
Windows 11 Pro

# Täydellinen tietoturvasuunnitelma hybridityöpaikalle

# Kyberturvallisuus on päällimäisenä mielessä kun 88 % tutkituista pk-yrittäjistä on riittämättömästi valmistautuneita selviämään kyberuhista.[1]

**Seuraavassa on joitakin tapoja, joilla suojattu ja tulevaisuuteen valmis IT-infrastruktuuri auttaa suojaamaan yritystäsi kyberuhilta:**

## Omaksu nollaluottamuksen periaate

Nollaluottamuksen suojausperiaate vähentää riskejä tarkistamalla poikkeuksetta jokaisen käyttöpyynnön tietopisteet, kuten käyttäjän henkilöllisyyden, sijainnin ja laitteen kunnon. Varmennuksen jälkeen käyttäjillä ja laitteilla on rajoitettu pääsy vain tarvitsemiinsa resursseihin.

Nollaluottamuksen periaatteet ovat kolmitahoisia:

**1** Ensin varmennetaan yksiselitteisesti. Tämä tarkoittaa aina tehtävää todentamista ja valtuutusta kaikkien käytettävissä olevien tietopisteiden perusteella, mukaan lukien käyttäjätunnus, sijainti, laitteen kunto, palvelu tai työmäärä, tietojen luokittelu ja poikkeamat.

**2** Toiseksi, käytä vähiten etuoikeutettua käyttäjäprofilia, joka rajoittaa käyttöoikeuden oikea-aikaiseksi ja riittäväksi. Käytä lisäksi riskiperusteisia mukautuvia käytäntöjä ja tietosuojaratkaisuja sekä tietojen että tuottavuuden suojaamiseksi.

**3** Kolmanneksi, oleta tietomurtoja tapahtuvan. Omaksu toimintatapa, joka minimoi vaikutusalueen ja pääsyn eri segmentteihin. Tarkista päästä päähän -salaus ja paranna uhkien havaitsemista ja suojausta analytiikan avulla.

Nollaluottamuksen periaatteen toteuttamiseksi organisaatioiden onymmärrettävä omat tietonsa ja niiden sijaintipaikat.

Yritysten on tiedettävä tietojen arkaluonteisuuden taso ja altistumisen mahdolliset riskit määrittääkseen, mihin nollaluottamusta on sovellettava. Pilvipohjaisessa tallennuksessa ja pilvisovelluksissa, kuten sähköpostipalveluissa ja pilvitietojen tallennuksessa, nollaluottamuksen ympäristön luominen on järkevää ja ratkaisevan tärkeää riskien vähentämiseksi. Ilman tätä lähestymistapaa yrityksen salasanat, laitteet ja arkaluonteiset tiedot ovat väistämättä hyökkäysvaarassa.

## Ota käyttöön kehittyneitä todennusmenetelmiä

Tietoturvaloukkaukset ovat paljon todennäköisempiä, jos käyttäjän todennusmenetelmät vaarantuvat. Työntekijän laitteen luvaton käyttö mahdollistaa usein pahantahtoisen toimijan pääsyn organisaation koko verkkoon. Turvallinen tapa varmistaa se, että käyttäjät ovat keitä kertovat olevansa, on oleellinen nykypäivän hybridityöympäristössä. Monivaiheinen todentaminen voi auttaa paljon turvallisemman ympäristön luomisessa. Salasanat eivät enää yksinään riitä yhä kehittyneempien uhkien lieventämiseen, koska usein ne päätyvät helposti vääriin käsiin. Kaksivaiheisen todennuksen kaltaiset tekniikat yhdistettynä monien nykyaikaisten laitteiden, kuten Windows Hello yrityksille, biometrisiin tunnistusominaisuuksiin suojaavat organisaatioita ja niiden verkkoja entistäkin tehokkaammin kyberhyökkäyksiltä erityisesti silloin, kun verkkoja vahvistetaan nollaluottamuksen suojausstrategialla.

## Paranna laitteistoturvallisuutta

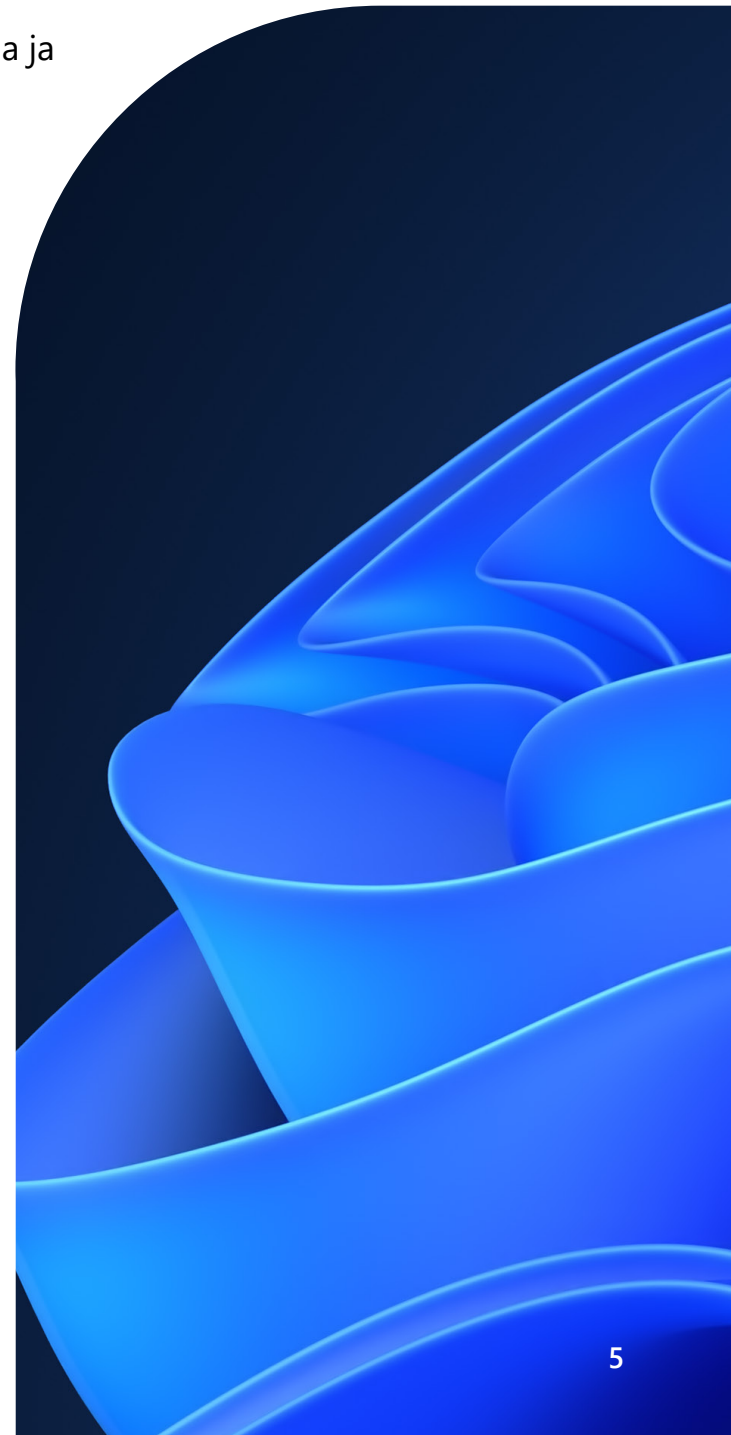
Pelkästään käyttöjärjestelmään ei voida luottaa, kun halutaan suojaa monilta erilaisilta työkaluilta ja tekniikoilta, joita verkkorikolliset voivat käyttää tietokoneen vaarantamiseen. Järjestelmän sisään päässeet tunkeutujat voivat asentaa vaikeasti poistettavia haittaohjelmia laiteohjelmistotasolla tai varastaa arkaluonteisia tietoja ja tärkeitä tunnistetietoja. Näiden tunkeutujien tunnistaminen voi olla vaikeaa heidän jo päästyään järjestelmään. Laitteisto- ja ohjelmistopohjaisten tietoturvasovellusten on oltava toisiaan tukevia. Nykyaikaiset uhat edellyttävät tietokonelaitteistoa, joka on suojattu siru- ja suoritintasolla ja joka suojaa arkaluonteiset liiketoimintatiedot juuri siinä paikassa, johon ne on tallennettu. On olemassa kokonaisia haavoittuvuusluokkia, jotka voidaan poistaa yksinkertaisesti laitteistotasolla sisäänrakennettujen tietoturvaominaisuuksien avulla.

Tällaisia ominaisuuksia on esimerkiksi kaikissa Windows 11 -tietokoneissa, joissa on suojattu ydin. Lisäksi suorituskykyä voidaan parantaa merkittävästi verrattuna samankaltaisten tietoturvaominaisuuksien käyttöönottoon pelkästään ohjelmistotasolla. Tämä parantaa järjestelmän yleistä tietoturvan tasoa vaarantamatta järjestelmän suorituskykyä.

## Käytä pääsynvalvonta-asetuksia identiteettipohjaisessa suojauksessa

Pilvipalveluissa järjestelmänvalvojat voivat hallita ja valvoa tunnistetietoja ja käyttöoikeuksia yhdestä sijainnista. Esimerkiksi Microsoft Azure Active Directoryn (Azure AD:n) avulla he voivat hallita keskitetysti henkilöstön identiteettejä sekä määrittää ja ottaa käyttöön sovellusten, toimipaikkojen ja ryhmien käyttöä koskevia käytäntöjä. Järjestelmänvalvojat voivat integroida vaatimustenmukaisuusvaatimuksia, ja uusia sääntöjä voidaan lisätä niiden tarpeen ilmetessä.

Pilvipohjaiset ohjausobjektit parantavat tietoturvaa ja parantavat vaatimustenmukaisuutta. Microsoftin tutkimusten mukaan monivaiheinen todennus voi yksinään estää yli 99,9 % tilin tietoturvahyökkäyksistä.[2] Ehdolliset käyttöoikeudet antavat järjestelmänvalvojille mahdollisuuden luoda toimintaan tai sijaintiin perustuvia sääntöjä, mikä vähentää hyökkääjien mahdollisuuksia hyödyntää haavoittuvuuksia. Esimerkiksi maan ulkopuolelta tulevat tai outoon aikaan saapuvat kirjautumisyritykset voidaan hylätä. Lisäksi järjestelmänvalvojat voivat ottaa käyttöön kertakirjautumisen, jolloin käyttäjät voivat käyttää sovelluksia turvallisesti missä tahansa ja samalla helpottaa salasanojen hallintaa IT-henkilöstön kannalta.



Microsoft esitteli hiljattain monipilvipalvelun tietoturvatuen. Yritykset voivat nyt ottaa käyttöön Azure Security Centerin monipilviresursseja, kuten Google Cloud Platformin (GCP) ja Amazon Web Servicesin (AWS) sekä suojata palvelimia Azure Defender for Servers -ratkaisulla Azure Arcin avulla.

## Suojaa etälaitteet

Microsoftin pilvipalvelut helpottavat laitteiden ja sovellusten hallintaa. Esimerkiksi Microsoft Intunella laitteiden käyttöönottoa voidaan hallinnoida turvallisesti ja kaukaa, samalla kun sovellukset voidaan helposti skaalata vaatimusten mukaan.

Microsoft Windows Autopilot käyttää suojausasetuksia ja muita ohjausobjekteja laitteiden suojaamiseen jo ennen kuin työntekijä muodostaa yhteyden resursseihin.

## Suojaa sovellukset

Paranna suojausta ei-luotettuja lähteitä vastaan avaamalla tiedostot ja sivustot eristetyssä säilössä Windows Defenderin sovellussuojan avulla. Pilvilähtöinen suunnittelu mahdollistaa helpon laajennettavuuden Microsoft 365:n, Microsoft Defender for Cloudin ja Microsoft Defender for Endpointsin avulla.[3]

Helpota tietoturvan hallintaa eri paikoissa ja laajenna suojaus pilviympäristöön. Suojaa laitteita, tietoja, sovelluksia ja käyttäjätietoja missä tahansa. Tee käyttöönotto luottavaisin mielin tietäen, että 99,6 % sovelluksista on yhteensopivia Windows 11:n kanssa.[4]

## Automatisoi tietoturvan ylläpito

Pilviperustaisten teknologioiden avulla IT-hallinnoijat voivat automaattisesti asentaa päivitykset, korjaustiedostot ja varmuuskopiot kaikille järjestelmille ja laitteille.  Tämä vähentää asennusvirheitä ja rajoittaa seisokkiaikaa suojellen järjestelmää samalla uusilta uhilta. Rutiinityöt voidaan automatisoida, jolloin järjestelmänvalvojat voivat keskittyä tärkeisiin tehtäviin, jotka todella vaativat heidän asiantuntemustaan.

# Pidä yrityksesi turvassa Windows 11 Pro -laitteilla

**Organisaation turvallisuustilanteen kehittäminen on ensisijaisen tärkeää, ja suojattujen laitteiden tarjoaminen työntekijöille on menestyksen kulmakivi. Uudet Windows 11 Pro -laitteet yhdessä Microsoft 365:n kanssa on suunniteltu turvallista hybridityötä varten.**

- Suojaa työntekijäsi haittaohjelmilta, viruksilta, tietojenkalasteluyrityksiltä, haitallisilta linkeiltä sekä auta pitämään liiketoiminnan kannalta tärkeät tiedot turvassa.

- Hanki kerroksittain laitteiden, tietojen, käyttäjätietojen, sovellusten ja pilvipalvelujen tinkimätöntä tietoturvaa.

- Yksinkertaista IT:tä yhtenäisillä, pilvipohjaisilla päätepisteiden hallintatyökaluilla, kuten Microsoft Endpoint Managerilla, Azure Active Directorylla ja Windows Autopilotilla. Määritä ja ota käyttöön IT-käytännöt etänä, hallitse sovelluksia ja käyttäjätietoja ja ota helposti käyttöön liiketoimintavalmiita laitteita.

- Voita etänä tehtävän yhteistyön esteet yhdellä ratkaisulla, joka sisältää muun muassa videoneuvottelut, tuottavuussovellukset ja tiedostojen jakamisen. Varmista työntekijöiden turvallinen pääsy tärkeisiin työsovelluksiin ja -tietoihin yhtenäisen yhteistyöratkaisun kautta.

- Dataintensiivisten alojen työntekijöille suojatut ydintietokoneet ovat turvallisimpia Windows-laitteita, ja niissä on kaikki Windows 11:n kehittyneet suojausominaisuudet, joita voidaan tarvita myös tietyissä liiketoimintaympäristöissä.

Vähennä kyberhyökkäysten riskiä merkittävästi korvaamalla ikääntyvät tietokoneet uusilla, nykyaikaisilla laitteilla, jotka on optimoitu suojausta ja hybridityötä varten. Windows 11 Pro ja Microsoft M365 tarjoavat tehokkaan ja käyttövalmiin suojauksen laitteille, tiedoille, sovelluksille, henkilötiedoille ja palveluille.

Windows 11 Pro



[1] *https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity*

[2] *https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/*

[3] *Myydään erikseen.*

[4] *App Assure -ohjelman tiedot lokakuusta 2018 helmikuuhun 2022. App Assure on työskennellyt vuodesta 2018 lähtien yhdessä tuhansien asiakkaiden kanssa ja arvioinut yli 1,1 miljoonaa sovellusta, joiden yhteensopivuusaste on 99,6 prosenttia. Jos haluat lisätietoja, käy App Assure -sivustossa ja tutustu Windows IT Pro -blogijulkaisuun App Assuressa*