Workplace Ninja

User Group Finland

Data framework policy with App Protection policies - Miten alkuun?

THANKS FOR THE SPONSORS!

PATCH MY PC

Microsoft

PLENTICS

Metropolia

twoday

NETOX

DELL

Workplace Ninja User Group Finland

intel

Esittely

Valtteri Aho

Vaasa

Vanhempi konsultti, Endpoint management tiimin vetäjä ja Microsoft Certified Trainer

Sulava Oy, osa The Digital Neighborhoodia

Yli 17 vuotta kokemusta kouluttajana, järjestelmänvalvojana ja monipuolisena helpdesk/datacenter-asiantuntijana. Ajan saatossa kerääntynyt mittavasti tietoa on-prem Microsoft teknologioista, Microsoftin Azure/M365 sekä Modernista laitehallinnasta SCCM:ää unohtamatta. Pian 6 vuotta Sulavalla keskittyen puhtaasti laitahallinnan modernisointi- ja kehitysprojekteihin sekä tottakai kouluttamiseen.

wallopro.bsky.social

valtteri-aho

https://wallo.pro/

Intune MAM yleiskatsaus

- Microsoft Intune Mobile Application Management (MAM) tarjoaa organisaatioille mahdollisuuden hallita ja suojata yrityssovelluksia ilman laitteen hallintaa tai parantaa suojausta myös hallituissa laitteissa.
- Ilman laitteen hallintaa (MAM-WE) tapahtuvat suojaukset ovat erityisen tärkeitä tilanteissa, joissa työntekijät käyttävät henkilökohtaisia laitteitaan työasioihin – eli BYOD tuki.
- Politiikkoja kutsutaan nimellä App Protection Policies (APP).

Intune MAM ja selective wipe

- Yritystietojen hallittu poisto
  Selective wipe poistaa yritysdataa sovelluksista sekä hallituilla että hallitsemattomilla laitteilla, ilman koko laitteen tyhjennystä.
- Laiteriippumaton tietoturva
  Ominaisuus toimii sekä IOS- että Android-laitteilla tarjoten kattavan ja joustavan suojan yrityksen tiedoille.
- Henkilökohtaisen laitteen suoja
  Selective wipe mahdollistaa yritystietojen poistamisen henkilöstön omilta laitteilta vaarantamatta henkilökohtaisia tietoja.

APP-politiikat turvaavat datan

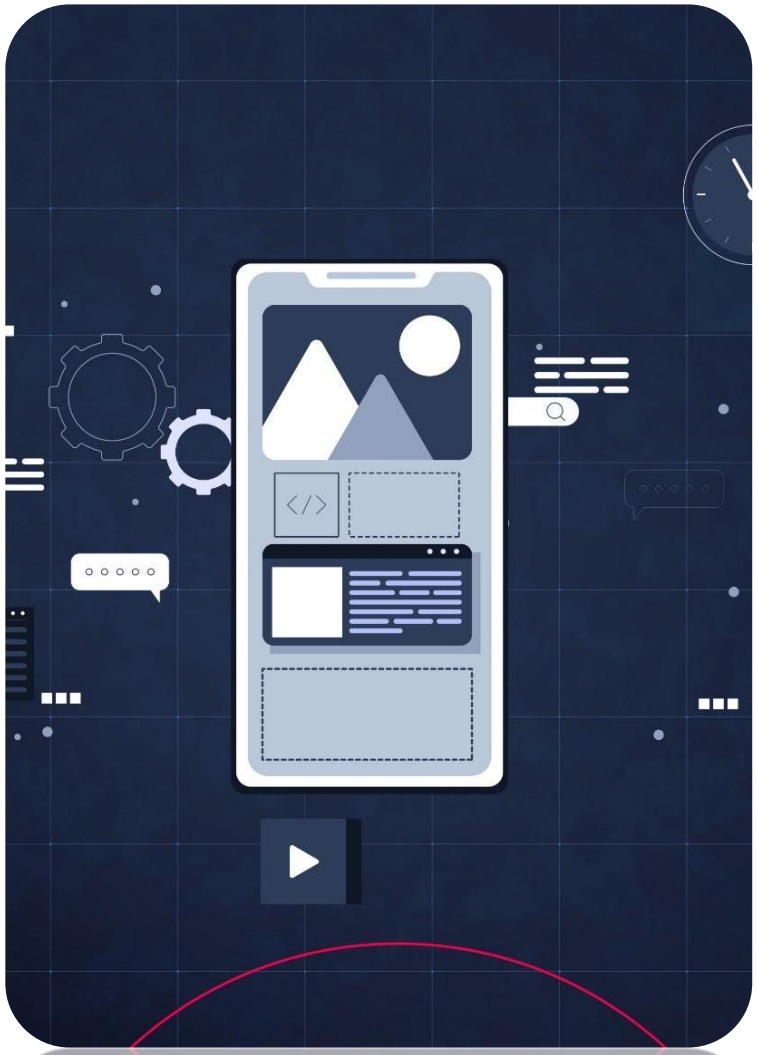
- **Tietojen suojaus sovelluksissa**
  APP-politiikat suojaavat yritysten tietoja Microsoftin tuottamissa sovelluksissa myös hallitsemattomilla laitteilla. Myös kolmannen osapuolen sovelluksia löytyy.

- **Sovellustason salaus**
  Tiedot voidaan salata suoraan sovelluksessa, mikä estää luvattoman käytön ja lisää tietoturvaa.

- **Kopioi/liitä-rajoitukset ja PIN-koodi**
  Politiikat voivat rajoittaa esimerkiksi kopioi/liitä-toimintoja tai edellyttää PIN-koodin käyttöä sovelluksen avaamiseksi.

Sekä paljon muita suojaustoimenpiteitä!

Intune MAM: Alkutoimet



- **Valitut sovellukset**
  Organisaation on mietittävä mitä sovelluksia halutaan suojata Intune MAM:lla. Tyypillisesti lähdetään liikkeelle sovelluksen tiedon sensitiivisyyden perusteella.

- **Sovellusten hallinta Intunella**
  Sovellusten on oltava hallittuja, jotta sovelluskonfiguraatioiden käyttöönotto onnistuu. Tämä tarkoittaa sitä, että Apple sekä Android laitteilla sovellusten jakelua ja käyttöönotto tehdään Intunen avulla hallituille laitteille.

- **iOS- ja iPadOS-tuki**
  Apple iOS- ja iPadOS-sovellusten hallinta Intunella vaatii erityishuomiota konfiguroinnissa. Sovellukset pitää ottaa käyttöön Company Portalista.

- **Lisenssit ja laitetyypit**
  Käyttäjillä on oltava Intune-lisenssi ja organisaation tulee miettiä sekä omien laitteiden että BYOD laitteiden tuki.

Conditional Access rooli

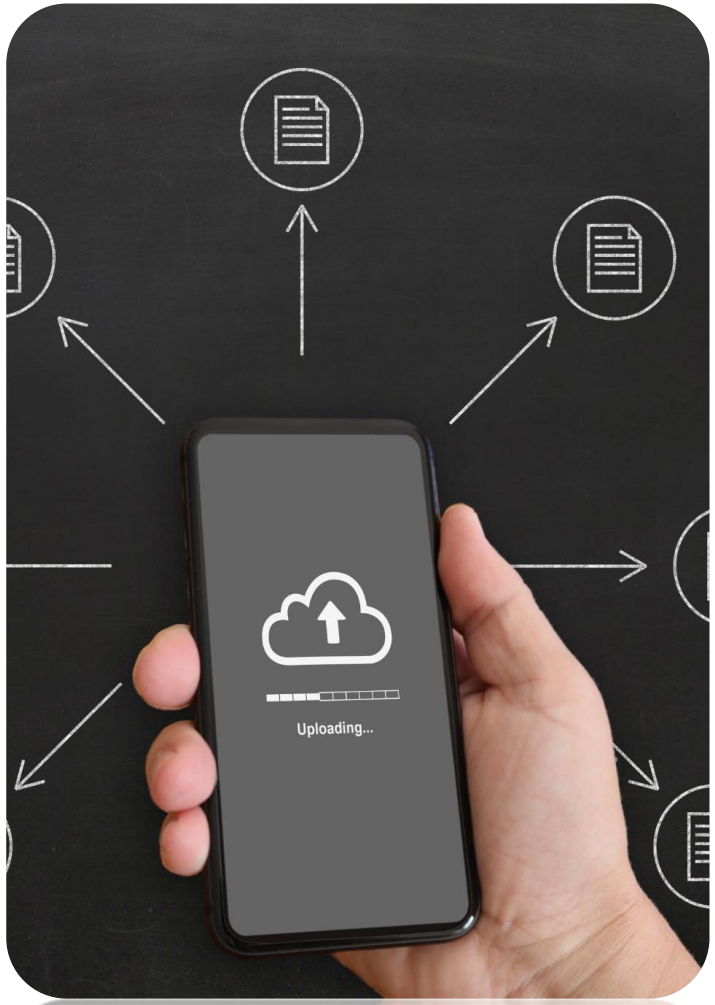
Conditional access pakottaa käyttöönottamaan App Protection Policyn client sovelluksessa

- Käyttäjän on noudatettava APP käytäntöjä päästäkseen pilvisovelluksiin turvallisesti.
- Client sovelluksen pitää myös tukea APP.

Rajoitettu sovellusten käyttö

- Vain tuetut sovellukset esim. Outlook, mahdollistaa pääsyn sähköpostilaatikkoon, kun APP kohdistuu kaikkiin Microsoft client sovelluksiin ja CA-policy vaatii APP tukevaa client sovellusta. Vaikutukset kolmannen osapuolen sovelluksiin on merkittävä!

CA + APP Esimerkkejä



- Mikä on oikea tapa? Riippuu aivan täysin halutusta lopputuloksesta.
- Rajataanko pääsy vain tietyillä client sovelluksilla, rajataanko pääsy pilvipalvelun mukaan vai näiden yhdistelmä?

APP-politiikka	CA-politiikka	Tulos
Kaikki Microsoft-sovellukset	Kaikki pilvipalvelut + vaadi APP	Pääsy vain Microsoftin mobiilisovelluksilla M365-palveluihin
Kaikki sovellukset	Microsoft 365 + vaadi APP	Pääsy M365-palveluihin kaikilla APP-yhteensopivilla sovelluksilla

Data protection framework using App Protection policies - Microsoft

- **Level 1 enterprise basic data protection** – Microsoft suosittelee tätä politiikkaa kaikille käyttäjien cleint sovelluksille ensimmäisenä politiikkana. Ei näkyviä muutoksia loppukäyttäjälle. Avaa selective wipe toiminnon.
- **Level 2 enterprise enhanced data protection** – Microsoft suosittelee tätä politiikkaa käyttäjien client sovelluksille joilla käsitellään sensitiivistä tai yrityksen kriittistä tietoa. Tämä tulee vaikuttamaan loppukäyttäjäkokemukseen.
- **Level 3 enterprise high data protection** – Microsoft suosittelee tätä politiikkaa käyttäjien client sovelluksille joilla on hyvät resurssit, erilliset tietoturvatiimit tai VIP-käyttäjille jotka ovat jatkuvasti erilaisten kyberuhkien kohteena, jotka käsittelevät erittäin sensitiivistä ja yrityksen toiminnan kannalta lamauttavaa tietoa.
  Tällä politiikalla on merkittävä vaikutus loppukäyttäjäkokemukseen.
  HARKITSE TARKOIN!

Minun suositukset

- **Level 1 enterprise basic data protection**
  Perustason suoja kaikille käyttäjille riippumatta laitteen hallinnasta Intunella.
- **Level 2 enterprise enhanced data protection – managed**
  Tehostettu suoja valituille käyttäjille, Intune hallittu laite.
- **Level 2 enterprise enhanced data protection – unmanaged**
  Tehostettu suoja valituille käyttäjille, ei-hallittu laite.
- **Level 3 enterprise high data protection**
  Korkein suoja VIP-käyttäjille joille taataan korkein tiedonsuoja hallituilla laitteilla, minimoiden tietoturvariskit.
  VIP-käyttäjillä VAIN Intune hallitut laitteet.

DEMO

Miltä minun suositukset näyttävät Intunessa?

Miten alkuun?

- Suunnittele suojattavat sovellukset ja niiden tietojen tärkeys/sensitiivisyys
- Suunnittele organisaation omat laitteet vs. BYOD vs. MAM-WE
- Varmista että sovellusten jakelu ja konfiguraatiot toteutetaan hallituissa laitteissa Intune MAM:lla
- Varmista että sovellusten konfiguraatiot toteutetaan hallitsemattomilla laitteilla myös Intune MAM:lla
- Mieti Conditional Access policyillä toteutettava APP vaatimus, valitse ensin selkeät pilviresurssit joihin löytyy hyvä sovellustuki
- Mieti kohdistukset Level 2-3 tasoilla tarkkaan, TESTAA!
- MAM tuo mukanaan Selective wipe toiminnallisuuden, mieti missä tilanteissa sitä käytetään

Lataa käyttöösi valmiit Level 1 – Level 3 APP!

https://bit.ly/4oDTfmO

THANK YOU ALL AND
A SPECIAL THANKS TO OUR SPONSORS!

Thank you!