



Microsoft 365
Copilot

Tietoturvan varmistaminen tekoälyn aikakaudella

Opas IT-johtajille

E-kirja



Tämä opas on IT-johtajille, joiden on edistettävä tekoälyn omaksumista ja varmistettava organisaation datan tietoturvallisuus. Se auttaa sinua ymmärtämään tekoälyn aiheuttamat riskit datan tietoturvalle ja yksityisyydelle sekä tarjoaa analytiikkaa, jonka avulla voit johtaa yrityksesi tekoälytransformaatiota luottavaisin mielin.

Sisällysluettelo

01

Tekoälypohjaisen työn
uudet säännöt

02

Tekoälyn vaikutus
datasuojaukseen

03

Varjotekoälyn
haaste

04

BYOAI-todellisuus

05

Säätelyviidakko

06

Tietoturvakeskeinen
kehys tekoälyratkaisujen
arviointiin

07

Microsoft 365 Copilot:
Luotettava tekoäly

08

Tietoturvallinen polku
tekoälytransformaatioon

01

Tekoälypohjaisen työn uudet säännöt

Generatiivinen tekoäly avaa uusia mahdollisuuksia innovaatioihin ja auttaa tiimejä työskentelemään nopeammin ja fiksummin kuin koskaan aiemmin. Edistyksellisille organisaatioille tekoäly ei ole vain uusi teknologiatrendi – se on liiketoiminnan välttämättömyys. Se on keskeistä toiminnassa, lisäarvon tuottamisessa ja kilpailuedun säilyttämisessä.

Tämä nopea omaksuminen tuo kuitenkin mukanaan uusia ja entistä suurempia haasteita, joita IT-johtajien on ennakoitava ja hallittava. Tekoälyjärjestelmät voivat hakea ja yhdistää tietoa koko dataekosysteemistä. Tämä kasvattaa tietoturvariskejä perinteisiin työkaluihin verrattuna. Tekoälyn nopeasta laajenemisesta huolimatta vain **1 %** organisaatioista on täysin integroitunut tekoälyyn työnkuluissaan asianmukaisilla suojausprotokollilla.¹ Kun otat alusta alkaen käyttöön vankat suojaus- ja hallinnointikäytännöt tekoälyprosessissasi, tiimisi voi suojata arkaluontoisen datan, täyttää säännösvaatimukset ja turvata organisaation tiedot – samalla mahdollistaen innovaatioiden syntymisen.

Tekoälyn omaksumisaalto on jo täällä



02

Tekoälyn vaikutus datasuojaukseen

Ennen kuin siirrytään yksittäisiin haasteisiin, on tärkeää ymmärtää, miten tekoäly mullistaa tietoturva-ympäristön. Toisin kuin perinteinen ohjelmisto, joka käyttää dataa vain erikseen käskettynä, generatiivinen tekoäly käsittelee, analysoi ja tuottaa sisältöä aktiivisesti kaiken saamansa datan pohjalta.

Tämä ero on merkittävä monesta syystä:

- Tekoälytyökalut löytävät datasta yhteyksiä, jotka ihmisiltä voivat jäädä huomaamatta
- Ne voivat yhdistää tietoja automaattisesti useista lähteistä
- Ne voivat generoida uutta sisältöä, joka sisältää elementtejä arkaluontoisista syötteistä

Perinteisiä suojaustyökaluja ei todennäköisesti ole suunniteltu näillä valmiuksilla. Vaikka perinteinen ohjelmisto käyttää dataa ennalta-arvattavasti, tekoäly voi edetä yllättävin tavoin tietoekosysteemissäsi ja tuoda arkaluontoista dataa esille tavoilla, joita et ole osannut ennakoida.

Tämä perustavanlaatuinen muutos edellyttää tietoturvaan ja datahallintaan uusia lähestymistapoja, jotka keskittyvät siihen, miten tekoäly toimii organisaatiosi tietoresurssien kanssa.

03

Varjotekoälyn haaste

Olitpa tekoälyn omaksumisen prosessin missä vaiheessa tahansa, työntekijäsi etsivät jo omia ratkaisujaan ja luovat niin sanottua varjotekoälyä.

Tämä luvaton käyttö aiheuttaa merkittäviä katvealueita tietoturva-asemassasi. Kun työntekijät jakavat yrityksen dataa ulkoisiin tekoälyjärjestelmiin, he ohittavat olemassa olevat tietoturvamekanismit ja luovat haavoittuvuuksia, joihin useimmat organisaatiot eivät ole varautuneet.

Varjotekoäly ei ole pelkkä tietoturvariski – se voi kertoa organisaation täyttämättömistä tuottavuustarpeista. Kun työntekijät turvautuvat luvattomiin työkaluihin, he osoittavat, missä viralliset järjestelmät eivät vastaa heidän tarpeitaan. Varjotekoälyn hallinta edellyttää vahvempaa hallinnointia ja parempia tuottavuusratkaisuja.



Miksi varjotekoäly syntyy:

- Työntekijät haluavat parantaa tuottavuuttaan hyödyntämällä tekoälyn vaikuttavia ominaisuuksia
- Päivittäinen työtaakka ylittää yhä useammin käytettävissä olevan ajan ja energian
- Tiimit kokevat yhä kovempaa painetta saada aikaan enemmän samoilla resursseilla
- Kuluttajien tekoälytyökalut tuovat heti käyttöön ratkaisuja ilman hyväksyntäesteitä
- Viralliset IT-hankintaprosessit eivät pysy innovaatiokehityksen vauhdissa

Varjotekoälyn riskit:

- Ei näkyvyyttä siihen, mitä yrityksen dataa ulkoiset tekoälyjärjestelmät käsittelevät
- Ei takuuta siitä, ettei arkaluontoista tietoa säilytetä
- Ei yhdenmukaisia tietoturvastandardeja eri tekoälyalustoilla
- Ei auditoitavuutta vaatimustenmukaisuustarkoituksiin
- Ei integraatiota nykyiseen tietoturvainfrastruktuuriin

A close-up photograph of a person's hands typing on a silver laptop keyboard. The person is wearing a red ribbed sweater. The background is a soft, out-of-focus white surface.

Pohdi tätä skenaariota:

Talousanalyytikko, jolla on vaikeuksia monimutkaisen laskentataulukon kanssa, lataa sen luvattomaan tekoälytyökaluun saadakseen apua. Tämä taulukko sisältää asiakkaiden talousdataa, sisäisiä mittarilukuja ja ennusteita. Vaikka analyytikko saa tarvitsemansa avun, organisaatiosi arkaluontoinen talousdata on nyt yrityksen tietoturvarajojen ulkopuolella. Se on täysin valvontajärjestelmiesi näkymättömissä.

04

BYOAI-todellisuus

Ilman selkeää johtoryhmän ohjeistusta työntekijät ottavat tekoälyn omaksumisen yhä useammin omiin käsiinsä – **78 %** tekoälyn käyttäjistä hyödyntää työssään BYOAI-mallia.² Tämä korostuu erityisesti pienissä ja keskisuurissa yrityksissä, joissa **80 %** työntekijöistä toimii näin.²

Tällä luvattomalla toimintatavalla on merkittäviä haittoja. Työntekijät salaavat usein tekoälyn käytön – **52 %** ei halua myöntää tekoälyn hyödyntämistä tärkeissä tehtävissä, ja **53 %** pelkää, että tekoälyn käyttö saa heidät näyttämään helposti korvattavilta.² Salailu estää organisaatioita hyödyntämästä tekoälyä täysimääräisesti ja aiheuttaa vakavia tietoturva- ja suojausriskejä ympäristössä, jossa johtajat pitävät kyberturvaa ja tietosuojaa **ykköshuolenaan**.²

Koska tekoäly on laajassa käytössä ja sen kasvu on väistämätöntä, kyse ei ole siitä, otetaanko tekoäly organisaatiossa käyttöön – vaan siitä, miten tarjota tietoturvallinen ratkaisu, joka vastaa työntekijöiden tarpeisiin ja suojaa organisaation dataa.

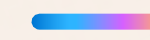
05

Sääntelyviidakko

Tietosuoja ja tietoturvan lainsäädäntö ja sääntely tuovat tekoälyn käyttöönottoon lisää kerroksia ja monimutkaisuutta. Vaikka jotkin viitekehykset on tehty erityisesti tekoälyn hallintaan, toiset soveltuvat laajemmin mutta vaikuttavat silti tiedon käsittelyyn – rikkomuksista seuraavat rangaistukset ovat yhä ankaria.

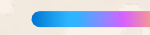
Kun työntekijäsi käyttävät tekoälytyökaluja ilman riittävää valvontaa, he voivat huomaamattaan rikkoa vaatimustenmukaisuutta. Tekoäly kasvattaa tätä riskiä, koska se voi käyttää, yhdistellä ja paljastaa säänneltyä tietoa tavoilla, joihin perinteiset teknologiat eivät pysty.

Keskeiset säädökset, jotka vaikuttavat tekoälyn käyttöön:



EU:n yleinen tietosuoja-asetus

Euroopan unionin yleinen tietosuoja-asetus antaa ihmisille oikeuden hallita henkilötietojaan ja vaatii selkeän suostumuksen niiden käsittelyyn.



EU:n tekoälylaki

Euroopan unionin laaja kehys, joka säätelee tekoälyjärjestelmiä niiden riskitason mukaan.



HIPAA

Tämä Yhdysvaltain liittovaltion laki terveydenhuollosta asettaa tiukat vaatimukset suojattujen terveystietojen käsittelyyn.



NIST AI Risk Management Framework

Tämä Yhdysvaltain vapaaehtoinen ohjeistus auttaa organisaatioita hallitsemaan riskejä tekoälyjärjestelmien suunnittelussa, kehityksessä ja käyttöönotossa.

Tekoälyn vaatimustenmukaisuusriskit:

- Asiakastietoja käsitellään palvelimilla hyväksytyjen alueiden ulkopuolella
- Henkilötietoja käytetään ilman asianmukaista suostumusta
- Arkaluontoista tietoa säilyy järjestelmissä ilman asianmukaisia säilytyksen hallintamekanismeja
- Ei kirjausketjua suojattujen tietojen käytöstä ja käsittelystä
- Tekoälyn generoima sisältö, joka rikkoo alakohtaisia säännösvaatimuksia

Nämä rikkomukset voivat aiheuttaa vakavia seurauksia:

- Suuret taloudelliset sanktiot (EU:n yleisen tietosuoja-asetuksen sakot voivat olla jopa **4 %** globaalista liikevaihdostasi)⁴
- Vaatimukset tietomurroista ilmoittamiseen asianomaisille
- Kanne asianomaisilta
- Vahinko yrityksesi maineelle ja asiakkaiden luottamukselle

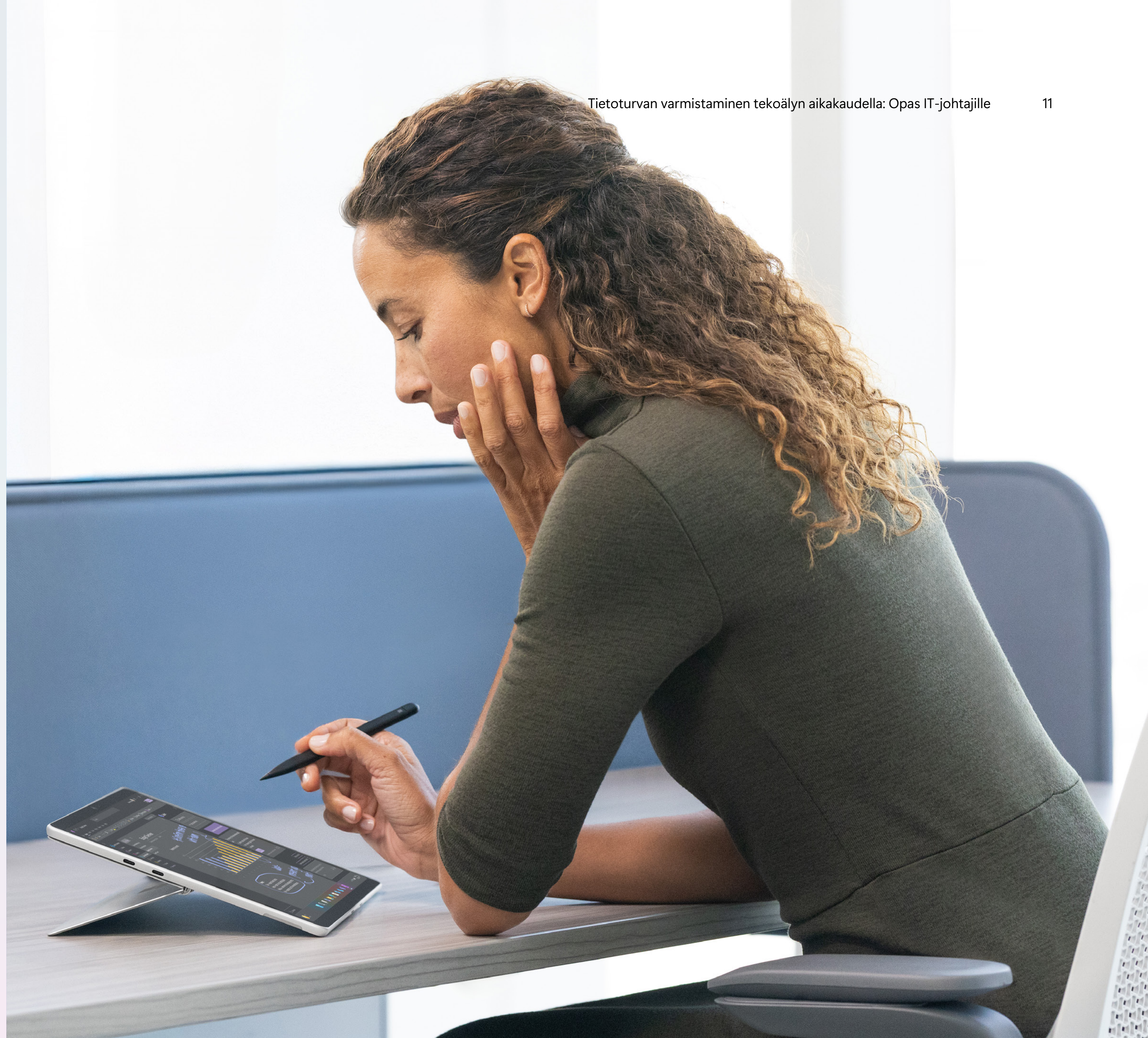
Tekoälyn käytön kasvaessa organisaatiossa tarvitset hallinnointia, joka tukee tehokasta työskentelyä ja varmistaa organisaation vaatimustenmukaisuuden liiketoimintaan ja asiakkaisiin vaikuttavien säädösten kanssa.

06

Tietoturvakeskeinen kehys tekoälyratkaisujen arviointiin

Varjotekoäly, BYOAI ja sääntely tuovat merkittäviä riskejä. Tarvitset rakenteisen tavan arvioida tekoälyratkaisuja, jotta ne tukevat organisaatiosi innovaatiota, suojaavat arkaluontoista dataa ja varmistavat vaatimustenmukaisuuden muuttuvien säädösten kanssa.

Seuraava viitekehys sisältää kuusi yksinkertaista kysymystä, joiden avulla arvioit, täyttääkö tekoälyalusta molemmat vaatimukset.



Kysymys 1

Tarjoaako se suuryritystasoista tietoturvaa alusta lähtien?

Oikealla ratkaisulla suojaus muuttuu reaktiivisesta ongelmien korjaamisesta proaktiiviseksi haavoittuvuuksien etsinnäksi organisaation datasta – jo ennen kuin niistä kehittyvät suurempia ongelmia.

Kysymys 2

Voiko ratkaisu helposti omaksua ja tehostaa olemassa olevia tietoturvamekanismeja?

Organisaatiosi tietoturvakäytäntöjen tulee toimia saumattomasti tekoälyn kanssa. Tekoälyratkaisujen toimittajan tulee kunnioittaa olemassa olevia tietoturvakehyksiä ja integroitua niihin – eikä edellyttää kokonaan uusien luomista.

Etsi ratkaisuja, jotka täyttävät seuraavat kriteerit:

- Reaaliaikaisen näkyvyys koko dataekosysteemiisi
- Mahdollisten datariskien automaattinen tunnistus ennen kuin niistä tulee ongelmatapauksia
- Arkaluontoisten tietojen suojaus kaikilla tasoilla

Etsi ratkaisuja, jotka täyttävät seuraavat kriteerit:

- Nykyisten tietoturvakäytäntöjesi, arkaluontoisuustunnisteidesi ja tietosuoja-asetustesi saumaton omaksuminen
- Tarkan käyttöoikeuksien valvonnan soveltaminen yksilötasolla, jotta kukaan käyttäjä ei pääse dataan, johon hänellä ei tulisi olla pääsyä
- Aktiiviset merkinnät yrityksistä kiertää käyttöoikeuksien valvontaa

Kysymys 3

Sisältääkö ratkaisut sisäiset hallinnointiin ja tietosuojaan liittyvät hallintamekanismit?

Koska tekoälytyökalut toimivat proaktiivisemmin, tietoturvatoimienkin on oltava proaktiivisia. Vahva datahallinnointi asettaa selkeät rajat, joiden sisällä työntekijäsi voivat innovoida turvallisesti vaarantamatta arkaluontoista dataa.

Etsi ratkaisuja, jotka täyttävät seuraavat kriteerit:

- Tekoälyn hallinnoinnin keskittäminen automatisoidulla käytäntöjen valvonnalla kaikissa toiminnoissa
- Mahdollisen datan ylijakamisen varhainen tunnistus
- Tekoälyn käytön linjaaminen sääntelyvaatimusten kanssa vaatimustenmukaisuuden varmistamiseksi

Kysymys 4

Voidaanko ratkaisu ottaa yhdenmukaisesti käyttöön koko organisaatiossa?

Työntekijöillääsi on omat työskentelytapansa ja aikataulunsa, ja he voivat työskennellä missä päin maailmaa tahansa. Tekoälyn tulee hyödyttää kaikkia.

Etsi ratkaisuja, jotka täyttävät seuraavat kriteerit:

- Vaivaton käyttöönotto ja tekoälyn omaksumisen helppous arjen työnkuluissa
- Joustava pääsy – maksuttomasta tekoälykeskustelusta skaalautuviin agenttiratkaisuihin
- Työntekijöiden auttaminen tekoälytaitojen kehittämisessä ja tekoälyn integroinnissa osaksi työtä

Kysymys 5

Integroituuko ratkaisu saumattomasti olemassa oleviin kehyksiin?

Yritykselläsi on oma digitaalinen infrastruktuuri: ohjelmistot, sovellukset ja muut työkalut.

Etsi ratkaisuja, jotka täyttävät seuraavat kriteerit:

- Saumaton yhdistyminen työkaluihisi ja ohjelmiisi häiriöiden minimoimiseksi
- Yhtenäinen tekoälykokemus kaikissa sovelluksissa, jolloin työt siirtyvät sujuvasti työkalusta toiseen
- Tehtävien automatisointi ja optimointi nykyisissä työnkuluissa

Kysymys 6

Onko käyttäjillä paremmat valmiudet innovoida?

Tekoälyn tulisi uudistaa työnteon tavat. Kyse ei ole vain automaatiosta vaan tuottavuuden tehostamisesta ja innovoinnin vauhdittamisesta.

Etsi ratkaisuja, jotka täyttävät seuraavat kriteerit:

- Ajanhukan muuttaminen sujuvoitetuiksi prosesseiksi
- Toistuvien tehtävien automatisointi
- Työntekijöiden valmiuksien parantaminen ajan säästämiseksi ja tärkeimpiin asioihin keskittymiseksi

07

Microsoft 365 Copilot: Luotettava tekoäly

Microsoft 365 Copilot on generatiivinen tekoälyratkaisu, joka tarjoaa vankan tietoturvan, hallinnoinnin ja käyttöoikeuksien valvonnan – varmistaen tietoturvallisen käyttöönoton ja jatkuvat innovaatiot. Se tehostaa tuottavuutta intuitiivisilla työkaluilla, kuten Copilot Chat, joka toimii siellä missä sinäkin, ja Copilot Studio, jossa tiimisi voi laatia mukautettuja tekoälyagentteja ilman koodausosaamista.

Copilot integroidaan saumattomasti Microsoft 365 -ympäristösi. Se perii käyttäjäoikeudet, arkaluontoisuustunnisteet, datahävikin estokäytännöt ja maantieteelliset datasijaintivaatimukset – ilman lisäasetuksia. Upottamalla tekoälyn työntekijöiden jo käyttämiin työkaluihin Copilot vähentää tietoturvariskejä ja pitää datan luotetussa Microsoft 365 -ympäristössä.

Microsoftin sitoumukset takaavat, että organisaatiosi säilyttää hallinnan:

- Datasi ovat suojattuna tallennettuna ja siirrettäessä
- Dataasi ei käytetä tekoälymallien koulutukseen
- Sinä päätät, mitä tietoja tallennetaan pilveen
- Olet suojassa tekoälyn tietoturva- ja tekijänoikeusriskeiltä

Erikoissuunnitellut hallinnointityökalut, kuten Copilot Control System ja SharePoint Advanced Management, tarjoavat IT-tiimeille tarvittavan näkyvyyden, hallintamekanismit ja auditointilokit vaatimustenmukaisuuden ylläpitämiseen.

Microsoft 365 Copilotin ansiosta sinun ei tarvitse valita innovaation ja tietoturvan välillä – saat molemmat.

Tietoturvallinen polku tekoälytransformaatioon

Tekoälyvallankumous tarjoaa IT-johtajille ainutlaatuisen mahdollisuuden tuottaa strategista lisäarvoa tasapainottamalla innovaatiot ja tietoturvan.

Ottamalla käyttöön tietoturvallisia tekoälyratkaisuja, kuten Microsoft 365 Copilotin, parannat työntekijöiden valmiuksia ja tuottavuutta sekä poistat varjotekoälyn riskit. Tie eteenpäin on innovaatioiden tietoturvallinen mahdollistaminen. Johtoryhmäsi rooli tietoturvallisen tekoälyn omaksumisessa nostaa IT-osaston uudistuksen mahdollistajaksi. Tämä tukee organisaatiosi menestystä uudella aikakaudella ja varmistaa, että data pysyy suojattuna ja vaatimustenmukaisena.



Ota käyttöön Microsoft 365 Copilot

Lähteet:

¹"Superagency in the workplace: Empowering people to unlock AI's full potential", McKinsey & Company, 28.1.2025. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work>.

²"Tekoäly on otettu työssä käyttöön. Suurin työ on kuitenkin vielä edessä." Microsoftin Työtrendien indeksi, 8.5.2024. <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>.

³"Onko tekoälystä hyötyä?", Microsoftin Työtrendien indeksi, 9.5.2023. <https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>.

⁴"Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27.4.2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä henkilötietojen vapaan liikkuvuuden turvaamisesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)", Euroopan parlamentti ja Euroopan unionin neuvosto, 27.4.2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.