

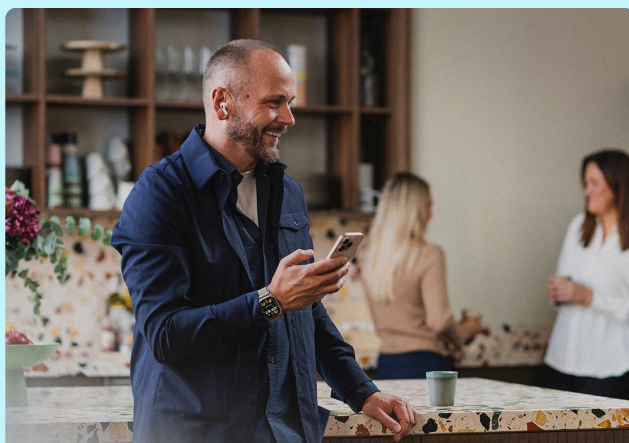
# Turvallista työtä iPhonella – älykäs hallinta, standardoitu tietoturva

## Miksi tietoturva ja hallinta kulkevat käsi kädessä?

Organisaatiot etsivät jatkuvasti keinoja suojata IT-ympäristöjään käyttäjäkokemuksesta tinkimättä. Tietoturvan ei koskaan pitäisi heikentää käytettävyyttä – ja juuri tämä on iPhone'n vahvuus. Sisäisillä tietoturvaominaisuuksilla ja tehokkailla hallintatyökaluilla varustettu iPhone on erittäin hyvä valinta organisaatioille, jotka haluavat yhdistää turvallisuuden ja tehokkuuden.

## Mitä Apple on luonut – ja kehittää edelleen

Tietoturva on iPhone'n ytimessä. Laitteistopohjainen suojaus, laitesalaus, turvallinen todentaminen ja sovellustason tietosuoja ovat iOS:n keskeisiä osia, ja niitä päivitetään jatkuvasti. Apple on edelleen markkinajohtaja tällä alalla, ja viime aikoina se on kehittänyt esimerkiksi Lockdown Moden, edistyneen tietojenkalastelun tunnistuksen ja parempia etäkäytön ohjaustyökaluja, jotka varmistavat, että alusta on valmiina kohtaamaan uudet uhat.



## Helppoa hallinnointia

MDM-ratkaisujen (Mobile Device Management), kuten Microsoft Intune, avulla organisaatiot voivat konfiguroida iPhone't automaattisesti, hallinnoida niitä etänä ja ottaa päivitykset käyttöön nopeasti. Silti monet yritykset kamppailevat sirpaleisen hallinnan tai manuaalisten prosessien kanssa. Ne johtavat helposti virheisiin ja tarpeettomaan työhön.

## Yleinen haaste:

IT-tiimit käyttävät yhä liikaa aikaa yksittäisten laitteiden asentamiseen tai vianmääritykseen, mikä johtaa viivästyksiin ja työntekijöiden turhautumiseen.



## Dustinin tarjoama tuki

Dustin auttaa organisaatioita ottamaan käyttöön mobiilin laitehallinnan (MDM) kosketuksettoman käyttöönoton, automaattisen konfiguroinnin ja vaatimustenmukaisuuden hallinnan.

## Lopputulos: Nopeampi perehdytys, parempi tietoturva ja vähentynyt IT-tuen tarve.

"Hallinta on tehokkainta silloin, kun kukaan ei huomaa sitä, mutta kaikki hyötyvät siitä."

– Dustin Apple-tiimi: [apple-fi@dustin.com](mailto:apple-fi@dustin.com)

## Oletko valmis aloittamaan?

Tutustu turvallisen ja tehokkaan iPhone-hallinnan tarkistuslistaamme tai varaa aika yrityksesi IT-järjestelmän analyysiin asiantuntijamme kanssa.



## Tarkistuslista: Turvallinen ja tehokas iPhone-hallinta

### Tärkeitä kysymyksiä:

- \* Konfiguroidaanko uudet iPhone't automaattisesti Apple Business Managerin ja MDM:n kautta?
- \* Onko mobiililaitteiden tietoturvakäytäntö ajan tasalla?
- \* Onko kaikki laitteet liitetty vaatimukset täyttävään MDM-profiiliin?
- \* Onko päivitysten ja tietoturvapäivitysten toteutus ja hallinta keskitettyä?
- \* Ovatko ominaisuudet kuten kasvojentunnistus, salaus ja etätyhjennys käytössä oletuksena?
- \* Näkeekö IT-tiimi kaikki liitetyt laitteet ja niiden tilat?
- \* Onko kadonneita laitteita tai väärinkäyttöksiä varten olemassa eskalaatioprosessi?

Lisähuomio: Kerro työntekijöille selkeästi yrityksen käyttämien iPhone-laitteiden tietosuojasta ja tietoturvasta.

Saitko rastin kaikkiin ruutuihin? Siinä tapauksessa yrityksesi on valmis tietoturvalliseen ja skaalautuvaan laitehallintaan.

