kehittyvää tilannetta.

Menetelmät

Microsoft tilasi analytiikkaan, suunnitteluun ja strategiaan erikoistuneelta Hypothesis Groupilta Zero Trust -strategian käyttöönottoa käsittelevän raportin ja tutkimuksen. Tutkimus koostui Yhdysvalloissa kahdesta vaiheesta, joissa pyrittiin esittelemään Zero Trust -strategian käyttöönoton trendejä ja tehokkuutta. Toiseen vaiheeseen sisällytettiin myös muita markkina-alueita, joiden avulla pystyttiin selvittämään maailmanlaajuisia trendejä.

Tutkimus aloitettiin elokuussa 2020, kun Yhdysvalloissa toteutettiin 15 minuutin verkkokysely. Siihen osallistui 300 tietoturvan päätöksentekijää, jotka olivat osallistuneet Zero Trust -strategiaa koskeviin päätöksiin eri alojen yrityksissä. Verkkokyselyn lisäksi syyskuussa 2020 järjestettiin viisi syvähaastattelua, joihin osallistui yhdysvaltalaisia tietoturvan päätöksentekijöitä eri toimialoilta.

Huhtikuussa 2021 Yhdysvalloissa, Saksassa, Japanissa ja Australiassa/Uudessa-Seelannissa toteutettiin globaali tutkimus, johon osallistui vastaava joukko tietoturvan päätöksentekijöitä. Yli 900 osallistujaa vastasi 15 minuutin verkkokyselyyn, jossa oli kysymyksiä Zero Trust -strategian käyttöönotosta, parhaista käytännöistä, hyödyistä, haasteista ja tulevista investointisuunnitelmista.



Tärkeitä faktoja Zero Trust -strategian käyttöönotosta

Heinäkuu
2021

Zero Trust -strategian
käyttöönottoraportti

5

01 / Organisaatiot ovat valmiita hyödyntämään Zero Trust -strategiaansa, ja koronaviruspandemia ja siirtyminen hybridityöhön on vain vauhdittanut prosessia

Tietoturvan päätöksentekijät kertovat, että Zero Trust -strategian kehittäminen on heidän tärkein tietoturvaprioriteettinsa, ja 96 % kertoo sen olevan kriittistä organisaation menestyksen kannalta. Ensisijaiset motivaattorit Zero Trust -strategian käyttöönotolle ovat yleisen tietoturva-aseman ja loppukäyttäjän kokemuksen parantaminen. Koronaviruspandemian vauhdittama siirtyminen hybridityöskentelyyn edistää myös Zero Trust -strategian laajempaa käyttöönottoa: 81 % yrityksistä ovat aloittaneet siirtymän kohti hybridityöskentelyä, ja 31 % niistä on jo saanut prosessin valmiiksi. 94 % ovat kuitenkin huolissaan siirtymisestä, lähinnä työntekijöiden väärinkäytön, IT-osaston kasvavan työmäärän ja kyberhyökkäysten vuoksi. Tämän vuoksi strategian kannalta keskeisiä tekijöitä ovat lisäkoulutuksen tarjoaminen työntekijöille sekä monimenetelmäisen todennuksen käyttöönotto sujuvan käyttäjäkokemuksen ja siirtymän varmistamiseksi.

02 / Zero Trust -strategia tarjoaa organisaatioille joustavuutta, sillä aloittaessaan käyttöönoton ne pystyvät mukauttamaan lähestymistavan tarpeidensa mukaan

Alle 15 % organisaatioista aloitti Zero Trust -strategian käyttöönoton samalla tietoturvan riskialueella. Tämä johtuu suurelta osin siitä, että käyttöönottoon suhtaudutaan prosessina, joka kattaa kaikki tietoturva-arkkitehtuurin pilarit ja ominaisuudet, ei niinkään erillisten yksittäisten teknologioiden sarjana. Samaan tapaan Zero Trust -strategian yksittäisten komponenttien käyttöönottojärjestys tietoturvan riskialueella vaihtelee suuresti, ja tietoturva-ammattilaisten välillä on suuria eroja siinä, minkä komponenttien käyttöönotosta he aloittavat.

03 / Vaikka Zero Trust -strategia on laajalti hyväksytty ja parantaa organisaatioiden kykyä hallita uhkia, vielä on paljon työtä jäljellä

76 % organisaatioista on ainakin aloittanut Zero Trust -strategian käyttöönoton, ja 35 % niistä väittää käyttöönoton olevan täysin valmis. Ne organisaatiot, jotka väittävät käyttöönoton olevan täysin valmis, myöntävät kuitenkin, etteivät ne ole vielä ottaneet Zero Trust -strategiaa käyttöön kaikilla tietoturvan riskialueilla ja komponenteissa. Zero Trust -strategia on vakuuttava, koska se parantaa ketteryttä, nopeuttaa uhkien havaitsemista ja parantaa kykyä hallita esineiden internetin (IoT) ja operationaalisen teknologian (OT) tietoturvaa. Käyttöönotto on lisääntynyt Yhdysvalloissa (70 % elokuussa 2020, 79 % huhtikuussa 2021); Yhdysvallat on myös muita, myöhemmin aloittaneita maita edellä Zero Trust -strategian käyttöönotossa, ja yhdysvaltalaiset organisaatiot väittävät, että niillä on vähemmän budjetista johtuvia rajoitteita. Vaikka 57 % organisaatioista väittää olevansa muita edellä, noin puolet näistä on sellaisia, joilla on vielä työtä jäljellä, sillä ne eivät ole täysin ottaneet Zero Trust -strategiaa käyttöön kaikilla tietoturvan riskialueilla ja komponenteissa.

04 / Tulevaisuudessakin Zero Trust -strategia tulee olemaan ensisijainen prioriteetti ja edellyttää huolellista työntekijöihin ja toimittajiin liittyvää päätöksentekoa

Zero Trust -strategian odotetaan olevan tärkein tietoturvaprioriteetti seuraavien kahden vuoden ajan ja organisaatiot ennakoivat suurempia investointeja. Kun yritykset panostavat Zero Trust -investointeihin, avainasemassa on haasteiden ylittäminen työntekijöiden avulla (mukaan lukien tietoturvatimien kehittäminen ja johdon hyväksyntä). Mitä tulee toimittajastrategiaan, tietoturvan päätöksentekijät työskentelevät hieman mieluummin kokonaisvaltaisten tai konsolidoitujen toimittajien kanssa, sillä toimittajan valinta riippuu usein sisäisen asiantuntemuksen saatavuudesta. Valmiin palvelupaketin etuja ovat muun muassa lisääntynyt asiantuntemus, resurssit ja yksinkertaisuus, mutta sen käyttöönotto voi kestää kauemmin, sen integrointi nykyiseen tietoturva-arkkitehtuuriin voi olla vaikeampaa ja se voi lisätä potentiaalisia haavoittuvuuksia.

Tutkimukseen osallistuneet



Globaali



*yli 1000 työntekijää Yhdysvalloissa; yli 500 työntekijää Saksassa, Japanissa, Australiassa/Uudessa-Seelannissa

Tutkimuksen yleiset opetukset

Organisaatiot ovat valmiita hyödyntämään Zero Trust -strategiaa

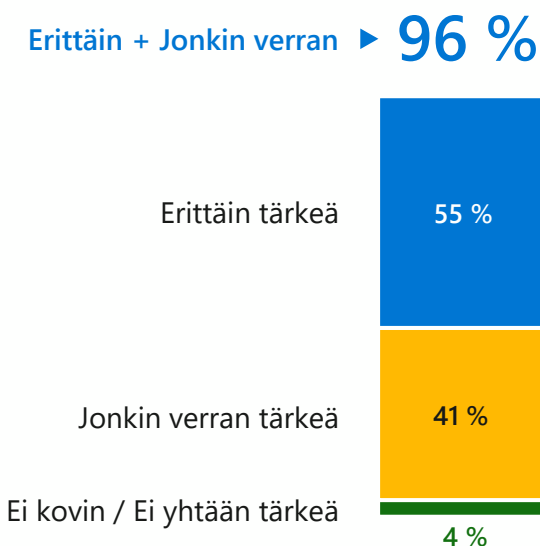
Zero Trust -strategia on tällä hetkellä tärkein tietoturvaprioriteetti eri markkina-alueilla ja toimialoilla, ja viime vuosina useat organisaatiot ovat ottaneet Zero Trust -strategian käyttöön. Vaikka Zero Trust -strategia on kaikkien mielessä (53 %), se on organisaatioiden prioriteetti etenkin Yhdysvalloissa (56 %) ja Saksassa (53 %).

Lähes kaikki tietoturva-ammattilaiset (96 %) uskovat, että Zero Trust -strategia on organisaation menestyksen edellytys. (Katso Todiste 1) Sen lisäksi, että tietoturva-ammattilaiset pyrkivät vahvistamaan yleistä tietoturva-asemaansa ja parantamaan loppukäyttäjän kokemusta, he haluavat myös hyödyntää Zero Trust -strategiaa yksinkertaistaakseen tietoturvamenetelmiä työntekijöitä varten. (Katso Todiste 2)

Kuten eräs yhdysvaltalainen majoitusalan päätöksentekijä totesi: *"Tavoitteena on parantaa yleistä tietoturva-asemaamme, mutta viime kädessä tarkoitus on yksinkertaistaa loppukäyttäjän kokemusta."*

Lisäksi 31 % tietoturva-ammattilaisista uskoo Zero Trust -strategian olevan tärkeä väline pandemian jälkeisessä siirtymisessä hybridityöskentelyyn. Tämä tekijä korostuu etenkin Australiassa/Uudessa-Seelannissa (44 %).

Todiste 1. Zero Trust on kriittisen tärkeä



Todiste 2. Zero Trust -motivaattorit

Tärkeimmät motivaattorit

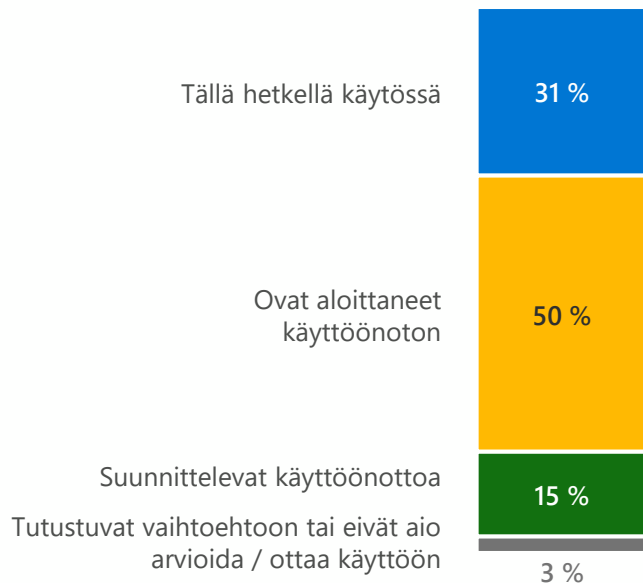
Yleisen tietoturva-aseman parantaminen	47 %
Loppukäyttäjän kokemuksen ja tuottavuuden parantaminen	44 %
Tietoturvatiimien työskentelytapojen uudistaminen	38 %
Tietoturvapinon yksinkertaistaminen	35 %
Tietoturvakustannusten pienentäminen	35 %

Siirtyminen hybridityöskentelyyn edistää Zero Trust -strategian laajempaa käyttöönottoa

81 % organisaatioista on aloittanut siirtymisen kohti hybridityöskentelyä, ja 31 % on jo saanut prosessin valmiiksi. Tästä huolimatta täysimääräisen käyttöönoton määrät vaihtelevat eri markkina-alueiden välillä: Australia ja Uusi-Seelanti ovat johdossa 37 %:lla, kun taas Saksassa vasta 20 % organisaatioista on siirtynyt hybridimalliin. [\(Katso Todiste 3\)](#)

Vaikka globaalit markkinat siirtyvät kohti hybridityöskentelyä vaihtelevalla vauhdilla, suurin osa (91 %) organisaatioista, jotka eivät ole vielä suorittaneet siirtoa, aikovat tehdä sen seuraavien viiden vuoden aikana. 94 % on kuitenkin huolissaan siirtymästä, ennen kaikkea työntekijöiden väärinkäytön, IT-osaston kasvavan työmäärän ja kyberhyökkäysten vuoksi. [\(Katso Todiste 4\)](#)

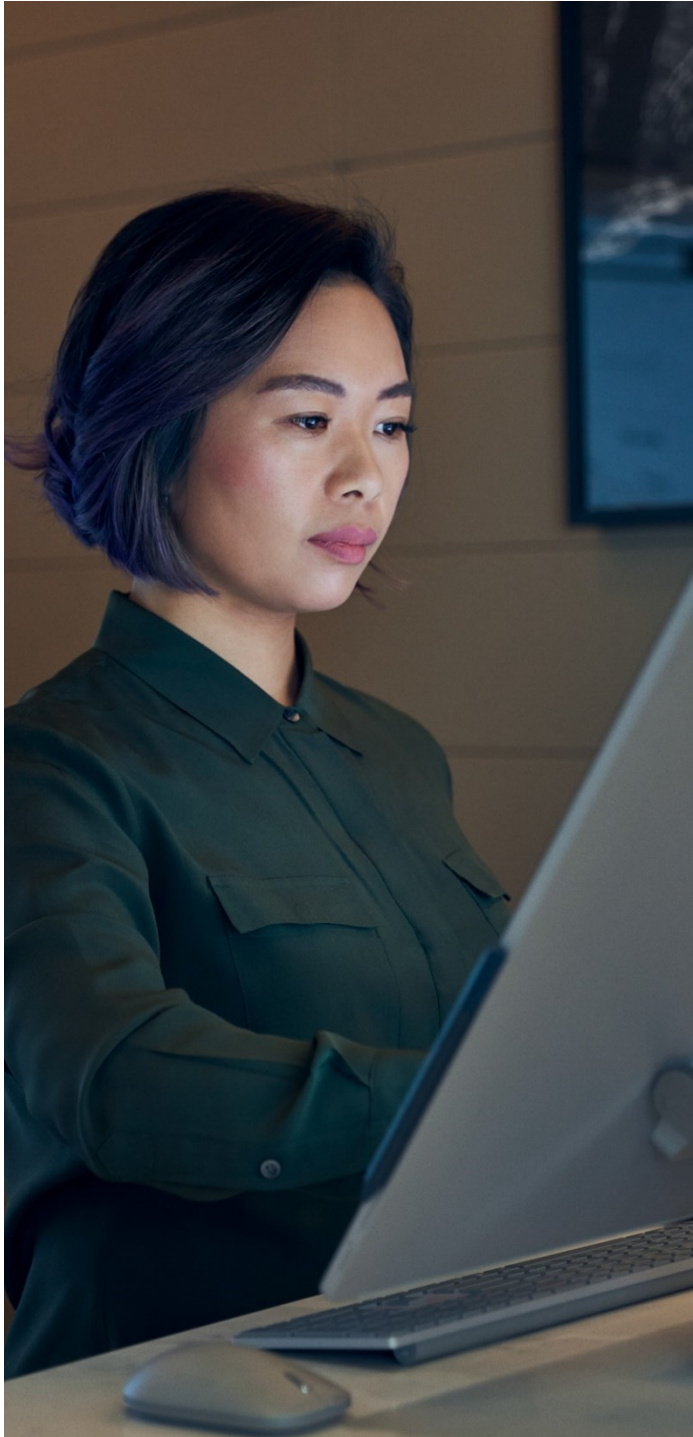
Todiste 3. Hybridityöskentely



Todiste 4. Hybridityöskentelyn huolenaiheet

Työntekijät lataavat epäluotettavia sovelluksia	37 %
IT-osaston työmäärän lisääntyminen	37 %
Kiristysohjelmahyökkäykset	36 %
Tietojenkalasteluhyökkäykset	35 %
Henkilökohtaisten laitteiden väärinkäyttö	34 %
Tietojen valtuuttamaton käyttö	31 %
Vaikeus hallita kaikkia laitteita	30 %
Henkilökohtaisten sähköpostitilien käyttö	30 %
Tietosuojasäännösten vaatimusten noudattamatta jättäminen	24 %

Koronaviruspandemia on paljastanut uusia näkökohtia, jotka nopeuttavat siirtymistä Zero Trust -strategiaan



Pyrkimyksenään minimoida mahdolliset ongelmat, sidosryhmät korostavat työntekijöiden koulutuksen lisäämisen tärkeyttä (54 %) (erityisesti Japanissa (61 %) ja Saksassa (58 %) ja monimenetelmäisen todennuksen (MFA) käyttöönoton merkitystä (50 %) (erityisesti Yhdysvalloissa (52 %) ja Saksassa (56 %), jotta voidaan varmistaa sujuva käyttäjäkokemus ja siirtyminen.

Zero Trust -strategia tukee etä- ja hybridityön tietoturvaa, joten koronaviruspandemia on vauhdittanut Zero Trust -strategian käyttöönottoa 72 % organisaatioista – vaikka markkina-alueiden välillä onkin eroja. Vaikka pandemia vauhditti käyttöönottoa noin 70 % yhdysvaltalaisissa (76 %), japanilaisissa (71 %) ja australialaisissa/uusiseelantilaisissa (69 %) organisaatioissa, käyttöönottomäärät ovat olleet huomattavasti alhaisemmat Saksassa (62 %). Tämä saattaa johtua hitaammasta siirtymästä hybridityöskentelyyn.

Zero Trust -strategia on otettu käyttöön laajalti ympäri maailmaa ja vauhti vain kasvaa Yhdysvalloissa

Zero Trust on muutakin kuin muotisana – se on todellisuutta. 76 % organisaatioista on ainakin aloittanut tämän strategian käyttöönoton, ja 35 % uskoo, että ne ovat suorittaneet sen loppuun. Nämä tiedot kuitenkin kertovat liian optimistisen tarinan, sillä monet organisaatiot, jotka uskovat suorittaneensa käyttöönoton loppuun, eivät ole tehneet sitä kaikilla tietoturvan riskialueilla. Nykyään Yhdysvallat on muita markkina-alueita edellä Zero Trust -strategian käyttöönotossa ja jatkaa nopeaa kasvuaan: elokuuhun 2020 verrattuna Zero Trust -strategian käyttöönotto Yhdysvalloissa nousi 70 %:sta 79 %:iin, mikä on merkittävä nousu vain kahdeksassa kuukaudessa.

(Katso Todiste 5)

Vaikka Zero Trust -strategia on hallinnut tietoturva-alaa jo jonkin aikaa, sen leviäminen kaikkialle on suhteellisen uusi ilmiö. 82 % yrityksistä otti Zero Trust -strategioita käyttöön viimeisten kolmen vuoden aikana, ja 21 % teki sen kuluneiden 12 kuukauden aikana. 26 % yhdysvaltalaisista organisaatioista kuitenkin aloitti käyttöönoton jo yli 3 vuotta sitten, kun vain 19 % japanilaisista organisaatioista, 6 % australialaisista ja uusiseelantilaisista sekä 3 % saksalaisista organisaatioista aloitti käyttöönoton yli 3 vuotta sitten. Aiempi käyttöönotto Yhdysvalloissa – yhdessä vähäisempien budjettirajoitteiden kanssa – saattaa selittää, miksi yhdysvaltalaiset organisaatiot ovat muiden markkina-alueiden organisaatioita edellä Zero Trust -strategian käyttöönotossa. Samaan tyyliin se, että Zero Trust -strategian käyttöönotto on Saksassa vasta aluillaan, auttaa kontekstualisoimaan sen alhaisia käyttöönottomääriä. 97 % saksalaisista organisaatioista aloitti käyttöönoton vasta viimeisten 3 vuoden aikana.

Todiste 5. Zero Trust -strategian käyttöönotto



- 35 % Täysin käyttöönotettu
- 42 % Käyttöönotto kesken

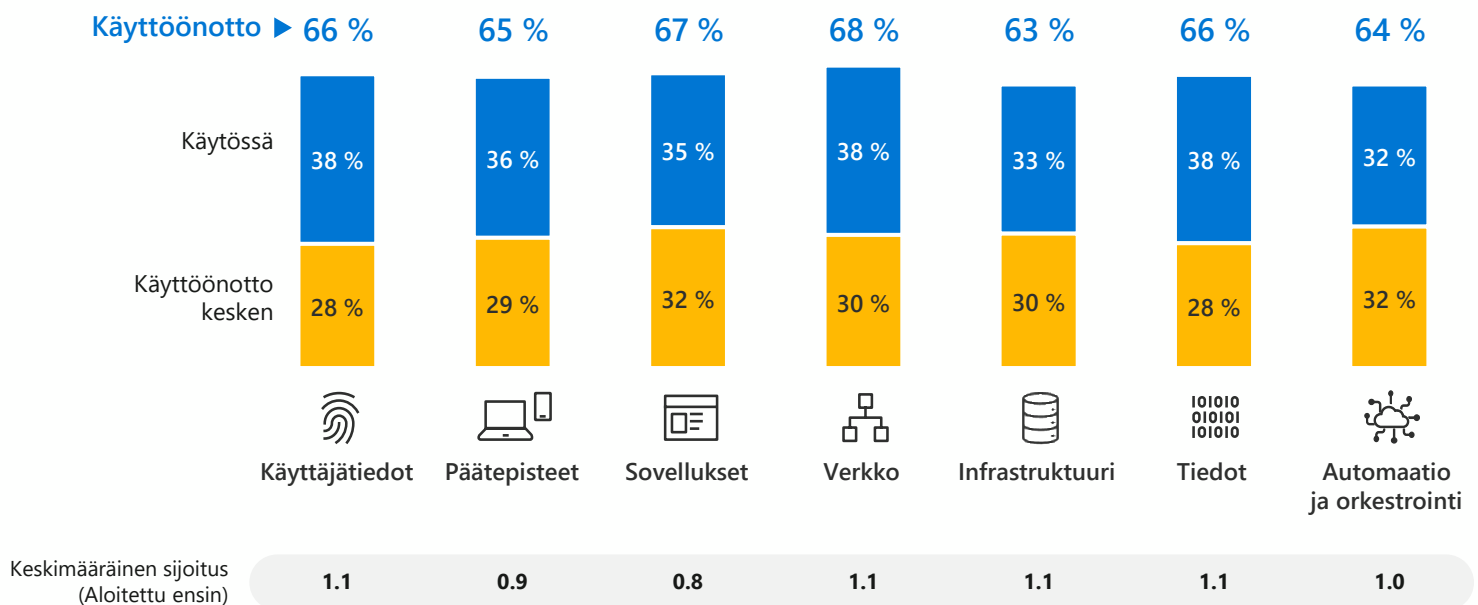
	US (2020)	US	DE	JP	AUS/NZ
Zero Trust -strategian käyttöönotto	70 %	79 %	75 %	76 %	71 %
• Täysin käyttöönotettu	27 %	44 %	19 %	32 %	28 %
• Keskenäisenä	43 %	35 %	56 %	44 %	43 %

Zero Trust -strategian käyttöönottoon ei ole olemassa kaikille sopivaa lähestymistapaa, vaan sen voi aloittaa mistä tahansa

Mikään yksittäinen tietoturvan riskialue (käyttäjätiedot, päätepiisteet, sovellukset, verkko, infrastruktuuri, tiedot, automaatio ja orkestrointi) ei erotu joukosta Zero Trust -strategian ensisijaisena aloituspisteenä, sillä alle 15 % organisaatioista aloittaa prosessin samalta tietoturvan riskialueelta. Alue, jolta organisaatiot aloittavat prosessin, riippuu todennäköisesti organisaation tarpeista ja käytettävissä olevista sisäisistä resursseista. Ennen pitkää ne pyrkivät ottamaan Zero Trust -strategian käyttöön kaikilla eri tietoturvan riskialueilla varmistaakseen, että ne pystyvät torjumaan uhkia. Tämän vuoksi Zero Trust -strategiaa pidetään kokonaisvaltaisena strategiana, joka on tarkoitus suorittaa loppuun ajan myötä. [\(Katso Todiste 6\)](#)

Zero Trust -strategian tietoturvan riskialueiden lisäksi organisaatioiden on tunnistettava komponentit, jotka priorisoidaan kullakin tietoturvan riskialueella. Päätepiisteiden, sovellusten, verkon, tietojen ja automaation/orkestroinnin kohdalla ei ole selkeää aloituspistettä; tietoturva-ammattilaisten priorisoimat komponentit vaihtelevat merkittävästi. Käyttäjätiedoissa vahva todennus on kuitenkin yleensä ensimmäinen komponentti, ja infrastruktuurissa selkeänä prioriteettina on uhkientunnistustyökalut. [\(Katso Todiste 7\)](#)

Todiste 6. Zero Trust -strategian käyttöönoton nykyinen tila – tietoturvan riskialueet



Todiste 7. Zero Trust komponenttien käyttöönotto (Top 3) – 1. sija (käytöön otettu ensin)

Käyttäjätiedot	
Vahva todennus (esim.monimenetelmäinen todennus, salasanan todennus)	32 %

Automaattinen riskien tunnistus ja korjaus	27 %
Mukautuvat käyttöoikeuskäytännöt resurssien käyttöoikeuksien valvontaa varten	22 %

Sovellukset	
Jatkuva Shadow IT Discovery ja riskinarviointi	23 %

Hajautettu sovellusten käyttöoikeuksien hallinta (esim. rajoitettu näkyvyys tai vain luku)	22 %
Sovellusten käyttöoikeuksien käytäntöpohjainen hallinta	20 %

Infrastruktuuri	
Tietoturvatietojen käyttöoikeudet uhkien havaitsemistyökaluihin	25 %

Pilvipohjaisten työkuormien suojaaminen hybridi- ja monipilviratkaisuissa	19 %
Hajautettu näkyvyyden ja käyttöoikeuksien hallinta kaikissa työkuormissa (virtuaalikoneet, palvelimet jne.)	17 %

Automaatio ja orkestrointi	
Kokonaisvaltainen näkyvyys varmistetaan keskitetyn tutkinta- ja reagoitinympäristön avulla	29 %
Eri toimialueiden (käyttäjätiedot, päätepiisteet, sovellukset, verkko, infrastruktuuri) uhkatiedot kerätään ja analysoidaan	28 %
Automaattinen tutkinta ja reagointi otetaan käyttöön	22 %

Päätepiisteet	
Tietojen menetyksen ehkäisyn käytännöt/meکانismit kaikille hallitsemattomille ja hallituille laitteille	27 %

Reaaliaikainen laitteen riskin arviointi / päätepiisteen uhkien havaitseminen	26 %
Laitteet on rekisteröity tunnistetietopalveluun	24 %

Verkko	
Turvallinen käyttöoikeuksien hallinta verkkojen suojaamiseksi	25 %

Uhkien torjunta ja suodatus kontekstipohjaisilla signaaleilla	24 %
Kaikki tietoliikenne salataan	20 %

Tiedot	
Käyttöoikeuksiin liittyviä päätöksiä hallinnoidaan tietoturvakäytäntöjen moduulilla	21 %

Tiedot luokitellaan ja merkitään	21 %
Kaikkein arkaluontoisimpia tiedostoja suojataan jatkuvasti salauksen avulla	20 %



Emme suhtautuneet
siihen pelkästään
teknologioiden sarjana,
vaan strategiana
ja lähestymistapana,
jolla käyttäjäresursseihin
suhtaudutaan
epäluotettavina, kunnes
ne voidaan todentaa –
riippumatta siitä, ovatko
ne verkkomme sisällä
tai sen ulkopuolella."

Yhdysvaltalainen tietoturvan
päättökentekijä
Majoitusala

Kun organisaatiot aloittavat Zero Trust -strategian käyttöönoton, tärkeimpiä hyötyjä ovat muun muassa lisääntynyt ketteryys, nopeus ja tietoturva; resurssiedut eivät ole yhtä yleisiä

Kun Zero Trust -strategia on otettu käyttöön, organisaatiot hyötyvät lisääntyneestä ketteryydestä (37 %), nopeudesta (35 %) ja asiakastietojen suojaamisesta (35 %). [\(Katso Todiste 8\)](#) Suoraan työntekijöille kohdistuvat hyödyt, kuten tietoturvatiimin resurssien vapautuminen (27 %) ja infrastruktuurin hallinta vähemmillä resursseilla (22 %), eivät ole yhtä yleisiä.

Ja mikä tärkeintä, organisaatiot uskovat Zero Trust -strategian auttavan heitä hallitsemaan useimpia uhkia ja ympäristöön kohdistuvia muutoksia, erityisesti IoT:n ja OT:n tietoturvan osalta (47 %).

Todiste 8. Zero Trust -strategian hyödyt





Organisaatiot uskovat käyttävänsä Zero Trust -strategiaa tehokkaasti

79 % uskoo osaavansa käsitellä tietoturvauhkia kokonaisuutena, vaikka enemmän epävarmuutta ilmenee, kun uhkaan liittyy totuuden vääristämistä: tietoturvan päätöksentekijöillä on vähiten itsevarmuutta, kun he kohtaavat synteettisiä identiteettejä (20 %) ja syvävääreännöksiä (10 %).

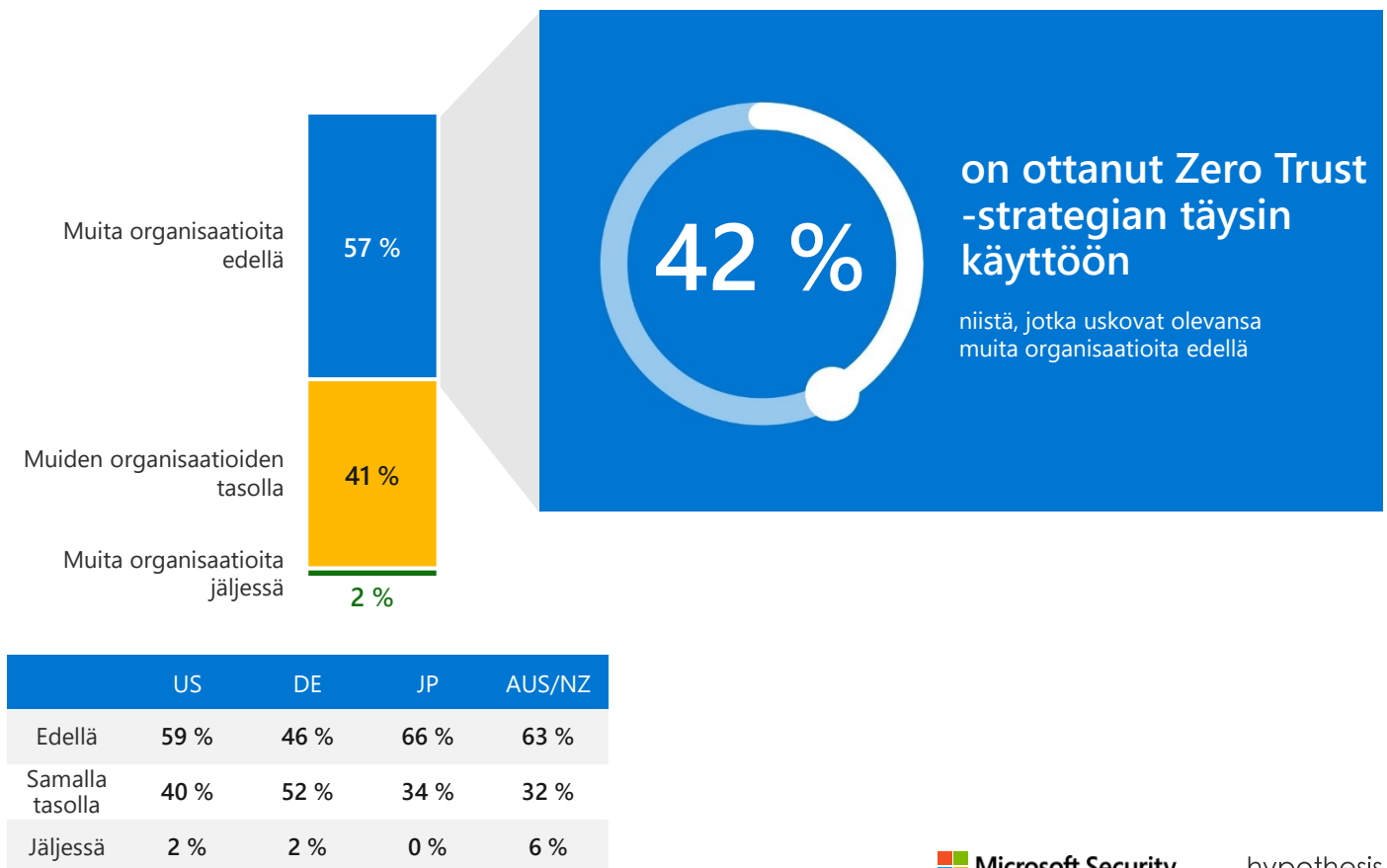
Kun otetaan huomioon saadut hyödyt, Zero Trust -strategioihin liittyy yleensä positiivisia ajatuksia. Kaikilla neljällä käsitellyllä markkina-alueella tietoturvan päätöksentekijät pitävät organisaationsa lähestymistapaa sekä käytännöllisenä että tavoitteellisenä. He kuvaavat sitä itsevarmaksi (37 %) ja tehokkaaksi (31%) sekä motivoivaksi (25 %), inspiroivaksi (25 %) ja jännittäväksi (25 %). Erityisesti Japanissa tietoturva-ammattilaiset kuvaavat Zero Trust -strategiaa sekä vaativaksi (27 %) että mullistavaksi (25 %), mikä viittaisi siihen, että vaikka sen käyttöönotto ei ole helppoa, sen hyödyt ovat kauaskantoisia.

Useat organisaatiot uskovat, että ne ovat muita edellä Zero Trust -strategian käyttöönotossa, mutta niillä on vielä paljon tehtävää

Vaikka vain 35 % organisaatioista on ottanut Zero Trust -strategian käyttöön täysin, 52 % kertoo olevansa suunnitelmiaan edellä ja 57 % uskoo olevansa muita organisaatioita edellä. Erityisesti Japanissa (66 %) ja Australiassa/Uudessa-Seelannissa (63 %) organisaatiot uskovat olevansa muita edellä. Vaikka samanlainen itsevarmuus vallitsee kaikilla markkina-alueilla, todellisuus on usein erilainen: niistä organisaatioista, jotka uskovat olevansa muita organisaatioita edellä, vain 42 % kertoo ottaneensa Zero Trust -strategian täysin käyttöön. (Katso Todiste 9)

Vaikka useat organisaatiot uskovat Zero Trust -strategiansa toimivan ja tuntevat olevansa valmiita kohtaamaan tulevat tietoturvaohauhat, niillä on vielä paljon tehtävää, ennen kuin strategia on otettu täysin käyttöön kaikilla riskialueilla. Esimerkiksi niistä organisaatioista, jotka uskovat Zero Trust -strategian käyttöönoton olevan täysin valmis, puolet eivät ole vielä ottaneet sitä käyttöön kaikilla tietoturvan riskialueilla – todennäköisintä on, että käyttöönottoa ei ole vielä suoritettu infrastruktuurissa ja käyttäjätiedoissa.

Todiste 9. Zero Trust -strategian käyttöönoton vertailu

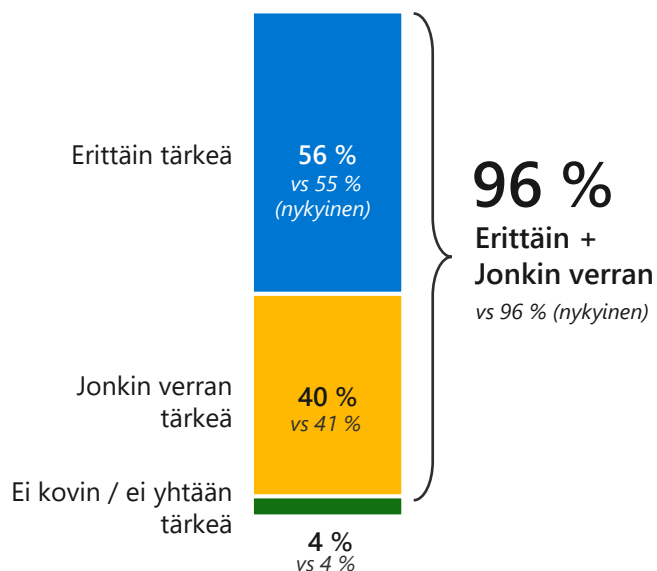


Zero Trust -strategia tulee olemaan ensisijainen tietoturvaprioriteetti seuraavien kahden vuoden aikana

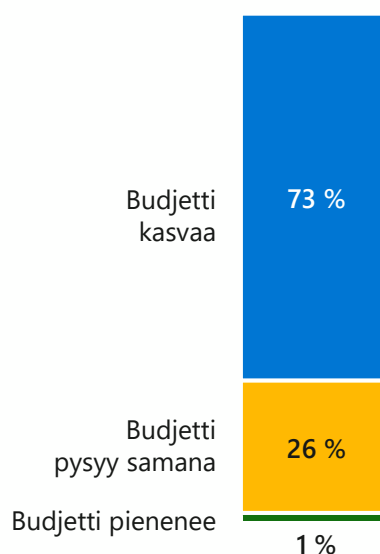
Organisaatiot ovat innostuneet Zero Trust -strategiasta, ja päätöksentekijät arvelevat sen olevan tärkeä tietoturvaprioriteetti seuraavien kahden vuoden ajan. Zero Trust -strategian suhteellisen merkityksen tietoturva-aloitteena ennustetaan kasvavan (53 %:stä 58 %:iin) vuoteen 2023 mennessä, sillä tietoturvan päätöksentekijät arvelevat, että strategia on jatkossakin ratkaisevan tärkeä yleisen menestyksen kannalta (96 %).
(Katso Todiste 10)

Ennen kaikkea japanilaisissa organisaatioissa merkityksen ennustetaan olevan erityisen korkea, sillä 70 % niistä arvioi Zero Trust -strategian olevan erittäin tärkeä seuraavien kahden vuoden aikana yleiseen 56 %:n keskiarvoon verrattuna. Myös Zero Trust -strategialle määritettyjen budjettien odotetaan kasvavan – 73 % organisaatioista uskoo budjettiansa kasvavan. Tämä luku on kuitenkin hieman alhaisempi Saksassa (67 %), jossa 31 % arvioi budjettiansa pysyvän samana.
(Katso Todiste 11)

Todiste 10. Zero Trust -strategian arvioitu merkitys seuraavien kahden vuoden aikana



Todiste 11. Zero Trust -strategian arvioitu budjetti seuraavien kahden vuoden aikana



Zero Trust -strategian onnistumisten todistaminen voi johtaa lisäinvestointeihin

Organisaatiot, jotka ovat omaksuneet Zero Trust -strategian täysin rinnoin, odottavat kaksinkertaistavansa investointinsa seuraavien kahden vuoden aikana. Ne, jotka eivät ole vielä aloittaneet käyttöönottoa, ovat vaarassa jäädä jälkeen. Sen lisäksi, että nämä organisaatiot ovat kollegoita jäljessä Zero Trust -strategian priorisoinnissa tietoturvasuunnitelmissa (42 % vs 66 %) ja budjetin kasvun ennakkoinnissa (66 % vs 72 %), ne myös suhtautuvat IoT:n ja OT:n hallintaan huomattavasti epävarmemmin (40 % vs 53 %).



Jotta Zero Trust -investoinnin kaksinkertaistaminen onnistuu, on tärkeää, että haasteet ratkaistaan työntekijöiden avulla

Zero Trust -strategian käyttöönoton nopeasta etenemisestä huolimatta organisaatioiden on ratkaistava lukemattomia haasteita, jos ne haluavat edistyä käyttöönotossa. (Katso Todiste 12) Näissä kategorioissa resurssien ja johdon haasteet ovat muita yleisempiä. Suurimpia esteitä ovat Zero Trust -strategioiden käyttöönottoon tarvittava aika ja johtoportaan tuen puute, joista jälkimmäinen on erityisen merkittävä Australiassa/Uudessa-Seelannissa (65 %).

Myös budjettirajoitukset – jotka 45 % organisaatioista on määrittänyt esteiksi – todennäköisesti vaikuttavat resurssien ja johdon haasteisiin.

Esimerkiksi 21 % tietoturvan päätöksentekijöistä pitää Zero Trust -investointiin sijoitetun pääoman tuoton todistamista yhtenä käyttöönoton esteistä, sillä tämä haaste voi vaikuttaa johtoryhmän hyväksyntään. Yhdysvaltojen ulkopuolisilla markkina-alueilla on todennäköisemmin budjettirajoituksia (60 % japanilaisista organisaatioista; 57 % saksalaisista organisaatioista; 57 % australialaisista ja uusiseelantilaisista organisaatioista), joten on mahdollista, että Zero Trust -strategioiden käyttöönotto on Japanissa, Saksassa ja Australiassa/Uudessa-Seelannissa lopulta vähäisempää ja hitaampaa kuin Yhdysvalloissa.

Todiste 12. Zero Trust -strategian esteet

Resurssihaasteet 60 %	Johtajuus 53 %	Teknologinen 46 %	Toimittaja 46 %	Budjettirajoitukset 45 %
20 % Käyttöönotto kestää liian pitkään	20 % Johtoportaan tuen puute	21 % Tietoturva-ratkaisujen integroinnin vaikeus	21 % Tarvitaan käyttöönottotukea toimittajilta	21 % Zero Trust -strategian käyttöönoton kustannukset
19 % Sisäisen muutoksenhallinnan puute	19 % Sidosryhmien tuen puute	19 % Yhteen-sopimattomuus vanhojen järjestelmien kanssa	21 % Vaikeus tunnistaa oikeat toimittajat	21 % Vaikeus todistaa sijoitetun pääoman tuotto
18 % Koulutus-materiaaleja tarvitaan enemmän	19 % Tarvitaan apua houkuttelevan liiketoimintatapauksen luomiseen	19 % Vaikeus skaalata koko organisaation käyttöön	17 % Vaikeus löytää innovatiivisia kumppaneita	14 % Budjetti ei ole riittävän suuri
17 % Se ei ole tarpeellinen tämän kokoiselle organisaatiolle	18 % Organisaation hyväksynnän puute			
16 % Ei ole oikeanlaista osaamista asianmukaista käyttöönottoa varten				

” Ensimmäisen hyväksynnän saaminen oli haastavaa, mutta kun me sidosryhmät päätimme investoida projektiin, kaikki olivat mukana.”

Yhdysvaltalainen tietoturvan päätöksentekijä
FinTech



Tietoturvan päätöksentekijöillä on hieman taipumusta valita kokonaisvaltaisia tai konsolidoituja palveluntarjoajia

Mitä tulee Zero Trust -toimittajastrategiaan, organisaatiot joutuvat valitsemaan palvelupaketin tai erilliset luokkansa parhaat ratkaisut. Näistä ensimmäisessä organisaatio ostaa palvelupaketin koko Zero Trust -arkkitehtuurille kokonaisvaltaiselta tai konsolidoidulta palveluntarjoajalta. Tietoturvan päätöksentekijät uskovat, että tämä ratkaisu tarjoaa enemmän asiantuntemusta, resursseja ja yksinkertaisuutta organisaatioille, joissa on rajalliset sisäiset resurssit. Tähän lähestymistapaan liittyy kuitenkin myös uudenlaisia haavoittuvuuksia ja joustavuuden puute. (Katso Todiste 13)

Todiste 13. Palvelupaketin hyödyt ja haasteet – 2 tärkeintä

+ Palvelupaketin hyödyt	
Toimittajalla on toimialakohtaista asiantuntemusta eri ratkaisuista	24 %
Enemmän resursseja saatavilla Zero Trust -strategian suunnittelun tueksi	23 %
Yksinkertaistettu tietoturvapino	22 %

- Palvelupaketin haitat	
Riippuvuus yhdestä toimittajasta lisää haavoittuvuutta	34 %
Integraatio vanhan arkkitehtuurin kanssa on monimutkaisempaa	33 %
Vähemmän joustavuutta erikoistuneeseen toimintaan	29 %

Jälkimmäinen strategia, luokkansa parhaiden ratkaisujen valinta, edellyttää yksittäisten Zero Trust -teknologiakomponenttien hankkimista erikoistuneilta toimittajilta. Toisin kuin palvelupaketti, tämä strategia perustuu erikoistuneisiin toimittajiin, ja sen vuoksi se tarjoaa enemmän joustavuutta ja voi sopia paremmin organisaation strategiaan. Tästä huolimatta tietoturva-ammattilaiset uskovat erillisten luokkansa parhaiden ratkaisujen olevan kalliimpia, vaativan enemmän resursseja ja estävän näkyvyyttä – nämä ovat haittoja, jotka viime kädessä johtavat toimittajiin ja budjettiin liittyviin haasteisiin. (Katso Todiste 14)

Vaikka organisaatiot ovat jakautuneet melko tasaisesti, hieman yli puolet tietoturvan päätöksentekijöistä (55 %) valitsee mieluummin kokonaisvaltaisia (palvelupaketin tarjoavia) palveluntarjoajia. (Australialaiset/uusiseelantilaiset organisaatiot eivät kuitenkaan ole täysin samaa mieltä, vaan 52 % valitsee mieluummin erilliset luokkansa parhaat ratkaisut.)

Todiste 14. Erillisten luokkansa parhaiden ratkaisujen hyödyt ja haasteet – 2 tärkeintä

+ Erillisten luokkansa parhaiden ratkaisujen hyödyt	
Joustavuus hankkia parhaat ratkaisut mille tahansa Zero Trust -strategian komponentille	33 %
Ratkaisu voi sopia organisaation arkkitehtuuriin tai strategiaan paremmin	30 %
Enemmän mahdollisuuksia innovoida eri toimittajien kanssa	26 %

- Erillisten luokkansa parhaiden ratkaisujen haitat	
Suuremmat kustannukset	29 %
Vaikeus jakaa tietoja eri ratkaisujen välillä	26 %
Suuri määrä ratkaisuja sisäisten tiimien käyttöön otettaviksi ja hallittaviksi	26 %

Yhteenveto

Kun tietoturvariskien vaikutukset kasvavat, eri markkina-alueiden ja toimialojen organisaatiot valitsevat Zero Trust -strategian, jonka lähestymistapana on olla luottamatta keneenkään ja todentaa käyttäjä tilanteesta riippumatta. Zero Trust -strategia on tärkein tietoturvaprioriteetti organisaatioissa, jotka pyrkivät parantamaan yleistä tietoturva-asemaansa, loppukäyttäjän kokemusta ja tuottavuutta, yksinkertaistamaan työntekijöiden tietoturvakäytäntöjä ja pienentämään kustannuksia. Vaikka Zero Trust -strategia todistetusti tarjoaa hyötyjä, rajalliset resurssit ja johtoportaan skeptisismi hidastavat universaalia käyttöönottoa.

Zero Trust -strategian käyttöönotto on kiihtynyt viimeisten kolmen vuoden aikana – osittain koronaviruspandemian vuoksi. Siirtyminen etä- ja hybridityöskentelyyn edistää Zero Trust -lähestymistapojen laajaa käyttöönottoa, sillä ne lupaavat suojata järjestelmiä ja tietoja silloinkin, kun työntekijät käyttävät niitä toimipaikan ulkopuolella ja joskus jopa henkilökohtaisilla laitteilla.

Koronaviruspandemian vuoksi vauhdittunut käyttöönotto ennustaa tehokkaasti Zero Trust -strategian yleistä valmiutta, sillä pandemian aikana strategian omaksuneet organisaatiot ovat ottaneet sen käyttöön useammalla tietoturvan riskialueella kuin kollegansa.

Tästä huolimatta jopa edistyneimmillä Zero Trust -strategian käyttöönottajilla on vielä paljon tehtävää, ja organisaatioiden harhakäsitykset Zero Trust -maturiteetistaan voivat johtaa siihen, että ne eivät ole tietoisia kaikista haavoittuvuuksistaan.

Suurin osa eri markkina-alueiden organisaatioista uskoo, että Zero Trust -strategian merkitys tulee vain kasvamaan ajan myötä, ja sen vuoksi ne arvelevat budjettien kasvavan. Tämä odotettu priorisoinnin muutos on erityisen tärkeä Yhdysvaltojen ulkopuolisille markkina-alueille, joissa budjettiin liittyvät huolenaiheet ovat tähän saakka olleet käyttöönoton kannalta merkittäviä esteitä. Kokonaisvaltainen käyttöönotto saattaa olla taloudellisesti ja logistisesti ylivoimaista; Zero Trust -lähestymistavan hyödyt ovat silti kiistattomia, ja Microsoft on organisaatioiden apuna ja tukena tässä haasteellisessa prosessissa.



Jos haluat lisätietoja Zero Trust -strategiasta ja haluat arvioida organisaatiosi Zero Trust -maturiteetin, siirry osoitteeseen

aka.ms/zerotrust

Yksityiskohtaiset tutkimustavoitteet ja kohderyhmän rekrytointi

Tutkimuksessa oli muun muassa seuraavat tavoitteet:

Zero Trust -lähestymistapojen nykytilan ymmärtäminen

Zero Trust -lähestymistapojen käyttöönoton asenteiden, parhaiden käytäntöjen, hyötyjen ja haasteiden selvittäminen

Zero Trust -lähestymistapojen tulevaisuuden ennakkointi

Zero Trust -lähestymistapojen innovaatioiden ja trendien kontekstualisointi

Tietoturvan päätöksentekijöiden on täytettävä seuraavat kriteerit:

Vastuussa organisaation tietoturvasta, mukaan lukien kyberturvallisuudesta, tietoturvatoimista, uhkien torjunnasta, käyttäjätietojen hallinnasta, riskinhallinnasta, sovellusten tietoturvasta, digitaalisten rikosten tutkinnasta sekä häiriötapauksiin reagoinnista

Työskentelee täysipäiväisesti suuressa yrityksessä (yli 1 000 työntekijää Yhdysvalloissa; yli 500 työntekijää Saksassa/Japanissa/Australiassa/Uudessa-Seelannissa)

25–75-vuotias

Perehtynyt Zero Trust -strategiaan

Osallistuu Zero Trust -strategian kehitystä/käyttöönottoa koskevaan päätöksentekoon

Huhtikuussa 2021 haastateltiin yhteensä 911 tietoturvan päätöksentekijää:

Yhdysvalloissa haastateltiin 477 tietoturvan päätöksentekijää

Saksassa haastateltiin 201 tietoturvan päätöksentekijää

Australiassa/Uudessa-Seelannissa haastateltiin 126 tietoturvan päätöksentekijää

Japanissa haastateltiin 107 tietoturvan päätöksentekijää

Huomautus: Tutkimus toteutettiin eri leviämisen/hallinnan vaiheissa olleen maailmanlaajuisen koronaviruspandemian aikana

© Hypothesis Group 2021. © Microsoft 2021.
Kaikki oikeudet pidätetään. 07/21