MOBIILITIETOTURVA YRITYSYMPÄRISTÖSSÄ

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Riihimäki, Tietotekniikan koulutusohjelma

Syksy, 2019

Mikko Pynnönen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietotekniikan koulutus
Riihimäki

Tekijä	Mikko Pynnönen	**Vuosi** 2019
Työn nimi	Mobiilitietoturva yritysympäristössä	
Työn ohjaaja/t	Marko Grönfors	

TIIVISTELMÄ

Tämän opinnäytetyön tarkoituksena oli perehtyä mobiililaitteiden hallintaan ja siihen, kuinka mobiilitietoturva otetaan osaksi yrityksen tietoturvakäytäntöjä. Työssä on käytetty lähtökohtana suomalaista kaupanalan yritystä, jossa on henkilökuntaa yli 600 sekä mobiililaitteita yli 200 kappaletta.

Workspace ONE UEM on VMwaren uusin laitehallinta ratkaisu, jolla voidaan hallita kaikkia yrityksen laitteita kuten kannettavia, puhelimia, tabletteja sekä puettavia älylaitteita. Opinnäytetyössä käydään läpi UEMin eri hallintaosia Workspace ONE tuotteen näkökulmasta.

Työssä esitetään hallitsemattoman ympäristön ongelmakohdat, kuten luvattomat käyttöönotot, haittaohjelmat, datan tietovuodot sekä miten ne näkyvät tietohallinnolle ja loppukäyttäjille. Opinnäytetyö on prosessikuvaus siitä, kuinka mobiililaitteet otetaan osaksi yrityksen tietoturvaa.

Mobiili- ja etätyöskentelyn rooli tulee nousemaan tulevaisuudessa suuremmaksi muun muassa siitä syystä, ettei se sido henkilöä aikaan eikä paikkaan. Koska mobiililaitteet ovat nykypäivänä suuri osa käyttäjien päivittäistä toimintaa, tulee yritysten ottaa mobiilityöskentely osaksi tietoturvastrategiaa. Yritysten tulee pystyä turvaamaan käyttäjille tietoturvalliset ratkaisut kaikkiin työhön liittyviin tarpeisiin päätelaitteesta riippumatta.

Avainsanat Airwatch, EMM, MDM, UEM, Workspace ONE

Sivut 16 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Information and Communication Technology
Riihimäki

Author Mikko Pynnönen **Year** 2019

Subject Mobile security in a business environment

Supervisors Marko Grönfors

ABSTRACT

The purpose of this project was to learn about mobile device management and how to integrate mobile security into the security policies of an enterprise. Project was based on a Finnish trade company with over 600 employees and over 200 mobile devices.

Workspace ONE UEM is the latest Device Management solution of VMware which allows one to manage all business devices such as laptops, phones, tablets and wearable smart devices. This thesis examines the various management components of UEM from the perspective of a Workspace ONE product.

This thesis presents problems in an unmanaged environment, such as unauthorized deployments, malware, data leaks, and how they manifest themselves to information management and end users. This thesis is a process description of how to integrate mobile devices into enterprise security.

The roles of mobile and teleworking will become more prominent in the future, not least because they do not bind employees to time or place. As mobile devices form a major part of the daily activities of users, nowadays companies should incorporate mobile work as part of their information security strategy. Companies must be able to provide users with secure solutions for all work related needs, regardless of the terminal.

Keywords Airwatch, EMM, MDM, UEM, Workspace ONE

Pages 16 pages

SISÄLLYS

TERMIT JA LYHENTEET

1 JOHDANTO 1

2 MOBIILITIETOTURVA 1

3 MOBIILITIETOTURVAN KARTOITUS 3

3.1 Palvelun tarjoajat 4
3.2 Käytettävät laitteet 4
3.3 Riskianalyysi 5

4 KOLMANNEN OSAPUOLEN SOVELLUKSET 5

4.1 Asennus omille palvelimille – On-Premise 6
4.2 Sovellusalustapalvelu – SaaS 7
4.3 AirWatch – Mobiililaitteiden hallinta 8

5 LAITEHALLINTA 9

5.1 MDM 10
5.2 EMM 11
5.3 Sisällönhallinta (MCM) 12
5.4 Sähköpostihallinta (MEM) 12
5.5 Sovellustenhallinta (MAM) 13
5.6 Käyttäjien omat laitteet (BYOD) 13
5.7 UEM 14

6 JOHTOPÄÄTÖKSET 16

LÄHTEET 17

Termit ja lyhenteet

BYOD	Bring Your Own Device
EMM	Enterprise Mobile Management
MAM	Mobile application management
MCM	Mobile content management
MDM	Mobile device management
MEM	Mobile email management
MSM	Mobile security management
SSO	Single Sign On
UEM	Unified Endpoint Management

1 JOHDANTO

Mobiililaitteet ovat yleistyneet viimeisien vuosien aikana nopealla vauhdilla. Suurimpana tätä trendiä on ollut vauhdittamassa käytön helppous sekä vapaus tehdä asioita ilman, että tarvitsee sitoutua yhteen paikkaan tai aikaan. Yritysympäristöissä on ollut useiden vuosien ajan hallinnassa pöytäkoneiden ja kannettavien tietoturva. Näitä ovat tukemassa Windows-ympäristössä toimialue sekä mahdolliset virustorjunnat ja palomuurit, sekä etäyhteyksiä varten on käytettävissä turvallinen VPN-putki. Tietokoneiden osalta myös verkkoon pääsy on erillisen verkkokaapelin päässä, eikä langatonta yhteyttä ole käytettävissä. Myös Offlinessa voidaan tehdä paljon töitä ilman, että verkkoyhteyttä tarvitaan. Mobiililaitteilla tilanne on hyvinkin erilainen. Monissa yrityksissä ei ole mitään ohjelmistoa, millä mobiililaitteita voitaisiin hallita. Ne ovat käytännössä koko ajan julkisessa verkossa.

Tämän opinnäytetyön tarkoituksena on kuvata niitä asioita, jotka tulisi huomioida puhuttaessa mobiililaitteiden tietoturvasta yritysympäristöissä. Työssä on käytetty lähtökohtana suomalaista kaupan alan yritystä, jossa on henkilökuntaa yli 600 sekä älypuhelimia yli 200 kappaletta. Erilaisia mobiilikäyttäjiä löytyy yrityksestä useita, joiden käyttötarpeet vaihtelevat paljon.

Työssä käydään läpi kolmannen osapuolen sovelluksia, joita löytyy markkinoilta paljon. Ala on kasvusuunnassa koko ajan. Kolmannen osapuolen sovellukset mahdollistavat kokonaisvaltaisen tietoturvan verkossa käytettäville mobiililaitteille. Työssä käytetty kolmannen osapuolen sovellus on valittu sen mukaan, mikä sopii parhaiten työssä sovellettavan yrityksen tarpeisiin.

2 MOBIILITIETOTURVA

Tietoturvalla tarkoitetaan tiedon suojaamista ulkopuolisilta, joille tieto ei kuulu, eli tiedolle pyritään takaamaan koskemattomuus. Yrityksissä tietoturva on yleisesti kohtalaisella tasolla, kun puhutaan lankaverkosta ja siihen liitettävistä koneista. Käyttäjien tiedostot on tallennettu palvelimelle, joista otetaan säännöllinen varmuuskopio. Tai ainakin asia tiedostetaan, ja käyttäjät saattavat ottaa mm. ulkoiselle kovalevylle varmuuskopioita tiedostoistaan. (Suomen Internetopas n.d.)

Mobiililaitteiden osalta tilanne on usein valitettavasti heikompi. Mobiililaitteet ovat usein myös käyttäjien henkilökohtaisessa käytössä ja yritystiedot saatetaan sotkea yksityiselämän kanssa. Yleisimpiä uhkia hallitsemattomilla mobiililaitteilla ovat mm. seuraavat:

- Erilaiset haittaohjelmat
- laitevarkaudet
- Datan hävitykset

(DNA 2019.)

Kuvasta yksi nähdään kattavasti mitä uhkia mobiililaitteille on, mikäli niitä ei ole mitenkään huomioitu tai turvattu. Erikseen asennettavilla mobiililaitteiden hallintaohjelmilla voidaan turvata käyttäjille turvallinen laitteen käyttö, yritysdata, sovellukset sekä verkon selailu. Erillinen mobiililaitehallinta on myös ainoa vaihtoehto, jolla yritys voi eriyttää käyttäjien yksityisen ja yritysdatan. (Hardy & Lingenfelter 2015.)

Kuva 1. Mobiilitietoturva uhat (LE VPN 2018.)

Kuvan kaksi mukaisesti mobiilitietoturvalla pitäisi saavuttaa yrityksessä:

- Suojatut laitteet
- Suojattu sisältö
- Suojatut sovellukset
- Suojattu verkon käyttö

Näiden lisäksi tärkeää on erottaa yritysdata henkilökohtaisestadatasta.

Kuva 2. Mobiilitietoturva (Hardy & Lingenfelter 2015, 17.)

Mobiilitietoturvaan liittyy käyttäjätasolle myös vääriä olettamuksia siitä, mitä yrityksen tietohallinto tai johto aiheesta ajattelee. Näitä oletuksia ovat mm.

- Käyttäjät suojaavat laitteensa
- Käyttäjien laitteissa ei ole yritykselle tietoturvallista materiaalia
- Mobiililaitteissa ei ole haittaohjelmia
- Mobiililaitteet eivät ole niin isossa roolissa kuin PC:t

Kuten on aikaisemmin todettu, mobiililaitteiden rooli on kasvamassa, ja tämä on myös heikentänyt niiden tietoturvaa. Mobiililaitteet ovat joka päivä suuremmassa roolissa käyttäjillä, johtuen niiden tuomasta helppoudesta verrattuna PC:hen. Valitettavasti mobiililaitteiden tietoturvan ymmärrys ei ole heillä useinkaan kovin hyvällä tasolla. Suurimmalla osalla käyttäjistä ei ole asetettu mitään suojausta laitteeseen estämään sen luvatonta käyttöä. Mobiililaitteiden monipuolisuus sekä lisääntynyt kapasiteetin määrä ovat lisänneet yritystietojen tallentamista laitteeseen. Nämä tiedot ovat usein tietoturvallista materiaalia, kuten asiakastietoja. Mobiililaitteiden yleistyessä myös niihin kohdistuvat haittaohjelmat ovat valitettavan yleisiä. Niitä voi tulla puhelimiin mm. sähköpostin kautta tai lataamalla epämääräisiä sovelluksia. Haittaohjelmat mahdollistavat mobiililaitteen luvattoman käytön sekä yrityksen tietoturvallisten materiaalien tietovuodon. (Gold 2019.)

3 MOBIILITIETOTURVAN KARTOITUS

Yrityksen mobiilitietoturvaa suunniteltaessa työ alkaa aina oikeanlaisesta kartoituksesta. Kartoituksessa on tarkoitus muun muassa selvittää

- Mobiilitietoturvan nykytilanne
    - Kuka sitä käyttää?
    - Mihin sitä käytetään?
    - Mitä laitteita käytetään?
- Riskianalyysi
- Palvelun tarjoajat

Kartoituksen lopputuloksena saadaan yleiskuva yrityksen nykytilanteesta mobiilitietoturvan osalta. Riskianalyysin perusteella voidaan tehdä tarvittavat jatkosuunnitelmat siitä, mitä toimenpiteitä tarvitaan. Perusteellisesti tehdyssä kartoituksessa tulee usein esille asioita, joita ei ole ennen kartoitusta ajateltu. Tällaisia asioita voivat olla esimerkiksi kysymykset siitä, onko erilliselle tietoturvaa parantavalle sovellukselle mitään käyttöä ja tulisiko käyttäjiä ohjeistaa tarkemmin mobiililaitteiden käytöstä.

kuva kolme on IBM:n näkemys siitä, miten voidaan saavuttaa tehokas mobiilitietoturva. IBM on jakanut mobiilitietoturvan neljään osa-alueeseen:

- Mobiililaite tietoturva
- Sisällön tietoturva
- Mobiilisovellusten tietoturva
- Pääsynhallinta

Nämä ovat lähtökohta mobiililaitteiden turvaamiselle ja niiden tehokäytölle. Yllä olevat kohdat käsitellään tarkemmin luvussa 5. Laitehallinta.

Kuva 3. Polku tehokkaaseen mobiilitietoturvaan (Hardy & Lingenfelter 2015, 8.)

3.1 Palvelun tarjoajat

Osana kartoitusta tulee selvittää mahdolliset palvelun tarjoajat. Palvelun tarjoajia kannattaa lähestyä ensin tarjouspyynnöillä, johon on liitetty palvelun vaatimukset. Tämän pohjalta voidaan rajata tarjoajista sopivin vaihtoehto. Tarjouskilpailu on julkisella puolella pakollinen protokolla, mutta yksityisellä sektorilla näin ei ole. Se on kuitenkin hyvin suotavaa, koska tällöin saadaan paras hinta halutuille palveluille. Tarjousten yhteydessä palvelun tarjoajat haluavat yleensä tarkennuksia kartoitukseen ja tarjota vaihtoehtoista ajattelua projektiin. Mikäli ulkopuolisen toimittajan palvelut koetaan tarpeelliseksi, valitaan tarjouskilpailun jälkeen oikea toimija. Tämän jälkeen aletaan työstää projektisuunnitelmaa.

3.2 Käytettävät laitteet

Osana kartoitusta tulee miettiä, mitä laitteita halutaan hallita. Laitteiden hallinnasta itsestään kerrotaan myöhemmin luvussa 5.1 MDM. Mobiililaitteiden kartoitus on hyvä tehdä suunnitellessa mobiililaitteiden kokonaishallintaa. Vuonna 2019 on käytännössä kaksi eri käyttöjärjestelmää Android sekä iOS. Nämä järjestelmät eroavat toisistaan ja niitä varten tarvitaan laitehallintaan omat säännöstöt (policy).

Yrityksessä, jota varten opinnäytetyö on tehty, on käyttäjillä käytössä joko Android- tai iOS-laitteita. Osalla käyttäjistä on myös omia laitteita, joita he käyttävät päivittäisessä työssään. Näiden laitteiden hallinta tulee myös ottaa huomioon. Omien laitteiden hallinasta kerrotaan myöhemmin luvussa 5.3 Käyttäjien omat laitteet (BYOD).

3.3 **Riskianalyysi**

Riskianalyysi on tärkeä osa puhuttaessa, mistä tahansa projektista. Riskianalyysillä pyritään tunnistamaan riskitekijät, niiden vaikutusalueet, syyt ja mahdolliset seuraukset. Mobiilitietoturvan suunnittelussa riskianalyysi on yksi iso tekijä. Riskianalyysin avulla saadaan projektille päämäärä ja mitä asioita sillä tulisi saavuttaa, lähtökohtaisesti nämä ovat:

- mobiililaitteiden hallinta
- sisällönhallinta
- sovellusten hallinta
- pääsyhallinta

Mobiilitietoturva on projektina myös iso investointi yritykselle. Tämän takia riskianalyysi on myös yrityksen johdolle tärkeä tapa perustella investointitarpeita. (Opi Tietosuojaa n.d.)

4 **KOLMANNEN OSAPUOLEN SOVELLUKSET**

Mobiilitietoturvasta puhuttaessa siihen yhdistetään hyvin usein jokin kolmannen osapuolen ohjelmisto. Ohjelmistot tarjoavat yritykselle kokonaisvaltaisen mobiilitietoturvan, jolla voidaan hallita käyttöönottoja, laitteiden elinkaarta sekä yleisiä tietoturvakäytäntöjä.

Kuva 4 on Gartnerin-kaavio mobiilitietoturvaa tarjoavista yrityksistä. Gartnerin-taulukoissa WMware on ollut lähes aina markkinajohtajan asemassa. Opinnäytetyössä käydään läpi luvussa 4.3 AirWatch – Mobiililaitteiden hallinta tarkemmin WMwaren AirWatchia.

Kuva 4. Gartner-taulukko vuoden 2018 mobiilihallinta johtajista (Anderson 2018.)

4.1 Asennus omille palvelimille – On-Premise

Työssä käytettävän WMwaren AirWatch voidaan asentaa käyttöön kahdella eri tapaa, On-Premise tai SaaS asennuksena. On-Premise asennukset ovat niin sanottu perinteinen tapa toteuttaa palvelun asennus. Asennus tehdään tässä tapauksessa omille palvelimille omaan ympäristöön. On-Premises ympäristöt tulevat kysymykseen silloin, kun halutaan itse hallita kaikkea, sekä silloin kun käytettävien laitteiden määrä on suuri. Tietoturvamielessä On-Premises malli on yhtä turvallinen kuin yrityksen verkko. Workspace ONE asennus kannattaa tehdä WMwaren ohjeiden mukaisesti jotka löytyvät osoitteesta https://docs.vmware.com. Tällä varmistetaan se, että asennus on tehty oikeaoppisesti ja tietoturva huomioiden. On-Premises ympäristöissä asiakas on vastuussa kaikesta mikä liittyy ympäristöön, näitä ovat mm:

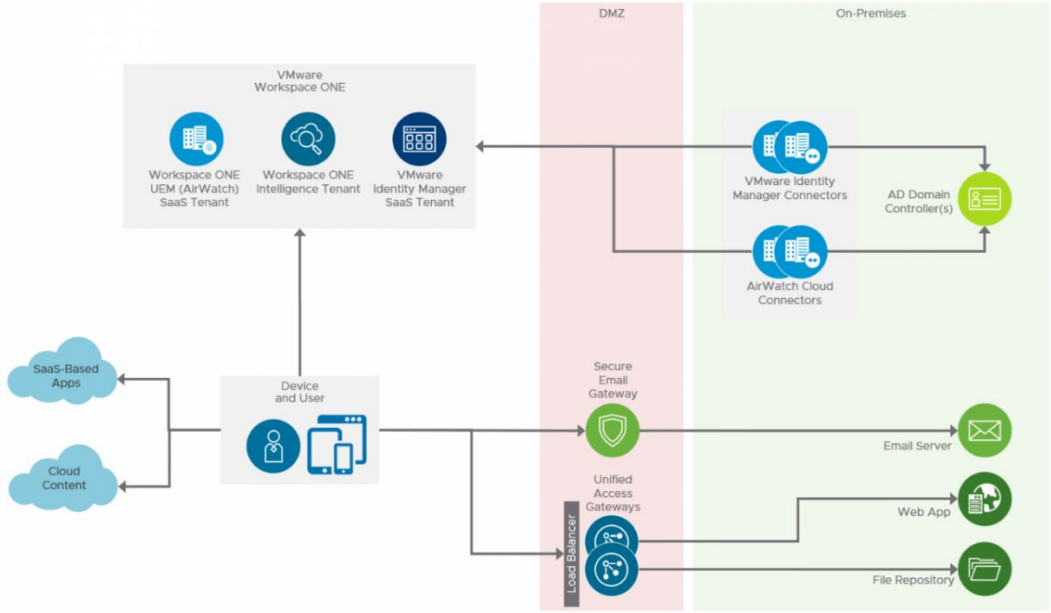
- Ohjelmisto
- Data
- Palvelimet
- Verkko
- Tietokanta

Workspace ONE ohjelmiston vaatimukset ovat listattuna alle:

- SQL Server 2012 tai uudempi
- SQL Server 2012 Native Client
- .NET 4.6.2 Framework
- Windows Server 2008 R2 tai uudempi
- PowerShell 3.0+ versio
- 64-bit Java (JRE 1.8)
- IIS

Yllä olevasta listasta on nähtävissä On-Premise asennuksen ohjelmiston vaatimukset. Itse palvelimen vaatimukset riippuvat ympäristön koosta ja käyttäjä määrästä.

Kuvassa viisi on Workspace ONE On-Premises arkkitehtuuri, joka lähtee toimialueesta, johon on asennettu VMwaren identity manager controller sekä AirWatch Cloud Connector, jotka ovat yhteydessä Workspace One pilvipalveluun.



Kuva 5. Workspace ONE On-Premises arkkitehtuuri (VMware n.d.b.)

Kustannusten minimoimiseksi kannattaa kartoittaa kaikkien ympäristöön liittyvien laitteiden määrä, ja tämän perusteella tarkastella kumpi tulee edullisemmaksi; On-Premises vai SaaS malli, jota käsitellään tarkemmin seuraavassa kappaleessa. On-Premises-asennuksissa tulee myös huomioida laitteiston vaihto, koska palvelimet eivät ole ikuisia. Palvelun jatkuva ylläpito on myös yksi piilevistä kuluista, jota ei aina huomioida kartoituksessa ja budjettia tehtäessä.

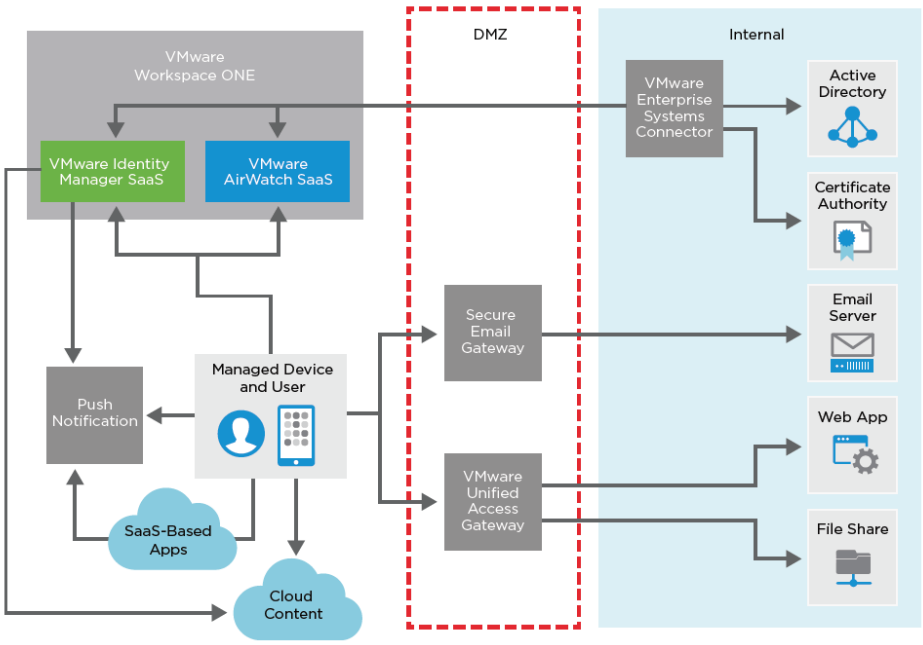
4.2 Sovellusalustapalvelu – SaaS

SaaS termi tulee sanoista Software as a Service eli sovellusalustapalvelu. SaaS-palvelu on nykyaikainen tapa toteuttaa ja toimittaa palveluita asiakkaalle, minkä on mahdollistanut verkkojen nopea kehitys. SaaS-palveluiden tuottaminen on erityisesti pienemmissä yrityksissä melkein ainoa vaihtoehto, sillä omat palvelimet aiheuttavat usein kohtuuttomat kustannukset. Usein yrityksissä ei ole myöskään tarvittavaa osaamista palvelimien tai palveluiden ylläpidosta. Tämä onkin yksi Saas-mallin suurimmista hyödyistä. SaaS-mallissa asiakkaan ei tarvitse huolehtia palvelimista eikä nii-

den palveluista. SaaS-malli on myös helppo asiakkaan budjetoinnin kannalta, kun tiedetään käytettävien laitteiden määrä sekä käyttäjät. (CommunicationPro n.d.)

4.3 AirWatch – Mobiililaitteiden hallinta

AirWatch on VMwaren tuottama ohjelmisto, jolla hallitaan siihen liitettyjä laitteita, sekä toteutetaan tietoturvallinen pääsy yrityksen tiedostoihin ja ohjelmistoihin. AirWatch on markkinoiden edelläkävijä, joka on ollut käytännössä aina markkinajohtaja, kun on puhuttu mobiilitietoturvasta. (Imobile n.d.) Nykyinen ohjelmisto AirWatchilta on Workspace ONE, joka perustuu Unified Endpoint Management eli UEM hallinta periaatteeseen. Käsitettä UEM käsitellään tarkemmin kappaleessa 5.4 UEM. Workspace ONE:n lähtökohtana on, että käyttäjällä voi olla mikä laite tahansa, ja Workspace ONE mahdollistaa tämän tietoturvallisen käytön. Workspace ONE yhdistää AirWatch Mobiilihallinnan ja VMware Identity Managerin siten, että kertakirjautumalla (SSO) Workspace ONE portaaliin valitsemallaan laitteella, käyttäjät saavat pääsyn kaikkiin tarvitsemiinsa organisaation applikaatioihin halutun tietoturvatason mukaisesti. Kuvassa kuusi on kuvattuna Workspace ONE toimintakaavio. Lähtökohtana kaaviossa on käyttäjä ja hallittu laite, joka ottaa yhteyden tarvitsemiin palveluihin ja sisältöihin.



Kuva 6. Workspace ONE toimintakaavio (Gordon 2018.)

Käyttäjät voivat kirjautua Workspace ONE portaaliin joko selaimella tai Workspace ONE Appsilla. Workspace ONE on saatava iOS- ja Android-versiona. Tietoturvan haluttu taso voidaan määritellä sovelluskohtaisesti

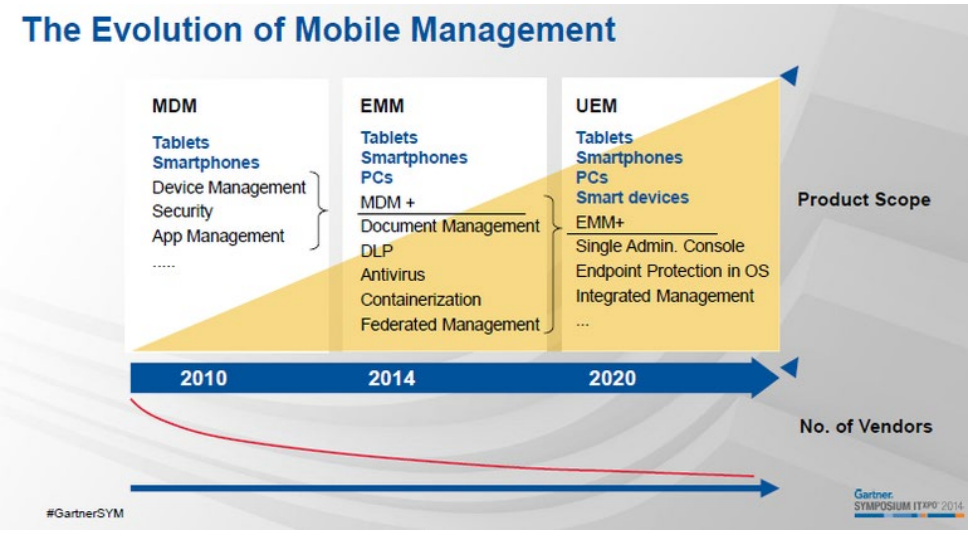
käyttäen AirWatch laitehallintaa ja Identity Managerin autentikointisääntöjä yhdistettynä VMware Verify two-factor autentikointiin sisäänkirjautumisen yhteydessä tarvittaessa.

Loppukäyttäjät hyötyvät erityisesti Workspace ONE UEM tuotteesta SSO:sta eli single sign-on:sta, joka mahdollistaa käyttäjän kirjautumisen kaikkiin hänelle kuuluviin resursseihin yhdellä autentikoinnilla. Tämän ansiosta jokaista sovellusta varten ei tarvita eri käyttäjätunnuksia ja salasanoja. Käyttäjä pystyy myös itse lataamaan workspace sovelluksen mihin tahansa päätelaitteeseen ja kirjautumaan siihen. Mikäli laite täyttää tietohallinnon määreet, saa käyttäjä tarvitsemansa resurssit käyttöönsä valitsemallaan laitteella ajasta tai paikasta riippumatta. (VmWare n.d.a.)
Tietohallinto hyötyy Workspace ONE:sta, kun sovellusten jakelu loppukäyttäjille nopeutuu, ne voidaan kohdentaa tarkasti halutuille ryhmille ja seurata reaaliajassa sovellusten käyttöönottoa. Haluttu tietoturvan taso saadaan määritettyä laite-, paikka- ja sovelluskohtaisesti, esim. yrityskriittisiin sovelluksiin pääsy vain AirWatch hallituilla laitteilla, joissa organisaation oma sertifikaatti. (Aerion n.d.)

5 LAITEHALLINTA

Puhuttaessa mobiilihallinnasta tänä päivänä, yhdistetään se termiin UEM eli Unified Endpoint Management. UEM on nykyaikainen käsite, jossa hallitaan kaikkia verkonlaitteita, joita käyttäjät käyttävät, oli kyse sitten matkapuhelimista, tableteista, kannettavista tai puettavista älylaitteista. Kaikkien näiden hallinta tapahtuu samasta pääkäyttäjä portaalista.

Kuvan 7 mukaisesti voidaan todeta, että mobiilihallinta on kokenut isoja muutoksia siitä pisteestä, kun mobiililaitteet alkoivat kehittyä ja alettiin puhua mobiililaitehallinasta.



Kuva 7. Mobiilihallinnan kehitys (Dignan 2014.)

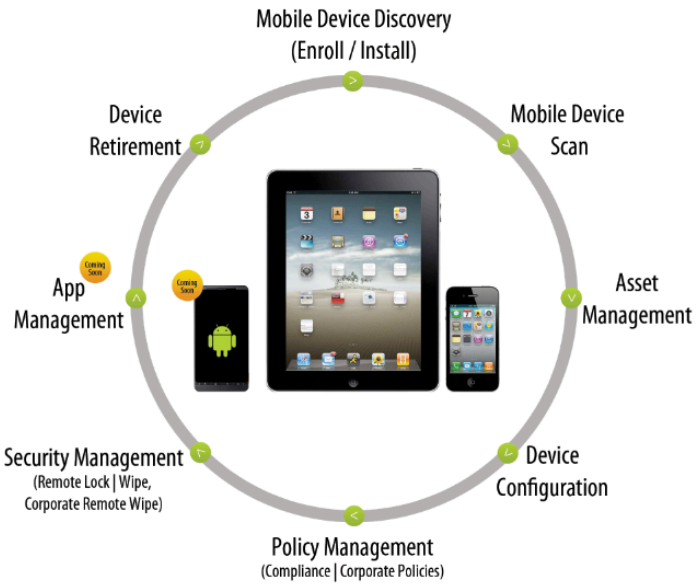
Alun perin laitehallinta on otettu käyttöön, kun markkinoille alkoi tulla ensimmäisiä älypuhelimia, ja niiden käyttö koettiin mullistavana yrityksissä. Näiden ongelma erityisesti tietohallinnolle oli se, että niissä saatettiin säilöä melkein samaa dataa kuin esimerkiksi kannettavissa tietokoneissa, mutta se ei ollut mitenkään hallittavissa. MDM:n avulla älypuhelimiin saatiin tuki tietohallinnolle hallintapäätelaitteeseen, joka mahdollisti tietoturvallisen käytön sekä ohjelmiston hallinnan eli Mobile Application Management (MAM). Myöhemmin MDM:stä julkaistiin kehittyneempi versio EMM eli Enterprise Mobile Management. EMM sisältää MDM:stä puuttuvat osat kuten dokumenttien hallinta eli MCM. Ennen EMM:tä MDM ja MCM olivat irrallisia toisistaan ja niillä oli usein eri toimittajat.

Opinnäytetyön tekijä on vuonna 2014 ollut suunnittelemassa opinnäytetyön yrityksen mobiilihallintaa ja silloin todettiin, että EMM:lle on yrityksessä käyttöä. Tärkeimpinä ominaisuuksina käyttäjille oli turvallinen pääsy yrityksen, sekä omiin tiedostoihin päätelaitteesta riippumatta, sekä toimiva sähköposti. Tietohallinnon kannalta tärkeimmät ominaisuudet olivat mobiilitietoturva, yritysdata ja henkilökohtaisen datan erottaminen sekä laite- ja dokumenttienhallinta.

5.1 **MDM**

Mobile device management (MDM) eli mobiililaitteiden hallinta. MDM oli ensimmäinen lähtökohta mobiililaitteiden hallintaan, kun yritykset halusivat hallita yrityksen mobiililaitteita samalla tavalla kuin esim. kannettavia tietokoneita. MDM:n avulla saadaan mobiililaitteisiin asennettua yrityksen käytännöt, ja laitteiden sisältöä voidaan hallita. MDM mahdollistaa laitteiden etähallinnan.

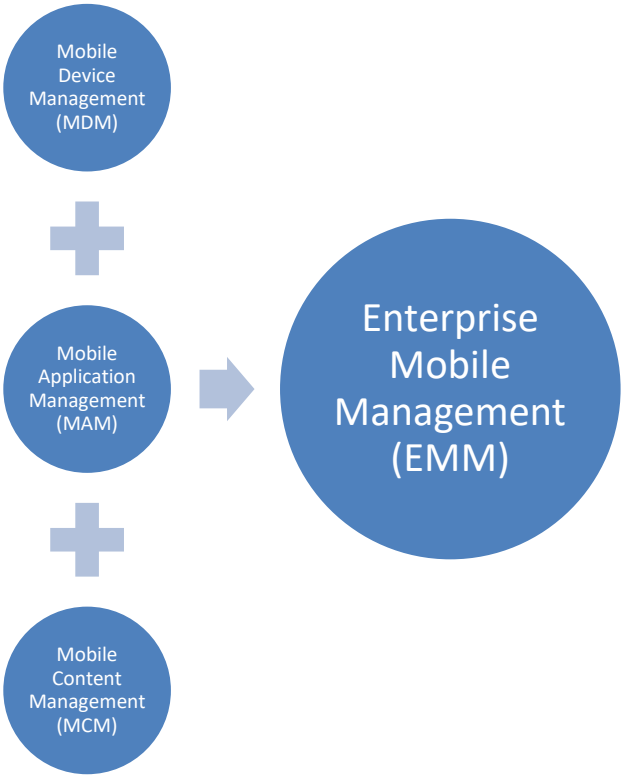
Kuvasta kahdeksan näemme, mitä MDM alun perin sisälsi. Mobiililaitteet otettiin hallintaan asentamalla sovellus, jolla laitteet saatiin pääkäyttäjän hallintaan. Tämän jälkeen laitteisiin voitiin ajaa yrityksen mukaiset säännöstöt (Policy management) sekä turva-asetukset (Security Management). MDM:ssä on huomioitu myös laitteen elinkaari. Kun laite poistuu käytöstä, se tyhjennetään pääkäyttäjän toimesta ja poistetaan hallittavien laitteiden joukosta.



Kuva 8. Mitä MDM sisältää (Manage Engine n.d.)

5.2 **EMM**

Enterprise mobility management eli EMM, on kehittynyt hallintamalli MDM:stä jossa laite- ja sisällönhallinnalle oli omat sovellukset sekä hallintaportaalit. Kuvan yhdeksän mukaisesti EMM yhdistää mobiililaite-, mobiilisovellus-, ja sisällönhallinnan yhdeksi kokonaisuudeksi, jonka tarkoitus on vastata yrityksen mobiilitietoturvan tarpeita.



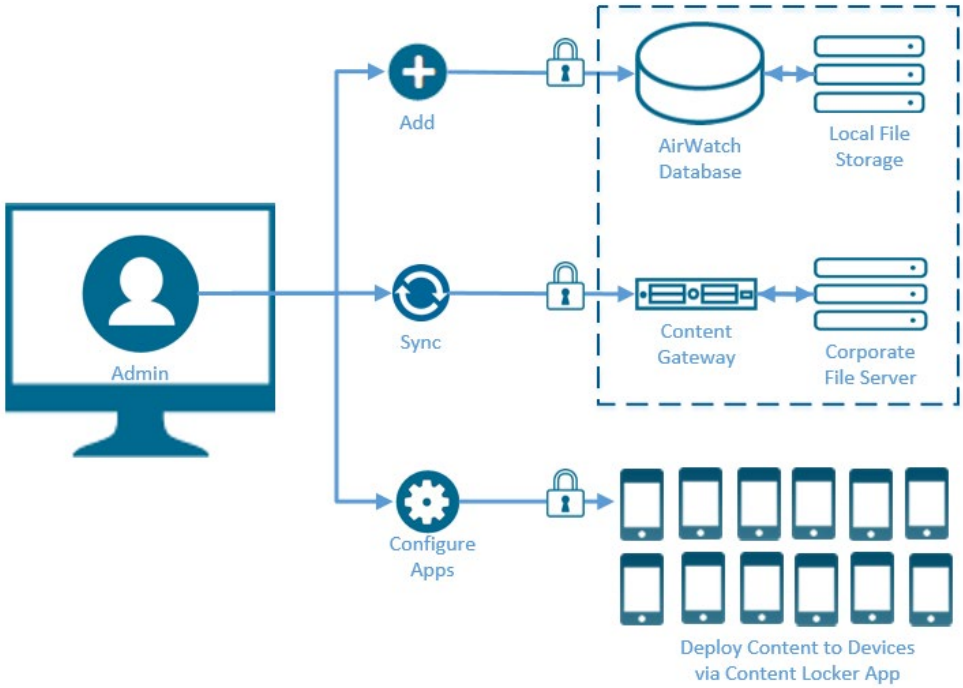
Kuva 9. EMM

EMM:n avulla haetaan loppukäyttäjiltä tehokkuutta työhön vähentämällä erilaisien sovellusten määrää ja tarjoamalla kaikki yhden kanavan kautta. Tietohallinnolle EMM tuo helpotusta tarjoamalla yhden portaalin kautta sekä laitteiden että sisällön hallinnan. (Rouse n.d.a.)

5.3 Sisällönhallinta (MCM)

Mobile content manager (MCM) eli sisällönhallinta on yksi osa EMM rakennetta. MCM:n avulla tarjotaan loppukäyttäjille heille tarkoitettu sisältö mahdollisimman yksinkertaisesti, kuitenkaan tietoturvaa vaarantamatta. Tietohallinnosta käsin voidaan määritellä erilaisille loppukäyttäjäryhmille erilaisten säännöstöjen kautta pääsy heidän tarvitsemiin sisältöihin.

Kuvan 10 toimintakaaviossa on kuvattuna sisällönhallinnan käyttöönotto tietohallinnon näkökulmasta. Tietohallinto luo pääsyn AirWatch tietokannalle paikallisiin tiedostoihin sekä synkronoi sisällönhallintaan yrityksen tiedostopalvelimen. Lopuksi loppukäyttäjille annetaan pääsy päätelaitteilta jaettuihin tiedostoihin.



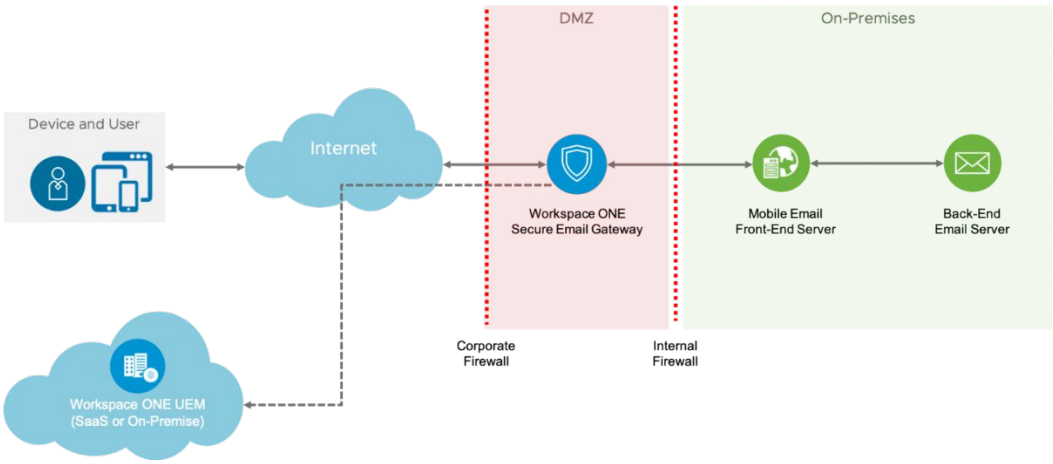
Kuva 10. AirWatch sisällönhallinta (VMWare Docs 2019.)

5.4 Sähköpostihallinta (MEM)

Mobile exchange management (MEM) eli sähköpostinhallinta. Sähköpostinhallinta on yksi perinteisimmistä osa-alueista koskien mobiilihallintaa. Sähköpostihallinnalla tuotetaan käyttäjälle mahdollisimman käyttäjäystävällisesti yrityksen sähköposti, yleensä joko puhelimen natiiviin ohjelmaan tai sitten hallintasovelluksesta riippuen oma sähköpostiohjelma.

Erillisten sähköpostiohjelmien hyödyt tulevat siitä, että siihen on saatu myös mukaan MCM. Tämä on hyvin käyttäjäystävällinen, kun käyttäjät saavat sähköposteihin liitettyä liitteitä saman sovelluksen sisällä.

Kuvassa 11 on toimintakaavio, kuinka Workspace ONE:n Secure Email Gateway toimii. Käyttäjän näkökulmasta palvelu toimii silloin, kun käyttäjällä on yhteys internettiin, josta on edelleen yhteys Workspace ONE Secure Email Gatewayhin. Tietohallinnon näkökulmasta asia ei kauheasti muutu. Secure Email Gateway on yrityksen DMZ-alueella, josta on yhteys palomuurin läpi sähköpostipalvelimeen.



Kuva 11. Workspace ONE Secure Email Gateway arkkitehtuuri (VMware n.d.b.)

5.5 Sovellustenhallinta (MAM)

Mobile Application Management (MAM) eli sovellusten hallinta. MAM oli alunperin oma yksittäinen osa mobiililaitehallintaa ennen EMM:tä. Nykyään se on kiinteä osa EMM:tä. MAM on erittäin olennainen osa mobiilitietoturvaa niin käyttäjien kuin tietohallinnon kannalta.

MAM turvaa käytettävät mobiilisovellukset sekä mahdollistaa yrityksen tietohallinnon etähallinnan sovelluksiin. Tietohallinto pystyy määrittelemään mobiilisovelluksiin käyttörajat mm. datan osalta, sekä erottelemaan yritys- ja henkilökohtaisen datan. MAM takaa sen, että käytettävät sovellukset yritysympäristössä ovat suojattuja eikä datavuotoja tule. Loppukäyttäjien kannalta olennaista on varmuus siitä, että laitteessa olevat sovellukset ovat tietohallinnon hallinnassa, ja data on turvassa. (Rouse n.d.b.)

5.6 Käyttäjien omat laitteet (BYOD)

BYOD eli bring your own device tarkoittaa oman laitteen tuomista yrityskäyttöön tai -ympäristöön. Tämä asettaa omat haasteensa suunniteltaessa yrityksen mobiilitietoturvaa, mikä pitää huomioida määrittelyvaiheessa.

Alun perin BYOD tuli yritysympäristöihin älypuhelimien yleistyessä, kun yritykset eivät välttämättä tarjonneet käyttäjälle hänen mieleistään laitetta. BYOD asettaa omat ongelmansa tietohallinnolle, mikäli yrityksellä ei ole mitään sääntöä omien laitteiden tuomisesta yrityskäyttöön. Näissä tapauksissa tietohallinnolla ei ole mitään mahdollisuutta valvoa, mitä sovelluksia ja dataa puhelimessa on. Myöskään puhelimen elinkaarta ei voida varmistaa mitenkään. Varkaustapauksissa taas saattaa hyvinkin arkaluontoista dataa päätyä vääriin käsiin. BYODin hyviin puoliin voidaan kuitenkin lukea, että työntekijät ovat motivoituneempia käyttämään laitteita, kun heillä on käytössään mieleisensä laitteet.

BYODille on olemassa eri vaihtoehtoja, kuten Choose Your Own Device eli CYOD. CYOD-malleja on erilaisia riippuen yrityksestä, lähinnä nämä koskevat omistussuhdannetta. CYOD-mallissa yritys saattaa omistaa x-osuuden laitteesta, ja työntekijä kustantaa loppuosuuden. Laitteen elinkaari on myös sellainen, että laite jää loppupeleissä loppukäyttäjän omistukseen. CYOD-malli on tietohallinnon ja yrityksen tietoturvapolitiikan kannalta turvallinen vaihtoehto, koska CYODissa voidaan määritellä mm:

- Rajoitettu laitekanta
- Saadaan testattua ohjelmistot tietyllä laitekannalla
- Tietoturvan ylläpito
- tietohallinnon hallinta

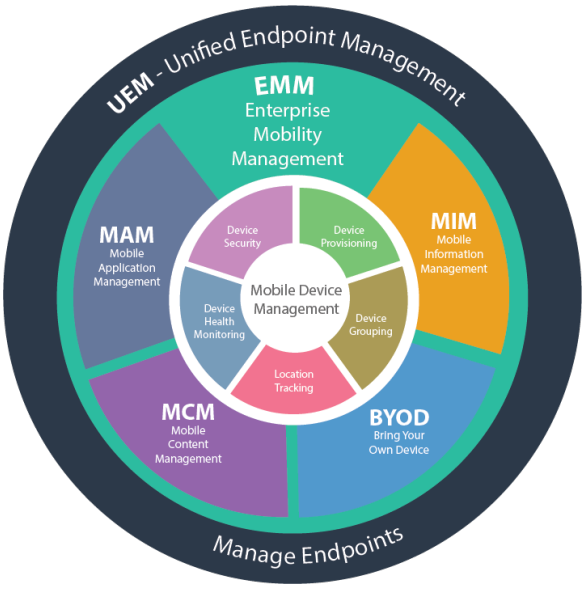
CYOD on perusteltu valinta, kun ympäristössä on käytössä laiteriippuvaisia sovelluksia ja tietoturvataso halutaan pitää korkealla kuitenkin niin, että loppukäyttäjillä on mahdollisuus vaikuttaa työkaluihin, mitä työssään käyttävät. (Jääskeläinen 2016.)

BYODille ja CYODille on myös vaihtoehto COPE- (corporate owned, personally enabled) malli, jossa yritys omistaa laitteen, mutta työntekijä saa käyttää laitetta henkilökohtaisessa käytössään. COPE on näistä malleista tietoturvallisin ja selkein tietohallinnolle. Tietohallinto voi ajaa laitteisiin mobiilihallinnan, jolloin saadaan täysihallinta sekä laitteelle sen oikea elinkaari täytettyä. Varjopuolena on tietenkin loppukäyttäjälle käytön vapaus riippuen yrityksen tietoturva politiikasta. (Digium n.d.)

5.7 **UEM**

Unifield endpoint management eli UEM on nykyaikainen hallintamalli. UEM yhdistää perinteisen laite-, mobiili- ja älylaitehallinnan yhdeksi kokonaisuudeksi. UEM tarjoaa tietohallinnolle yhden hallintapaneelin, jonka kautta voidaan hallita kaikkia yrityksen laitteita. (VMware n.d.c.)

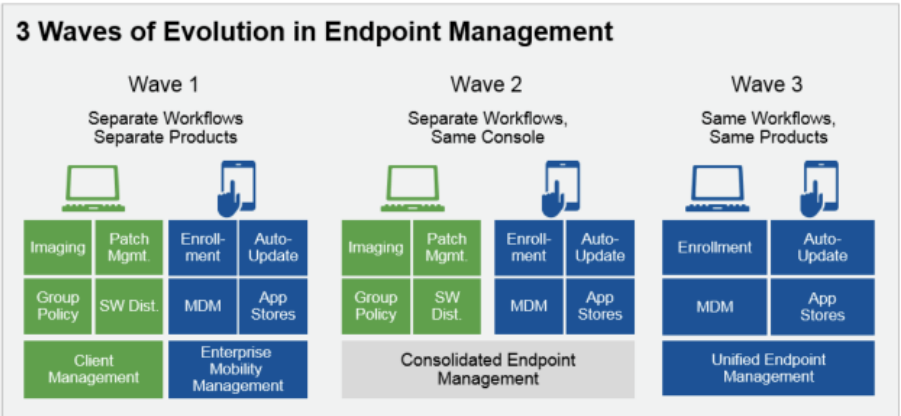
Kuvan 12 malli kuvaa hyvin mobiililaitteiden näkökulmasta, mitä UEM oikein sisältää. UEM yhdistää mobiililaitehallinnan, sisällönhallinnan, sovellustenhallinnan sekä käyttäjien omat laitteet yhdeksi kokonaisuudeksi, jota hallitaan yhden hallintapaneelin kautta.



Kuva 12. UEM malli (42 Gears 2017.)

UEM helpottaa niin yrityksen tietohallintoa kuin loppukäyttäjiä saamaan tuotteesta täyden käyttäjäkokemuksen. Loppukäyttäjien laitteisiin asennetaan yksi agenttisovellus, jonka avulla päätelaite saadaan tietohallinnon hallintapiiriin.

UEM-malliin siirto perinteisestä hallintamallista tulee tapahtumaan vaiheittain. Gartner on luokitellut yritykset kolmeen luokkaan, miten siirtymä tulee todennäköisesti tapahtumaan. Type A yritykset, jotka menevät ajan hermoilla ja siirtyvät välittömästi käyttämään yrityksessä UEMia. Type B tulee siirtymään alla olevan kuvan mukaisesti vaiheittain perinteisestä hallintamallista nykyaikaisen hallintaan.



Kuva 13. Hallintamallien kehittyminen (Lewis 2018.)

Viimeinen malli Type C yritykset eivät Gartnerin arvion mukaan tule

siirtymään UEM-malliin ennen vuotta 2022. (Lewis 2018.) Opinnäytetyön yritys putoaa Type B ja Type C luokitusten väliin. Käyttöönottoa ei tulla tekemään suoraan kaikkiin laitteisiin, vaan käyttöönotot tehdään osissa, pääpainona mobiililaitteet.

6 JOHTOPÄÄTÖKSET

Mobiililaitteet ovat nykypäivänä iso osa käyttäjien päivittäistä toimintaa. Tämä johtaa siihen, että yritysten pitää ottaa mobiilityöskentely osaksi tietoturvastrategiaa. Mobiili- ja etätyöskentely tulee nousemaan tulevaisuudessa suuremmaksi ja suuremmaksi jo siitä syystä, ettei se sido henkilöä mihinkään aikaan eikä paikkaan. Yritysten pitää siis pystyä turvaamaan käyttäjille tietoturvalliset ratkaisut kaikkiin työhön liittyviin tarpeisiin, mitä käyttäjä tekeekin. Yksinkertaisuudessaan se voi olla käyttäjälle turvallinen sähköpostin käyttö. Kannettaville on turvattu käyttö jo pitkään liittämällä ne yksityiseen toimialueeseen, jolloin niitä voidaan edes jonkun verran etähallita mm. estämällä niihin kirjautuminen. Mobiililaitteet kuten älypuhelimet ovat kuitenkin kaikkien käyttäjien jokapäiväistä arkea. Siinä missä kone laitetaan kiinni työpäivän jälkeen, älypuhelinta käytetään jatkuvasti, ja se otetaan joka paikkaan myös mukaan. Älypuhelin altistuu näin isommalle riskille. Niille voidaan tehdä luvattomia käyttöönottoja, mikäli niissä ei ole mitään näyttölukkoja. Kuka tahansa voi päästä lukemaan jopa tietoturvallista sisältöä.

Tulevaisuudessa UEMin myötä erilaiset käyttömahdollisuudet vaan lisääntyvät. Mikäli tähän ei ole mitään kokonaisvaltaista strategiaa, miten ne yrityksessä hoidetaan, tietoturvaongelmat tulevat leviämään käsiin ja pahasti.

Sokeasti ei kuitenkaan kannata tehdä ratkaisua, että hankitaan ohjelma ilman perusteellista kartoitusta. Perimmäisenä kysymyksenä on, mihin me tätä tarvitsemme, ja miten me hyödymme sitä? Kun nämä kysymykset kartoitetaan kunnolla ja otetaan mobiililaitteet osaksi tietoturvastrategiaa, saadaan kustannustehokas ratkaisu, joka palvelee yrityksen johtoa, tietohallintoa ja tärkeimpänä loppukäyttäjiä.

LÄHTEET

42 Gears. (2017). What is the Difference Between MDM, EMM and UEM?. Haettu 15.10.2019 https://www.42gears.com/blog/difference-between-mdm-emm-uem/

Aerion. (n.d.) vmware workspace one. Haettu 18.11.2019 http://www.aerion.fi/15-finnish-products/118-vmware-workspace-one

Anderson, B. (2018). Microsoft emerges as a Leader in Gartner MQ for Unified Endpoint Management (UEM). Haettu 20.2.2019 https://www.microsoft.com/en-us/microsoft-365/blog/2018/07/25/microsoft-emerges-as-a-leader-in-gartner-mq-for-unified-endpoint-management-uem/

Communication Pro. (n.d.). Materiaalinhallinta – Investointina vaiko pilvipalveluna? Haettu 1.4.2019 https://www.communicationpro.com/materiaalinhallintaa-investointina-vaiko-pilvipalveluna/

Digium. (n.d.) BYOD, CYOD, or COPE? Which Mobile Model Should Your Business Choose?. Haettu 14.11.2019 http://www.digium.com/blog/2016/06/14/byod-cyod-cope-mobile-model-should-your-business-choose/

Dignan, L. (2014) Buying enterprise mobility management: How important is independence? Haettu 4.2.2019 https://www.zdnet.com/article/buying-enterprise-mobility-management-how-important-is-independence/

DNA. (2019). 10 vinkkiä työpuhelimen tietoturvaan. Haettu 29.9.2019 https://www.dna.fi/yrityksille/blogi/-/blogs/10-vinkkia-tyopuhelimen-tietoturvaan

Gold, J. (2019) Mobile security: 5 misunderstandings that persist. Haettu 4.12.2019 https://enterprisersproject.com/article/2019/10/mobile-security-5-misunderstandings

Gordon, G. (2018). VMware Workspace ONE Reference Architecture for SaaS Deployments. Haettu 15.1.2019 https://techzone.vmware.com/blog/updated-vmware-workspace-one-reference-architecture-saas-deployments

Hardy, J. & Lingenfelter, D. (2015). 2015 Mobile Security Trends: Are You Ready? Haettu 2.4.2019 https://www.slideshare.net/ibmsecurity/2015-mobile-security-trends

Imobile. (n.d.) MOBIILILAITEHALLINTA – AIRWATCH. Haettu 8.5.2019 https://www.imobile.fi/palvelut/mobiililaitehallinta-airwatch/

Jääskeläinen, T. (2016) BYOD, CYOD ja firman laitepolitiikka. Haettu 17.11.2019 https://blogi.mpy.fi/byod-cyod-ja-firman-laitepolitiikka

LE VPN. (2018). Security Challenges On Mobile Devices. Haettu 2.4.2019 https://www.le-vpn.com/security-challenges-on-mobile-devices/

Lewis, M. (2018) Unified Endpoint Management to displace MDM and CMT says Gartner. Haettu 24.11.2019 https://blog.voiceplus.com.au/unified-endpoint-management-to-displace-mdm-and-cmt-says-gartner

Manage Engine. (n.d.) Enterprises & Mobile Device Management. Haettu 30.9.2019 https://www.manageengine.com/mobile-device-management/register.html

Opi Tietosuojaa. (n.d.) ICT Riskienhallinta. Haettu 2.12.2019 https://opitietosuojaa.fi/fi/53-tyokalupakki/riskienhallinta/46-ict-riskienhallinta

Rouse, M. (n.d.a.) enterprise mobility management (EMM). Haettu 27.10.2019 https://searchmobilecomputing.techtarget.com/definition/enterprise-mobility-management-EMM

Rouse, M. (n.d.b.) mobile application management (MAM). Haettu 10.11.2019 https://searchmobilecomputing.techtarget.com/definition/mobile-application-management-MAM

Suomen Internetopas. (n.d.) Tietoturva. Haettu 24.2.2018 http://www.internetopas.com/yleistietoa/tietoturva/

VMware Docs. (2019) Local File Storage for AirWatch Managed Content. Haettu 27.10.2019 https://docs.vmware.com/en/VMware-AirWatch/9.3/vmware-airwatch-guides-93/GUID-AW93-AWMC_Stor_LFS.html

VMware. (n.d.a.) How Does Workspace ONE Work?. Haettu 17.11.2019 https://techzone.vmware.com/resource/how-does-workspace-one-work

VMware. (n.d.b.). VMware Workspace ONE and VMware Horizon Reference Architecture. Haettu 26.2.2019 https://techzone.vmware.com/resource/workspace-one-and-horizon-reference-architecture#sec4-sub2

VMware. (n.d.c.) Workspace ONE Unified Endpoint Management (UEM) Powered by AirWatch. Haettu 18.10.2019 https://www.vmware.com/products/workspace-one/unified-endpoint-management.html