CSO

Microsoft Security

SPONSOROITUA SISÄLTÖÄ

Zero Trust -tietoturva: **oppeja varhaisilta käyttäjiltä**

CSO Microsoft Security

Sisällysluettelo

CSO Microsoft Security

Johdanto

Perinteiset IT- ja tietoturvamallit ovat järkkyneet kahden edellisen vuoden aikana. Tämän johdosta Zero Trust -tietoturva on kehittynyt nopeasti kiinnostavasta konseptista yritysten nykyaikaisen tietoturvan perustaksi.

Foundryn uudet tutkimustulokset osoittavat, että 52 prosenttia on ottanut käyttöön Zero Trust -arkkitehtuurin tai ainakin pilotoinut sitä. Lisäksi 15 prosenttia yrityksistä tutkii Zero Trust -malleja. Nämä varhaisen vaiheen käyttäjät kertovat monista käyttöönottojen tuomista eduista: näitä ovat esimerkiksi asiakastietojen parempi suojaus, monimutkaisuuden väheneminen ja yritysresurssien turvallinen sekä luotettava käyttö.

Tässä e-kirjassa käsitellään Foundryn tutkimustuloksia, jotka osoittavat, miten Zero Trust auttaa tietoturvajohtajia suojaamaan organisaatioitaan useiden eri hyökkäyspintojen monilta erilaisilta riskeiltä. Lisäksi kirja sisältää ohjeita Zero Trustin toteuttamiseen organisaatioille, jotka ovat vasta aloittamassa Zero Trust -polullaan.

Tietoja tutkimuksesta

Foundry kyseli yhdysvaltalaisilta yrityksiltä helmi- ja maaliskuussa 2022 niiden Zero Trust -käyttöönottotilannetta. Vastaajien täytyi olla vähintään IT-johtajia tai korkeammassa asemassa olevia, jotka työskentelivät vähintään 500 työntekijän yrityksessä. Lisäksi vastaajien piti olla mukana kyberturvallisuustuotteiden ja -palveluiden hankintaprosessissa.

23 kysymystä kattavaan kyselyyn vastasi yhteensä 250 vastaajaa.

CSO Microsoft Security

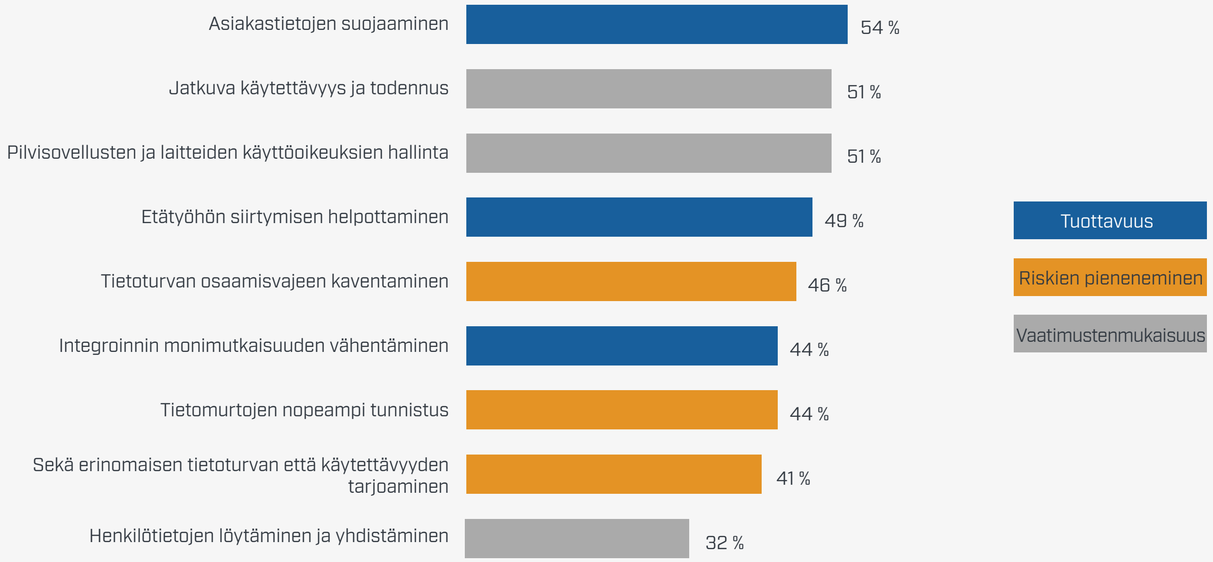
Zero Trust on täällä – ja se tuottaa lisäarvoa

Kyselyn tulokset ja laajemmat haastattelut IT- ja tietoturva-asioista vastaavien johtajien kanssa osoittavat, että Zero Trust on useimmilla organisaatioilla kirkkaana mielessä. Lisäksi tulokset osoittavat, että erilaisia Zero Trust -komponentteja jo käyttöön ottaneet organisaatiot ovat saaneet tästä jo etua.

Useimmat Zero Trust -arkkitehtuurin toteuttaneet (87 %) sanovat, että sen tulokset vastaavat alkuperäisiä tavoitteita toteutukselle, käyttöönotolle ja integroinnille tai ylittävät ne.

"[Zero Trustista] on tullut meille vakiotoimintatapa. En usko, että palaamme enää koskaan aiempaan", sanoo maailmanlaajuisen vähittäismyyntiyrityksen IT-johtaja. (Vastaajien sallittiin vastata nimettömästi, jotta he voisivat puhua vapaasti tietoturvasuunnitelmistaan.)

Zero Trustin käyttöönoton tuomat edut



12 prosenttia vastaajista sanoi saavuttaneensa *kaikkia* näitä etuja.

Lähde: Zero Trust Adoption Survey -kysely, maaliskuu 2022, Foundry. Vastaajien määrä: 250

CSO Microsoft Security

Noin 44 prosenttia vastaajista kertoi, että Zero Trust oli myös vähentänyt integroidun tietoturva-arkkitehtuurin toteutuksen monimutkaisuutta. "Koska kyseessä on kehysratkaisu, se tekee asioista vähemmän monimutkaisia", kertoo 3 500 työntekijän asiakaspalvelukeskusyrityksen tietoturvajohtaja.

17 000 työntekijän rahoituspalveluyrityksen tietoturvajohtaja (ja varapääjohtaja) sanoo Zero Trustin osana toteutetun monimenetelmäisen todentamisen olevan todella suosittua työntekijöiden keskuudessa. "Se on parantanut työntekijöiden tyytyväisyyttä, koska nyt heidän ei tarvitse päästä yrityksen työkoneelle ja käyttää VPN-asiakasohjelmaa, vaan he voivat käyttää resursseja sijainnistaan riippumatta", hän kertoo.

Tietoturvajohtajan mukaan myös pienimpien mahdollisien käyttöoikeuksien periaate on tuonut tuloksia. "Meillä on ollut vähemmän järjestelmänvalvojatason vakavia virheitä tällaisen käyttöoikeusjärjestelmän käyttöönoton jälkeen", hän huomauttaa. "Käyttäjät saavat käyttöoikeudet tiettyyn tarkoitukseen ja tietyksi ajaksi, joten virheiden tekemisen todennäköisyys pienenee."

Koska tietojenkalastelu ja muut kyberhyökkäykset ovat entistä yleisempiä, vähittäismyyntiyrityksen IT-johtaja kertoo Zero Trustin eduista seuraavasti: "Jos meillä ei olisi näitä työkaluja, olisimme todennäköisesti liemessä ja maksaisimme varmaan jollekin juuri nyt bitcoineja."

CSO Microsoft Security

Zero Trust -käyttöönottoa puoltavat seikat

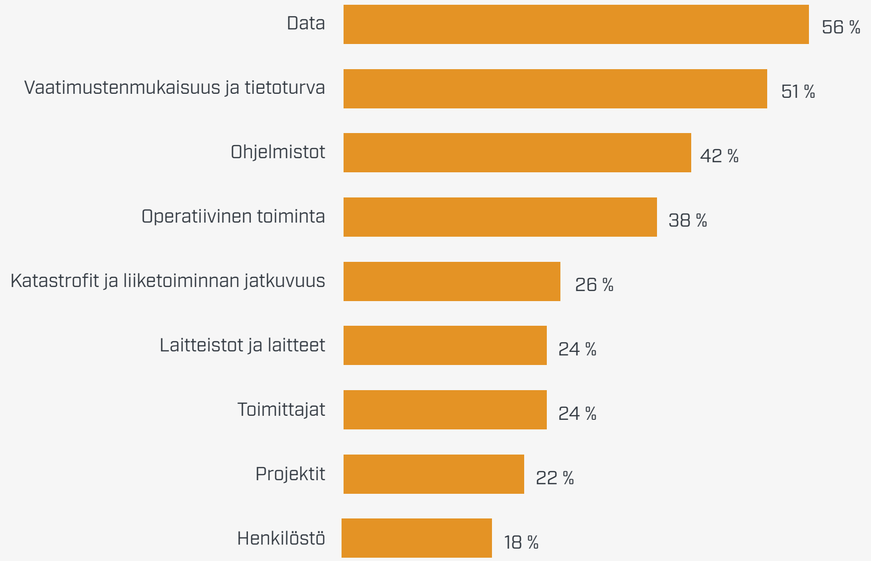
Monet eri seikat saavat yrityksiä ainakin harkitsemaan Zero Trust -arkkitehtuuria. Yksi merkittävimmistä tekijöistä on tarve hallita useiden eri resurssien riskejä useita erilaisia uhkia vastaan. Kyselyyn vastaajien mukaan vuoden aikana tietoturvaongelmia esiintyi monista eri syistä, ja yleisimpiä syitä olivat tietoturvahaavoittuvuudet, joita aiheuttivat ulkopuoliset käyttäjät tai organisaatiot. Muita syitä olivat esimerkiksi seuraavat:

- odottamattomat liiketoiminnan riskit
- väärin määritetyt palvelut tai järjestelmät
- tahalliset sisäpiirin hyökkäykset
- tahattomat käyttäjien virheet, muun muassa tietojenkalasteluun lankeaminen
- vääriin käsiin joutuneet tai murretut käyttäjätiedot
- päivittämättömät ohjelmistot
- varastetut tunnistetiedot.

Nämä ongelmat aiheuttavat monia erilaisia riskejä, eritoten datan suhteen.

Monissa organisaatioissa pandemian aiheuttama äkillinen siirtymä etätöihin nopeutti Zero Trust -käyttöönottosuunnitelmia, sillä perinteisistä raja-aitoihin perustuvista tietoturvamalleista tuli vanhentuneita. Monet organisaatiot olivat jo matkalla tähän suuntaan, kun ne siirsivät yhä enemmän sovelluksia ja IT-infrastruktuuria pilveen, mutta pandemia antoi kehitykselle lisävauhtia.

Kyberturvallisuusuhkien merkittävimmät riskiluokat



Lähde: Zero Trust Adoption Survey -kysely, maaliskuu 2022, Foundry. Vastaajien määrä: 250

CSO Microsoft Security

Esimerkiksi 1 700 työntekijän lääketieteellisen tekniikan alan yrityksen tietoturvajohtaja sanoo pilven ja pandemian olleen vaikuttimia Zero Trustin käyttöönotolle. Zero Trust tarjoaa nyt turvallisen perustan mille tahansa työpaikkamallille tulevaisuudessa.

"Liiketoiminnallisia vaikuttimia olivat se, että olemme pilvipohjainen yritys ja meidän täytyi kyetä suojaamaan ympäristömme", hän kertoo. "Lisäksi meidän täytyi kyetä tarjoamaan etätyömahdollisuudet ja -työkalut pandemian aikana. [Zero Trust] antoi meille mahdollisuuden pienentää kiinteistöjalanjälkeämme merkittävästi, ja todennäköisesti olemme jatkossa ainakin 60-prosenttisesti virtuaalietätyötä tekevä yritys."

CSO Microsoft Security

Uhkia on runsaasti

Vaatimustenmukaisuustarpeet vauhdittavat myös siirtymistä tehokkaampiin tietoturvamalleihin. "Viranomaiset valvovat meitä ja odottavat meidän jatkavan tietoturvamme parantamista", kertoo 290 000 työntekijän kansainvälisen rahoitusalan yrityksen tietoturvajohtaja.

Jotkin organisaatiot ovat edenneet aktiivisesti kohti Zero Trustia välttääkseen paljon julkisuutta vääristä syistä tuovia tietomurtoja. "Halusimme myös olla aktiivisia ja pysyä poissa uutisista", sanoo 3 500 työntekijän korkeakoulun tietohallintojohtaja. "Olemme kuulleet todellisia kauhutarinoita muista samankokoisista oppilaitoksista, joiden palvelut olivat pitkään poissa pelistä."

Jotkin organisaatiot ovat taas kokeneet vakavia kyberturvallisuusongelmia, joiden johdosta ne ovat halunneet uudistaa tietoturvastrategiaansa nopeasti. Kun 6 000 työntekijän vakuutusyhtiö joutui kiristysohjelmahyökkäyksen kohteeksi ja sen yritysverkko oli poissa pelistä kaksi viikkoa, päätöksen Zero Trustin käyttöönotosta teki itse toimitusjohtaja. "Laitoimme toteutuksessa turbovaihteen silmään", kertoo yrityksen IT-kehitysjohtaja. "Alussa kyse oli ehdottomasti parhaista käytännöistä, mutta sitten hommat saivat todella vauhtia kiristysohjelmahyökkäyksemme jälkeen."

Pilvipohjainen katalyytti

Merkittävän rahoituspalveluyrityksen tietoturvajohtaja ja varapääjohtaja sanoo hänen tiiminsä tajunneen tarpeen uudelle tietoturva-arkkitehtuurille jo vuosia sitten, kun se aloitti pilvipohjaisten resurssien laajemman käytön ja työntekijät käyttivät entistä enemmän mobiililaitteita.

"Tajusimme, että perinteinen muureihin ja estämiseen perustuva tietoturva-arkkitehtuuri, johon olimme luottaneet aiemmin, ei suojaisi meitä hyökkääjiltä enää jatkossa", hän kertoo.

Tämä todellisuus löi toden teolla vasten kasvoja alkuvuodesta 2020, kun yritys huomasi, että edellisenä vuonna hyökkääjä oli päässyt tunkeutumaan yrityksen ympäristöön ja kyenneen toimimaan siellä huomaamatta. "Tarvitsimme uuden arkkitehtuurin, jolla kykenisimme suojaamaan resurssit ja todentamaan niiden käytön sijainnista riippumatta, ja Zero Trust -arkkitehtuuri on suunniteltu juuri tätä varten."

CSO Microsoft Security

Esteitä Zero Trust -käyttöönotolle

Monille organisaatioille Zero Trust on perustavanlaatuinen muutos tietoturvan rakenteeseen, prosesseihin ja ajattelutapaan. Tämä selittää osaltaan joitain esteistä, jotka täytyy ylittää ennen sen käyttöönottoa.

"Organisaatiossamme oli lopulta todella paljon eri siiloja", asiakaspalvelukeskuksen tietoturvajohtaja sanoo. Hän myös kertoo, että palvelin-, verkko- ja tietokantatiimeillä täytyi lopulta kaikilla olla omat verkkopalvelimensa ja työkalunsa sekä niiden varmistukset. "Tämä hidasti meitä, koska kaikilla oli eri ajatus siitä, mihin tulisi edetä ja miten."

Mikä estää Zero Trustin käyttöönottoa?

Lähde: Zero Trust Adoption Survey -kysely, maaliskuu 2022, Foundry. Vastaajien määrä: 250

CSO Microsoft Security

Microsoftin Zero Trust -tuotepäällikön Anthony Mocnyn mukaan tällaisten ongelmien esiin tuominen ja ratkaiseminen saattaa olla yksi Zero Trustin myönteisistä seurauksista. "Arkkitehtuurina Zero Trust on suunniteltu rikkomaan tietoturvatiimien siiloja eri tekniikkapinoissa ja auttaa tiimejä työskentelemään yhdessä entistä yhtenäisemmin", hän kertoo. "Tämä saattaa tarkoittaa myös kulttuurin muutosta siinä, miten tiimit työskentelevät yhdessä."

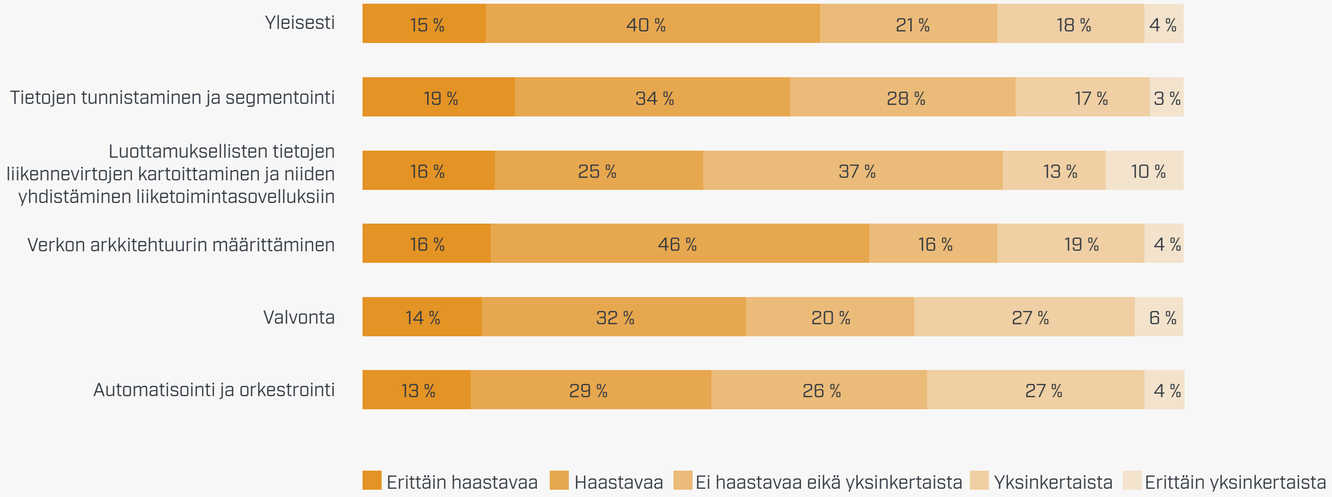
Rahoituspalveluyrityksen tietoturvajohtajan mukaan erään esteen Zero Trust -polulla muodostivat vanhat sovellukset. "Niihin täytyy sisällyttää nykyaikaista todennustekniikkaa", hän sanoo. "Sovellusten iästä riippuen tämä ei välttämättä ole kovinkaan helppoa."

CSO Microsoft Security

Käyttöönoton haasteet

Kun yritys lähtee Zero Trust -polulle, se kohtaa väistämättä esteitä toteutuspolullaan. Yli puolet (56 %) kyselyyn vastaajista kertoi, että Zero Trustin toteuttaminen oli haastavaa tai erittäin haastavaa. Haasteita aiheuttivat erityisesti seuraavat asiat:

Miten vaikeaa Zero Trustin toteutus on?



Lähde: Zero Trust Adoption Survey -kysely, maaliskuu 2022, Foundry. Vastaajien määrä: 168

CSO Microsoft Security

Tarkemmissa haastatteluissa kävi usein ilmi haasteita liittyen segmentointiin ja mikrosegmentointiin.

"Verkko segmentoidaan aina yksittäiseen isäntään saakka", sanoo rahoituspalveluyrityksen tietoturvajohtaja. "Se on kuin laittaisi pienen palomuurin sisäisen verkon jokaisen isännän väliin, jotta näet kaiken liikenteen ja voit hallita sinä aina yksittäisten koneiden tasolla. Tämä tuo merkittäviä etuja tietoturvaan, mutta sen toteutus on todella vaikeaa, koska se edellyttää käytännössä kymmenien tuhansien palomuurien hallintaa."

Liikenteen kartoittaminen voi myös olla useiden kuukausien prosessi. 5 000 työntekijän julkaisu- ja mediayrityksen tietohallintojohtaja kertoo, että tärkeiden suojattavien tietojen, sovellusten ja verkkopalveluiden määrittämisen jälkeen he "kartoittivat verkon tapahtumakulut ja yrittivät ymmärtää niitä tietojen joukkoina". "Sitten segmentoimme osia näistä tiedoista ja siitä, miten ne todella kulkevat verkossa, jopa yksittäisten tietopakettien tasolle." Tässä vaiheessa yritys käytti Zero Trust -käytäntöjä eri liikennetyypeissä. "Kehitimme myös uusia toimintoja verkon valvontaan ja ylläpitoon."

Haasteista huolimatta monet vastaajat uskovat Zero Trustin yksinkertaistavan lopulta päivittäistä toimintaa. Perinteisillä tekniikoilla "muutosten tekeminen kestää päiviä, ne täytyy lähettää kaikkiin laitteisto- ja ohjelmistokomponentteihin, ja käytämme tähän paljon resursseja", kertoo rahoituspalveluyrityksen tietoturvajohtaja. "Kun tarkastelimme Zero Trustia, huomasimme, että se todella minimoi arkkitehtuurin monimutkaisuutta pitkällä aikavälillä ja edellyttää vähemmän työntekijöitä samojen hommien hoitamiseen."

CSO Microsoft Security

Zero Trust -toteutuksen parhaat käytännöt

Kun entistä useammat yritykset ottavat käyttöön Zero Trust -arkkitehtuurin, ne luovat toteutussuunnitelmia ja parhaita käytäntöjä, joita muutkin voivat noudattaa. Tässä on viisi huomioitavaa seikkaa, kun suunnittelet käyttöönottoa.

Älä haukkaa heti alussa liian suurta palaa

Zero Trust -strategioiden laatiminen voi tuntua pelottavalta urakalta, jos katsot sitä vain laajasta kontekstista, jossa sinun täytyy uudistaa käytännöt ja suojaukset verkoille, tiedoille, sovelluksille, käyttäjätiedoille, päätepisteille ja infrastruktuureille. "Alussa se näytti vain valtavalta vuorelta, jolle meidän täytyisi kiivetä, emmekä oikein meinanneet uskoa kykyihimme", sanoo korkeakoulun tietohallintojohtaja. "Täytyy vain edetä askel kerrallaan."

Tietohallintojohtaja ja hänen tiiminsä omaksuivat lopulta Seuraa rahaa -lähestymistavan, jossa he priorisoivat talous- ja palkanmaksusovellusten segmentoinnin erillisessä verkossa.

Tärkeimpien suojattavien resurssien tunnistaminen on Mocnyn mukaan järkevä lähestymistapa. "Muista syy, miksi olet ottamassa Zero Trustia ylipäätään käyttöön", hän muistuttaa.

Jos epäilyttää, aloita monimenetelmäisyydestä

Kun priorisoit tietoturvapinoa, monet tietoturvajohtajat ja tietoturvatoimittajat suosittelevat keskittymistä aluksi todentamiseen ja muihin käyttäjätietopohjaisiin suojauksiin. "Jos et tiedä mistä aloittaa, monimenetelmäinen todennus on aina hyvä paikka aloittaa", Mocny sanoo. Microsoft arvioi, että monimenetelmäinen todennus voi estää yli 90 prosenttia käyttäjätietopohjaisista hyökkäyksistä.

Rahoituspalveluyrityksen tietoturvajohtaja on samaa mieltä. "Todennus on keskeinen elementti Zero Trust -arkkitehtuurin toteutuksessa. Mitkään muut komponentit eivät toimi, jos et voi vahvistaa loppukäyttäjän henkilöllisyyttä, joten aloitimme siitä."

Seuraavaksi rahoituspalveluyrityksen tietoturvajohtaja siirtyi verkkokomponentin pariin, mikä toikin välittömästi etuja etätyöntekijöiden tukemiseen. Tiimi jätti mikrosegmentoinnin odottamaan myöhempään, koska se ei ole helposti nähtävillä yritykselle yleisesti. "Kun se on tehty, tietoturva on merkittävästi parempi, mutta kukaan ei huomaa eroa", hän huomauttaa.

CSO Microsoft Security

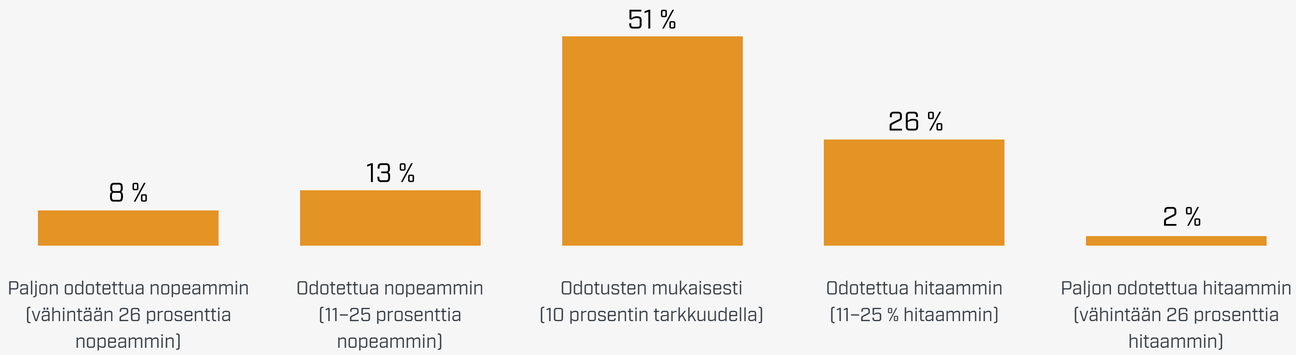
Laadi realistinen aikataulu

On tärkeää, että tietoturvajohtajat asettavat realistisia odotuksia Zero Trust -käyttöönotoille. "Zero Trust -arkkitehtuurin toteutus on ohjelma, ei projekti", sanoo rahoituspalveluyrityksen tietoturvajohtaja. "Tämä oli valtava muutos. Sen tekeminen oikein edellyttää useita vuosia – ja se kestää todennäköisesti vuosia. Zero Trust -arkkitehtuuria ei voi toteuttaa nopeasti ja helposti."

Toinen yritysjohtaja talousalalta on samaa mieltä. "En usko, että saamme kaikkea koskaan valmiiksi, sillä uutta tekniikkaa tulee koko ajan, uusia haittaohjelmia ja uusi uhkia ilmaantuu myös koko ajan", hän muistuttaa.

Valtaosa kyselyn vastaajista (72 %) sanoo aikataulun pitäneen tai valmista tulleen jopa etuajassa. Lopuilla vastaajista toteutus kesti odotettua kauemmin.

Täyttääkö Zero Trust aikataulutavoitteesi?



Lähde: Zero Trust Adoption Survey -kysely, maaliskuu 2022, Foundry. Vastaajien määrä: 168

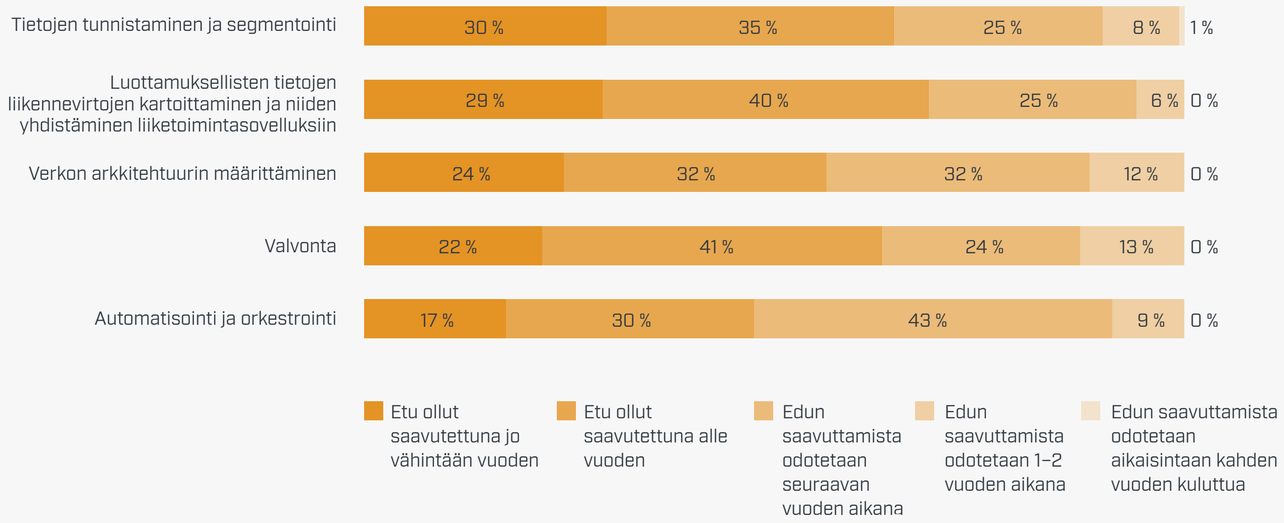
CSO Microsoft Security

Mittaa matkan varrella

Vaikka Zero Trust -käyttöönotto on käynnissä, tietoturvajohtajat voivat ja heidän tulisi luoda välitavoitteita edistymisen mittaamiseksi. On hyvä merkki, että noin kaksi kolmasosaa vastaajista sanoi saavuttaneensa etuja projektin useimmilla osa-alueilla jo vuoden kuluessa. Näin neljännes taas odottaa saavuttavansa etuja seuraavan vuoden aikana muun muassa tietojen tunnistamisen ja segmentoinnin, liikenteen kartoittamisen ja verkon arkkitehtuurin määrittämisen kaltaisilla tärkeillä osa-alueilla.

"Zero Trust on jatkuva prosessi, polku, koska muuttuvilta hyökkäyksiltä suojautuminen edellyttää jatkuvaa arviointia", Mocny sanoo. "Pidä aina silmät auki parannuksille."

Aikajana Zero Trust -etujen saavuttamiselle



Lähde: Zero Trust Adoption Survey -kysely, maaliskuu 2022, Foundry. Vastaajien määrä: 103

CSO Microsoft Security

Keskity ihmisiin, älä pelkkään tekniikkaan

Zero Trust -tietoturvamallin laaja kattavuus tarkoittaa sitä, että se vaikuttaa kaikkiin työntekijöihin, myös sen käyttöönotosta vastaaviin IT- ja tietoturvatiimeihin. Siksi, kuten missä tahansa suuressa teknisessä projektissa, on tärkeää varmistaa, että käyttöönotot ovat synkronoituja uusien prosessien kanssa. Muutostenhallintakäytännöt takaavat sujuvan ja onnistuneen käyttöönoton.

"Teknisen muutoksen lisäksi myös kulttuuri muuttuu", Mocny kertoo. "Jos sinulla on useita tiimejä tietoturvan parissa, esimerkiksi verkkoarkkitehteja ja käyttäjätietoasiantuntijoita, sinun täytyy muuttaa myös tapaa, jolla nämä tiimit työskentelevät yhdessä. Sinun täytyy murtaa siilot ja varmistaa, että kaikki tekniikka toimii yhtenäisesti."

Siilojen murtaminen tarkoittaa eri alojen tiimien saamista tiiviisti mukaan pilotointiin ja konseptin toimivuustarkistusprojekteihin. Noin 2 000 työntekijän tietoliikenneyrityksen IT-johtaja oppi tämän kantapään kautta, kun käyttöönotossa epäonnistuttiin useissa asioissa: palveluiden todentaminen ei esimerkiksi onnistunut, jolloin niihin ei luotettu – ja jotkin järjestelmät eivät tämän vuoksi olleet käytettävissä ollenkaan.

"Yhden palvelun käyttöönotolla voi olla dominovaikutus: se voi kaataa muita palveluita", hän kertoo. Jatkossa "aiomme olla paljon varovaisempia, testaamme konseptin paremmin, teemme enemmän tarkistuksia ja käymme arkkitehtuurin läpi asiantuntijoiden kanssa ennen käyttöönottoa."

Zero Trust -investoinnin tuotto

Vuonna 2021 tilattu **Forrester Consulting Total Economic Impact™ -tutkimus** kvantifioi Microsoft Zero Trust -ratkaisujen kustannussäästöt ja liiketoiminnalliset edut. Viiden Forresterin haastatteleman suuryrityksen perusteella yhdistelmäorganisaatio sai kolmessa vuodessa sijoitetulle pääomalle tuottoa 92 prosenttia toteuttamalla Zero Trust -arkkitehtuurin Microsoftin avulla.

Tällainen yhdistelmäorganisaatio säästi keskimäärin lisäksi noin 20 dollaria per työntekijä kuukaudessa, kun Zero Trustin ansiosta ei enää tarvittu monia tietoturvatyökaluja, esimerkiksi päätepistehallintaratkaisuja, virustorjuntaratkaisuja ja haittaohjelmien torjuntaratkaisuja.

CSO Microsoft Security

Miten Zero Trust -polkusi etenee?

Kuten kysely osoittaa, Zero Trust -tietoturvamallin edut ovat selkeästi suurempia kuin ne käyttöönoton haasteet, joita tietoturvajohtajat ja heidän tietoturvatiiminsä joutuvat kohtaamaan. Näiden haasteiden kohtaaminen tarkkaan mietityn suunnitelman avulla voi auttaa organisaatiotasi parantamaan suojausta nopeasti, pienentämään riskejä sekä tuottamaan lisäarvoa koko yrityksessä.

Jos haluat arvioida organisaatiosi Zero Trust -kypsyystasoa ja tutustua käytännöllisempiin käyttöönottoresursseihin, suorita Microsoftin **Zero Trust -mallin kypsyysarviointi**.