Atea M365 Tietoturvapilotti ja IT-ympäristön kehitys

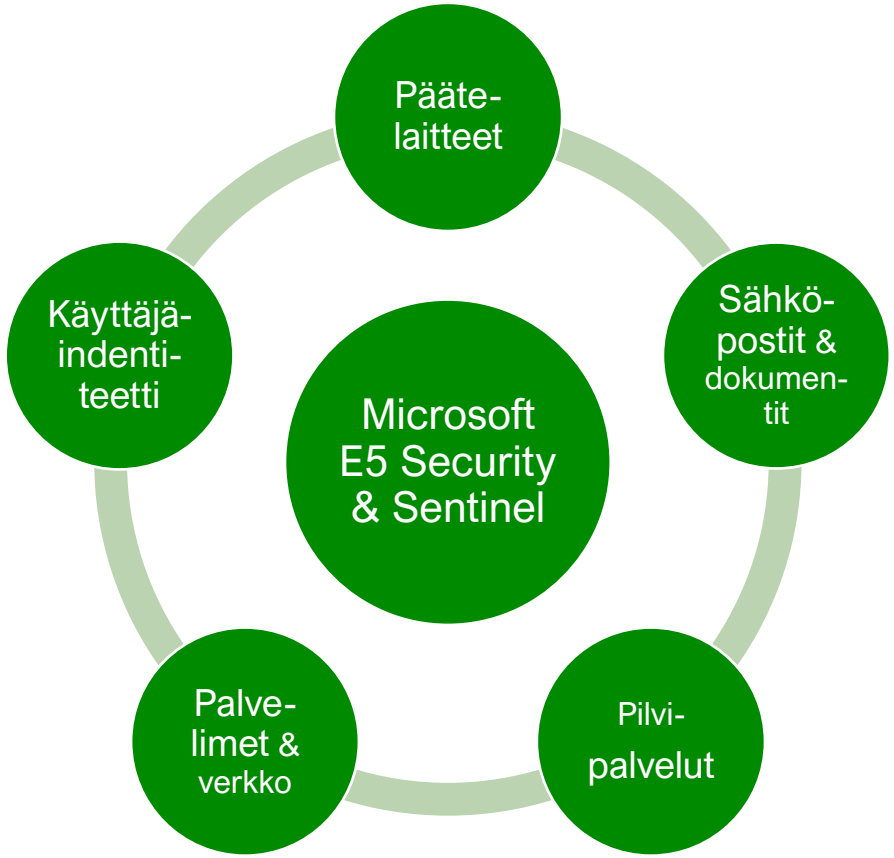
Microsoft E5 Security POC -ratkaisu

Atea Finland Oy
Kimmo Kivistö
Etunimi.sukunimi@atea.fi

Tietoturvan kokonaisvaltainen modernisointi

Koko ympäristön näkyvyys ja keskitetty suojaaminen kehittyneitä uhkia vastaan

- **Kaikki päätelaitteet:** modernien uhkien suojaus ja haavoittuvuuksien valvonta
- **Sähköpostit ja dokumentit:** kaikkien linkkien ja liitetiedostojen tarkistus ja suojaaminen
- **Pilvipalvelut:** Sovellusten ja tiedon suojaaminen, varjo-IT:n hallinta
- **Verkko:** liikenteen analysointi / valvonta
- **Käyttäjäidentiteetti:** identiteetin jatkuva seuranta ja analysointi



- Keskitetty hallinta ja näkyvyys palveluiden käyttöön
- Tietoturvahaavoittuvuuksiin ennakoiva reagointi

Asiakkaalle kehityskohteiden priorisointi, suunnitelma, mittarointi.

Pilotoinnin **sisältö ja rajaukset**

- Sisältää M365 Defender -tuotteiden käyttöönoton siinä mittakaavassa, jossa se on mahdollista asiakkaan ympäristössä (Defender for O365, Defender for Endpoint, Defender for Identity ja Defender for Cloud Apps)
- Pilotti ei sisällä incidenttien ratkaisua (erillisveloitteinen)
- Mikäli E5 Security tuotteet halutaan kytkeä mahdollisen kolmannen osapuolen SOC-palveluun, konsultointi laskutetaan erillisveloitteisesti
- Ei sisällä Sentinelin käyttöönottoa / konfigurointeja (Atea Sentinel Pilotti)
- Vaatimuksena pilotin toteuttamiselle on, että asiakas toimittaa tarvittavat tunnukset pilvi-/on-premises ympäristöön

Atea **M365 Tietoturvapilotti -projektimalli**

- Aloituspalaveri – E5 Security tuotteiden läpikäynti, asiakas ympäristön kartoitus ja esivaatimukset
- Workshop 1 – E5 Security tuotteiden käyttöönotto, lisenssien aktivointi ja noin viikon tiedonkeruujakso
- Workshop 2&3&4 – Analysointi, tietoturvakuvan tarkastus ja kehityskohteiden määrittely
- Workshop 5 – loppuraportti ja jatkokehitystoimenpiteet IT-ympäristön ja lisenssien suhteen.