Plataformes *Endpoint*. Gestionant el dispositiu IT des del *Cloud*.

Estudis	Grau en Enginyeria Informàtica
Menció	Tecnologies de la Informació
Àmbit	Administració de xarxes i sistemes operatius
Tipus de document	Treball fi de grau
Títol del document	Plataformes Endpoint. Gestionant el dispositiu IT des del Cloud
Alumne	Josep Xiqués Hernández
Professor consultor	Miguel Martín Mateo
Data	06/06/2021

ÍNDEX DE CONTINGUTS

ÍNDEX D'IL·LUSTRACIONS

RESUM DEL TREBALL

El present treball consisteix en estudiar les plataformes *Endpoint* com a solució per a la governança de qualsevol tipus de dispositiu IT enrolat en entorns *cloud*. Aquesta gestió ha de ser possible en dispositius ubicats en qualsevol lloc i ser efectiva en qualsevol moment.

Per poder realitzar una anàlisi enfocada en la gestió de la governança dels dispositius, es duu a terme un estudi del funcionament de diferents plataformes *Endpoint* presents al mercat IT i de les seves prestacions clau.

ABSTRACT

The present work consists of studying Endpoint platforms as a solution for the governance of any type of IT device enrolled in cloud environments. This management must be possible on devices located anywhere and be effective at any time.

In order to do an analysis focused on the management of the governance of devices, a study is carried out on the operation of different Endpoint platforms present in the IT market and their key benefits.

1. INTRODUCCIÓ

El present document exposa l'estudi realitzat i les conclusions aconseguides del treball fi de grau "*Plataformes Endpoint. Gestionant el dispositiu IT des del Cloud*."

En una primera part, es presenten els objectius i el pla de treball, i després es continua amb un estudi dels elements més rellevants de la solució *Endpoint* relacionada amb l'objecte del projecte.

Després, en el document, s'aborden les prestacions i potencialitats d'aquesta tecnologia i es descriu l'arquitectura i l'entorn de gestió per a la governança dels dispositius d'usuari. Finalment, resultat de l'anàlisi, s'acaba amb unes conclusions de forma comparada de diverses propostes Endpoint.

1.1. MOTIVACIÓ I CONTEXT DEL PROJECTE

La situació pandèmica, produïda l'any 2020, ha provocat un increment exponencial de la demanda de connexió remota a les infraestructures IT per part dels usuaris per tal d'accedir als sistemes d'informació. Les infraestructures TIC de les organitzacions han hagut d'adequar-se a aquesta necessitat sobtada de teletreball i proporcionar una cobertura operativa global, ja no només local, al conjunt de dispositius IT administrats. El teletreball ha passat de ser un aspecte menor a adquirir un valor de màxima rellevància a dotar de servei.

La finalitat del projecte és l'estudi de les plataformes *Endpoint* sota enrolaments *cloud computing* que donin resposta al nou paradigma de mobilitat dels usuaris i dels seus dispositius assignats.

1.2. INTRODUCCIÓ A ENDPOINT

Una plataforma de gestió *Endpoint* inclou tota una sèrie de serveis i eines que s'utilitzen per administrar i supervisar qualsevol punt que sigui la part final d'una xarxa. Aquests *endpoints* o punts finals poden ser dispositius mòbils, equips d'escriptori, màquines virtuals o servidors.

Un *Endpoint Manager* proporciona l'àrea de treball i les funcions d'administració per mantenir les dades i els equips IT en condicions de seguretat, tant al núvol com a

l'entorn local. Aquesta gestió, per tant, ajuda a garantir la funció operacional, un accés segur, protegint les dades i responent i administrant els riscos en la capa de dispositius IT.

1.3. OBJETIUS DEL PROJECTE

Per aconseguir la finalitat del projecte, s'identifiquen els següents objectius:

- Descripció de la tecnologia *Endpoint*.
- Realitzar un *screening* de solucions de gestió *Endpoint* que recullin els serveis i les eines per a l'administració dels punts finals.
- Identificar aquells *Endpoints* amb més potencialitats resultat de la selecció.
- Comparació i *scoring* de plataformes.

1.4. ENFOC I METODOLOGIA A APLICAR

La metodologia a seguir es basa en una anàlisi el més exhaustiva possible que abasti tots els aspectes funcionals de les plataformes *Endpoint* millor posicionades en el *quadrant màgic de Gartner 2020*. La solvència de *Gartner* ens assegura una selecció de solucions consolidades que permeti obtenir unes conclusions significatives i concloents sobre l'objecte d'estudi.

El seguiment del grau d'avanç en el calendari de projecte serà fonamental per complir amb els objectius marcats en cada fase de lliurament (PAC). A continuació, es descriuen els eixos principals del mètode de treball a seguir.

1.5. PLA DEL PROJECTE

La planificació té com a fites principals les dates de lliurament de les diferents PACs. Així mateix, també ha d'estar orientada al fet que en cada PAC es lliuri la part de projecte que correspongui.

En concret, les fases principals del projecte són les següents:

Lliurable	Durada	#ID fase	Descripció de fase
PAC1	17/02 – 06/03	1	Pla de treball
PAC2	07/03 – 08/04	2	Procés de Screening
PAC3	09/04 – 12/05	3	Procés de Scoring
PAC4	13/05 – 06/06	4	Conclusions, memòria i presentació

1.5.1. Activitats principals

Les tasques a desenvolupar en el projecte son:

- **Descripció de la tecnologia Endpoint**
  Descripció de l'arquitectura, les funcionalitats, prestacions i entorns d'aplicació.

- **Procés de screening**
  Preselecció de solucions *Endpoint* en base al rànquing establert per la consultora tecnològica *Gartner*. A priori, l'estudi de tres opcions haurien de ser suficients.

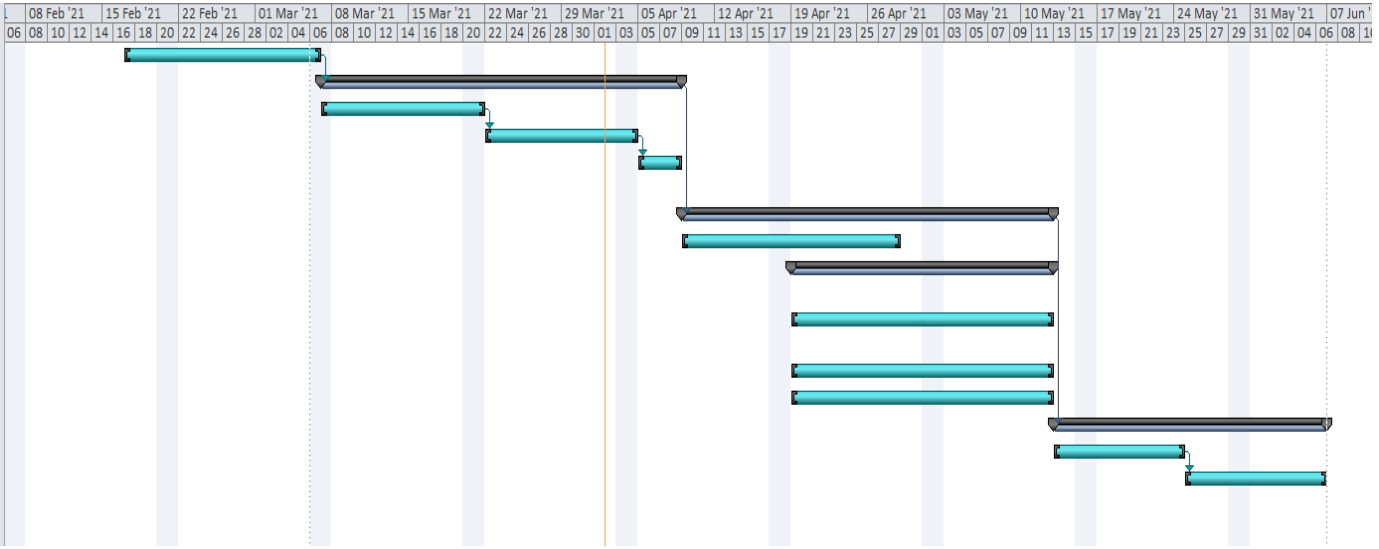
- **Procés de scoring**
  Definir els principals criteris d'avaluació de la solució que s'utilitzaran per establir el procés de *scoring*.

- **Conclusions sobre l'anàlisi realitzada**
  Recopilació de tota la informació obtinguda, analitzar-la, i desenvolupar las conclusions pertinents.

- **Elaboració de la memòria del projecte**
  Redacció de la memòria i del material requerit per a la presentació del projecte.

1.5.2. Planificació del projecte

	Task Name	Duration	Start	Finish
1	PAC1 - Pla de treball	14 days	Wed 17/02/21	Sat 06/03/21
2	**PAC2 - Procés de screening**	**25 days**	**Sun 07/03/21**	**Thu 08/04/21**
3	Descripció Endpoint	12 days	Sun 07/03/21	Sun 21/03/21
4	Procés de Screening	11 days	Mon 22/03/21	Sun 04/04/21
5	Documentació per la fase de scoring	4 days	Mon 05/04/21	Thu 08/04/21
6	**PAC3 - Procés de scoring**	**24 days**	**Fri 09/04/21**	**Wed 12/05/21**
7	Establir criteris d'avaluació	14 days	Fri 09/04/21	Wed 28/04/21
8	**Avaluació de les opcions seleccionades**	**18 days**	**Mon 19/04/21**	**Wed 12/05/21**
9	Endpoint Manager Microsoft	18 days	Mon 19/04/21	Wed 12/05/21
10	Endpoint Manager Vmware	18 days	Mon 19/04/21	Wed 12/05/21
11	Endpoint Manager IBM	18 days	Mon 19/04/21	Wed 12/05/21
12	**PAC4 - Entrega final**	**18 days**	**Thu 13/05/21**	**Sun 06/06/21**
13	Conclusions de l'anàlisi	8 days	Thu 13/05/21	Mon 24/05/21
14	Redacció I presentació de la memòria TFG	10 days	Tue 25/05/21	Sun 06/06/21



Il·lustració 1. Planificació del projecte

1.5.3. Riscos preliminars

A continuació, es relacionen els riscos de projecte identificats, conjuntament amb les corresponents mesures mitigadores:

#ID risc	Descripció del risc	Tipus de risc	#ID Fase	Mitigació
1	Falta d'informació	baix	2	Contactar directament amb el fabricant o partner de la solució Endpoint
2	Abast del projecte respecte les limitacions de temps d'elaboració	baix	2,3,4	Ajustar els continguts als temps planificats al calendari
3	Enfoc de l'anàlisi	baix	2,3,4	Reconduir l'enfoc a una visió més pràctica o de més valor.

2. DESCRIPCIÓ GENERAL D'ENDPOINT

Tot seguit, es passa a descriure allò que ha motivat el sorgiment d'aquesta tecnologia, la seva història i com ha evolucionat. També ens endinsarem en la seva arquitectura i funcionalitats.

2.1. HISTÒRIA I CONTEXT

Les eines de gestió d'extrems resideixen tradicionalment dins de les infraestructures informàtiques corporatives, sovint instal·lades en els sistemes dedicats a les operacions de seguretat de xarxa. Bàsicament, les plataformes locals de protecció de punt final estan centrades en desplegar polítiques als dispositius, i gestionar i prevenir amenaces o incompliments.

Avui dia, les solucions en el núvol s'han intensificat, tornant-se un mètode de treball cada vegada més freqüent. La mobilitat i adaptabilitat que ofereix el *cloud* és un gran avantatge, sobretot per al teletreball cosa que aquests últims mesos s'ha pogut constatar de forma clara.

No obstant això, una altra cosa que també s'ha pogut constatar és que els *ciberatacs* s'han intensificat considerablement, aprofitant que molts empleats que treballaven en remot no disposaven de la mateixa seguretat que treballant des de les oficines, a conseqüència de que moltes organitzacions no estaven o no estan preparades per a aquest nou entorn operatiu.

Davant d'això, el procés de centralització del desplegament, manteniment i control del programari i maquinari del dispositiu *endpoint* és un aspecte que s'ha convertit en indispensable en les infraestructures IT actuals. Per tant, avui dia, les eines de gestió de punt final han de procurar una plataforma administrativa que ajudi a simplificar o automatitzar la implementació i configuració dels dispositius, siguin allà on siguin, per reduir la càrrega en operacions IT de les organitzacions.

2.2. ARQUITECTURA ENDPOINT

Entendre les principals diferències entre les funcionalitats i el valor de les eines de gestió d'extrems és fonamental per triar la solució que coincideixi amb les necessitats presents i futures de l'organització. Això s'ha tornat encara més

important amb el creixement de la força de treball remota i els dispositius mòbils omnipresents a totes bandes.

La gestió de punt final engloba un conjunt d'eines relacionades que treballen conjuntament per administrar els múltiples dispositius, les funcions i les tasques en la majoria de xarxes. Tot seguit, analitzem les diferents iniciatives de gestió que s'han implementat fins l'actualitat.

2.2.1. MDM (*Mobile Device Management*)

Amb MDM, o gestió de dispositius mòbils, neix la primera iniciativa per donar cobertura a l'administració de dispositius mòbils. MDM permet una gestió remota i el manteniment de telèfons mòbils, tauletes i dispositius similars des d'una consola d'administració. MDM és la base de qualsevol suite de mobilitat empresarial i cobreix l'enrolament o inscripció del dispositiu, el control remot, el bloqueig del dispositiu i el seguiment de la seva ubicació.

Les eines MDM tenen la capacitat de fer complir polítiques de seguretat de dispositiu, fer un seguiment de l'inventari i les aplicacions, i controlar els dispositius en temps real. Aquestes eines donen als equips IT la visibilitat i els controls necessaris per controlar els riscos de seguretat dels dispositius mòbils que han de gestionar.

MDM és basa en la combinació d'una aplicació agent, que s'instal·la en un dispositiu endpoint, i el programari del servidor que s'executa al centre de dades corporatiu o en el núvol. Els administradors utilitzen la consola d'administració del servidor MDM per definir polítiques i configurar els paràmetres, i l'agent aplica aquestes polítiques i configura aquests paràmetres que s'integren amb les API incloses en els sistemes operatius mòbils.

MDM ha estat la primera solució i una solució raonable per gestionar el constant augment de dispositius mòbils de propietat corporativa i al mateix temps ha permès reduir l'esforç de suport IT sobre el parc gestionat.

No obstant això, cada vegada més, molts empleats segueixen utilitzant els seus propis telèfons o bé empren múltiples dispositius per a ús empresarial i personal. Això requereix, per tant, d'una solució que pugui donar també cabuda al fenomen conegut com a *bring-your-own-device* (*BYOD)* o porta el teu propi dispositiu.

2.2.2. EMM (*Enterprise Mobility Management*)

EMM, o gestió de la mobilitat empresarial, és l'evolució de la tecnologia MDM. Aquesta amplia els processos de gestió envers les xarxes sense fils i els serveis de computació mòbil. A més d'abordar assumptes de seguretat, el programari EMM també ajuda als usuaris a ser més productius, ja que els administradors IT poden proporcionar-los les aplicacions i les dades que necessiten per dur a terme tasques relacionades amb la seva activitat en els seus respectius dispositius mòbils.

Les solucions EMM van sorgir com a resultat del moviment BYOD. En lloc de restringir els dispositius mòbils només al mon de treball, moltes organitzacions opten per implementar solucions EMM per permetre la flexibilitat d'ús del dispositiu per part dels usuaris, però mantenint el control IT sobre aquests. Davant de la promiscuïtat i riscos afegits d'un dispositiu BYOD, les solucions EMM utilitzen un contenidor segur que manté les dades empresarials segures i separades de la informació personal de l'usuari.

Normalment, EMM implica una combinació de MDM, de gestió d'aplicacions mòbils (MAM), de gestió de continguts mòbils (MCM) i de gestió d'identitat i accés (IAM). Aquestes quatre tecnologies van començar com a productes individuals, però cada vegada més es presenten junts mitjançant paquets complets de programari de gestió de mobilitat.

EMM va comportar el desenvolupament de tres components de seguretat relacionats amb l'operativa del dispositiu que son necessaris ser comentats en el marc de la gestió del dispositiu.

MAM (Mobile Application Management)
MAM, o gestió d'aplicacions mòbils, proporciona una gestió més granular i més segura del dispositiu IT. Permet als administradors definir polítiques per a una aplicació o un conjunt específic d'aplicacions, en lloc de per a tot el dispositiu sencer. Algunes aplicacions mòbils disposen d'API MAM integrades, mentre que altres es basen en l'API MAM a nivell de dispositiu per als principals sistemes operatius mòbils.

MCM (Mobile Content Management)
Amb MCM, o gestió de continguts mòbils, només aquelles aplicacions aprovades poden accedir o transmetre dades corporatives. Al mateix temps, es protegeixen els continguts mitjançant xifratge.

IAM (Identity and Access Management)
La gestió d'identitat i d'accés controla com, quan i on els usuaris poden utilitzar les aplicacions i les dades corporatives, alhora que proporciona funcions d'autenticació avançades com ara l'inici de sessió únic (Single Sign-On (SSO)), o bé autenticació de doble factor o multifactor (MFA).

MDM, MAM i MCM aborden problemes específics, i la superposició entre les 3 tecnologies és mínima. A mesura que més organitzacions van abraçar la mobilitat empresarial, els fabricants van començar a produir productes EMM, generalment afegint funcions MAM i MCM als seus productes MDM.

Les solucions EMM ofereixen aplicacions de productivitat mòbil com ara correu electrònic, calendari, edició de documents i un navegador web segur. Aquestes solucions, també, proporcionen accés remot als recursos empresarials, com ara aplicacions, escriptoris i fitxers, que permeten als usuaris mòbils ser tan productius com si fossin a l'oficina.

Però tot i que les aplicacions són fàcils d'utilitzar i estan optimitzades pel seu ús, no ofereixen el nivell de funcionalitat que els usuaris necessiten per dur a terme tasques empresarials rutinàries, i molt menys el nivell de seguretat que pot necessitar l'empresa.

La gestió EMM està en constant evolució per donar cabuda a un conjunt canviant de plataformes de dispositius, tendències de mobilitat i la requerida seguretat en tots els seus aspectes. Quan Microsoft va crear les API MDM per Windows 10, va obrir la porta al programari EMM a gestionar els ordinadors de la mateixa manera que es gestionen els telèfons intel·ligents i tauletes. Apple, també, ja permet que els ordinadors MacOS portàtils i d'escriptori es gestionin d'aquesta mateixa manera. Tots els principals proveïdors d'EMM ja estan donant suport a aquesta funcionalitat, marcant així ja el canvi de tendència, des d'Enterprise Mobility Management (EMM) cap a Unified Endpoint Management (UEM).

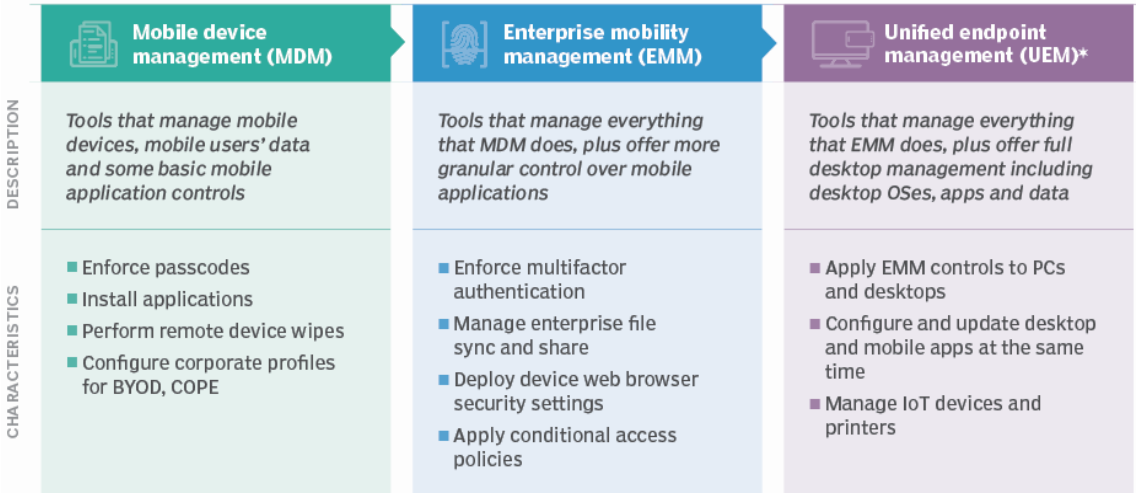
2.2.3. UEM (*Unified Endpoint Management*)

Finalment, l'estratègia, UEM, o gestió unificada del punt final, és l'estadi, ara per ara, més elevat de gestió de la mobilitat d'extrems. UEM és la cartera completa d'eines MDM i EMM per a la gestió de dispositius a través d'una única consola. Aquesta gestió inclou telèfons intel·ligents, tauletes, PCs fixes i portàtils, impressores,

dispositius IoT, i qualsevol altra plataforma o dispositiu informàtic dins de l'organització.

UEM pot aplicar de forma ràpida i senzilla polítiques de seguretat i configuracions de manera global i integrada a tota l'organització, independentment del tipus de punt final. UEM, també, és capaç d'avaluar i informar ràpidament sobre tots els dispositius i aplicacions en ús. El cas d'ús principal d'UEM es manté encara molt centrat en tauletes i telèfons intel·ligents. No obstant això, les organitzacions estan demandant eines unificades de gestió per a qualsevol tipus d'endpoint amb l'objectiu de continuar alleugerint les càrregues de suport IT dedicades al dispositiu, sobretot quan s'ha de fer front a la força de treball remot just quan ha experimentat grans creixements en aquests darrers temps.

A mode de síntesi, es pot observar en la següent il·lustració l'evolució de les estratègies de gestió.



Il·lustració 2. Evolució de la gestió de l'Endpoint (Font: TechTarget)

2.3. FUNCIONALITATS I PRESTACIONS

En aquest apartat, es descriuen les principals funcionalitats de valor d'una plataforma de gestió unificada *Endpoint*. Cada funció te els seus propis requisits de configuració de sistema, i l'ús de cadascuna d'elles podria influir en el disseny i la implementació de l'entorn. Per exemple, si es volen implementar les actualitzacions de software en els dispositius, serà necessari establir un rol en el sistema que habiliti un *site* com a punt de distribució de les actualitzacions.

Un entorn complet de gestió unificada *Endpoint* hauria d'admetre les següents operatives d'administració:

1. Administració conjunta i connectada a núvol

Aquesta és una de las principals implementacions que han d'existir en una plataforma unificada *Endpoint*. El seu objectiu és permetre la gestió de forma simultània i única de qualsevol dispositiu inscrit o enrolat en la infraestructura IT corporativa, amb independència del sistema operatiu instal·lat (Windows, MacOS, iOS i Android) i de la seva ubicació (local, internet o remota).

Amb la inscripció dels clients a l'*Endpoint*, s'obtenen capacitats d'acció sobre els dispositius com poden ser:

- Visibilitat centralitzada de l'estat dels dispositius.
- Vinculació d'usuaris, dispositius i aplicacions amb el sistema informàtic corporatiu.
- Accions remotes sobre el dispositiu (reinici, control remot o restablir de fàbrica).
- Accés condicional dels dispositius i usuaris dins l'entorn de treball.
- Distribució de les directives d'acompliment, d'actualitzacions, d'accés als recursos, de protecció dels dispositius i altres.
- Configuracions generals o granulars dels dispositius.

Per contra, en cas de tenir més d'un comandament d'administració per a un sol dispositiu, pot ser complicat fer una gestió òptima si no hi ha una orquestració correcta entre les unitats gestores. Aquesta coexistència de gestió generalment comporta conflictes o limitacions de funcionalitats i poden produir experiències d'usuari poc satisfactòries.

2. Anàlisi d'escriptori

És un servei que proporciona informació detallada i intel·ligent per prendre les decisions més oportunes sobre les accions necessàries a aplicar en els dispositius gestionats. Aquesta anàlisi es basa en la combinació de les dades de configuració desplegades dins l'organització i addicionalment complementar-les amb el coneixement general que aporten multitud de dispositius d'igual condició connectats a serveis en el núvol.

Amb anàlisi d'escriptori es podrà conèixer en tot moment l'estatus de:

- L'inventari d'aplicacions que s'executen a l'organització i el versionatge present en els dispositius.
- Avaluació de la compatibilitat d'aplicacions amb les darreres actualitzacions de sistema operatiu.
- Identificació de problemes de compatibilitat i rebre suggeriments per mitigar-los a través de la base de coneixement que proporciona el fabricant de la solució.
- Grups pilot de distribució amb un estat determinat de l'aplicació, o el control simulat en un conjunt mínim de dispositius.
- Implementació del sistema operatiu als dispositius.

3. Administració en temps real

Consulta de l'estat dels dispositius connectats en un moment donat, obtenint dades detallades per, en cas de ser necessari, poder actuar a diferents nivells d'administració.

4. Administració d'aplicacions

Ajuda a administrar, implementar i supervisar les aplicacions que son requerides al parc de dispositius. D'igual manera, actua en el desplegament de les actualitzacions de software. Opcionalment, es pot també oferir desplegaments de software mitjançant un repositori d'aplicacions o botiga (*Store)* disponible al núvol on els usuaris poden escollir, d'aquelles eines que tenen permeses, aquelles que li seran útils per a la seva activitat.

5. Implementació del sistema operatiu i l'entorn d'usuari

S'ha de permetre la implementació d'actualitzacions del sistema operatiu per un dispositiu específic, o bé capturar i implementar imatges del sistema operatiu. La implementació d'imatges, normalment, empra *PXE*, *multidifusió* o algun sistema o medi d'arrancada per desplegar-les. També, participa en la implementació dels nous dispositius o dels ja existents, mitjançant l'automatització del desplegament del software a partir d'imatges creades per a l'entorn productiu de l'usuari.

6. Accés als recursos de l'organització

Ha de concedir als usuaris accés a les dades i a les aplicacions des d'ubicacions locals o remotes. Aquesta funció també s'ocupa de la gestió dels perfils WiFi, *VPN*, i l'autenticació o certificació d'usuari per a un accés segur als recursos i la corresponent securització per protegir les dades.

7. Configuració de compliment

Ajuda a avaluar, controlar i corregir el compliment de normatives legals i les directives internes dels dispositius de l'organització. La configuració de compliment entrega las eines i els recursos per establir les característiques i opcions de seguretat i de control que requereixen els endpoint.

Aquesta funcionalitat ha de permetre:

- Comparar la configuració dels equips Windows, Mac, i dispositius mòbils amb les configuracions dels procediments IT recomanats o obtinguts de proveïdors.
- Definir la configuració de dispositiu no autoritzat.
- Identificar vulnerabilitats de seguretat.
- Proporcionar informació per detectar les causes probables de les configuracions no compatibles, i fer les correccions necessàries d'algunes configuracions de forma automàtica.

8. Protecció Endpoint

Per als ciberdelinqüents, els punts finals esdevenen els punts més febles que poden ser atacats mitjançant l'execució de codi maliciós, l'explotació de vulnerabilitats, i el segrest d'informació a través de xifratge de les dades. Amb els usuaris amb cada vegada més mobilitat i connectant-se a recursos des de fora de l'organització, els punts finals són cada vegada més susceptibles als ciberatacs. Durant dècades, les organitzacions han confiat molt en l'antivirus com a mitjà per assegurar la protecció dels punts finals. No obstant això, amb només l'antivirus tradicional ja no és suficient per guardar-se de les sofisticades amenaces d'avui en dia.

Protecció Endpoint ha de proporcionar seguretat, *antimalware* i configuració de *firewall* als equips de l'organització. Aporta l'administració i l'actualització de manera centralitzada del conjunt d'aplicacions destinades a la protecció del dispositiu allà on aquest sigui:

- Antivirus.
- Protecció i mitigació contra amenaces.
- Protecció contra *exploit*.
- Protecció i control d'aplicacions i sistema operatius.
- Polítiques de Firewall.
- Notificacions, alertes i reporting.

9. Administració d'actius Endpoint

Ajuda a identificar i supervisar els recursos. Aquesta administració ofereix:

- Inventari de hardware: Recopila informació detallada sobre el hardware dels dispositius de l'organització.
- Inventari de fitxers: Recopila i proporciona informació sobre els arxius que s'emmagatzemen en els equips client.
- Inventari i disponibilitat de programari: Proporciona eines per recopilar i administrar l'ús de les llicencies de software dins l'organització. Informa de les dades d'ús de software dels clients per saber si el software s'usa després d'instal·lar-lo.

10. Administració d'energia

Administra i supervisa el consum d'energia dels equips client de l'organització. Proporciona la configuració i el desplegament de plans d'energia en base a diferents situacions i horaris.

11. Control remot

Aprovisiona eines per administrar de forma remota els equips client des de la plataforma Endpoint, cosa que facilita solucionar problemes de configuració de hardware i software i donar suport tècnic a distància a l'usuari, bàsicament per l'entorn Windows i Mac.

12. Generació d'informes

Aquesta característica entrega i crea informes que ajuden a recavar, organitzar i presentar informació sobre les abundants dades obtingudes des del dispositius IT gestionats. Ajuda a la presa de decisions sobre l'entorn.

2.4. MODALITAT DE FUNCIONAMENT: CLOUD COMPUTING

Aquest estudi de la solució UEM es centrarà en les implementacions basades en el cloud computing tot i que aquestes també puguin admetre el model local o l'opció hibrida d'implementació.

El cloud computing tracta sobre la nova forma de prestar serveis TIC que s'aplica a empreses, administracions i ciutadans a través d'Internet. Aquest model permet l'accés sota demanda a diferents recursos TIC (xarxes, servidors, sistemes d'emmagatzematge, programari, solucions, serveis o dades) i sempre ajustat a la

necessitat de recursos que el client sol·licita. La configuració d'aquests recursos es pot modificar ràpidament, en funció de les necessitats de l'usuari i sense massa esforç de gestió.

La computació al núvol suposa un canvi important en el paradigma informàtic, sobretot perquè es transforma l'esquema on les infraestructures i aplicacions instal·lades i gestionades dintre de les organitzacions ara es traslladen a un altre lloc, on un tercer de confiança lloga la seva infraestructura i capacitat de servei a les empreses.

L'extraordinari desenvolupament dels dispositius mòbils i de l'accés a Internet, juntament amb les necessitats dels usuaris, han fet de la computació en el núvol una eina fonamental perquè els ciutadans i les organitzacions treballin, busquin informació o accedeixin a serveis des de qualsevol ubicació i en qualsevol moment, d'una manera senzilla i econòmica. Cloud computing realment no només aporta canvis tecnològics, sinó que comporta grans transformacions empresarials i dona peu a la creació de nous models de negoci.

Les característiques específiques de la computació en el núvol són aquelles que es distingeixen pel següents aspectes principals:

- Configuració i modificació dels recursos IT a demanda, de manera flexible i escalable.

- Disponibilitat en tot moment, amb les tecnologies més innovadores aplicades pels proveïdors del servei.

- Accés a través de xarxes i dispositius estàndard.

- Compartir recursos amb altres usuaris.

- Transparència per conèixer el nivell de servei rebut, en base al temps de processament, l'espai d'emmagatzematge, el nombre d'usuaris, etc, la qual cosa facilita els mecanismes de pagament.

- Seguretat i privacitat de la informació.

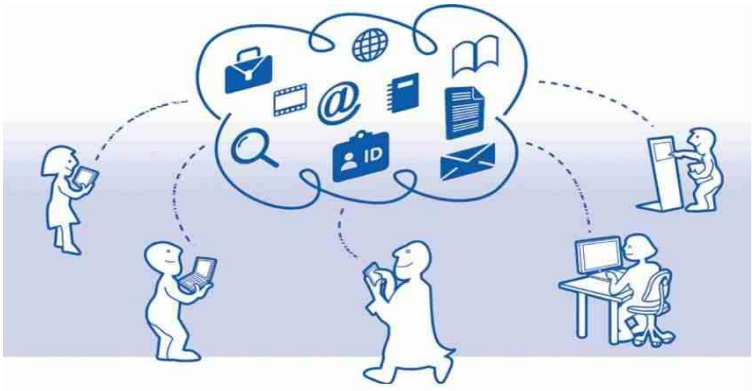
- Facilitat per recuperar dades esborrades o malmeses.

Els proveïdors de cloud computing, que per la naturalesa de la tecnologia es poden ubicar a qualsevol part del món, ofereixen diferents nivells i tipus de serveis als clients. Aquests subministren el servei als seus clients mitjançant tres modalitats bàsiques: infraestructura informàtica (IaaS), plataformes informàtiques (PaaS) i aplicacions com a servei (SaaS).

Aquests recursos i serveis són desplegats i compartits entre usuaris de diferents maneres. Un és a través d'un núvol públic, al qual accedeixen tota mena de clients a través de xarxes convencionals. Un altre és a través d'un núvol privat, que exclusivament utilitza i controla el client. I el tercer en importància és el núvol híbrid, que es caracteritza per barrejar les possibilitats dels núvols públics i privats. Tots aquests tipus de cloud tenen com una de les seves prioritats salvaguardar la seguretat i privacitat de la informació que emmagatzemen.

Les peculiaritats de la computació al núvol imposen més exigències tant a proveïdors com a usuaris i fan necessari cuidar diferents aspectes, per aprofitar tots els avantatges i possibilitats de la tecnologia. Aquests aspectes inclouen els nivells de seguretat, la protecció de les dades dels usuaris, les característiques legals dels contractes de proveïment, bàsicament condicionats per la deslocalització dels serveis, els models de pagament per ús, etc.

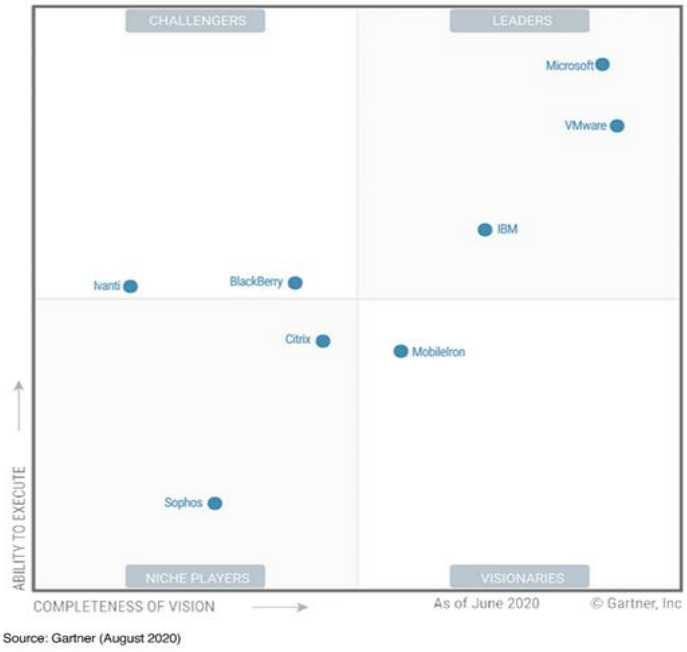
En el món tecnològic actual, dominat per la innovació contínua i accelerada, el cloud computing és pot dir que ja és una realitat consolidada. Les organitzacions s'adapten cada vegada més a la nova manera d'entendre i de disposar de maquinari i programari, alhora que tenen cada vegada més experiència en aprofitar al màxim la tecnologia. Aquest camí, que és irreversible, tot just acaba de començar i, superant la reticent barrera més gran per al seu ús com és la seguretat de l'entorn, té un recorregut extraordinari. El núvol ja és la base per a l'ús de les TIC per part dels usuaris que busquen mobilitat, potència de recursos, facilitat de funcionament i baix cost.



Il·lustració 3: Concepte de Cloud Computing

3. PROCÉS DE SCREENING

La font de selecció per al procés de screening es centrarà en els fabricants líders de productes de Gestió Unificada d'Endpoint (*Unified Endpoint Management*) que estan més ben posicionats en el quadrant màgic de Gartner publicat l'any 2020. Tal com es mostra en la següent il·lustració, les solucions escollides seran les de Microsoft, VMware i IBM.



Il·lustració 4. Magic Quadrant for Unified Enpoint Management

Per la consultora Gartner, els líders son els proveïdors de solucions UEM que obtenen les millors puntuacions en l'avaluació de l'execució i visió dels seus productes, els quals exemplifiquen el conjunt de funcions que assisteixen la gestió tant els dispositius mòbils com els PCs. Els líders també donen orientació i eines per ajudar a migrar des d'una gestió tradicional del client fins a una gestió moderna, així com una integració d'eines analítiques i de seguretat que contribueixen a una simplificació de la gestió del dispositiu i una millorada experiència d'usuari.

3.1. CONSULTORA TECNOLÒGICA GARTNER

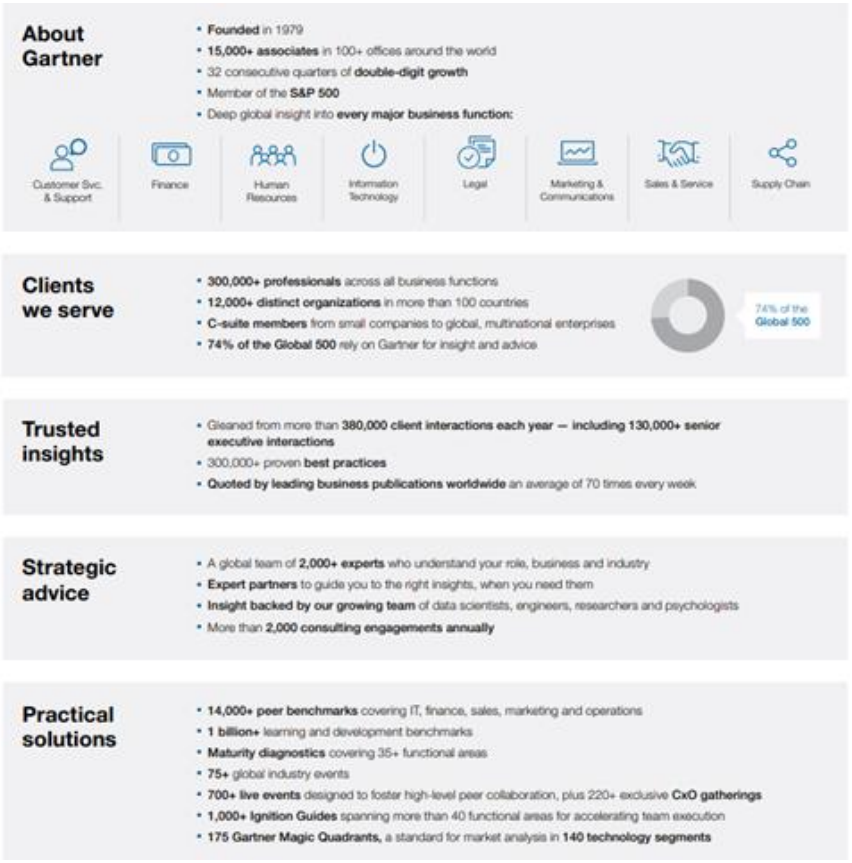
Gartner Inc. és líder mundial en consultoria i recerca en el mercat de les noves tecnologies. El seu focus principal és investigar i analitzar quines són les noves tendències tecnològiques del mercat de les TIC. Amb les dades obtingudes de les

seva recerca desenvolupen rànquings de les millors empreses o fabricants amb els millors productes i solucions presents en el mercat IT. Els clients de Gartner son un important número de grans corporacions i agències governamentals, així com destacades empreses d'IT, d'inversió i de consultoria.

El resultat de les seves prospeccions de mercat i de recerca es detalla gràficament en el que es coneix com el Quadrant Màgic de Gartner (vegis Il·lustració 4). En aquesta gràfica, s'hi posicionen les diferents solucions de fabricant respecte un segment tecnològic i la visió obtinguda al respecte per part dels experts de Gartner que compte amb més de 2000 consultors en diversos camps.

Aquestes anàlisis tenen molta acceptació i credibilitat en el conjunt de tecnòlegs que tenen responsabilitats i prenen decisions IT dins les organitzacions. Per tant, la idea d'obtenir un bon posicionament en aquests informes motiva als fabricants a millorar constantment els seus serveis o productes.

En els últims anys, els serveis de Gartner s'han expandit més enllà de la investigació i l'anàlisi de mercats de les tecnologies de la informació per incloure també en la seva cartera estratègia, organització i lideratge.



il·lustració 5. Gartner, a cop d'ull. (Font: Gartner)

La visió de Gartner sobre el mercat de la gestió unificada d'endpoint (UEM) no es situa en el mercat tal com és avui, sinó que es centra en les propostes tecnològiques transformadores que pretenen donar resposta a les necessitats futures dels usuaris finals. En concret, defineix el mercat d'eines UEM com el conjunt de propostes que engloben la gestió dels dispositius mòbils i els ordinadors personals, des d'una única consola, procurant per la protecció de les dades, i la configuració i les polítiques d'ús del dispositiu. Gartner entén que una gestió UEM ha d'incloure:

- Una visió centrada en l'usuari del dispositiu.
- Gestió del PC via els controls natius de Windows10, macOS i Chrome OS.
- MDM a través de controls natius d'iOS i Android.
- Analítica agregada i telemetria d'usuaris, i aplicacions per ajudar a definir la política i les accions relacionades.
- Proporcionar informació sobre l'experiència de l'usuari a través de l'agregació dels indicadors de telemetria, esdeveniments i registres.
- Integrar eines unificades de seguretat de punts finals (UES) per donar suport a les polítiques de seguretat, executar accions administratives i permetre la integració amb eines de gestió d'identitat i accés (IAM).

A més, UEM pot oferir la gestió directa de dispositius no tradicionals, com ara dispositius d'Internet de les Coses (IoT) i *wearables*; No obstant això, Gartner no considera que aquestes extensions de gestió siguin bàsiques, ara per ara.

3.2. MICROSOFT ENDPOINT MANAGER

La companyia multinacional creada pels emprenedors Bill Gates i Paul Allen, que dissenya i comercialitza múltiples solucions de programari i dispositius, ofereix un producte, sota la plataforma Microsoft365, que dona cobertura a la gestió del dispositiu: Microsoft Endpoint Manager.

Microsoft Endpoint Manager assisteix als equips IT entregant funcions d'administració i control per garantir un accés segur, protegir les dades i respondre als riscos que s'enfronten els dispositius IT. Els endpoint poden estar al núvol o a l'oficina, ser mòbils o estàtics, o bé tenir un sistema operatiu o altre.

Microsoft Endpoint Manager és un lloc web únic per crear directives i administrar els dispositius, i per facilitar una gestió unificada es connecta a diversos serveis

d'administració com Microsoft Intune, Configuration Manager, Anàlisis d'escriptori, Administració conjunta i AutoPilot, juntament, amb els grups d'usuaris, la seguretat, l'accés condicional i els informes.

3.2.1. Microsoft Intune

Microsoft Intune, és el servei principal de la plataforma UEM de Microsoft. És un servei basat en el núvol que es centra en l'administració de dispositius (MDM) i d'aplicacions mòbils (MAM). Pot controlar com es fan servir els dispositius de l'organització, és a dir, els telèfons mòbils, les tauletes i els equips PC. També, pot configurar directives específiques per controlar les aplicacions, com per exemple, evitar que s'enviïn missatges de correu electrònic a persones alienes a l'organització. Intune permet que les persones de l'organització facin servir els seus dispositius personals per la feina, però fent que les dades de l'organització romanguin protegides i aïllades de les dades personals.

Intune forma part del conjunt d'aplicacions Enterprise Mobility + Security (EMS) (plataforma intel·ligent de seguretat i d'administració de la mobilitat) de Microsoft. Intune s'integra amb Azure Active Directory (Azure AD) per controlar qui té accés i a què es pot tenir accés. També, s'integra amb Azure Information Protection per a la protecció de les dades i el compliment dels requisits de seguretat del dispositiu d'usuari.

Administració dels dispositius

Intune adopta estratègies adaptades a les necessitats de gestió de dispositius:

Per als dispositius que pertanyen a l'organització, és pot aplicar un control total, com ara la configuració, les característiques de treball i la seguretat. En aquest enfoc, els dispositius i els seus usuaris s'inscriuen a Intune per rebre les regles i els paràmetres de configuració establerts en les polítiques de dispositiu. Per exemple, es poden definir requisits de contrasenya, crear una connexió VPN, l'accés als continguts, configurar la protecció contra amenaces, i molt més.

Per a dispositius personals o BYOD, és possible que els usuaris no vulguin que els administradors IT hi tinguin un control total. En aquest cas, es donen diferents opcions: els usuaris inscriuen els seus dispositius si volen accés complet als recursos de l'organització, talment com si fos corporatiu; o bé, si aquests usuaris només volen accedir al correu electrònic o d'altres aplicacions, s'hi apliquen polítiques de protecció d'aplicacions que requereixen d'autenticació multifactor (MFA).

Quan els dispositius s'inscriuen i es gestionen a Intune, els administradors poden:

- Visualitzar els dispositius inscrits i obtenir un inventari de dispositius que accedeixen als recursos de l'organització.
- Configurar els dispositius per complir amb els estàndards de seguretat i de manteniment que s'estableixin.
- Inserir certificats als dispositius perquè els usuaris puguin accedir de manera fàcil i segura a la xarxa o utilitzar una VPN per connectar-se a l'organització.
- Visualitzar informes respecte a dispositius i usuaris.
- Suprimir les dades d'empresa davant d'un cas de pèrdua o robatori del dispositiu.

Gestió d'aplicacions

A Intune, la gestió d'aplicacions mòbils (MAM) està dissenyada per protegir les dades de l'organització a nivell d'aplicació tant en dispositius propietat de l'organització com personals. Quan les aplicacions es gestionen a Intune, els administradors poden:

- Afegir i assignar aplicacions a grups d'usuaris i dispositius.
- Configurar les aplicacions per executar-les amb entorns específics i actualitzar les aplicacions al dispositiu.
- Visualitzar els informes d'ús de les aplicacions i fer-ne un seguiment.
- Realitzar una neteja selectiva, eliminant només les dades de l'organització de les aplicacions.

Una de les maneres en que Intune proporciona seguretat a les aplicacions mòbils és mitjançant polítiques de protecció, i per fer-ho:

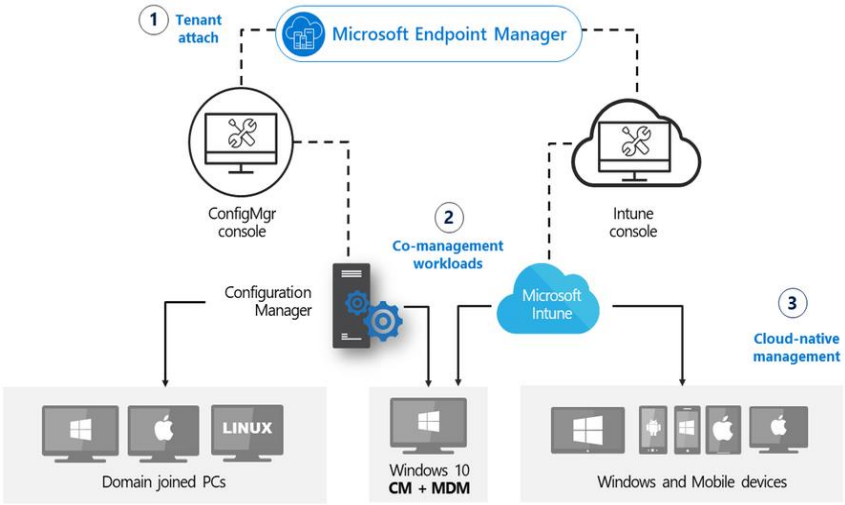
- Utilitza la identitat d'Azure AD per aïllar les dades de l'organització de les dades personals. Les dades a les quals s'accedeix mitjançant credencials d'organització tenen protecció de seguretat addicional.
- Ajuda a protegir l'accés des dels dispositius personals, restringint les accions que els usuaris poden fer, com ara copiar i enganxar, desar i visualitzar.
- Es poden crear i desplegar polítiques als dispositius que estiguin inscrits a Intune o bé que estiguin inscrits en un altre servei de gestió de dispositius mòbils, o inclús que no estiguin inscrits en cap servei MDM. Als dispositius inscrits, les polítiques de protecció d'aplicació poden afegir nivells de protecció addicional.

Per exemple, un usuari que inicia la sessió en un dispositiu amb les seves credencials d'organització li permet accedir a dades que amb la identitat personal li serien denegades. Quan s'utilitzen les dades de l'organització, les normes de protecció d'aplicacions controlen com es desen i es comparteixen les dades, i quan els usuaris inicien la sessió amb la seva identitat personal, no s'apliquen les mateixes proteccions. D'aquesta manera, es controlen les dades empresarials, mentre que l'usuari manté el control i la privadesa de les seves dades personals.

Intune està agregat dins la plataforma EMS de Microsoft la qual cosa proporciona un conjunt més ampli de funcions de protecció de les dades i d'aplicacions mòbils.

3.2.2. Administrador de configuració

Configuration Manager és una solució de gestió local per a la gestió de PCs que es troben a la xarxa o a Internet. Es pot connectar al núvol i integrar amb Intune, Azure Active Directory, Microsoft Defender i altres serveis Microsoft en el núvol. Des d'aquí, es poden implementar aplicacions, actualitzacions de programari i sistemes operatius. També es pot controlar el compliment, consultar els dispositius en temps real i actuar sobre aquests. Aquest servei participa en la cogestió davant d'instal·lacions ja existents de dispositiu, bàsicament on-premise. Tant mateix, i observant les tendències, les organitzacions que fan ús de Configuration Manager és de preveure que no dubtin a evolucionar cap una administració completa de l'entorn endpoint des del núvol.



Il·lustració 6. Cogestió entre Configuration Manager i Intune (font: Microsoft)

3.2.3. Desktop Analytics

Aquest servei proporciona informació detallada i intel·ligent per poder prendre decisions sobre la preparació d'actualitzacions per als clients Windows. Combina les dades de l'organització amb les dades agregades de milions de dispositius connectats als serveis de Microsoft en el núvol per proveir una base de dades de coneixement operacional. L'anàlisi d'escriptori ofereix les següents prestacions:

- Inventari de maquinari i programari.
- Identificació del conjunt més petit de dispositius que proporcionen la cobertura més àmplia de factors. Amb el resultat del pilot que té més èxit, els desplegaments en producció es poden continuar escalant de forma ràpida i confiable.
- Identificació de problemes en base a les informacions habilitades al núvol i en combinació amb les dades del propi entorn de l'organització. El servei prediu problemes potencials davant de les actualitzacions i suggereix possibles mitigacions.
- Integració amb Configuration Manager per habilitar en el núvol la infraestructura local existent. Les dades i analítiques seran d'útilitat per implementar i administrar Windows als dispositius.

3.2.4. Windows Autopilot

Windows Autopilot és una col·lecció de funcions utilitzades per configurar nous dispositius i preparar-los per a un ús productiu. També s'utilitza per reinicialitzar, reassignar i recuperar dispositius mitjançant un procés fàcil i senzill.

AutoPilot simplifica el cicle de vida dels dispositius Windows tant per al servei IT com per als usuaris finals, des de la implementació inicial fins al final de vida, aportant aquestes avantatges:

- Reducció del temps dedicat a distribuir, administrar i suprimir dispositius.
- Redueix la infraestructura necessària per mantenir els dispositius.
- Maximitza la usabilitat del dispositiu per a tot tipus d'usuaris.

Els professionals IT dediquen molt temps a crear i personalitzar imatges que s'han de desplegar als dispositius. No obstant, usant Autopilot, des del punt de vista IT, l'única interacció que es requereix és que l'usuari és connecti a una xarxa amb les

seves credencials i tota la resta està automatitzada. Des de la perspectiva d'un usuari, només es esperar que algunes operacions acabin perquè el dispositiu estigui llest per utilitzar-lo. Windows Autopilot assumeix les següents funcions UEM:

- Uneix automàticament els dispositius a l'Azure Active Directory.
- Inscripció o enrolament automàtic de dispositius al servei Intune.
- Crea i assigna automàticament dispositius als grups de configuració en funció del perfil d'ús.

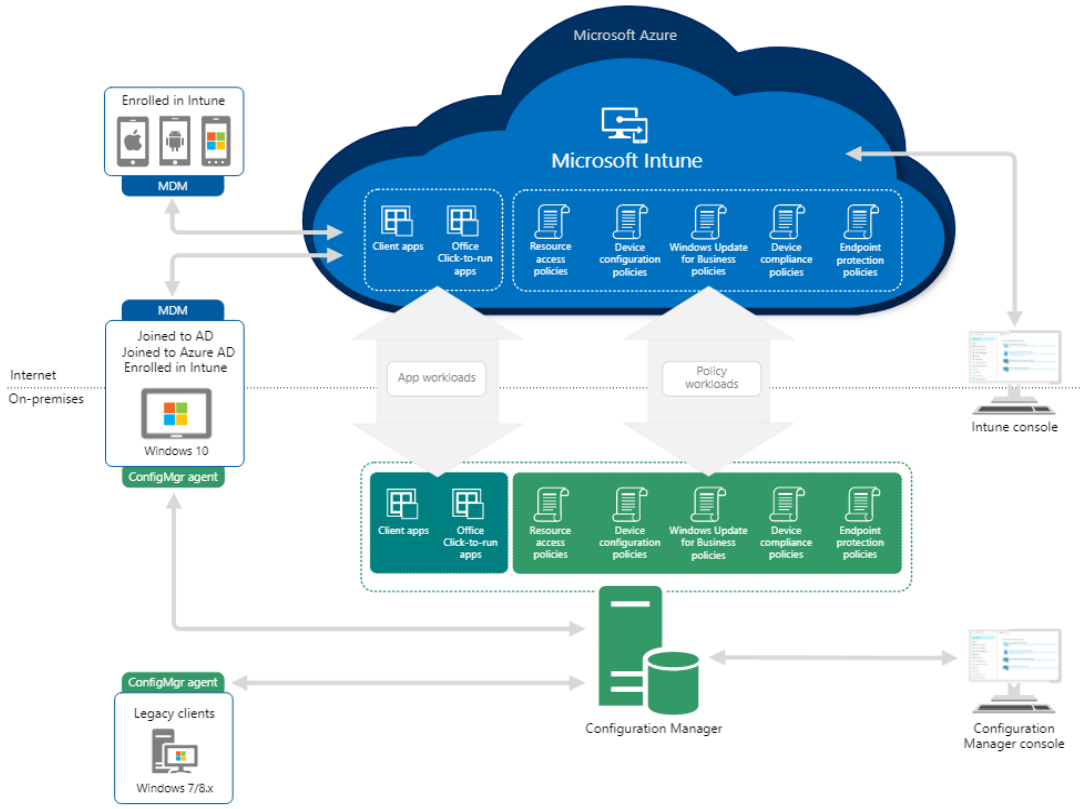
Per distribuir nous dispositius Windows, Autopilot utilitza la versió optimitzada OEM de Windows 10 que ve preinstal·lada al dispositiu, de manera que no cal mantenir imatges i controladors personalitzats per a cada model de dispositiu. La instal·lació resultant de Windows 10 en el dispositiu adopta l'estat de "business-ready", i ja s'hi podran aplicar les configuracions i polítiques, instal·lar les aplicacions o canviar l'edició de Windows 10 que s'està utilitzant (per ex. de Windows 10 Pro a Windows 10 Enterprise) per admetre característiques operatives avançades.

Un dispositiu ja existent també es pot preparar ràpidament per a un nou usuari amb l'opció de restabliment de l'AutoPilot. La capacitat de reinicialització també és d'utilitat en escenaris d'interrupció de funcionament per retornar en poc temps un dispositiu a un estat estable i preparat per treballar de nou.

A mode de resum, es pot fer una ullada a la següent il·lustració on es descriuen les capacitats funcionals clau de la plataforma UEM de Microsoft:

Il·lustració 7. Capacitats clau de Microsoft Endpoint Manager (font: Microsoft)

Tot seguit es mostra el model operatiu conjunt que engloba la plataforma UEM de Microsoft.



Il·lustració 8. Model operatiu de Microsoft Endpoint Manager (font: Microsoft)

3.3. VMWARE Workspace ONE Unified Endpoint Management

La companyia que subministra la major part del programari de virtualització de computadors a arreu del mon, també ha desenvolupat una solució completa per la gestió de l'endpoint: Workspace ONE Unified Endpoint Management.

VMware Workspace ONE UEM és una plataforma d'administració de dispositius IT que permet la gestió completa del cicle de vida d'una àmplia varietat de punts finals, com poden ser telèfons intel·ligents, tauletes, equips Windows i també dispositius de propòsit especial.

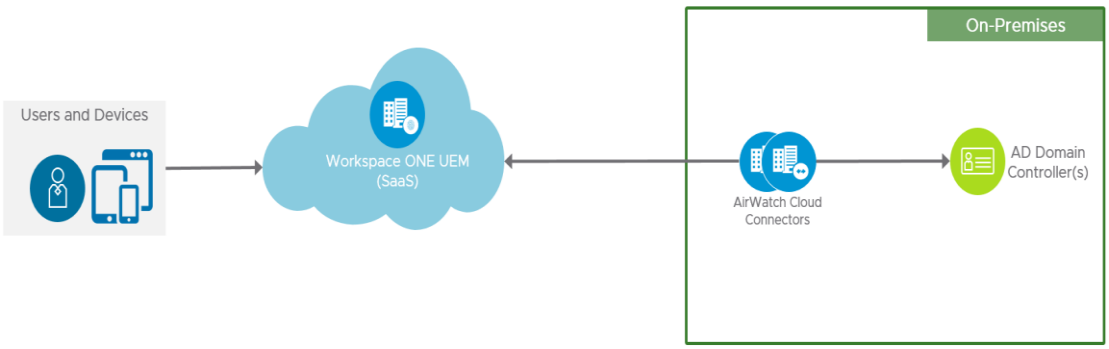
Aquesta plataforma integra l'enrolament dels dispositius, un catàleg d'aplicacions mòbils, l'aplicació de polítiques pel que fa al compliment del dispositiu i la integració amb serveis empresarials, com ara correu electrònic, programari i continguts. Les

característiques destacables de Workspace ONE Unified Endpoint Management son les següents:

- Capacitat d'implementació d'aplicacions de forma automàtica o a través d'autoservei.
- Serveis de perfils d'usuari i de dispositiu que garanteixen la configuració per complir amb els requisits de seguretat de l'empresa i simplificar l'accés de l'usuari a les aplicacions.
- Eines de productivitat que inclouen un client de correu electrònic segur, una eina d'administració de continguts per emmagatzemar i gestionar la informació de forma segura, i un navegador web per garantir un accés securitzat a la informació i a les eines corporatives.

Workspace ONE UEM es pot implementar mitjançant un model local o basat en el núvol (SaaS). Tots dos models ofereixen les mateixes funcionalitats. Amb una implementació basada en el núvol, el programari UEM de Workspace ONE es lliura com un servei (SaaS). Per sincronitzar aquest servei amb els recursos interns com Active Directory o una autoritat de certificació, cal emprar un connector en el núvol.

Una implementació senzilla sol consistir en un Tenant del Wokspace ONE UEM i un VMware AirWatch Cloud Connector, tal com es presenta en la següent il·lustració.



Il·lustració 9. Model de funcionament Workspace One UEM (font: vmware)

La plataforma UEM de VMware forma part del conjunt de components integrants de la plataforma Workspace ONE i es recolza en altres serveis de la mateixa família per donar solució als aspectes d'autenticació d'accés (Workspace ONE Accés), i per a la distribució de continguts i aplicacions empresarials (Workspace ONE Intelligence).

3.3.1. Workspace ONE

VMware Workspace ONE és la solució d'àrea de treball de VMware. És una plataforma digital que proporciona i gestiona qualsevol aplicació en qualsevol dispositiu mitjançant el control d'accés, la gestió d'aplicacions i una gestió multiplataforma dels punts finals.

VMware Workspace ONE es basa en la tecnologia de gestió unificada de punts finals de Workspace ONE UEM, i s'integra amb el component de lliurament d'aplicacions virtuals VMware Horizon en un marc d'identitat única que proporciona Workspace ONE Access. D'aquesta manera, la plataforma permet oferir un espai de treball digital que inclou els dispositius i les aplicacions d'empresa, sense renunciar a la seguretat i control. Les propietats de Workspace ONE es descriuen tot seguit.

Autenticació d'accés a les aplicacions

Els usuaris, mitjançant l'inici de sessió únic (SSO), obtenen entrada a un catàleg que els dona accés a les aplicacions. Aquest catàleg inclou aplicacions mòbils, aplicacions web, aplicacions en el núvol i aplicacions Windows. Un cop iniciada la sessió, els usuaris poden seleccionar les aplicacions que necessiten i simplement posar-se a treballar sense cap mena de suport tècnic addicional. Aquesta característica, per tant, aporta les següents prestacions:

- Proporciona un accés fàcil a totes les aplicacions que els usuaris necessiten per fer la seva feina, ja sigui a través d'un catàleg disponible a través del navegador o des de Workspace ONE Intelligent Hub.
- Habilita un accés d'autoservei on agafar les aplicacions que necessiten els usuaris.
- L'inici de sessió únic significa que els usuaris no han de recordar un munt de credencials ni escriure la mateixa contrasenya cada vegada que accedeixen a una aplicació. Mitjançant, també, l'ús de certificats, Workspace ONE proporciona una manera segura i senzilla d'accés i una millor experiència d'inici de sessió.

Administració unificada de punts finals

Workspace ONE és transparent sobre quines plataformes s'ha de desplegar la gestió i centra el seu objectiu en donar suport en qualsevol tipus de dispositiu. Des del sistema operatiu d'escriptori fins al sistema operatiu mòbil, o bé si l'endpoint és de propietat corporativa o és de tipus byod, podran ser configurats i gestionats amb seguretat i compliment.

Control d'accés a la xarxa

Per protegir la informació més sensible, Workspace ONE combina la identitat i la gestió de dispositius per fer complir les directives d'accés. Aquestes directives poden ser en base a una sèrie de condicions: l'autenticació, la xarxa, la ubicació i el compliment del dispositiu. Per tant, proporciona un potent motor de polítiques que seran aplicades segons els nivells d'accés que han d'obtenir els usuaris:

- Les polítiques d'accés condicional es poden desplegar per aplicació mitjançant l'autenticació o bé restringir l'accés per àmbit de xarxa o per qualsevol restricció de dispositiu.
- Aplica proteccions contra dispositius alliberats i estableix la llista d'aplicacions permeses i denegades. Controla les restriccions de les apps, l'ús de cut/copy/paste, més una sèrie de polítiques i restriccions avançades.
- Exploració en temps real de dispositius, aplicacions i consoles que proporcionen informació detallada per la monitorització del sistema Endpoint, juntament amb una visualització d'informes predefinits.

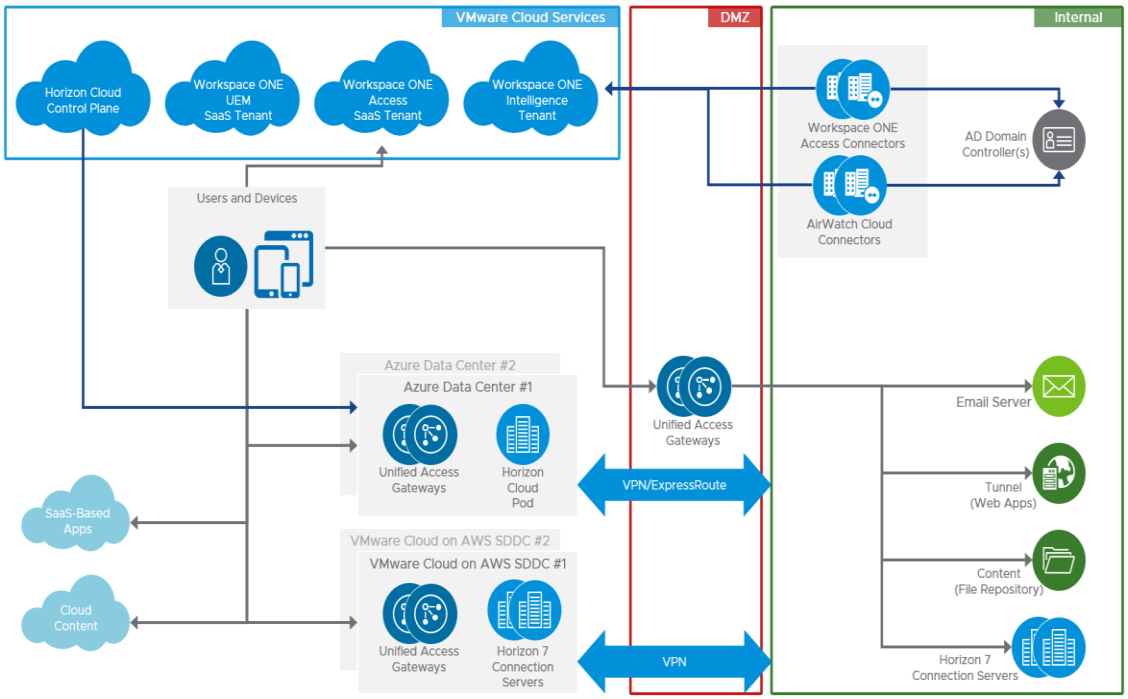
Gestió automatitzada d'aplicacions

Workspace ONE, suportat per les tecnologies de Workspace ONE UEM i Horizon virtualization, permet als administradors automatitzar la distribució de les aplicacions i les actualitzacions, tant si es despleguen aplicacions Windows o aplicacions mòbils o, fins i tot, aplicacions virtualitzades. Workspace ONE proporciona una única plataforma que cobreix tota l'automatització del procés de lliurament d'aplicacions de manera segura i amb compliment en qualsevol dispositiu gestionat:

- La gestió simplificada i l'aprovisionament de dispositius permet a Workspace ONE fer desaparèixer la necessitat d'imatges de dispositiu. Amb la funció de grups intel·ligents dinàmics, que utilitzen informació del dispositiu i els atributs dels usuaris, el sistema sempre te disponible la configuració necessària per ser reproduïda de nou als dispositius.
- Instal·la, actualitza i suprimeix paquets de programari. Crea un flux de treball, sota una varietat de condicions definides pels administradors per a les aplicacions d'usuari, els fitxers, els scripts i les ordres per instal·lar els punts finals i la seva configuració durant l'enrolament.
- Horizon proporciona aplicacions i escriptoris virtuals que permeten als usuaris treballar amb informació sensible i confidencial sense comprometre les dades corporatives. Els usuaris poden accedir a les seves aplicacions i

escriptoris virtuals des del Workspace ONE Intelligent Hub, permetent-los la flexibilitat de ser productius allà on necessitin.

La següent il·lustració mostra l'arquitectura Workspace ONE.



Il·lustració 10: Arquitectura Workspace ONE (font: vmware)

3.3.2. Components de Workspace ONE UEM

En el marc de la plataforma Workspace ONE de vmware, els elements que participen de manera directa en la gestió unificada del punts finals son els següents:

Consola UEM

Consola d'administració per supervisar i dur a terme la gestió dels dispositius gestionats i el seu entorn de treball. Des de la consola, també, es configuren les polítiques UEM definides per l'organització.

Serveis de dispositius

Conjunt de serveis que es comuniquen amb els dispositius gestionats. Workspace ONE UEM es basa en aquest component per a la inscripció dels dispositius, la provisió d'aplicacions, el lliurament d'ordres, la recepció de dades del dispositiu i el

hosting que subministra el catàleg d'autoservei d'aplicacions que han de ser lliurades als usuaris.

API Endpoint

Col·lecció d'APIs que permet als programes externs ó de tercers utilitzar les funcionalitats bàsiques del producte, integrant les API en infraestructures IT existents i en aplicacions. Aquestes API també són utilitzades per diversos serveis Workspace ONE UEM, com per exemple, Secure Email Gateway per a les interaccions i recopilacions de dades.

Connector Cloud AirWatch

Component que realitza la sincronització i l'autenticació d'usuaris mitjançant un recurs local com pot ser Active Directory o una entitat emissora de certificats de confiança. Aquest servei està allotjat a la xarxa interna.

Servei de missatgeria AirWatch

Servei utilitzat conjuntament amb l'AirWatch Cloud Connector per proporcionar una comunicació segura amb els sistemes locals. AirWatch Cloud Connector també utilitza aquest servei de missatgeria per comunicar-se amb la consola UEM i agilitza el lliurament de missatges i ordres, eliminant la necessitat que els usuaris accedeixin a Internet o utilitzin comptes personals, com ara els ID de Google.

Serveix com a substitut de Google Cloud Messaging per a dispositius Android i és l'única opció per proporcionar capacitats de gestió de dispositius mòbils per a entorns Windows. Els dispositius d'escriptori Windows que actuen amb Workspace ONE Intelligent Hub utilitzen aquest serveis de missatgeria per a notificacions en temps real.

Túnel VMware

VMware Tunnel proporciona un mètode segur i eficaç perquè les aplicacions accedeixin als recursos corporatius allotjats a la xarxa interna. Aquest servei utilitza un certificat X.509 per autenticar i xifrar el trànsit de dades de les aplicacions dels dispositius.

VMware Tunnel té dos possibles components: Proxy i Per-App VPN. El component proxy s'encarrega d'assegurar el trànsit des dels dispositius fins als recursos locals o intranet, a través de Workspace ONE Web App (navegador propi de Workspace ONE). El component Per-App Tunnel permet túnels a nivell d'aplicació (en lloc de túnels a nivell de dispositiu) per a aplicacions en dispositius iOS, MacOS, Android i Windows.

3.4. IBM MaaS360

El gegant blau de la informàtica també fabrica i comercialitza un software en modalitat de servei al núvol (SaaS) que s'ocupa de la gestió del dispositiu IT: IBM MasS360.

MaaS360 és un servei per al control, la mobilitat i la gestió dels dispositius mòbils. Subministra el software des d'una plataforma cloud integrada que s'adapta a les necessitats de cada negoci, oferint funcionalitats i eficiència. És compatible amb qualsevol tipus de dispositiu mòbil i la majoria de sistemes operatius.

El programari MaaS360 és una eina que es gestiona de forma remota i segura, aportant visibilitat de l'ús i l'estat dels diferents dispositius, alhora que s'ocupa de protegir les dades corporatives.

Aquesta solució es pot integrar fàcilment en l'estructura TIC ja existent de l'empresa, proporcionant nous escenaris de treball per als usuaris. Amb MaaS360, l'usuari mateix pot realitzar una administració dels diferents dispositius mòbils que usa i pot gestionar tant el treball professional com el personal. D'aquesta manera, facilita una millor continuïtat de les tasques dels usuaris i permet fer un seguiment detallat de l'activitat empresarial. El control d'accés segur, la localització o l'intercanvi de documents proporcionen a l'usuari un entorn de confiança i de seguretat per desenvolupar la seva activitat.

3.4.1 Característiques funcionals

Registre i Integració

El registre de dispositius mòbils es realitza de forma remota per SMS, correu electrònic o una URL personalitzada. La seva senzilla integració amb el sistema empresarial dona noves opcions d'executar l'activitat professional sense necessitat d'incorporar nous servidors locals ni reconfiguracions de xarxa.

Gestió central de dispositius mòbils

La gestió centralitzada permet administrar tots els dispositius des d'un únic lloc, proporcionant un ús més adequat i eficient de les característiques mòbils. MDM permet la configuració de perfils de correu electrònic, calendari i aplicacions d'usuari. També permet la distribució i actualització de les aplicacions, l'enviament de documents de forma segura, la definició de drets d'accés, o la creació de grups personalitzats per a una gestió més granular.

Gestió d'aplicacions mòbils

MaaS360 mostra als dispositius un catàleg d'aplicacions empresarials i personalitzades que aprovisionen a l'usuari les diferents aplicacions mòbils. També s'ocupa d'instal·lar les actualitzacions de les aplicacions. L'usuari rep les millores funcionals en el seu dispositiu, per continuar operant amb els fluxos de treball empresarial establerts.

Seguretat proactiva del dispositiu mòbil

MaaS360 protegeix i aplica control sobre smartphones, tablets o PC portàtils, adoptant les mesures de seguretat adequades per a cada dispositiu. El sistema especifica les normes de d'accés amb capacitat per poder configurar la complexitat, l'extensió i el temps de vida de les credencials. En cas de pèrdua o robatori d'un dels dispositius, permet remotament la seva localització, el bloqueig i l'esborrat de les dades que conté. Detecta i restringeix l'accés als recursos als dispositius alliberats o manipulats.

Seguretat de l'aplicació mòbil

MaaS360 aporta seguretat, autenticant els usuaris abans d'accedir a les aplicacions. Permet realitzar un encapsulat a nivell d'aplicació per protegir l'accés a les dades corporatives, sense necessitat d'una VPN de dispositiu. A més, restringeix les accions de còpies locals de dades per evitar-ne un mal ús. En cas d'infraccions d'incompliment, l'eina enviarà diferents alertes en temps real i així poder verificar el funcionament del dispositiu mòbil.

Seguretat de correu electrònic i navegació

Admet encriptació AES-256 per obtenir compatibilitat per al correu en el núvol com Office 365 i Gmail. Abans d'accedir al servei, deixa habilitar l'autenticació i comprovar el compliment en línia i fora de línia. MaaS360 MDM també restringeix el reenviament i lliurament d'altres aplicacions, així com també limita la funció copiar-i-enganxar i les captures de pantalla. De la mateixa manera, permet accedir de manera segura a llocs d'intranet corporatius sense VPN, bloquejar llocs web maliciosos a través d'un motor d'anàlisi i una base de dades de reputació. Alberga una selecció de categories d'URL per permetre l'accés, el bloqueig i l'execució de traces de navegació.

Seguretat en l'intercanvi de documents

MaaS360 visualitza i emmagatzema el contingut de forma segura en un contenidor xifrat. També restringeix la funció copia-i-enganxa fora del contenidor, l'accés als continguts, i l'intercanvi de fitxers corporatius. A més, ofereix la possibilitat de configurar la data i hora de caducitat dels documents.

Assistència tècnica

La plataforma MaaS360 proporciona suport 24×7 per diagnosticar i resoldre problemes de dispositiu, usuari o aplicació. Proporciona un control complet i garanteix una productivitat òptima dels dispositius mòbils. De la mateixa manera, permet localitzar dispositius perduts o robats, actualitzar la configuració en temps real i ajudar als usuaris a solucionar incidències.

Reporting amb Watson

MaaS360 realitza en temps real informes detallats i resums interactius de les operacions de gestió. Ofereix la creació de diferents tipus d'informes: documents detallats i personalitzats sobre el seguiment de l'activitat; informació sobre la configuració i gestió d'alertes per detectar vulnerabilitats dins del sistema; llistes de vigilància personalitzables; historial de compliment; privadesa dels dispositius personals; així com inventaris de maquinari i programari i cerques intel·ligents integrades.

Watson és una plataforma d'intel·ligència artificial desenvolupada també per IBM que MaaS360 utilitza per lliurar els informes de referència que ajuden a configurar i validar de manera òptima l'entorn Endpoint.

Il·lustració 11. Diagrama funcional IBM Maas360 (font: IBM)

3.4.2. Arquitectura de MaaS360

L'eina MaaS360 administra plenament els dispositius mòbils des del núvol mitjançant tres components:

- Un servidor integrat a la plataforma digital on es desenvolupa la gestió de dispositius mòbils (MDM).
- Una base de dades que permet l'emmagatzematge de tota la informació processada a través dels diferents dispositius mòbils.
- Un agent que s'instal·la automàticament en cadascun dels smartphones, tablets o portàtils que es vulguin gestionar.

Els tres elements que estructuren MaaS360 interactuen de manera coordinada per a l'execució de les seves funcions. Concretament, els agents mantenen una connexió directa amb el servidor integrat en el núvol a través de mitjans de transmissió de dades físiques com son les xarxes cablejades o bé les xarxes sense fils (WiFi, 4 ó 5G, etc.)

Il·lustració 12. Arquitectura IBM Maas360 (font: IBM)

4. PROCÉS DE SCORING

Una vegada realitzat el procés de screening de les solucions proposades pels tres fabricants que donen resposta a la gestió de l'endpoint, es necessari definir els principals criteris de valoració que s'utilitzaran per establir el procés de scoring.

Es aconsellable també determinar un sistema de ponderació per a la valoració dels diferents criteris, i agrupar els elements de valoració en base a criteris funcionals i tècnics, i en cada cas, fer les valoracions de cadascuna de les solucions.

4.1. CRITERIS D'AVALUACIÓ

Els criteris es basaran en identificar si unes característiques clau estan presents o no en els productes UEM de Microsoft, VMware i IBM. S'ha fet una agrupació en les següents set categories de característiques:

Opcions d'implantació i sistemes operatius suportats

Aquest grup engloba totes les característiques relacionades amb el sistema operatiu i les formes d'implantació que entrega el producte UEM, és a dir, per una banda, si es pot implementar de manera local, en núvol o de manera híbrida, o per altra banda, si s'admeten versions anteriors de Windows. Si aquest aspecte és important per a una organització, cal assegurar-se quins SO *legacy* suporta el programari, o bé si admeten Linux, *VDI*, o suport per IoT i weareables.

Seguretat i privacitat

El programari UEM ha de proporcionar seguretat i privacitat per a les dades, connexions i aplicacions a través d'una àmplia varietat de mètodes. Uns fabricants confien en una connexió VPN segura, mentre que altres es basen en el xifratge dels contenidors.

Una contenidorització d'aplicacions és un mètode per privatitzar les aplicacions i les dades corporatives, però no tots els proveïdors utilitzen contenidors sinó que apliquen la seguretat de diferents maneres.

Alguns productes poden detectar dispositius alliberats i aplicacions malicioses, mentre que altres se centren més en les capacitats antimalware. Atès que la seguretat és una característica crítica en una solució UEM, la selecció ha de considerar plenament les capacitats del producte en aquesta categoria.

Gestió de dispositius i cicle de vida

El programari UEM ha de ser capaç de realitzar una àmplia varietat de tasques de gestió ja que aquesta administració és fonamental per a la seguretat de l'empresa, especialment, en entorns BYOD. La solució ha de ser capaç de gestionar un gran ventall de dispositius, des de PC fins a dispositius IoT. El sistema també ha de oferir un quadre de comandament que pugui servir com un únic punt de monitorització de l'entorn.

Gestió d'aplicacions i programari

Els administradors IT han de tenir un catàleg d'aplicacions controlat que permeti als usuaris descarregar i treballar amb les aplicacions empresarials aprovades.

Una característica destacable que tenen algunes eines UEM és la capacitat d'interactuar amb les aplicacions de l'Office 365. Cal tenir present que les diferents solucions proporcionaran diferents experiències, per tant, aquest és un aspecte important per a les empreses que han invertit en aplicacions Office de Microsoft.

Desplegament i inscripció (enrollment)

A l'hora d'avaluar les capacitats d'implementació i enrolament, s'ha de tenir en compte els dispositius, les aplicacions i el seus tipus d'usuaris. Les eines natives del sistema operatiu sovint contemplen la implementació i la inscripció o enrolament al servei, no obstant això, alguns productes UEM poden necessitar de la seva pròpia eina per implementar el servei.

La facilitat d'ús és fonamental, ja que els administradors haurien de poder cedir als usuaris la tasca de connectar-se amb un dispositiu i inscriure'l automàticament de manera segura amb poca o cap intervenció IT. D'igual forma, el sistema ha de poder desplegar aplicacions de manera granular, massiva o self-service.

Una característica addicional, que molt pocs fabricants inclouen o anuncien, és el suport remot que permet connectar-se als dispositius per resoldre les incidències dels dispositius desplegats.

Gestió d'identitat i accés (IAM)

IAM controla l'accés d'usuari i dispositiu en base els comptes d'usuari, contrasenyes i polítiques de seguretat. No tot el programari UEM proporciona les seves pròpies capacitats IAM, sinó que pot utilitzar eines de tercers com ara Active Directory (AD).

Reporting

Les analítiques i els informes són importants per tal que el personal IT examini les tendències de problemes, el rendiment i faci les correccions necessàries.

4.2. AVALUACIONS

Opcions d'implantació i sistemes operatius suportats

	Microsoft Endpoint Manager	**VMware** Workspace ONE	**IBM** MaaS360
Cloud/SaaS	✔	✔	✔
On-premises	✔	✔	✘
Windows 10	✔	✔	✔
Windows legacy	✔	✔	✔
iOS/macOS	✔	✔	✔
Android	✔	✔	✔
IoT/Wearables	✔	✔	✔
Linux	✔	✔	✔
VDI	✔	✔	✘
Chrome OS	✔	✔	✔

Seguretat i privacitat

	Microsoft Endpoint Manager	**VMware** Workspace ONE	**IBM** MaaS360
App containerization	✔	✔	✘
Contenidor xifrat	✔	✔	✔
Polítiques i perfils per protegir les dades, separació entre dades corporatives i personals	✔	✔	✔
Seguretat WiFi, VPN, email, desplegament de certificats	✔	✔	✔
Habilitar seguretat i control sobre el dispositiu	✔	✔	✔
Restriccions per compartir fitxers o dades, copy/paste	✔	✔	✔
Control d'accés a dades corporatives	✔	✔	✔
Esborrat remot de dades dels dispositius perduts o robats	✔	✔	✔
Detecció de dispositius alliberats (jailbroken/rooting)	✔	✔	✔
Navegador web segur	✔	✔	✔
Data lost prevention	✔	✔	✔
Detecció d'aplicacions prohibides o pernicioses	✔	✔	✔
Detecció malware	✔	✔	✔
Firewall	✔	✔	✔

Gestió de dispositius i cicle de vida

	Microsoft Endpoint Manager	**VMware** Workspace ONE	**IBM** MaaS360
Gestió de dispositius byod	✔	✔	✔
Gestió disp. legacy	✔	✔	✔
Visibilitat en temps real dels dispositius enrolats	✔	✔	✔
Gestió de tots els dispositius des d'un únic tauler	✔	✔	✔
Control, gestió i diagnòstic de dispositius corporatius	✔	✔	✔
Gestió byod IoT/weareables	✔	✔	✔
Inventari de hardware	✔	✘	✔
Redesplegaments automatitzats del SO	✔	✔	✘
Automatització d'imatges per cada tipus de dispositiu gestionat	✔	✔	✘
Bloqueig remot	✔	✔	✔
Desactivar WiFi/Bluetooh	✔	✔	✔
Desactivar operadora	✔	✔	✔
Monitoritzar configuració	✔	✔	✔
Suport multiusuari per disp.	✔	✔	✔
Desactivar càmera	✔	✔	✔

Gestió d'aplicacions i programari

	Microsoft Endpoint Manager	**VMware** Workspace ONE	**IBM** MaaS360
Entrega d'aplicacions via catàleg	✔	✔	✔
Gestió del cicle de vida de les aplicacions	✔	✔	✔
Actualitzacions automàtiques d'apps, continguts, OS updates	✔	✔	✔
Monitoratge de software usat i llicències als dispositius	✔	✔	✔
SDK per desenvolupament i adaptació d'apps internes	✔	✔	✔
Desplegament granular d'apps	✔	✔	✔
Inventari de software dels disp.	✔	✔	✔
Quadre únic d'anàlisis	✔	✔	✔
Gestió de l'Office365, accés a Sharepoint	✔	✔	✔
Suporta controls natius iOS/Android	✔	✔	✔
Capacitat de desplegar apps en dispositius no gestionats	✔	✔	✔
Accés per remote desktop	✔	✔	✔

Desplegament i inscripció

	Microsoft Endpoint Manager	**VMware** Workspace ONE	**IBM** MaaS360
Enrolament/registre en totes les plataformes suportades	✔	✔	✔
Procés d'enrolament simple o automatitzat (zero touch)	✔	✔	✔
Desplegament d'apps en base el tipus de disp., SO, ubicació	✔	✔	✔
Capacitat de desplegament en totes les plataformes suportades	✔	✔	✔
Procés senzill pel registre d'usuaris	✘	✔	✔
Desplegaments de test	✔	✔	✘
Control remot del disp.	✔	✔	✔
Monitorització del servei	✔	✔	✔
Help desk del fabricant	✔	✔	✔
Suport Chatboot	✔	✔	✔
Portal d'usuari self-service	✔	✔	✔

Gestió d'identitat i accés

	Microsoft Endpoint Manager	**VMware** Workspace ONE	**IBM** MaaS360
Suport SSO	✔	✔	✔
Polítiques d'accés per aplicació	✔	✔	✔
Contrasenyes xifrades i complexes	✔	✔	✔
Polítiques d'autenticació i accés	✔	✔	✔
Suporta grups de seguretat	✔	✔	✔
Autenticació multifactor	✔	✔	✔
Autenticació biomètrica	✔	✔	✔
Identitat mòbil	✔	✔	✔
Autenticació risk-based	✔	✔	✔
Administració de drets d'accés	✔	✔	✔

Reporting

	Microsoft Endpoint Manager	**VMware** Workspace ONE	**IBM** MaaS360
Alertes	✔	✔	✔
Resposta automatitzada a les alertes	✔	✔	✔
Entrega programada d'informes	✔	✔	✔
Quadres de control en temps real	✔	✔	✔
Anàlisis a nivell de dispositiu	✔	✔	✔
Anàlisis a nivell d'aplicacions	✔	✔	✔
Aprofitar dades de servei agregades per obtenir informació i millors pràctiques	✔	✔	✔
Informes personalitzats	✔	✔	✔

5. CONCLUSIONS DE L'ANÀLISI

Fins i tot en temps pre-COVID, l'evolució de la mobilitat empresarial ja estava ben iniciada i moltes empreses van trobar que les opcions de treball flexibles produïen un augment de la productivitat, ajudaven a la conciliació laboral i familiar i reduïen els costos associats d'estar en una oficina.

Aquesta transformació del teletreball també s'ha sumat a la complexitat de la majoria de programes de mobilitat empresarial. Hi ha més dades, aplicacions i dispositius per gestionar, a més els ciberdelinqüents i els esquemes de *phishing* són cada vegada més perfectes. Aquesta combinació està obrint bretxes de seguretat potencialment perilloses a les organitzacions.

Per tant, segurament, una de les principals raons per les quals les empreses es plantegen UEM és per continuar mantenint la seguretat davant del creixent ecosistema de la mobilitat. Centrar-se en la seguretat del punt final no és només protegir l'empresa dels atacs sinó impedir que es filtrin dades corporatives que diàriament els usuaris tracten des dels seus dispositius. Per tancar aquestes bretxes de seguretat, les plataformes UEM supervisen contínuament el que fan els empleats quan utilitzen les aplicacions corporatives i els repositoris de dades.

La gestió de la mobilitat empresarial és una elecció necessària perquè està destinada a oferir una major visibilitat de tots els punts finals i al mateix temps facilitar la productivitat dels empleats. Les eines UEM i els serveis de mobilitat intuïtius, senzills d'utilitzar i que aporten valor a les TI i als usuaris proporcionaran beneficis significatius i rendibilitat a les organitzacions.

Com s'ha vist en l'anàlisi, totes les necessitats de gestió de la mobilitat IT ara s'integren en una única entitat d'administració en comptes d'usar diversos programaris, com s'estava fent fins ara per cadascuna de les funcions de gestió. Seleccionar el programari UEM adequat depèn molt de les plataformes de sistema operatiu implicades, els requisits de seguretat, els tipus de dispositius, les aplicacions i les infraestructures IT actuals de les empreses.

En la comparativa, s'hi descriuen les extenses capacitats de gestió que presenten totes 3 solucions estudiades. No es pot dir que una destaqui clarament per damunt de les altres sinó que les diferències son subtils i de mers detalls de visió entre elles.

És evident que els 3 productes cobreixen les prestacions essencials que ha de recollir un bon producte UEM per a una gestió moderna del dispositiu.

Els factors de decisió per l'elecció de la solució vindran més determinats per l'escenari on s'ha d'ubicar la implantació que no pas per les sobrades potencialitats que s'ha vist entreguen cadascun dels productes UEM estudiats. Si l'entorn de treball està fortament centrat en Microsoft, és possible que la decisió de tria s'orienti en alinear-se amb la solució UEM d'aquest fabricant per tal d'aprofitar les possibles sinergies i integracions que li vindran donades. D'igual manera, aquest criteri decisori es podrà establir per la resta de fabricants.

Un altre enfoc de selecció es podria basar en determinar quins components ja existeixen en les instal·lacions IT en quan a MDM, MAM, MCM i valorar aprofitar aquestes en lloc de començar el projecte UEM de zero. En aquest cas, caldria explorar les alternatives d'integració dels diferents components existents, i ja no només comptar amb les solucions UEM estudiades sinó també optar per d'altres UEM consolidades que puguin existir en el mercat IT que siguin capaces d'adaptar-se a la infraestructura i objectius de mobilitat IT de l'organització.

S'ha iniciat la transformació de la informàtica de l'usuari final i el que va començar com una resposta al suport de plataformes mòbils ja s'ha expandit al mon del PC completant així la provisió de la gestió de l'Endpoint a tot tipus de dispositiu IT.

Es podria concloure aquesta anàlisi amb l'afirmació que la complexitat dels sistemes IT de les organitzacions no para de créixer i UEM ha vingut al rescat per fer més fàcil la gestió d'aquesta complexitat.

6. BIBLIOGRAFIA

- https://www.manageengine.com/mobile-device-management/enterprise-mobility-management-emm.html?index
- https://www.manageengine.com/products/desktop-central/unified-endpoint-management-solutions.html
- https://docs.microsoft.com/en-us/learn/modules/intro-to-m365-unified-endpoint-management/
- Gartner at a glance; https://www.gartner.com/imagesrv/pdf/gartner_at_a_glance_1Q18.pdf; (PDF). *Gartner.com*.
- https://www.gartner.es/es/acerca-de
- https://www.computerworld.com/article/3304583/what-is-microsofts-intune-and-how-well-does-it-really-work.html
- https://www.microsoft.com/es-es/microsoft-365/microsoft-endpoint-manager
- https://www.ibm.com/es-es/products/unified-endpoint-management
- https://www.vmware.com/products/workspace-one/unified-endpoint-management.html

7. GLOSARI

Active directory / Azure AD: servei de directori en una xarxa distribuïda de computadors Windows. El directori està composat per objectes tals com usuaris, grups o equips amb l'objectiu d'administrar els inicis de sessió d'usuari en els dispositius connectats a la xarxa, així com l'administració de polítiques. La versió Azure AD es el mateix directori però ubicat en l'entorn núvol de Microsoft 365.

Antimalware: tipus de programa dissenyat per prevenir, detectar i posar remei a programari maliciós en els dispositius informàtics. Els termes antivirus i antimalware s'utilitzen sovint com a sinònims, ja que els virus informàtics són un tipus específic de malware.

API: conjunt de definicions i protocols que permeten la comunicació entre dues aplicacions de programari a través d'un conjunt de regles.

BYOD (bring your own divice): tendència cada vegada més estesa en què les empreses permeten als treballadors aportar els seus dispositius portàtils personals per dur a terme tasques empresarials i connectar-se a la xarxa i als recursos corporatius.

Chatboot: programa que simula mantenir una conversa amb un ésser humà. Habitualment, la conversa s'estableix a través d'un teclat, encara que també hi ha models que disposen d'una interfície d'usuari multimèdia, dotant de major realisme la interacció amb l'usuari.

Ciberamenaces: acte maliciós que busca perjudicar les dades, robar dades o afectar la vida digital en general. Els ciberatacs inclouen amenaces com virus, violacions de dades, atacs DDoS, etc.

COPE (Corporate owned, personally enabled): dispositiu de propietat corporativa però també habilitat per a usos personals de l'usuari.

Exploit: atac que explota vulnerabilitats en aplicacions, xarxes, sistemes operatius o maquinari amb la finalitat de prendre el control dels ordinadors o robar dades.

Firewall: sistema de seguretat que supervisa i controla el trànsit de xarxa entrant i sortint en base a regles de seguretat predeterminades. Un tallafocs normalment estableix una barrera entre una xarxa de confiança i una xarxa no fiable, com internet.

Legacy: sistema informàtic que s'ha quedat obsolet però que encara és utilitzat per l'usuari o empresa i no es vol o no es pot substituir ni actualitzar fàcilment.

Multidifusió (multicast): enviament de paquets d'informació a múltiples destinataris d'una xarxa informàtica, habitualment Internet, simultàniament.

Phishing: missatge fraudulent dissenyat per enganyar a un usuari per tal de que aquest reveli informació sensible a l'atacant o per instal·lar programari maliciós en l'equip de la víctima.

POCE (Personally owned, company enabled): dispositiu de propietat personal però habilitat per a usos empresarials.

PXE (Preboot eXecution Environment): opció freqüent per a l'arrencada, instal·lació i desplegament del sistema operatiu d'un dispositiu mitjançant la xarxa.

Scoring: valoració de les diferents propostes de producte presentades sota uns criteris de puntuació obtenint uns resultats.

Screening: cribratge o destriament de les diferents propostes tecnològiques que contemplen unes característiques desitjades.

SDK (Software Development Kit): conjunt d'eines de desenvolupament de software que permet al programador crear aplicacions o adaptacions per a un sistema concret.

Site: adreça d'Internet en què una persona o organització proporciona informació.

SSO (Single Sign-On): procediment d'autenticació que permet a l'usuari accedir a múltiples sistemes amb una sola instància d'identificació.

VDI (Virtual Desktop Infrastructure): La virtualització de l'escriptori és un procés de separació de l'escriptori, que engloba les dades i programes que els usuaris usen per treballar, de la màquina física. L'escriptori virtualitzat s'emmagatzema remotament en un servidor central en lloc de fer-ho al dispositiu IT d'usuari.

VPN (Virtual Private Network): tecnologia de xarxa que permet una extensió de la xarxa local sobre una xarxa pública o no controlada, com per exemple Internet. Mètode molt usat per l'accés remot de l'usuari als sistemes d'informació de les organitzacions.

Wearables: dispositius electrònics que s'incorporen en algun lloc del nostre cos interactuant contínuament amb l'usuari per realitzar alguna funció específica: rellotges intel·ligents o polseres que controlen l'estat de salut són exemples entre molts d'altres.