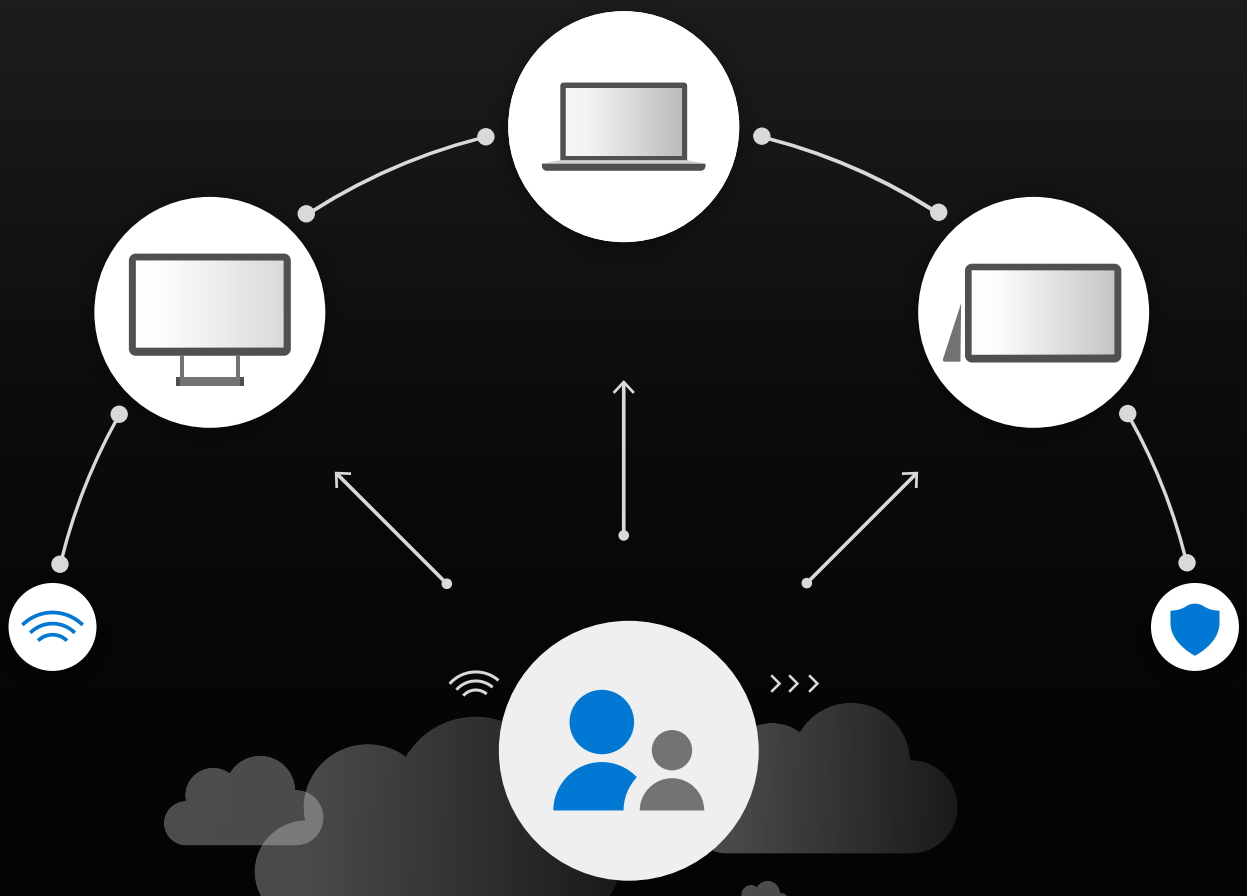
Microsoft Surface

Modern eindpuntbeheer

Waarom ‘ingebouwd’ beter is dan ‘eraan gehangen’



Inhoudsopgave

03
Introductie

04
De evolutie van mobiel beheer

05
Het moderne beheermodel

08
Een modern bureaublad, gemaakt voor modern beheer

12
De transitie maken

14
Conclusie

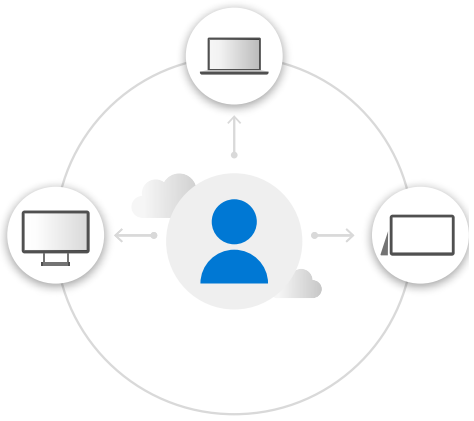
Introductie

Het beheren van endpointapparaten wordt voor bedrijven steeds complexer en is vaak erg frustrerend. De moderne werkomgeving wordt gekenmerkt door een gevarieerde mix aan desktops, laptops, tablets en smartphones, verspreid over een groot aantal locaties en met gebruik voor veel verschillende doeleinden.

Door het complexe IT-landschap is het moeilijk om de groeiende ondersteuningskosten binnen de perken te houden en gebruikers van de nieuwste apps en functionaliteiten te voorzien. Wat misschien nog belangrijker is, is dat inconsequent beheer van endpointapparatuur beveiligingsrisico's met zich meebrengt. Reden hiervoor is dat het onmogelijk is om alle appraten steeds van de nieuwste patches en bescherming te voorzien. IDG's Onderzoek beveiligingsprioriteiten 2019 concludeerde dat verbetering van de bescherming van vertrouwelijke en gevoelige data voor bijna 6 op de 10 beveiligingsprofessionals prioriteit nummer 1 is. Data beschermen is rechtstreeks gerelateerd aan beter apparaatbeheer.

Het traditionele antwoord op deze uitdaging is strikt beleid dat de toegang tot bedrijfsnetwerken, -applicaties en -data beperkt. Dit beleid zorgt voor een ander IT-pijnpunt: gefrustreerde gebruikers. **Werknemers zijn gewend aan naadloze toegang tot informatie** via **hun persoonlijke apparaten en ze willen dezelfde naadloze ervaring** op het werk. IT-teams begrijpen die vraag: in IDG's Onderzoek beveiligingsprioriteiten 2019 gaven IT-leiders aan dat verbetering van de productiviteit van werknemers een essentieel onderdeel van de digitale transformatie is. Daarnaast stellen ze dat hogere productiviteit de belangrijkste statistiek is waarmee digitaal zakelijk succes kan worden gemeten.

Om deze voortdurende uitdagingen van de moderne onderneming aan te gaan, **hebben IT-teams een moderne benadering van apparaatbeheer nodig**. Daarin is het van belang dat **alle componenten, van de chip tot de cloud, zijn geïntegreerd.**



De evolutie van mobiel beheer

Mobiliteitsbeheer is van oudsher een wirwar van afkortingen, van MDM (mobile device management) en MAM (mobile application management) tot EMM (enterprise mobility management) en recentelijk UEM (unified endpoint management). Al deze termen hebben hetzelfde doel: zorgen voor een uitgebreid, maar toch gestroomlijnd overzicht van endpointapparatuur. Zo kunnen IT-teams effectiever met beleid, applicaties en updates omgaan.

De noodzaak voor een moderne aanpak van endpoint management, met gestroomlijnde beleidshandhaving, is een drijvende factor achter de opkomst van UEM. Analist Jack Gold verwacht dat ondernemingen UEM gaan omarmen om de overlap tussen mobiele en pc-beheeroplossingen weg te nemen.

"Als je strategisch kijkt naar endpoint management, en ook niet voorbereidt bent op de volgende fase aan mogelijkheden, loop je het risico dat je bedrijf lagere productiviteit, een groter bedreigingsoppervlak en hogere totale eigendomskosten krijgt," schrijft Gold in Computerworld.

De cloud speelt een cruciale rol in deze transitie naar modern mobiel beheer.

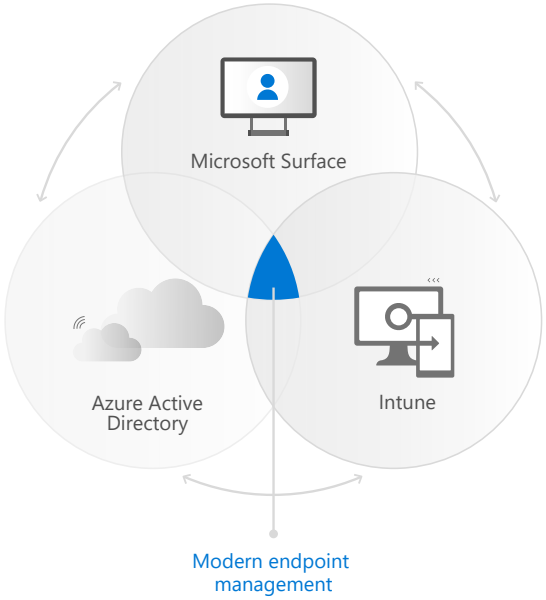
De volledige voordelen van modern beheer ontstaan door met een schone lei in de cloud te beginnen. Start met cloudbeheer waarin alle functionaliteiten met een sterke integratie zijn ingebouwd; van het silicium tot in de cloud. Dit staat in contrast met het simpelweg toevoegen van steeds meer en steeds complexere oplossingen.

Het moderne beheermodel

Bij traditioneel endpoint management wordt ervan uitgegaan dat elk apparaat dat IT beheert, ook echt in het bezit is van de organisatie en daarmee ook verbonden is met een lokaal netwerk. Groepsbeleid beperkt hoe gebruikers de apparaten gebruiken die aan ze zijn toegewezen.

IT-teams worstelen vaak met het bijhouden van het groeiende aantal beveiligingsrisico's en de toenemende snelheid waarmee besturingssystemen en applicaties veranderen. Het gevolg is dat ze vaak reactief werken (ze lossen problemen op), in plaats van proactief functies en mogelijkheden toe te voegen die de gebruikerservaring verbeteren in plaats van beperken. IT ervaart daarnaast potentiële hinder door verwarrend of achterhaald beleid dat door een eerdere leiding is ingesteld. Het gevolg? De algemene complexiteit wordt verder vergroot.

Gebruikers klagen op hun beurt steen en been bij IT deze beperkende aanpak. Moderne werknemers zijn gewend aan een bestaand ecosysteem van apps waarmee ze toegang krijgen tot een constante stroom aan nieuwe mogelijkheden en hun eigen keuze voor gebruiksvriendelijke apparaten en apps. Ze willen een nieuw apparaat instellen naar wens én zonder problemen. Meer selfserviceopties voor het aanpassen van hun gebruikservaring horen daar ook bij. Ze willen dat de technologie zich aanpast aan hun werkstijl in plaats van dat ze hun eigen gedrag moeten aanpassen. Met andere woorden: de technologie moet bijna onzichtbaar zijn terwijl ze hun normale activiteiten uitvoeren.



Microsoft helpt IT-teams bij het oplossen van deze uitdagingen met de moderne benadering van modern endpoint management. Deze benadering bestaat uit drie hoofdcomponenten: Azure Active Directory, Intune en Microsoft Surface.

Azure Active Directory

Met Azure Active Directory kan je als beheerder via bestaande groepen in Active Directory applicatiebevoegdheden toewijzen en beheren. Met functies zoals Conditional Access bescherm je diensten op meerdere manieren (waaronder meervoudige verificatie). Daarnaast kan je kiezen voor beleid waarin automatisch passende maatregelen worden genomen als een gebruiker of inloggebeurtenis als riskant wordt aangemerkt.

Intune

Intune is het platform voor beheer van Surface en vele andere moderne endpoints, zoals apparaten die eigendom zijn van werknemers. Intune werkt samen met Azure Active Directory voor identiteits- en toegangsbeheer en met Azure Information Protection voor databescherming. InTune, in combinatie met de System Center Configuration Manager (SCCM) van Windows 10, maakt het instellen van beleidsregels voor beheer van toegang tot specifieke apps eenvoudiger voor IT-beheerders, zonder dat controle over het hele fysieke apparaat nodig is. Intune biedt ook mogelijkheden voor self service, zodat gebruikers gemakkelijk zelf toegang tot benodigde apps krijgen en IT minder wordt belast.

Microsoft Surface

Microsoft Surface-apparaten zijn ontworpen voor modern beheer en bieden de optimale balans tussen productiviteit en beveiliging, terwijl de totale eigendomskosten worden verlaagd. Uit een recent onderzoek van Forrester Consulting blijkt dat het rendement van Microsoft 365-investeringen met Surface toeneemt, en dat Surface nog meer voordelen biedt, zoals:

- Het verhogen van de productiviteit van werknemers.
- Het verbeteren van de creativiteit en het teamwerk.
- Het besparen van de kosten en benodigde IT-beheer.
- Het verbeteren van de beveiliging en compliance.

Modern beheer: het investeringsrendement maximaliseren

Hoeveel kunnen Surface-apparaten toevoegen aan het zakelijke voordeel van Microsoft 365? Best veel, blijkt uit een Total Economic Impact™-onderzoek van Forrester Consulting. In het onderzoek worden de mogelijke investeringsrendementen onderzocht die bedrijven kunnen behalen door Microsoft 365 Enterprise op Microsoft Surface-apparaten te implementeren. Forrester maakte voor het onderzoek gebruik van een samengestelde organisatie van 1500 gebruikers en kwam tot de volgende conclusies:

De herstelkosten voor beveiligingslekken namen met 80 procent af en het aantal jaarlijkse lekken nam 50 procent af. Met tweevoudige verificatie, Advanced Threat Analytics en de Surface Enterprise Management Mode (SEMM) kon de samengestelde organisatie de herstelkosten voor lekken verminderen met een voor risico gecorrigeerde contante waarde van bijna $1 miljoen in een analyse van drie jaar.

Lagere kosten voor externe technologie, apparaten, infrastructuur en IT-ondersteuningsvereisten. De hoeveelheid externe technologie en apparaten en ondersteuningskosten werden gereduceerd of geëlimineerd door Surface-apparaten op basis van Microsoft 365 te gebruiken. Dit leverde de organisatie over een periode van drie jaar een besparing in contante waarde van $1,9 miljoen op.

Helpdeskverzoeken voor het opnieuw instellen van wachtwoorden daalden met meer dan 86 procent, en het aantal ondersteuningsaanvragen voor slecht presterende apparaten en applicaties nam met 15 procent af. Door de stabiliteit van Surface waren er minder incidenten met vastlopende appratren en werden de verzoek van Surface-gebruikers met Microsoft 365 bijna om wachtwoorden te herstellen bijna helemaal voorkomen. In een periode van drie jaar was de totale voor risico gecorrigeerde contante waarde meer dan $150.000.

Veiligheid Helpdesk Kosten

Bron: Je investeringsrendement van Microsoft 365 Enterprise met Microsoft Surface maximaliseren

Een modern bureaublad, gemaakt voor modern beheer

Surface is ontworpen met ingebouwde ondersteuning voor eenvoudig modern beheer van de hele levenscyclus van het apparaat: **voordat het wordt geïmplementeerd, tijdens het gebruik en nadat het is ingeleverd om opnieuw te worden verstrekt of afgeschreven.**

Voor

Al voordat gebruikers het apparaat krijgen, denkt Microsoft aan het beheer. Door het apparaat voor het verstrekken al in te stellen, wordt de IT-afdeling sterk ontlast.

Een Microsoft Cloud Solution Provider (CSP) voegt een nieuw apparaat toe aan de hand van het serienummer aan de Azure Active Directory-omgeving van de klant. Zo kunnen apparaatprofielen worden aangemaakt, voordat het apparaat naar de klant wordt gestuurd. Denk bijvoorbeeld aan applicaties, beleid en instellingen. Een klant kan voor verschillende groepen (bijv. technici, marketing of personeelszaken) profielen maken. Zo heeft de gebruiker bij de eerste keer opstarten via Windows Autopilot alle juiste instellingen en applicaties heeft, zonder overbodige of ongewenste software.

Windows Autopilot maakt gebruik van de OEM-geoptimaliseerde versie van Windows 10 die vooraf op een apparaat is geïnstalleerd. Op deze manier hoeven organisaties niet voor elk model aangepaste installatiekopieën en stuurprogramma's te onderhouden. In plaats van een nieuwe installatiekopie op het apparaat te installeren, kan een bestaande Windows 10-installatie bedrijfsklaar worden gemaakt door instellingen en beleid in te stellen, apps te installeren en zelfs de gebruikte Windows-versie te veranderen (bijv. van Windows 10 Pro naar Windows 10 Enterprise) om geavanceerde functies te kunnen ondersteunen.

Tijdens

Microsoft Surface bevat geavanceerde, volwassen hardware en firmware die zijn ontworpen voor uitgebreid beheer. Zo kunnen beheerders zelfs het laagste niveau van de hardware-instellingen beheren, zonder dat ze de machine ook maar hoeven aan te raken.

Op eerdere generaties apparaten was het beheren van firmware-instellingen juist een enorme uitdaging. Voor elke configuratie- of beheeroptie was aangepaste of door de fabrikant geleverde software nodig, die bekend staat als UEFI (Unified Extensible Firmware Interface). Surface heeft echter een door Microsoft ontworpen UEFI, waarmee zowel het besturingssysteem als de UEFI/firmware in één handeling automatisch kunnen worden bijgewerkt. Deze aanpak biedt niet alleen een gestroomlijnd beheer, maar ook vebeterde beveiliging.

Het beheren van UEFI-firmware-instellingen gebeurt via de Device Firmware Configuration Interface (DFCI), een onderdeel van Intune en een openbron, standaard UEFI voor Surface van Microsofts Project Mu. Intune gebruikt DFCI om Autopilot te laten bevestigen of een klant die de firmware probeert te beheren ook echt de eigenaar van het apparaat is. Nadat Autopilot de eigenaar heeft bevestigd, past Intune de juiste instellingen toe zonder tussenkomst van de gebruiker. Op Surface-apparaten kunnen IT-beheerders ook de Surface Enterprise Management Mode (SEMM) gebruiken om het apparaat op het opstartniveau met aangepaste firmware-besturingselementen te beheren. Intune kan veel Surface-apparaatinstellingen met SEMM rechtstreeks beheren, waaronder:

- Certificaten
- Update-instellingen
- Bitlocker
- Apparaatfuncties
- E-mail
- VPN-verbindingen
- Windows-beveiligings-basislijnen
- Wifi-verbindingen

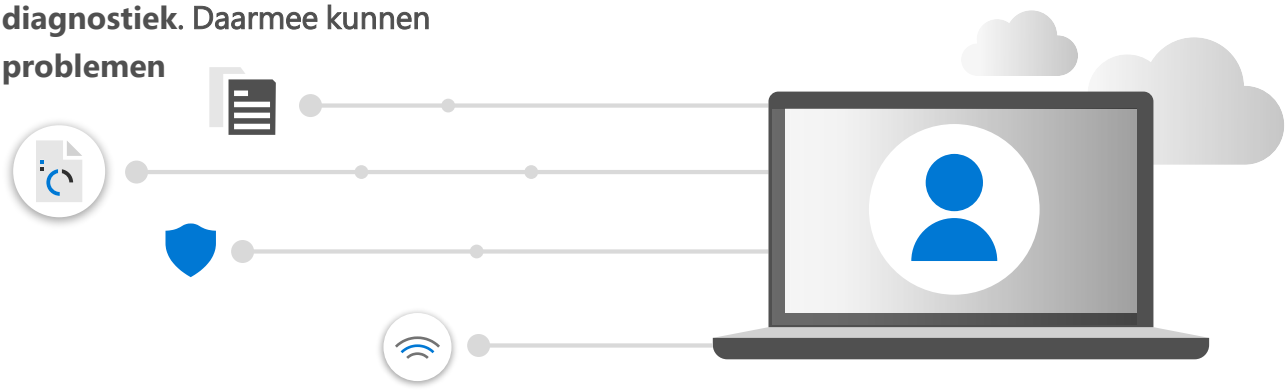
Elk Surface-onderdeel, van de firmware tot Windows 10-beleidsinstellingen, kan door Intune worden beheerd en via Windows Update for Business worden bijgewerkt.

Surface integreert ook in de beveiligingsstack van Microsoft 365 om kwetsbaarheden over de hele wereld te detecteren en apparaten automatisch te beschermen, zelfs als ze in de slaapmodus zijn. Surface-apparaten hebben een moderne energiebesparende stand-bystand waarin het apparaat in de slaapstand lijkt te staan en erg weinig stroom verbruikt. Toch houdt het apparaat via Windows Update for Business bij of er updates zijn en worden datastromen van applicaties zoals e-mail bijgehouden. Zo kan een Surface die op zijn accu actief is lang stand-by blijven, terwijl hij ook op de hoogte blijft van applicatiedata en beveiligingsupdates automatisch doorvoert, zelfs naar de UEFI.

Daarnaast bevat **Surface speciaal gebouwde tools voor** bijvoorbeeld **diagnostiek**. Daarmee kunnen **problemen automatisch opgelost worden of wordt er advies gegeven om deze op te lossen. Ook wordt functionaliteit geoptimaliseerd, van schermhelderheid tot accugebruik**. Met de Surface Diagnostic Toolkit for Business (SDT) kunnen IT-beheerders bijvoorbeeld snel hardware-, software- en firmwareproblemen met Surface-apparaten onderzoeken en oplossen.

Surface-apparaten zijn zo afgestemd dat ze de perfecte balans tussen accuduur en prestaties bieden. Windows' energiebeheermodus op Surface is het resultaat van belangrijk onderzoek naar de warmteproductie en prestaties van processors in combinatie met de noodzaak dat een accu de hele dag mee moet gaan.

Ten slotte kunnen beheerders dankzij de integratie tussen Intune, Surface en Microsoft 365 aangepaste suites van Office 365-apps configureren. Ook hebben zij de mogelijkheid om te bepalen hoe en wanneer deze apps worden bijgewerkt en zelfs welke apps verplicht zijn.



Na

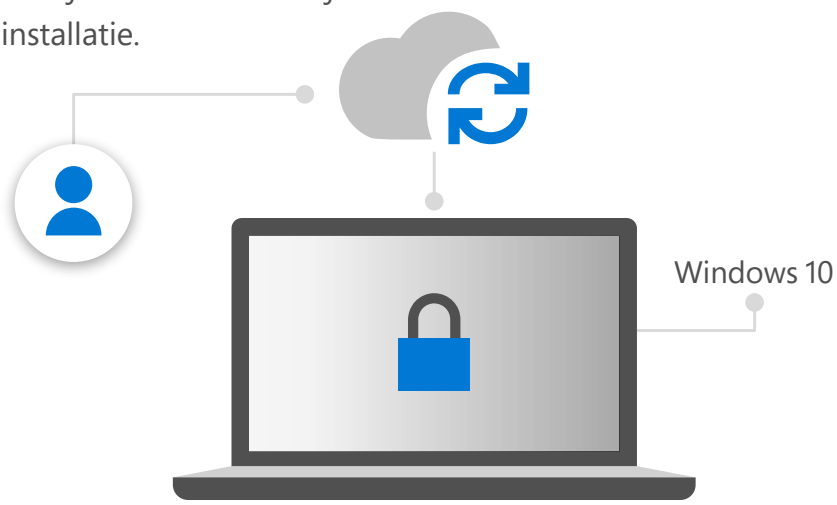
Endpoint management moet ook rekening houden met het moment dat een apparaat aan IT wordt teruggegeven om opnieuw te worden verstrekt of om geschreven te worden, of als het apparaat kwijtraakt of wordt gestolen. Door de afschrijving van apparaten te beheren, kunnen beheerders er gerust op zijn dat instellingen en andere data op het apparaat niet in handen komt van ongeautoriseerde gebruikers.

Met Intune kan een IT-beheerder een apparaat op afstand vergrendelen, wachtwoorden herstellen of het apparaat volledig wissen. Zo wordt de data beschermd als het apparaat kwijtraakt of wordt gestolen. Na het wissen wordt het apparaat opnieuw ingesteld op de standaardervaring, waarbij opnieuw de juiste referenties zijn vereist voor de installatie.

Bovendien kan een beheerder met de optie Nieuwe Start in Windows 10 alle applicaties verwijderen en de nieuwste versie van Windows installeren.

Als een werknemer het bedrijf verlaat, kan IT het apparaat op afstand opnieuw inrichten, zonder dat het apparaat op een centrale locatie moet worden ingeleverd. Het apparaat terugsturen is geen vereiste om een nieuwe installatiekopie te installeren.

Via het Azure Active Directory-portaal kan IT ook de inrichting van apparaten die zijn afgeschreven of vernietigd op afstand ongedaan maken.



De transitie maken

Overstappen op modern beheer is niet altijd makkelijk. IT-teams hebben namelijk al tijd en middelen in hun infrastructuur geïnvesteerd. Helaas blijven oude IT-processen en hardware de grootste obstakels voor het overstappen op modern beheer.

Surface maakt deze overstap makkelijker, omdat het aan IT-behoeften kan voldoen, ongeacht waar de organisatie in zijn modernisatietraject is:

Traditioneel lokaal beheer:
lokaal apparaatbeheer biedt een lichte benadering waarbij SCCM wordt gebruikt om apparaten te beheren. Deze optie is afhankelijk van de mogelijkheden voor apparaatbeheer die in Windows 10 zijn ingebouwd en biedt niet alle opties van beheer op cliëntbasis. Voor lokaal apparaatbeheer is een Microsoft Intune-abonnement nodig. Intune wordt hierbij alleen gebruikt om de licenties van de apparaten bij te houden, en niet voor het beheren of opslaan van beheerinformatie. Alle beheerdata wordt met de lokale Configuration Manager-infrastructuur in je organisatie opgeslagen.

Hybride/co-beheer: met co-beheer kunnen IT-beheerders Surface-apparaten gelijktijdig beheren door zowel SCCM als Intune te gebruiken. Door een verbinding te maken tussen Active Directory en Azure Active Directory kunnen beheerders nieuwe cloudfunctionaliteit, zoals voorwaardelijke toegang, inschakelen.

Met co-beheer heb je de flexibiliteit om een technologieoplossing te gebruiken die voor jouw organisatie het beste werkt. IT bepaalt of er workloads van SCCM naar Intune worden overgezet en zo ja, welke. Bestaande SCCM-cliënten gebruiken in co-beheer biedt een aantal directe voordelen:

- Voorwaardelijke toegang met apparaatcompliance.
- Ondersteuning voor handelingen op afstand via Intune, zoals herstarten, externe besturing of fabrieksinstellingen herstellen.
- Gecentraliseerde zichtbaarheid van apparaatstatus.
- De mogelijkheid om gebruikers, apparaten en apps met elkaar te verbinden via Azure Active Directory.
- Moderne provisionering met Autopilot.

Volledig beheer in de cloud: Intune biedt een zeer schaalbaar, geïntegreerd platform voor endpointapparatuur dat de cloud gebruikt om IT-teams te helpen bij het stroomlijnen en automatiseren van de implementatie, provisioning, beleidsbeheer, het leveren van apps en updates. Een wereldwijd gedistribueerde cloudarchitectuur zorgt dat apparaten altijd actueel zijn. Intune's beleidsregels voor appbescherming zorgen voor fijnmazige controle over Microsoft 365-data op endpointapparatuur. Andere voordelen van de Intune-ervaring in Azure Portal zijn:

- Een geïntegreerde console voor alle bedrijfsmobiliteit- en beveiligingscomponenten.
- Een HTML-console op basis van webstandaarden.
- Ondersteuning voor de Microsoft Graph-API voor het automatiseren van vele handelingen.
- Toegang tot Azure Active Directory-groepen om compatibiliteit binnen alle Azure-applicaties te bieden.
- Ondersteuning voor de meeste moderne webbrowsers.

Microsoft Surface

Conclusie

Bedrijven omarmen digitalisering en dat biedt IT-teams veel uitdagingen. Het beheren van endpointapparatuur met verouderde tools of processen maakt het moeilijk om apparaten en data veilig en gebruikers productief en tevreden te houden. Voor de moderne werkomgeving is het niet langer voldoende om stukjes endpoint management aan elkaar te hangen.

Microsoft heeft veel innovatieve beheerfuncties in Windows 10 geïntegreerd, maar als de fabrikant van je apparaat modern beheer niet omarmt en geen gebruik van deze mogelijkheden maakt, benut je niet de volledige toegevoegde waarde van modern endpoint management.

De apparaten van Microsoft Surface voor zakelijk gebruik bieden moderne hardware en software die zijn ontworpen voor gebruik van de beheermogelijkheden van Windows 10.

Elk Surface-onderdeel, van de firmware tot Windows 10-beleidsinstellingen, kan door Intune worden beheerd en via Windows Update for Business worden bijgewerkt. Surface integreert ook in de beveiligingsstack van Microsoft 365 om kwetsbaarheden over de hele wereld te detecteren en je apparaten automatisch te beschermen, zelfs als ze in de slaapmodus zijn. Surface-tools kunnen problemen automatisch oplossen, je helpen problemen op te lossen en functionaliteit te optimaliseren, van helderheidsinstellingen tot accugebruik.

Vind een wederverkoper >

© 2019 Microsoft Corporation. Alle rechten voorbehouden. Dit document wordt 'in de huidige staat' geleverd. Informatie en meningen in dit document, inclusief URL's en andere verwijzingen naar websites op internet, kunnen zonder kennisgeving worden gewijzigd. Gebruik is op eigen risico. Dit document geeft je geen enkel recht op enig intellectueel eigendom van om het even welk Microsoft-product. Je mag dit document kopiëren en gebruiken voor je eigen interne referentiedoeleinden.