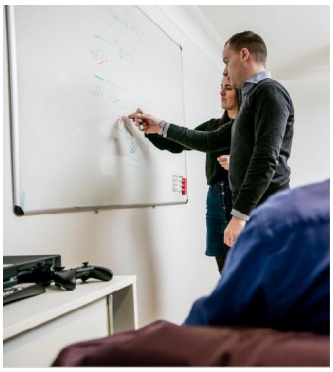
Microsoft Partner
Gold Cloud Platform
Gold Identity and Access
Gold Datacenter
Gold Devices and Deployment
Gold Enterprise Mobility Management

INK
UBA
TOR
% SUNET



Slutrapport Windows 10 och molnet

Leif Lagebrand, Nickolaj Andersen och Stefan Schörling

2017-01-13

Lumagate

TABLE OF CONTENTS

WORLD WIDE CONTACT
www.lumagate.com
info@lumagate.com

SWEDEN
Lumagate AB
Birger Jarlsgatan 62
114 29 Stockholm
+46 (0)8 665 33 00

NORWAY
Lumagate AS
Strandveien 10
1366 Lysaker
+47 22 44 33 23

DENMARK
Lumagate A/S
Nybrovej 97
2820 Gentofte
+45 36 94 44 37

WORLD WIDE CONTACT
www.lumagate.com
info@lumagate.com

SWEDEN
Lumagate AB
Birger Jarlsgatan 62
114 29 Stockholm
+46 (0)8 665 33 00

NORWAY
Lumagate AS
Strandveien 10
1366 Lysaker
+47 22 44 33 23

DENMARK
Lumagate A/S
Nybrovej 97
2820 Gentofte
+45 36 94 44 37

Författare	Titel	Företag	Email
Leif Lagebrand	Projektledare	BTH	leif.lagebrand@bth.se
Stefan Schörling	CTO och Microsoft MVP	Lumagate	stefan.schorling@lumagate.com
Nickolaj Andersen	Principal Consultant och Microsoft MVP	Lumagate	nickolaj.andersen@lumagate.com

WORLD WIDE CONTACT
www.lumagate.com
info@lumagate.com

SWEDEN
Lumagate AB
Birger Jarlsgatan 62
114 29 Stockholm
+46 (0)8 665 33 00

NORWAY
Lumagate AS
Strandveien 10
1366 Lysaker
+47 22 44 33 23

DENMARK
Lumagate A/S
Nybrovej 97
2820 Gentofte
+45 36 94 44 37

1 UPPDRAGET

Projektet Windows 10 och molnet startades under sommaren 2015 i regi av SUNET Inkubator. Här är adressen till hemsidan.
https://portal.nordu.net/display/Inkubator/Windows+10+och+molnet

I en andra fas under 2016 så beskrivs projektet så här i projektspecifikationen:

Projektdirektiv:
Administration av datorer och mobila enheter med Microsofts verktyg i molnet Universitet och högskolor använder relativt mycket tid på att administrera datorer och i framtiden även mobiler och plattor. Microsoft har uppmärksammat detta och skisserar en väg där maskin-och programvara för detta finns i molnet (Azure AD, Intune, Store for Business osv). Det innebär att processer kan förändras och att de klassiska verktygen på Campus som SCCM och MDT kan ersättas eller få en ny roll. Och naturligtvis sker detta inte över en natt utan på många U/H så kommer det att vara en kontinuerlig process med både och (hybrid-scenariot). En annan trend är att både personal och studenter använder egna mobiler och datorer i arbetet. Kan U/H dra nytta av det och kanske hjälpa till med administration så att alla parter blir nöjda?

Projektet ska beskriva fördelar, nackdelar och utmaningar i denna process. Ett fokus är att hitta en nivå för högskolesektorn som skall balansera administrativa kostnader samtidigt som tillräcklig säkerhet skall upprätthållas. Praktiska tester genomförs inom ramen för projektet. Projektet är en fortsättning på Inkubatorprojektet Windows10 och molnet som startade hösten 2015.

Mål
Leverera information, rekommendationer och scenarior för införande av molnbaserad administration av mobiler och datorer.

Förväntat resultat:

- Erfarenhetsspridning runt molnbaseradadministration av mobiler och datorer
- Underlag för att lärosäten skall kunna ta beslut om och forma ett projekt för införande.
- Webinarer och redovisning i slutrapport med rekommendationer

Avgränsningar: Lösningarna kommer att fokuseras runt Microsofts produkter inom detta område.

Projektet har haft en referensgrupp bestående av Per Hörnblad (projektägare) Umu, Justin Nichols Liu, Anders Näslund MdH, Bo Simonsson LNU, Brian Berg LNU, Göran Sedvall Liu, Magnus Olofsson LU, Martin Gumucio SLU, Mattias Andersson Chalmers, Mikael Zewgren HiG och Niklas Lundgren Umu.

2 PRESENTATION AV FÖRFATTARNA

2.1 LEIF LAGEBRAND

Leif Lagebrand arbetar som Projektledare och IT-arkitekt på Blekinge Tekniska Högskola.

2.2 NICKOLAJ ANDERSEN

Nickolaj Andersen arbetar idag som Principal Consultant på Lumagate där han är rådgivare och implementerar moderna klienthanteringslösningar. Nickolaj har ett stort fokus på automation kring klienthantering med System Center Configuration Manager och dess kring komponenter som bas.

Nickolaj blev under 2016 utnämnd till Microsoft Most Valuable Professional av Microsoft inom området Enterprise Mobility

Nickolaj finns på twitter under **@NickolajA**

2.3 STEFAN SCHÖRLING

Stefan Schörling arbetar idag som Nordisk CTO på Lumagate med ansvar för teknisk utveckling och erbjudanden inom Lumagate. Stefan har närmare 20 års erfarenhet av IT Industrin och de senaste har varit väldigt fokuserade på Microsoft Infrastruktur. Stefan har under 9 år blivit utnämnd till Microsoft Most Valuable Professional av Microsoft inom System Center configuration Manager och nu senaste inom området Enterprise Mobility.

Stefan driver även den mycket uppskattade användarföreningen System Center User Group, https://sv-se.facebook.com/scugse/. Stefan finns på twitter under ***@stefanschorling***

3 REKOMMENDATIONER: WINDOWS 10 OCH MOLNET

3.1 WINDOWS 10

Sedan första versionen av Windows 10 kom ut i juli 2015 har Microsoft släppt nya och förbättrade versioner av operativ systemet, vilken är en viktig aspekt att ha i åtanke vid planering, testning och införande av operativ systemet. Det nya operativsystemet har förändrat landskapet avseende hur vi framöver behöver tänka och managera Windows enheter. Traditionellt sett har de flesta företag och organisationer valt att uppgradera till den senaste versionen av Windows vid en ”hårdvaru-refresh” där stora delar av enheter byts ut och samtidigt levereras med en ny version av Windows. Framöver med Windows 10 behöver man tänka om eftersom det 2-3 gånger per år släpps nya versioner av operativ systemet. Microsoft kallar detta för ”Windows-as-a-Service” (WaaS), ett begrepp som är viktigt att känna till i framtiden. För mer djupgående information kring WaaS, beskrivs i kapitel 6.2.

På grund av den här ökade takten med nya versioner av Windows 10, kan det vara lägligt att tänka om vad gäller den form av anpassning och konfigurering man gör av operativsystemet idag. Tidigare har det varit populärt att ”curla” slutanvändarna genom att konfigurera deras enhet exakt enligt deras och eller organisationens önskemål. För att kunna upprätthålla takten med de nya versionerna av Windows 10, är Microsofts officiella rekommendation att man ser över den här specifika anpassningen av operativsystemet, och lägger över ansvaret på slutanvändaren. Detta medför också en förenklad utrullnings- och uppgraderingsprocess mellan de olika versionerna av Windows 10.

3.2 MOLNET

Idag ser man en ökad efterfrågan på molntjänster och Microsoft ligger i framkant inom många områden, däribland identitet och samarbetsplattformar. Ett område som har Microsoft de senaste åren har släpat efter är inom Mobile Device Management (MDM), med tjänsten Microsoft Intune. Sedan den första versionen av Intune, har funktionerna blivit fler och fler givetvis, men Microsoft har haft en uppförsbacke gentemot sina konkurrenter i form av funktionalitet. Gapet mellan Microsoft och konkurrenterna har det senaste året täppts igen mer och mer, och vår analys av nuläget är att skillnaden nästintill är försumbar.

Under kommande år, 2017, släpps en ny version av Microsoft Intune som baseras på Azure framework, vilken skall anses som en ny version av Microsofts MDM plattform. I sin helhet tillkommer mycket efterlängtad funktionalitet men även ny funktionalitet som ingen av konkurrenterna i dagsläget innehar.

Microsoft är en stor leverantör av MDM-system och deras lösning omfattar mycket mer, däribland identiteter. Microsoft har som fokus att skydda identiteter, data och appar och inte specifikt enskilda enheter. Detta framgår tydligt i deras tjänst Mobile Application Management without Enrollment, som ingår i Enterprise Mobility + Security paketering.

Vad gäller hantering av Windows 10 i Microsofts Mobile First, Cloud First strategi, så finns det olika metoder och rekommendationerna är inte helt tydliga från Microsofts håll. Sammanfattningsvis pratar de om två olika scenarion, traditionell management och modern management. Det traditionella sätter att

hantera Windows 10 inkluderar det som många företag idag redan användare, däribland Active Directory, Group Policy Management, System Center Configuration Manager m.m. Med modern management, menas att en enhet och identitet hanteras av Azure AD och Microsoft Intune. Windows 10 stödjer båda dessa scenarion, där Microsoft framtida planer är att utveckla och bygga vidare på modern management metoden som de ser som en ersättare eller komplement till den traditionella metoden som vi använder idag. På lång sikt kan man se att Modern Management är det uteslutande sätt vi kommer hantera enheter.

Microsofts framtida satsningar och budskap är tydliga, och det handlar kort och gott om molnet (Azure) primärt. Denna vision tror vi är något som inom en obestämd framtid kommer falla in, men alla kommer inte vara redo samtidigt och därför är det viktigt att, vilket Microsoft också inser, att kunna supportera ett hybrid läge mellan dessa två manageringsmetoder.

3.3 SAMMANFATTNING OCH REKOMMENDATIONER

Inom de närmaste åren kommer vi se en utveckling av nya molntjänster och lösningar, en del som vi redan idag har på campus (on-premise), men nuläget visar på ett tydligt tecken oberoende av vilken manageringsmetod som används, så finns det begränsningar inom båda. Det finns inget ”one-size fits all” lösning för alla scenarion. Framöver under ett par år kommer vi se satsningar från Microsofts sida med hybrida lösningar med avsikten att möjliggöra användande av molntjänster, är vår bedömning.

Då utvecklingen går så rasande fort så behöver man som organisation förändra hur man förvaltar och bevakar ”Molntjänster”. När det gäller tjänster som man har driftsatt så kräver dessa en mycket mer aktiv förvaltning, men behöver bevaka vad som händer med plattformen då det inte längre är du som bestämmer när saker ändras eller under vilka förutsättningar de införs utan du får anpassa din organisation efter detta. Även för att dra nytta av tjänsterna och den innovation och ny funktionalitet som man kontinuerligt får behöver man fortlöpande se till så ens användare får utbildning och information om de förändringar som sker i tjänsten.

När det gäller möjligheterna och innovationen som kontinuerligt kommer i Microsoft Molntjänster så behöver man ha en löpande omvärldsbevakning. Ungefär var 6e vecka kommer det ny funktionalitet som kan lösa affärsbehov eller innovation som kan göra er affärsverksamhet effektivare. Detta är en stor utmaning vi ser i många organisationer då man inte avsätter tillräckligt med resurser för förvaltning eller till nyutveckling utan man budgetmässigt fastnar i de gamla mönster man har i sin budgetering.

Vi ser ofta att kostnaderna att införa molntjänster initialt blir högre hos IT Avdelningen medan den istället kan spara pengar eller möjliggöra mer affärsvärde ute i verksamheten. För organisationer som sitter fast med många äldre ”standardsystem (legacy systems) så kommer komplexiteten att införa en del molntjänster att vara utmanande. Detta då man ofta har stora beroendekartor och genom att man själv inte styr över när förändringar på tjänster skall ske i särskilt stor utsträckning så kan man hamna i utmanande situationer där man får driftpåverkan.

Detta är viktiga aspekter att ta med i sin IT-strategi för att införa molntjänster och få en acceptans på chefsnivå (CxO).

4 FRAMTIDSSPANING 2017 OCH FRAMÅT

Microsoft har en vision om att hjälpa företag och organisationer att bli effektivare både ur ett produktivitets- och kostnadsperspektiv. Fler och fler unga (Millenials) kommer in i arbetslivet och denna generation är uppvuxen med IT och Digitala verktyg på ett helt annat vis än många av de som är i arbetslivet idag. Detta ställer högre krav på hur vi utformar IT för att möta behoven både från arbetsgivaren och arbetstagarens sida. Detta är en utveckling som Microsoft noga följer i sin produkt utveckling och anpassar sina produkter och tjänster kring. Vi har delat in hantering under fyra områden när det gäller Windows 10. Dock är det viktigt att man sätter samman dessa områden till en helhet och en väg framåt, helheten är oerhört viktig då det är då man som organisation får ut den samlade innovation som Microsoft investerar sin framtid inom.

4.1 ENHETSHANTERING

När det gäller enhetshantering så går tillverkarna mer och mer mot att använda MDM /OMA-DM [1].

Apple har idag ett program som heter DEP[2] (Device Enrollment Program) och de tendenser vi ser är att andra leverantörer såsom Microsoft ser denna typ av process som en möjligväg framåt för att på liknande sätt även administrera/managera och kontrollera Windowsenheter.

Windows 10 och de molnscenarier som finns idag är idag mycket kopplade till BYOD (Bring your Own Device). Dvs ett koncept där man tar med sin egen dator och utför arbetsuppgifter för sin arbetsgivare. Dessa koncept är idag ganska begränsade i vad man kan managera på de enheter som finns men vi ser en stark drivkraft till att utveckla dessa molnbaserade scenarion mot att även fullt ut stödja organisationer som vill hantera sina enheter via endast en molnlösning som tex Intune[3] och Azure Active Directory[4].

Tittar man även på hur man sköter operativsystem så ser vi en tydlig trend i att detta kommer reformeras och Microsoft har redan nu varit tydliga att Windows 10 kommer vara deras sista operativsystem och att det kommer ständigt att uppdateras med nya funktioner två till tre gånger per år. Detta betyder att vi löpande kommer få nya versioner med mot tidigare relativt kort supporterad livslängd och att man har investerat mycket i att man på ett enkelt sätt skall kunna uppgradera sin Windows Installation. Detta är en process som initialt varit lite smärtsam men längs vägen så kommer detta att trimmas in efter kunders behov.

Vad det gäller att ominstallera en enhet så går man mot en ”reset” baserad typ av hantering där man istället för att ominstallera enheten gör en återställning av enheten med eller utan data. Liknande hur man idag återställer en Apple iPad.

---

[1] http://openmobilealliance.org/about-oma/work-program/device-management/
[2] http://www.apple.com/business/dep/
[3] https://www.microsoft.com/en-us/cloud-platform/microsoft-intune
[4] https://azure.microsoft.com/en-us/services/active-directory/

Vad vi ser händer här är att System Center Configuration Manager (Current Branch) knyts mer och mer ihop med molntjänsterna i Azure, dvs man behåller den stora investering man har gjort i produkten medan man tillför innovation från molnet genom att hybrid ansluta den. Detta för att stödja flera nya scenarier och för att snabbt få tillgång till innovation. Dvs man kan fortfarande hantera sina befintliga campussystem (on prem) som man stödjer Cloud Only scenarior med enhetshantering där.

Likaså fortsätter man att utveckla sin Intune tjänst för att stödja Modern Management for de organisationer som inte har behov av lika omfattande hantering som man har idag med System Center Configuration Manager.

De närmsta 10 åren är vi övertygade om att åren så kommer det finnas organisationer som kommer använda båda varianter av hantering helt beroende på kravbild. Vad som är klart är att ju mer tjänster man lägger i Leveransformen SaaS så kommer organisationers behov för en on-prem lösning övergå till att täckas av en ren cloud only lösning. Dock ser vi att merparten av organisationer kommer inom de närmsta 5 åren ha behov som kommer kräva en hybridlösning. Exempelvis så ser vi inte att en molnbaserad Intune lösning skulle lösa att ominstallera en traditionell datorsal med en stor mängd äldre applikationer inom en överskådlig framtid.

Microsoft kommer även under de kommande åren satsa mer på Modern Management, dvs ett nytt modernt sätt att hantera enheter på där man ger användaren större ansvar att sköta om sin egen enhet men IT Avdelningen får tillräckliga kontroller för att säkerställa det man som IT avdelning kräver enheten uppfyller. Mer kring Modern Management finns i Kapitel 10.

4.2 APPLIKATIONSHANTERING - PROGRAMVARA

Med intåget av SaaS tjänster och digitaliseringen så kommer fler och fler applikationer kräva andra metoder för distribution, distributionen kommer vara knuten till "app stores" där man publicerar eller knyter applikationer till enheter eller användare. Den traditionella distributionen av EXE och MSI filer kommer kraftigt minska i den takt applikationer transformeras.

Intune med Modern Management har idag en ganska svag motor för Applikations Distribution då man förlitade sig på att organisationer skulle merparten använda SaaS tjänster, detta är ett GAP Microsoft arbetar med att brygga. När i tiden detta GAP kan vara stängt är svårt att säga men en rimlig gissning skulle vara att inom två år så finns en grundläggande funktionalitet som stödjer en stor mängd av kundbasens behov.

4.3 IDENTITETSHANTERING

Identitetshanteringen blir idag viktigare då applikationerna flyttar ut i SaaS tjänster och är den barriär som gäller för säkerhet istället för tidigare där det var den lokala brandväggen som stod för barriären. Då applikationerna förflyttar sig ut på Internet i större grad så är vikten av federation och provisionering en viktig faktor att ta höjd för.

Då en användare slutar så skall den inte längre ha access till de SaaS applikationer som den blivit tilldelad, med en federation eler koppling via tex Azure Active Directory skulle denna hantering förenklas. Idag är tyvärr fallet oftast inte så utan det finns stora brister i dessa processer för livscykelhantering.

Det finns även en ekonomisk aspekt i denna del och det är att SaaS tjänster betalar man ofta per aktiva användare och har man ingen fungerande provisionering så kan man förutom informationssäkerhetsrisker

även ekonomiska risker där man riskerar att få betala för tjänster som man inte längre använder om man inte har en fungerande process för provisionering av identiteter.

I dag kan man läsa många rapporter om att Identitetsstölder ökar och antalet dataintrång som sker på grund av stulna identiteter står för en väldigt stor del av intrången så är det viktigt att ta ett grepp om säkerheten kring identiteterna. Man behöver skapa sig en lägesbild över hur ens identiteter används och om de är utsatta för kapning eller används från riskzoner. Microsoft har genom dess Enterprise Mobility Suite och kring denna svit skapat en plattform för att säkra upp och underlätta hanteringen av identiteter som utnyttjar molntjänster. Man har ett kraftigt utvecklingsfokus på detta område de senaste åren och vi ser att det fortsätter i oförminskad takt. Azure AD har på senaste månaderna fått stöd för Risk Baserad Åtkomstkontroll och Priviligerad Identitets hantering. Detta för att kunna blockera åtkomst eller kontrollera åtkomst till tjänster baserat på vilken risk varifrån en användare loggar in. På detta sätt så har man flyttat mycket av säkerheten till identiteten istället för som traditionell kring nätet eller brandväggarna.

4.4 SÄKERHET

Säkerhet är ett ämne som är väldigt aktuellt idag, utvecklingen har gått från att vara ett ganska begränsat hot till att vara ett allvarligt hot [5] där det finns en hel industri som tjänar stora pengar på digital kriminalitet. Detta i kombination med nationella intressen från främmande makt så behöver företag och institutioner ta nya grepp om hur man skyddar sig mot IT-angrepp. Angreppen blir mer avancerade och verksamheterna behöver behöva investera mer inom området Informations och IT-säkerhet.

Med intåget av den nya dataskyddsförordningen[6] som träder i kraft i Maj 2018 så behöver organisationer redan nu börja titta över sina processer och användande av IT-system för att se till så man uppfyller de nya krav som träder i kraft.

När det gäller Windows 10 och dess kringliggande tjänster så är dessa väldigt bundna till det publika Microsoft molnet. Och där behöver man som organisation se över hur man konfigurerar och utnyttjar dessa tjänster för att följa nuvarande och kommande lagstiftning. Man skall inte glömma att det är användningen i sin helhet som behöver hanteras och inte bara om molntjänsten[7] i sig är godkänd.

Microsoft har även ambitionen att minska beroendet till lösenord då det ofta är en svag länk och det ökade fokuset på SaaS tjänster där Identiteten och användarnamnet blir den nya säkerhetsbarriären så vill man förstärka denna hantering med starkare faktorer, ett exempel är hur man introducerat Windows Hello med stöd för biometrisk inloggning. Denna utveckling kommer fortsätta och Microsoft har uttalat sig om att man vill få bort användandet av lösenord helt, så vi ser en stark utveckling även inom detta området.

---

[5] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
[6] https://skl.se/naringslivarbetedigitalisering/digitalisering/informationssakerhet/juridikochdataskydd/dataskyddsforordningen.9215.html
[7] https://www.microsoft.com/en-us/trustcenter

5 PROJEKTLEDARENS KOMMENTARER

Projektet startade sommaren 2015 med en hypotes om att med programvaran Microsoft Intune i molnet (Azure) skulle det bli enklare att administrera PC och därmed ersätta, helt eller delvis, dagens campus-verktyg SCCM, MDT, WSUS osv. Så blev det inte, vi är inte där ännu, men vi kommer nog dit under 2017.

Att hypotesen inte kunde infrias bidrog också till att fokus flyttades till de gamla vanliga administrationsverktygen, SCCM, MDT, WSUS osv och den nya hanteringen av Windows 10 med kontinuerliga uppdateringar/uppgraderingar. Ursprungligen skulle även administration av mobiler behandlas i projektet och det har det gjorts till en del. Men intresset har varit svalt från U/H och därmed har även denna del tappat fokus.

En spaning är att under 2017 kommer Intune att slå igenom och med det en lättare och enklare administration av Windows 10 PC, det som Microsoft kallar Modern Management. Intune hanterar redan idag mobiler på ett bra sätt och tar enligt Microsoft marknadsandelar från andra lösningar. Men om universitet och högskolor är intresserade av att ta på sig administrationen av mobiler är tveksamt, personalen sköter ju det själva idag och det fungerar ju bra. Även Macintosh-datorer får ofta sköta sig själva och även det fungerar ju bra. Intune har ett outvecklat stöd för Mac som förmodligen kommer att utvecklas under 2017, det återstår att se om det är innebär att IT-avdelningar vill administrera Macar eller om de får sköta sig själva.

Under maj 2015 frågade SUNET Inkubator efter idéer till projekt. BTH hade sex månader tidigare tagit Office365 för personal i drift. I samband med det dök Azure AD upp och även något som kallades Intune[1].

Windows Intune, som lanserades i mars 2011[2], lovade något nytt, ett enklare och billigare sätt att hantera Windows PC, ett sätt som redan användes för mobiler. Allting fanns i molnet (på den tiden inte Azure utan vid sidan om) och man kunde hantera alla PC som fanns på Internet, de behövde inte vara kopplade till campusnätverket.

BTH hade redan under slutet av 2014 tillsammans med Lumagate AB skissat på en test av Intune för administration av PC. Detta projekt är inte avslutat, vi har inte riktigt kommit i mål.

I maj 2015 skickade BTH in ett förslag till SUNET Inkubator på ett projekt ”Windows 10 och molnet” som pågick under 2015 som sedan följdes av detta projekt under 2016 ” Administration av datorer och mobila enheter med Microsofts verktyg i molnet” [3].

Det är dyrt att hantera Windows 10 med SCCM, programpaketering, radera innehållet på skivminnen göra om allt, installera varje ny uppgradering av drivrutiner, varje större ändring av programvaror ger ompaketering osv. Hypotes med Intune är ”Ligth management, modern management” dvs något enklare och därmed billigare. En hantering som påminner om den för hemdatorer – ingen SCCM, ingen IT-avdelning utan användaren sköter det mesta själv. Man använder det operativsystem som ligger på datorn vid leverans. Hämtar hem programvara som är gratis eller köper till det som behövs. Datorn skyddas mot alla andra PC - den misstror alla andra även datorer på samma nätverk. Windows Defender slås på med automatik om inget annat installeras.

Windows 10 Home, som de flesta hemdatorer har, uppdateras alltid, det går ej att hindra. Man bygger helt enkelt vidare på den dator som levereras från tillverkaren. Ny finns även en variant av operativsystemet som inte innehåller några tillagda programvaror, den är ren förutom Windows 10[4].

Microsoft har sneglat på Apple, MacOS och iOS. Ett operativsystem som bara rullar vidare, gratis och med kontinuerliga uppdateringar. Tittar man på iPhone har majoriteten uppdaterat till senaste iOS till skillnad från Android där många enheter har tidigare och osäkrare versioner av operativsystemet. Ett måste för att ha hög säkerhet är just att uppdateringar sker.

Många lade även märke till IBMs administration av hundratusentals Macar och PC. IBM menar att det är tre gånger dyrare med PC än Mac.
http://computersweden.idg.se/2.2683/1.667828/windows-pc-dyrare-drift-mac
https://www.youtube.com/watch?v=NLgvIarqdDM&feature=youtu.be

BYOD dvs du tar med din egen privata dator eller mobile till jobbet är en trend. Hur hantera man det? Och om många anställda arbetar på andra ställen än på campus då når de ju aldrig det interna nätverket. Hur hanterar man det? Intune som befinner sig i molnet ser ut att vara svaret på dessa frågor.

Så min spaning och det är även vad Microsoft själva säger att varje dator måste skydda sig själv, den är inte alltid inom den gamla klassiska brandväggen och brandväggen räcker inte. Det måste bli enklare och billigare att administrera Windows datorer och de måste hela tiden uppdateras, det kommer alltid nya säkerhetshot.

[1] https://en.wikipedia.org/wiki/Microsoft_Intune

[2] http://www.zdnet.com/article/microsofts-windows-intune-cloud-management-service-to-go-on-sale-march-23/

[3] https://portal.nordu.net/display/Inkubator/Windows+10+och+molnet

[4] https://www.microsoftstore.com/store/msusa/en_US/cat/Signature-Edition-PCs/categoryID.69916600

6 WINDOWS 10

För att kunna möjliggöra en snabbare leverans av nya versioner av Windows 10, har Microsoft behövt göra en hel del förändringar internt, speciellt gällande kring hur de distribuerar operativsystemet och gör det tillgängligt för sina kunder. Ytterligare ett begrepp som är viktigt att känna till är så kallade ”Servicing Branches”. Eftersom takten av nya versioner av Windows 10 ökar, har Servicing Branches tillkommit för att ge företag och organisationer en möjlighet att välja hur ofta de vill uppgradera till en nyare version av Windows 10. Varje ny version av Windows 10 har en livscykel på ett minimum av 18 månader, men kan vid vissa tillfällen vara längre (det sistnämnda kan variera från version till version). Respektive versioner genomgår olika faser som omfattar preview, officiell release, business ready och till sist end of life. Under dessa faser, klassificeras Windows 10 versioner in i de så kallade Servicing Branches.

6.1 SERVICING BRANCHES

Idag finns det 4 olika Servicing Branches för Windows 10 och dessa har vi försökt beskriva nedan med en rekommendation kring den.

6.1.1 Insider Previews

Insider Previews är till för att hålla sig uppdaterad på vilka nya funktioner som komma skall i den nästkommande officiella versionen av Windows 10. Här finns det möjlighet att tidigt göra interna tester för applikationer och processer. Under den här perioden har man möjlighet att påverka och skicka feedback till Microsoft kring nya funktioner eller förändringar som gjorts sedan den föregående versionen. Vår rekommendation är att ett litet antal personer inom IT-organisationen har registrerat antingen sin egen Windows 10 enhet eller en virtuell maskin i Insider Preview branchen. Det man skall tänka på att det går inte att stänga av telemetri i en Insider Build dvs data kommer att skickas från datorn till Azure.

6.1.2 Current Branch (CB)

Den första publika versionen som görs tillgänglig för allmänheten på en bred skala klassificeras som Current Branch. Det betyder att Microsoft anser sig att versionen är redo att användas bland många 100 miljoner användare, där buggar som upptäckts under tiden versionen varit under Insider Preview branchen har rättats till. Här är rekommendationen att företag och organisationer väljer ut nyckelanvändare samt hela eller större delar av IT-organisationen som tidiga användare. När en version av Windows 10 nått till Current Branch, så bör detta inte anses som business ready. Anledningen till detta är att det även i den här versionen finns potentiella problem som Microsoft inte haft möjlighet att fånga upp i sina interna tester, men som kommer uppmärksammas när den breda skaran av användare börjar använda versionen.

6.1.3 Current Branch for Business (CBB)

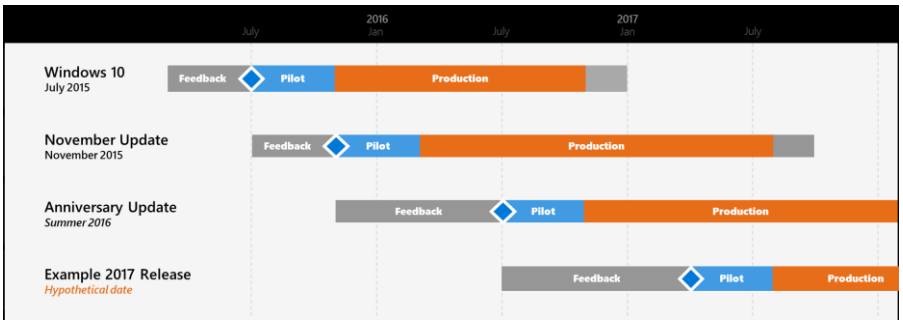
Ungefär 4-5 månader efter att den officiella versionen släppts i Current Branch, klassificerar Microsoft om versionen av Windows 10 till Current Branch for Business. Vid en sådan omklassificering anses versionen av Windows 10 redo för att användas av företag och organisationer. Den största andelen av Windows 10 enheter inom företag och organisationer rekommenderas att använda en supporterad Windows 10 version som är klassificerad som Current Branch for Business.

6.1.4 Long-term Servicing Branch (LTSB)

LTSB eller Long-Term Servicing Branch är en version för verksamheter som har speciella behov av att man inte kan förändra funktionalitet I operativsystemet. Man kan tänka sig exempel inom försvarsindustrin, hälsovården och annan kritisk verksamhet. Rekommendationen vad det gäller LTSB är att inte använda detta som en standard version utan just i de unika fallen där man verkligen har behov av att förändring inte får ske. Livslängden för en LTSB version räknas vara 5 år för att det sedan skall komma en ny LTSB version. LTSB Versionen får heller inte alla kritiska uppdateringar som släpps för de vanliga versionerna.

6.2 WINDOWS AS A SERVICE

Nedanstående bild illustrerar den uppdateringstakt som Windows 10 har haft fram tills idag, men försöker också ge en bild av hur framtiden kommer se ut. I dagsläget finns det ingen utvecklingskarta (roadmap) som visar när nya versioner framöver kommer släppas. Microsoft har i ett uttalande sagt att man kommer trappa ned takten med nya versioner av Windows 10, där man tidigare gått ut och meddelat att deras mål är att släppa två till tre versioner per år, framöver kommer vara en till två nya versioner istället. Detta kan dock förändras i framtiden, så det bör man ta höjd för.



Det är viktigt att känna till att man inte behöver installera om en Windows 10 enhet om den har uppgraderats till en Current Branch version som sedan omklassificerats till Current Branch for Business. En så kallad in-place upgrade är endast nödvändig när man går från t.ex. en specifik version av Windows 10 i Current Branch eller Current Branch for Business till en annan (se exempel nedan).

Windows 10 version 1511 (CB, CBB) --> Windows 10 version 1607 (CB, CBB)

Windows 10 ställer även nya och förändrade krav på hanteringen av enheterna på ett flertal punkter utöver uppdateringen av versioner. Det kommer framöver vara viktigt att inför varje ny version av Windows 10 säkerställa att t.ex. applikationer fungerar i den nya versionen, men även konfiguration och utrullning av Windows 10. Ett exempel på detta är mellan Windows 10 version 1511 och 1607 versioner, så bestämde Microsoft sig för att ändra hur TPM Owner Password hashen hanteras. Detta medförde att tidigare processer för hantering av TPM och BitLocker inte längre fungerade i den nya versionen. Därför är det ytterst viktigt att man bygger upp ett ramverk för att hantera interna processer och rutiner vid utrullning och uppdatering mellan de olika versionerna av Windows 10.

Se följande dokumentationssidor från Microsoft samt artikel för en mer djupgående beskrivning av WaaS:

https://technet.microsoft.com/en-us/itpro/windows/manage/waas-overview?f=255&MSPPError=-2147217396

https://redmondmag.com/articles/2016/11/29/windows-10-servicing-clarifications.aspx

https://technet.microsoft.com/en-us/itpro/windows/manage/waas-quick-start

6.3 DEPLOYMENT RINGS

Nya versioner av Windows 10 kräver som tidigare diskuterats ett annorlunda upplägg kring hur man validerar funktionalitet och hanterar distribution. Windows 10 introducerar ett löpande underhåll och kräver därför en fungerande metod för validering av ny funktionalitet, kompabilitet och distributionshanterings.

Microsoft föreslår att man enligt tabellen nedan delar upp och skapar vad man kallar ”Deployment Rings” (ringar). Deployment ringar för Windows 10 är ingen ny funktionalitet som tillkommit, utan ringarna definierar olika grupper av enheter. I System Center Configuration Manager, så kan man definiera ringarna genom att skapa Device Collections. För Modern Management scenarion så finns det möjlighet att skapa dynamiska security groups i Azure AD baserat på operativsystems version och/eller annan gruppmedlemskap. Ringarna används sedan för att styra i vilken grad som uppgraderingen sker till den senaste versionen av Windows 10.

Förslagsvis så använder man tabellen[8] nedan som utgångspunkt i framtagandet av interna ringar. Anledningen till att ha en uppdelad pilotstruktur ligger i att man vill fånga de mest uppenbara eventuella problem som en ny Windows 10 version kan medföra i organisationen, innan man går vidare med utsedda användare som har en specifik funktion eller är kända som ”heavy-users” av applikationer bland annat.

[8] https://technet.microsoft.com/en-us/itpro/windows/manage/waas-deployment-rings-windows-10-updates?f=255&MSPPError=-2147217396

Historiskt sett är nedan beskriven en redan beprövad metod som ofta använts i större utrullningar eller uppgraderingar av Windows, t.ex. övergången mellan Windows XP till Windows 7.

Deployment ring	Service Branch	Schema
Preview	Windows Insider	Innan CB
Ring 1 – Pilot för IT	CB	CB + 0 veckor
Ring 2 – Pilotanvändare	CB	CB + 4 veckor
Ring 3 – IT-avdelning	CB	CB + 6 veckor
Ring 4 – Alla #1	CBB	CBB + 0 veckor
Ring 5 – Alla #2	CBB	CBB + 2 veckor

6.4 UPPDATERA / UPPGRADERA

Det finns flera metoder att använda sig utav för att uppgradera till Windows 10, där i dagsläget System Center Configuration Manager är det bäst lämpade verktyget för en enkel och smidig uppgradering. Metoderna som kan användag är antingen In-Place upgrade, Refresh eller Replace. Microsoft har lagt mycket energi och resurser på att förbättra In-Place upgrade funktionaliteten, som i tidigare versioner av Windows inte fungerat i många scenarion, eller helt enkelt inte varit stabil nog. De andra två metoder är redan väl beprövade och skiljer sig i stora drag inte för Windows 10 gentemot tidigare versioner av Windows.

När man uppgraderar mellan olika Windows 10 version, t.ex. Windows 10 version 1511 (CBB) och Windows 10 version 1607 (CBB), så görs en In-Place upgrade (även kallat för ”servicing”), en del av Windows as a Service. I dagsläget finns det en del begränsningar i hur den här metoden fungerar, men med varje ny version som släppts av Windows 10, har dessa begränsningar blivit mindre. Det går också att använda sig utav In-Place upgrade metoden för att göra en uppgradering från t.ex. Windows 7 till en supporterad version av Windows 10.

För att under kontrollerade former kunna hantera uppgraderingar till Windows 10 eller uppdateringar mellan olika Windows 10 versioner, rekommenderar vi i dagsläget att man använder sig utav System Center Configuration Manager när det gäller traditionellt managerade enheter.

Windows Update for Business (WUfB) marknadsför Microsoft som en tjänst som skall förenkla uppdateringar mellan olika Windows 10 versioner i ett modern management scenario. I själva verket handlar det om en konfiguration som görs på respektive enhet och bestämmer vilken Servicing Branch enheten skall tillhöra. Därefter får man utnyttja de konfigurationsmöjligheter som finns för Windows Update agenten att hantera uppdateringarna av Windows 10. Om man är ute efter kontrol och ge slutanvändare möjlighet att agera inför uppdateringen, eller utföra någon åtgärd innan uppdateringen sker, är WUfB inget alternativ i dagsläget. Istället bör man vända sig till System Center Configuration Manager, och hantera uppdateringarna med en Task Sequence.

6.5 AZURE AD JOIN OCH INTUNE ENROLLMENT

Med Windows 10 och Azure Active Directory så får man möjligheten att ansluta datorn till Azure AD istället för sitt traditionella Active Directory. Samtidigt som man ansluter enheten så kan man få den att ansluta till Intune för att automatiskt kunna bli managerad med den funktionalitet som finns i Intune

Använder man sig av Windows 10 Signature Edition så får man inte med någon onödig programvara (bloatware) direkt från tillverkaren och kan på så sätt få in en modern klient i sitt Azure AD.

Enkelheten innebär att vi slipper hantera OS Deployment på dessa datorer och användaren kan ta en dator direkt och ansluta denna.

Vi ser idag svårigheter med att endast Azure AD joina datorn då vi inte kan göra särskilt mycket i konfigurationsväg men eftersom funktionaliteten utökas så får man utvärdera detta alternativ.

Azure AD Join kan göras av användaren själv, via Out of the box Experience eller via sk provisionerings paket som man från IT-avdelningen kan förbereda och lämna ut till användare/ IT-personal.

Med Creators Update[9] i mars 2017 så kommer möjligheterna för Modern Management utökas dock har vi idag ingen färdig bild vi kan ge kring detta.

6.6 ENTERPRISE STATE ROAMING

ESR (Enterprise State Roaming) är en tjänst från Microsoft som tillhandahåller möjligheten att synkronisera användares profiler mot Microsoft Azure denna tjänst kräver att man har Azure Active Directory Premium. Detta är liknande UE-V som finns för campus (on-prem) installation idag. Fördelarna är att användarens inställningar synkroniseras från de datorer han använder och lagras krypterat i molnet för att vara tillgängligt från andra enheter görs synkronisering av användares inställningar till Azure AD så att användarupplevelsen blir densamma när användaren t ex. byter dator.

Exempel på inställningar som synkroniseras är

- Bakgrundsbilder
- Internet Explorer Inställningar
- Edge Inställningar
- Sparade Lösenord
- Profiler för trådlösa nätverk
- Etc.

[9] I mars 2017https://blogs.windows.com/business/2016/12/06/windows-10-creators-update-advances-security-best-class-modern-tools/#oV3xu9h8yGSFRFpq.97

6.7 SÄKERHET

Windows 10 kommer med en rad säkerhetsfunktioner men som med all annan säkerhet är det helheten som räknas. Med Windows 10 så tillkommer en del nya funktioner och metoder nedan tar vi upp de mest vanligt förekommande.

6.7.1 Bitlocker

Windows tillhandahåller hårddiskkryptering för att säkerställa att lagrad data sparas på en krypterad enhet. Denna funktionalitet finns bara i Enterprise och Education. Bitlocker är ingen ny funktion för Windows 10 utan man har bara förbättrat den med en del ny funktionalitet. Vi rekommenderar att använda Bitlocker i sitt Windows 10 införande.

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/bitlocker-overview

6.7.2 Applocker

Applocker är en funktion för att styra vilka applikationer som får exekveras på en dator, tex att filer inte får exekveras från användaresn hemkataloger eller profiler. Applocker är relativt enkelt att implementera och kan bidra till ett skydd i er miljö mot exempelvis en del kryptolocker virus. Då filerna inte får exekvera kan heller viruset inte kryptera datorns filer. Vi rekommenderar att använda Bitlocker i sitt Windows 10 Införande.Applocker saknar en central rapportering så vi rekommenderar att man samtidigt inför event forwarding för att centralt få en punkt man kan följa upp sin implementation.

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/applocker-overview

6.7.3 Credential Guard

Credential Guard är en funktion för att skydda från identitetsstölder.

Credential Guard kan dock orsaka problem för applikationer och trådlösa nätverk som inte är konfigurerade enligt best practises då Creedential Guard förhindrar autentisering med vissa äldre protokoll. Vi rekommenderar att använda Bitlocker i sitt Windows 10 Införande men även att man utför den testning som detta kräver.

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard

6.7.4 Windows Hello for Business

Windows Hello är Microsoft satsning för att minska antalet lösenord och ersätta dessa med Biometri och förenklad inloggning. Med introduktionen av nya formfaktorer på enheter så ökar behovet att komma ifrån lösnord i samma takt ökar behoven att minska beroenden till lösenord som idag ofta används vid datorintrång.

Vi rekommenderar att man tar hänsyn till Windows Hello och gör ett aktivit val av detta vid sitt Windows 10 införande.

https://technet.microsoft.com/sv-se/itpro/windows/keep-secure/windows-hello-in-enterprise

6.7.5 Device Guard

Device Guard är en funktion för att blockera att osginerad kod exekveras på datorerna. Detta är en utmärkt funktion för att säkerställa att ingen osignerad kod eller utbrott med tex Kryptolocker sker. Denna funktionalitet passar sig bra på funktions PC och kiosk scenario där man inte har omfattande testning och hantering av mjukvara att göra då det kräver en hel del i en större organisation för att få sin mjukvara signerad. System Center Configuration Manager kan underlätta denna hantering något med hjälp av sin integration med mjukvaru distribution där man i princip giodkänner all mjukvara som den distribuerar.

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/device-guard-deployment-guide

6.7.6 Windows Defender

Windows 10 innehåller som standard en antimalware lösning, även om man inte har tänkt att använda denna funktion så är det bra om man tar hänsyn till den. För om det är så att man väljer ett skydd från en annan leverantör så är det så om detta skydd slås ut eller definitionsfilerna blir inaktuella så kommer Defender att aktiveras för att ta över skyddet och se till så enheter har en aktuell antimalware lösning.

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-defender-in-windows-10

6.7.7 Windows Information Protection

WIP är en funktion för att separera företags data och privat data och säkra företagsdata med kryptering och stöd för användaren att spara och hantera informationen på rätt sätt. Denna funktionalitet är relativt ny och vi har i dagsläget ingen erfarenhet om hur bra den är.

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/protect-enterprise-data-using-wip

6.7.8 Windows Defender ATP

Windows Devender Advanced Threat Protection är en molntjänst som analyserar vad som sker på Windows 10 enheterna och kan utifrån det detektera och larma om potentiella datorintrång eller utbrott av skadlig kod. I den värld vi lever i i dag så är nästan Windows Defender ATP ett måste för att ge oss någon insyn i vad som sker i våra IT-miljöer. Idag är inte ett virusskydd tillräckligt för att skydda våra enpoints. Det finns en rad uppsjö konkurrerande produkter som denna tjänst skall jämföras med.

Vad som skiljer denna tjänsten från ovan är att den inte ingår i någon Windows 10 licens utan får köpas separat. Antingen löst eller via Microsoft Paketering Secure Productive Enterprise 5 där Windows 10 E5 ingår.

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-defender-advanced-threat-protection

7 SYSTEM CENTER CONFIGURATION MANAGER

När takten ökas med flera nya Windows 10 versioner varje år, uppdateringar till Microsoft Intune månadsvis och kravet på integration mot fler molntjänster, så har System Center Configuration Manager behövt genomgå en förändring för att kunna följa denna utveckling. Detta har medfört vad man refererar till System Center Configuration Manager Current Branch[10] (Configuration Manager as a Service, benämns också som CaaS). Många tror att Configuration Manager Current Branch är ”SCCM 2016”, vilket inte stämmer. Configuration Manager Current Branch är en fristående version som uppdateras 3 gånger per år, där nya versioner hämtas ned automatiskt och presenteras i gränssnittet där administratören enkelt kan initiera en uppdatering.

Detta medför att Configuration Manager som produkt, har möjlighet att i den takt som nya molntjänster eller Windows 10 versioner lanseras, inom en betydligare kortare tid, supportera dessa. Tidigare uppdateringar till Configuration Manager har släppts i form av Service Packs eller Releases (R2, R3 osv), där det ibland varit upp till ett år mellan de olika versionerna. I en Mobile First, Cloud First värld, fungerar det tidigare sättet inte längre för att hänga med.

Diskussioner kring detta nya sätt att uppdatera Configuration Manager har lett till frågan, kommer produkten att en dag byggas om till en molntjänst? Det går idag inte att besvara frågan hur Microsoft kommer göra i framtiden, men Brad Anderson har tydligt gått ut och sagt att Configuration Manager Current Branch tillsammans med Microsofts Enterprise Mobility + Security[11] paketering av molntjänster är vad Microsoft i dagsläget satsar på för att ge sina kunder möjligheten att välja mellan eller kombinera de olika manageringsscenarion som Windows 10 ger.

Vår uppfattning är att Configuration Manager som produkt kommer leva kvar, åtminstone i många år till, men allt eftersom modern management tar över, i ett sådant scenario finns det eventuellt en möjlighet att man kan uppnå behoven med en version av Microsoft Intune.

Det är även viktigt att man förhåller sig till de nya livscykelplaner som det innebär att gå till System Center Configuration Manager Current Branch. Livslängden för support är kortare och det är viktigt att man följer med i versions uppgraderingar så man inte fastnar i ett osupporterat läge.

---

[10] https://blogs.technet.microsoft.com/enterprisemobility/2015/10/27/system-center-configuration-manager-support-for-windows-10-and-microsoft-intune/

[11] https://blogs.technet.microsoft.com/enterprisemobility/2015/08/18/managing-windows-10-with-ems-configmgr/

8 MICROSOFT OPERATIONS MANAGEMENT SUITE

OMS eller Microsoft Operations Management Suite är Microsoft nya molnbaserade Managerings plattform för att stödja Hybrida och rena Molnbaserade lösningar. Fokuset är mycket kring servernära tjänster och inte så mycket på klient. Det som rör Klient handlar främst om Insight and Analytics samt Security and Compliance.

Man utvecklar just nu en lösning för att patcha system men denna lösning är inriktad på Server System och inte klienter.

8.1 OMS TEMAN

När det gäller OMS så består den idag av fyra teman som beskriv nedan.

8.1.1 Insights and Analytics

I detta tema så finner man tjänsterna som fokuserar på Log Analytics där man kan samla in loggar och utifrån detta sammanställa och ställa frågor mot dessa data för att effektivt kunna hitta problem eller följa trender i sin IT-miljö.

8.1.2 Automation & Control

I detta tema så har man fokuserat på tjänsterna Azure automation som är en motor för att Automatisera likanande System Center Orchestrator som man kanske är van vid från System Center familjen.

8.1.3 Protection & Recovery

I detta tema finner man Microsofts Backup Tjänster men även deras tjänst för Disaster Recovery (ASR). Azure Site Recovery kan inte bara sköta replikering av virtuella maskiner utan även hela orchestreringen av hur man kan ta den i bruk igen efter en katastrof.

8.1.4 Security & Compliance

I detta tema har Microsoft utvecklat säkerhetsmoduler som analyserar och fokuserar på säkerhetsrelaterad information. Exempel kan vara saknade säkerhets patchar, analys mot Microsofts Threat Intelligence data.

8.2 WINDOWS UPGRADE ANALYTICS

Med Windows 10 så har Microsoft utvecklat en tjänst som bygger på OMS i botten som heter Windows Upgrade Analytics Service[12], detta är en tjänst för att analysera befintliga och nya klienter om hur de klarar en Windows 10 uppgradering. Detta för att underlätta för kunder att identifiera eventuella problem i sin Windows 10 livscykelhantering.

Det man har gjort är att I System Center Configuration Manager så har man utvecklat en Integration för Windows 10 Upgrade Analytics så man kan ansluta sin ConfigMgr miljö och följa statusen för hur ens ”Windows 10 Readiness” ser ut och vilka eventuella problem man kan tänkas stöta på.

Detta är en molnbaserad tjänst som bygger på telemetri från klienterna och dessa samlas då in och sammanställs för alla kunder som ansluter sig så man gemensamt kan få ut värde av tjänsten.

[12] https://technet.microsoft.com/en-us/itpro/windows/deploy/manage-windows-upgrades-with-upgrade-analytics

9 MICROSOFT INTUNE

Microsofts lösning för att hantera mobila enheter såsom iOS, Android och Windows Phone, men även Windows 10 Desktop enheter, kallas för Microsoft Intune[13], en molnbaserad lösning. Ser man till de olika produkter som Microsoft erbjuder, så nämns även MDM for Office 365 och System Center Configuration Manager (hybrid). Alla dessa produkter bygger i grund och botten på Microsoft Intune. En kombination av dessa produkter är inte att rekommendera, utan man behöver göra ett aktivt val innan man påbörjar en implementation.

För den som vill veta mer om skillnaden mellan dessa produkter, finns det ett flertal olika artiklar samt även dokumentation från Microsoft:

https://support.office.com/en-us/article/Choose-between-MDM-for-Office-365-and-Microsoft-Intune-c93d9ab9-efb2-4349-9b93-30c30562ee22?ui=en-US&rs=en-US&ad=US

En mer fördjupad förklaring kring vad Microsoft Intune är, vilka möjligheter produkten ger samt utmaningar den hjälper till att lösa, se följande dokumentation från Microsoft:

https://docs.microsoft.com/en-us/intune/understand-explore/introduction-to-microsoft-intune

Microsoft Intune erbjuder device management hantering för Windows 10 Desktop (inte Mobile), vilket innebär att molntjänsten kan hantera enheter antingen via en agent, som installeras på respektive Windows 10 enhet, eller med denn inbyggda MDM agenten som finns inbyggd i Windows 10. Respektive metod har olika nivåer av funktionalitet som de supporterar. Se länk nedan för en sammanställning av funktionalitet mellan dessa två hanteringsmetoder:

http://stealthpuppy.com/windows-10-management-intune/

Inför planering och och konfiguration av Microsoft Intune, är det viktigt att man gör ett aktivt val mellan dessa två hanteringsmetoder. Det är inte rekommenderat att blanda mellan metoderna, eftersom det kommer att medföra inkonsekvent nivå av enhetshantering. Vår rekommendation är att man undersöker om hantering av enheter via MDM agenten (modern management) uppfyller de krav som existerar.

En av de största fördelarna med Microsoft Intune är just att det är en molntjänst, vilket betyder att on-premise infrastruktur inte behövs. Varje månad så uppdaterar Microsoft molntjänsten vilket medför att ny funktionalitet som tillkommer i varje ny version finns tillgänglig direkt.

9.1 ENHETSHANTERING MED INTUNE

Microsoft Intune supporterar att hantera ett flertalet olika operativsystem i olika utsträckningar, varav följande:

- iOS
- Android
- Windows 10 Desktop (MDM eller med agent)
- Windows 10 Mobile
- OS X

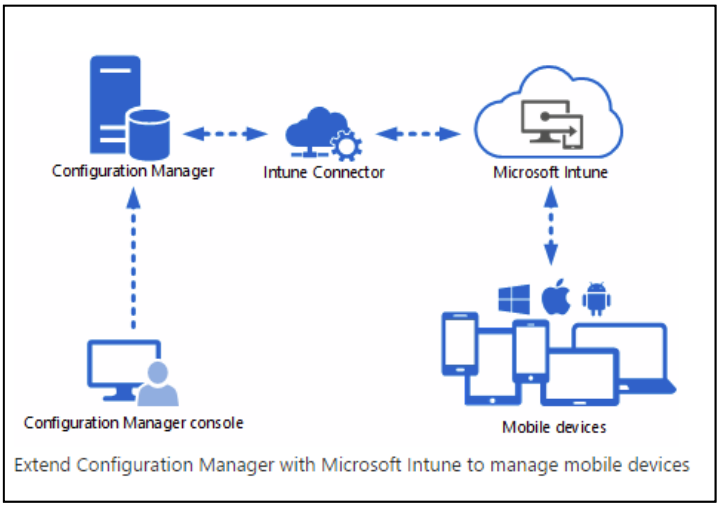
[13] https://docs.microsoft.com/en-us/intune/

Microsoft har ett förhållningssätt vad avser 0-day support med Microsoft Intune där syftet är att erbjuda support för de senaste versioner av de supporterade operativsystemen ovan på dagen när versionerna offentliggörs. Detta är möjligt eftersom Microsoft Intune har byggts som en molntjänst, och inte en produkt som kräver on-premise infrastruktur.

Populära tredjepartstjänster för hantering av enheter, t.ex. Apple Device Enrollment Program (DEP) och Android for Work stödjs av Microsoft Intune. Med dessa tjänster kan man utöka hanteringen av iOS och Andriod enheter för att uppnå en förbättrad slutanvändare upplevelse men också säkerhetsnivå.

För organisationer som mestadels eller enbart köper in iOS enheter, rekommenderar vi att undersöka möjligheten att gå med i Apple Deployment Programs. Detta gör utökad funktionalitet, såsom Apple DEP men också Apple VPP (se applikationsdistribution under punkt 10.4 nedan).

9.2 HYBRID ELLER STANDALONE MED INTUNE



Vid införande av Microsoft Intune för mobile device management, behöver man svara på frågan ”hybrid eller standalone”. Frågan uppstår av den anledning att Microsoft Intune kan användas i två olika lägen, nämligen i ett cloud-only (även kallat för Standalone) läge där molntjänsten inte har några kopplingar till befintlig on-premise infrastruktur. Det andra läget som kallas för Hybrid, är en sammankoppling mellan System Center Configuration Manager och Microsoft Intune där Configuration Manager’s befintliga funktionalitet utökas med avancerat stöd för mobile device management via molnet.

I Microsoft Intune finns en inställning för vilken MDM Authority är satt, en inställning som styr vilket läge som Microsoft Intune är konfigurerat för, antingen hybrid eller cloud-only. Varför man behöver svara på frågan om hybrid eller cloud-only har tidigare varit viktigt av följande anledning; processen för att MDM Authority inställningen från ett läge till ett annat har varit stökig och involverat supportsamtal till Microsoft, re-enrollment av devices samt omskapande av policies, applikationer osv. Med andra ord är det ingen simpel process, vilket leder till vikten av det val man initialt bestämmer sig för att använda sig utav.

Vi har sett en del organisationer och företag som initialt valt att införa Microsoft Intune i ett cloud-only läge, men av olika anledningar sedan har valt att slå om till hybrid. Några av de största av dessa anledningar beskrivs nedan:

- Enklare managering från en singel konsol (System Center Configuration Manager)
- Inget stöd för automatisering
- Undermåliga rapporter och inventering av enheter
- Inget stöd för rollbaserad accesshantering

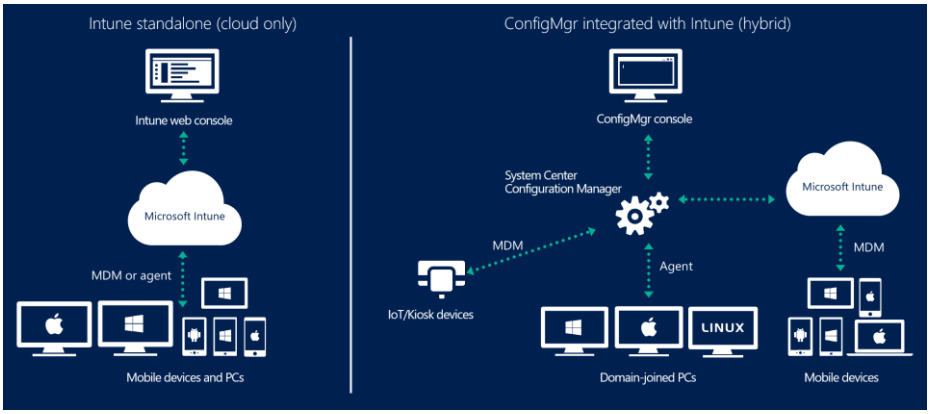
En annan anledning eller faktor som lett till att företag och organisationer valt hybrid framför cloud-only är att cloud-only läget tillåter hantering av maximalt 50 000 enheter. Detta tvingar fram valet av hybrid läget eftersom Microsoft Intune i cloud-only inte skalar upp såsom System Center Configuration Manager sammankopplat med Microsoft Intune.

Som det tidigare beskrivits i den här rapporten så har Microsoft Intune som en separat molntjänst (cloud-only) legat efter konkurrenterna vad gäller funktionalitet. Under början av 2017 kommer en ny och omarbetad version av Microsoft Intune att släppas. Den här versionen förväntas innehålla mycket funktionalitet som tidigare varit en anledning till att organisationer och företag valt att gå från cloud-only till hybrid. Nedan listas de höjdpunkter gällande ny funktionalitet som komma skall under 2017, vilket förenklar valet mellan hybrid och cloud-only[14].

- Automatisering via Microsoft Graph API
- Avancerad rapportering
- Rollbaserad accesshantering
- Support för fler än 50 000 enheter (bättre skalbarhet)
- Singel konsol hantering av tjänsten

Står man inför ett kommande projekt för mobile device management, är det viktigt att man väljer rätt från början. Vilka krav på funktionalitet eller beroende finns det internt som behöver uppfyllas, är något som vi ofta behöver fråga innan man påbörjar en implementation. Vår rekommendation är att avvakta med kommande projekt till dess att Microsoft har släppt den nästkommande versionen av Microsoft Intune som beräknas komma under våren 2017 och först utvärdera om cloud-only läget uppfyller kraven.

[14] https://docs.microsoft.com/en-us/sccm/mdm/understand/choose-between-standalone-intune-and-hybrid-mobile-device-management



9.3 INTUNE I AZURE

Under första kvartalet av 2017 lanseras en ny version av Microsoft Intune i Azure. Tidigare har Microsoft Intune varit en separat molntjänst från Microsoft's Azure platform. I skrivande stund av rapporten så är Microsoft Intune i Azure under "Public Preview". Under 2017 kommer arbetet med att migrera befintliga kunder att fortlöpa under första halvåret, men nya kunder som ännu inte har registrerat en Microsoft Intune tenant har möjlighet att hamna direkt på den nya platformen i Azure efter det att public preview har avslutats och tjänsten finns tillgänglig som "General Availibility".

9.4 APPLIKATIONSDISTRIBUTION OCH PAKETERING

Att branschen går mer mot SaaS- och webbapplikationer är tydligt men behoven för att distribuera rika klienter kommer finnas kvar ett tag framöver. För att hantera SaaS och webbapplikationer så har Microsoft tre spår.

Ett spår går ut på att man genom en användarportal kan publicera länkar till SaaS-applikationer myapps.microsoft.com. Vi se tecken på att denna kanske kommer att slås samman med portal.office.com men det råder en viss osäkerhet om det.

Sen för att leverera nya moderna applikationer så har man det man kallar Store, dvs en butik där man kan köpa och ladda ner applikationer som utvecklare publicerar. Denna store finns i två varianter och det är en företagsprivat "Windows Store for Business" och den vanliga publika storen. Som företag kan man styra vilken store man vill använda och hur man vill tilldela applikationer till användare. Idag kan bara publicera Moderna Applikationer i dessa Stores. Vi har sett antydningar på att man vill möjliggöra andra applikationstyper även via denna kanal men det är inget vi ser inom en snar framtid.

Andra leverantörer har ju sina motsvarande butiker/stores där Apple har sin Appstore och Google har Google Play som bygger på samma princip. Apples model för VPP (Volume Purchase Progam) tror vi är en modell som de övriga tillverkarna kommer följa efter.

Sen finns det tredje spåret där man jobbar med sideloading där man med något management system distribuerar moderna applikationer via något verktyg exempelvis Configuration Manager.

När de gäller de traditionella mjukvarudistributions sätten så ser vi inga större förändringar i dem utan de kommer vara som de alltid har varit och ha möjlighet för att distribuera appar och Script i Configuration Manager, då mycket av nyutvecklingen sker i moderna appar och webb så är incitamenten för Microsoft att göra stora investeringar på detta område ganska små.

Tittar man på ”Modern Management med Intune så finns där idag en distributionskanal via MDM Managerings kanalen. Denna kanal är tyvärr väldigt begränsad idag och skapar utmaningar för vi skall lyckas med Modern Management. Vi kan tex idag inte distribuera script via denna kanal om vi vill göra en anpassning eller inställning, utan det som idag är supporterat är distribution av ”Single MSI”. Dvs MSI Installationer som har allt sitt innehåll inuti MSI-filen.

Andra begränsningar och möjligheter med denna modell

- MST Filer är inte supporterade
- MSI Filens Produktkod används för detektion
- MSI Filens Standardläge för omstart kommer användas
- Användarbaserade MSI filer kommer installeras för enskild användare
- Maskinbaserade MSI filer kommer installeras för alla användare
- Användar- och maskinbaserade MSI Filer installerar bara för alla användare
- Applikationsuppdateringar är supporterade när MSI-files produktkod är samma för alla versioner
- Det går inte att styra vilken ordning en applikation installeras i.
- Man kan inte skapa beroenden till andra applikationer

Detta gör att man stöter på en del begräsningar av vilka applikationer man kan distribuera och det ställer krav på de som paketerar på ett annat sätt för att denna modell skall kunna användas.

När det gäller Intune-agenten så är detta ingen agent Microsoft satsar någon utveckling på och den är heller inte supporterad på Windows 10 vilket gör att vi inte kan använda denna mjukvarudistribubutionskanal som finns via den.

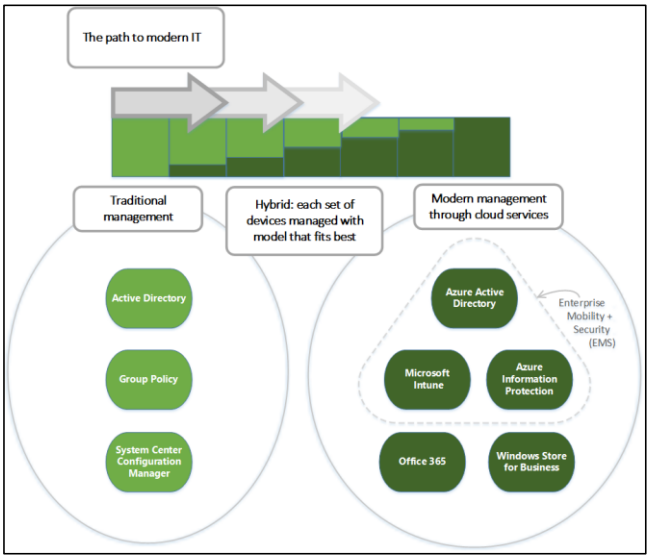
Vår slutsats idag är att man med MDM kanalen endast kan lösa ett begränsat antal behov men man behöver utvärdera om den kan lösa tillräckligt mycket för att man skall vara nöjd med denna modell. Vi ser att Configuration Manager kommer finnas kvar över väldigt lång tid samtidigt som man kommer utveckla mer funktioner och utveckla möjligheterna för mjukvarudistribution via Intune MDM då det är en av de stora hinder många av Microsoft kunder har för att anamma MDM Managering av Windows 10.

10 MODERN MANAGEMENT

En modernt managerad klient hanteras på nya sätt med större friheter för användaren. Man bygger lösningen på komponenter som är molnbaserade. Användaren star för mer egen administration och säkerheten följer antingen identitet, enhet eller information utan så stort fokus på var enheten, informationen eller användaren befinner sig för att utföra sitt arbete.

Byggstenar som ofta används för detta är:

- Windows 10
- Office 365
  - Onedrive för fillagring
  - Sharepoint, Skype mfl för collaboration
- Enterprise Mobility Suite
  - Azure Active Directory Premium
    - Azure AD Join
    - Enterprise State Roaming
    - Applikations Access
  - Intune
    - Device Management
  - Azure Information Protection
    - Data Security



Detta är en modell som ofta är enklare att införa på nya organisationer eller organisationer vi ofta refererar till ”Born in the Cloud”. När man kommer ifrån en traditionell verksamhet så har man ofta beroenden och arv som gör att man är i behov av mer funktionalitet än vad som idag är tillgängligt i Microsoft koncept för Modern Management. Jämför man med JAMFs (https://www.jamf.com/) lösning för Modern Management for Apples macOS så har Microsoft en bit kvar för att uppnå samma flexibilitet och möjlighet till konfiguration.

Microsoft inser att sina kunder står inför ett scenario där modern management inte kan implementeras direkt, och det finns hinder längs vägen som måste lösas. Därför arbetar man på att förbättra möjligheten till en hybrid lösning mellan traditionell hantering och modern management. Ett exempel på detta är möjligheten att med Microsoft Intune distribuera System Center Configuration Manager klienten till en Azure AD registrerad maskin som därefter avregistreras i Microsoft Intune och hanteras av Configuration Manager. Tills dess att modern management kan tillämpas fullt ut, hanteras en Azure AD registrerad enhet av Configuration Manager.

Följande länk visar på en övergripande nivå vad modern management för Windows 10 innebär:

https://youtu.be/g1rlcBhhxpA

10.1 MODERN MANAGEMENT I PRAKTIKEN

Efter släppet av den första versionen av Windows 10, har BTH tillsammans med Lumagate arbetat med visionen om modern management av Windows 10. Tanken var att gå ifrån System Center Configuration Manager och managera Windows 10 enheter med hjälp av molntjänster från Microsoft, i form av Azure AD och Microsoft Intune.

Microsofts vision på modern management betyder egentligen att man managerar enheter med den inbyggda MDM agenten i Windows 10. Microsoft Intune har möjlighet att distribuera konfigurationspolicies till enheter som ansluts till molntjänsten (även kallat för enrollment). Samverkan mellan Windows 10, Microsoft Intune och Azure möjliggör följande scenario:

- Användaren startar en ny enhet/dator med Windows 10 förinstallerat och som kommer direkt från leverantören.
- Användaren anger användarnamn och lösenord (eventuellt vald metod för multi-faktor autentisering om sådan konfigurerats i Azure AD)
- Enheten registreras i Azure AD och en automatisk enrollment mot Microsoft Intune för managering sker
- Policies från Microsoft Intune laddas ned och appliceras på enheten i bakgrunden som konfigureras
- Applikationer distribuerade från Microsoft Intune, t.ex. Office 365 ProPlus, installeras på enheten

Nedanstående beskrivs den kravställning som användes det arbetades med inom projektet som utgångspunkt:

- Windows 10 Signature Edition förinstallerad på enheter
- Registrera enheten i Azure AD med automatisk anslutning till Microsoft Intune
- Automatisk uppgradering av Windows 10 SKU från Professional till Education
- Möjlighet att definiera ytterligare lokala administratörer på enheterna
- Ge användare möjlighet att installera applikationer manuellt från software portal
- Tvingad installation av Office 365 ProPlus

- Säkerställa att följande funktioner är aktiverade och konfigurerade:
  - Windows Update
  - Windows Defender
  - Windows Firewall
- Hantering av Windows as a Service (WaaS)
- BIOS uppgraderingar med HP Support Assistant
- Konfigurering av operativsystems funktioner såsom Cortana, Telemetry bland annat

Under projektets start visade det sig att kravställningen inte kunde uppfyllas till fullo. Problemen hopade sig och det var tydligt att modern management scenariot ur BTHs vision inte var genomförbart med de första versionerna av Windows 10, men även Microsoft Intune hade begränsningar.

Kvartalsvis gjordes det avstämningar mellan BTH och Lumagate för en genomgång av nyheter kring Microsoft Intune och Windows 10. Strax före sommaren 2016 genomfördes en proof-of-concept av projektet. Resultatet av detta visade på en instabil lösning med många lösa trådar, när det kommer till granulär konfiguration som vid tillfället inte supporterades.

Projektet tog en vändning efter att Windows 10 version 1607 släppts, där ny funktionalitet tillkom i form av bland annat möjligheten att automatiskt uppgradera från Windows 10 Professional till Education utan att en omstart krävdes.

För att komma i mål utefter den kravställning som BTH satt upp, behöver man förstå att det finns ett samband mellan Microsoft Inte och Windows 10 i form av vilka funktioner i operativsystemet som molntjänsten supporterar. MDM agenten (modern management) i Windows 10 kommunicerar med såkallade Configuration Service Providers (CSP) vars syfte är att konfigurera olika delar av operativsystemet. En CSP kan liknas med Group Policies, på ett mer fördelat och strukturerat vis. I dagsläget finns det inte möjlighet att beröra alla delar av operativsystemets funktioner eller inställningsmöjligheter via MDM, men för varje ny version av Windows 10 har det tillkommit fler CSP's. Detta skall tolkas på det viset att den första versionen av Windows 10 innehöll ett fåtal konfigureringsmöjligheter via MDM, men fler har tillkommit för respektive version av Windows 10. Microsoft har som mål att fortsätta att bygga ut möjligheterna till konfiguration via MDM, men det betyder inte att man en dag kommer vara i paritet med vad som går att konfigurera med Group Policies. Frågan man också bör ställa sig när man ser på modern management är, vilka behov har vi egentligen?

Projektet för modern management i praktiken med Windows 10 och Microsoft Intune, enligt den kravställning som BTH gjorde, kan enkelt sammanfattas att många delar idag går att genomföra, men vitala delar som säkerhet och applikationsdistribution inte lever upp till de önskemål som finns.

Med den nya version av Windows 10 som benämns Creators Update (kommer förmodligen i marsr 2017), har Microsoft annonserat att den kommer innehålla många förbättringar kring modern management scenariot. Ny funktionalitet tillkommer ständigt, månadsvis för Microsoft Intune och en till två gånger per år för Windows 10, vilket man i projektet med BTH och Lumagate har tagit höjd för. Under våren 2017 kommer Microsoft även att göra en stor uppdatering av Microsoft Intune, där förhoppningarna ligger på att modern management scenariot skall kunna genomföras tillsammans med Creators Update.

Det senaste om Intunes decemberuppdatering finns på denna länk
https://docs.microsoft.com/en-us/intune/whats-new/whats-new-in-microsoft-intune
Portal preview
https://docs.microsoft.com/en-us/intune-azure/introduction/what-is-microsoft-intune

11 ERFARENHETER FRÅN UNIVERSITET OCH HÖGSKOLOR

Commented [NA1]: Leif vad tänker du här? (Stefan)
jag skriver något om vad som hänt, kan hända jag hinner få ut en kort enkät (Leif)

En enkät skickades ut i juni 2016. Av den framgår bland annat att de flesta använder eller kommer att använda SCCM. Ingen använder Intune för administration av Windows PC. Två universitet, Linköping och Chalmers, har däremot testat att använda Intune för mobiler.

Den traditionella processen med att "blåsa" skivminnet och lägga på ett helt ny image är den metod som de flesta kommer att använda.

De flesta kör i december 2016 version 1607 eller 1610 av SCCM.

Många kommer att ha kvar Windows 7 på gamla datorer till dess att de skrotas.

Få av de som arbetar med administration av PC har erfarenhet av Microsofts moln Azure. Ingen eller väldigt få har testat och ännu färre använder Operations Management Suite, OMS i Azure för övervakning och statistik.

12 STATUS I DECEMBER 2016

Vi är nu framme i december 2016 och Microsoft har hunnit släppa sin tredje version av Windows 10 som idag är uppe i version 1607. Man inledde med 1507 som senare blev 1511 som följdes av den nuvarande 1607. Microsoft har lyckts ställa om sitt sätt att leverera Windows och tyvärr har det inte varit smärtfritt att flytta mellan de olika versionerna 1507-1511-1607. Det har varit många fallgropar och utmaningar men ju mer tiden har gått har vi sett Microsoft finslipa denna process för att nå det mål man har om hur enkelt det skall vara att uppgradera Windows 10.

System Center Configuration Manager Current Branch har även den utvecklats och uppgraderas löpande under det gågna året och man är idag uppe i version 1610. Man har haft stor framgång i detta arbete och man har sett en stor acceptans och stor utvecklings hos kunderna att kunna följa mer i version. Brad Andersson har uttalat sig om denna succé[15] som vi till fullo håller med om.

När det gäller Intune så har även den fått löpande versioner men när det gäller funktioner är vi lite missnöjda med takten man har släppt ny funktionalitet. Dock finner det sin förklaring i att man har under de senaste 18 månaderna lagt stora utvecklingsresurser att flytta plattformen som Intune ligger på till det ramverk som Azure använder, den så kallade Ibiza Portalen som återfinns för Microsoft Azure. Vi är övertygade att mängden ny funktionalitet kommer öka markant när man har fått den nya portalen lanserad under 2017.

12.1 SLUTSATSER MODERN WINDOWS 10 HANTERING

Idag når vi inte hela vägen med de versioner som finns av Intune och Windows 10 för att skapa Modern Management till fullo. Vi har identifierat tre huvud områden som funktionaliteten behöver utvecklas inom innan vi kan se att det till fullo går att använda sig av Modern Management konceptet från Microsoft för de kravställningar som idag finns för merparten av verksamheter.

12.1.1 Säkerhet

I dagens Modern Management-lösningar så kan vi inte möte de behov som finns hos IT-avdelningarna. Det vi i första hand saknar inom säkerhetsområdet är:

- Möjligheten att tvinga Bitlocker kryptering detta går idag endast på datorer med InstantGo[16] Stöd vilket idag bara Microsoft Surface har.
- Vi saknar stöd för rapportering av Windows Defender så vi kan följa upp Virus/Malware Incidenter, detta får man idag lösa med att använda en tredjeparts antivirus.

12.1.2 Mjukvarudistribution

När det gäller mjukvarudistribution så når vi inte hela vägen fram med de behov som finns idag med att installera mjukvara.

---

[15] https://blogs.technet.microsoft.com/enterprisemobility/2016/11/18/configmgr-current-branch-surpasses-50m-managed-devices/
[16] https://en.wikipedia.org/wiki/InstantGo

- Vi saknar möjlighet att underhålla firmware eller BIOS via Intune och alternativet Windows Update. Detta är något Microsoft löst på sina egna enheter men vi har inte sett någon antydan från andra tillverkare att följa efter än.
- Mjukvarudistributions möjligheterna i Intune är väldigt begränsade och ställer krav på ompaketering i de fall det går medan andra fall kan man inte lösa det alls pga av begränsningar i MSI Standarden.
- Vi saknar möjligheten att avvända .MST filer
- Vi är tvingade att använda single MSI Filer utan content.

12.1.3 Konfigurationshantering

- När man gör en Reset av en PC så tappar Windows sin Intune-koppling.
- Vi kan inte kontrollera hur datorer skall namnges.
- Vi har stora begränsningar i vilka konfigurations möjligheter vi kan göra på en enhet. Windows 10 saknar helt enkelt CSPer för att kunna göra denna konfiguration via MDM. Dock så ser vi ju ett minskat behov av detta i en modern Management lösning men granularliteten och utbudet av inställningsmöjligheter saknas.
- Utskrifter är en svårighet att hantera då vi inte på samma sätt som tidigare kan kontrollera skrivarinstallationer.

■