De route naar een optimale digitale werkplek

Waarom het belangrijk is om de volwassenheid van de tien belangrijkste werkplekcomponenten te meten.

orange™ Business

Inleiding

De digitale werkplek speelt een cruciale rol in het verbeteren van productiviteit, samenwerking en efficiëntie, maar ook in het versterken van de betrokkenheid van werknemers. Vandaag de dag staat het optimaliseren van de digitale werkplek bij veel organisaties dan ook hoog op de agenda.

Een digitale werkplek die goed is ingericht, stelt medewerkers in staat om efficiënter te werken, naadloos samen te werken en gemakkelijk toegang te krijgen tot de nodige informatie en tools. In een tijd waarin getalenteerde professionals een schaars goed zijn geworden, vormt een geoptimaliseerde digitale werkplek een essentieel onderdeel in het aantrekken en behouden van werknemers. Het gaat niet alleen om het bieden van de nieuwste technologieën, maar ook om het creëren van een digitale werkplek die inspirerend, flexibel en gemakkelijk te navigeren is, zodat de employee experience optimaal is.

In deze whitepaper lees je meer over welke werkplekcomponenten van cruciaal belang zijn binnen een optimaal ingerichte digitale werkplek én hoe je een maturity assessment - met aandacht voor deze essentiële onderwerpgebieden - in kunt zetten als strategisch hulpmiddel bij innovatie.

Inhoudsopgave

In kaart brengen van de volwassenheid van de digitale werkplek

In een tijd waarin technologie en werknemerservaring hand in hand gaan, is een maturity assessment voor de digitale werkplek van onschatbare waarde.

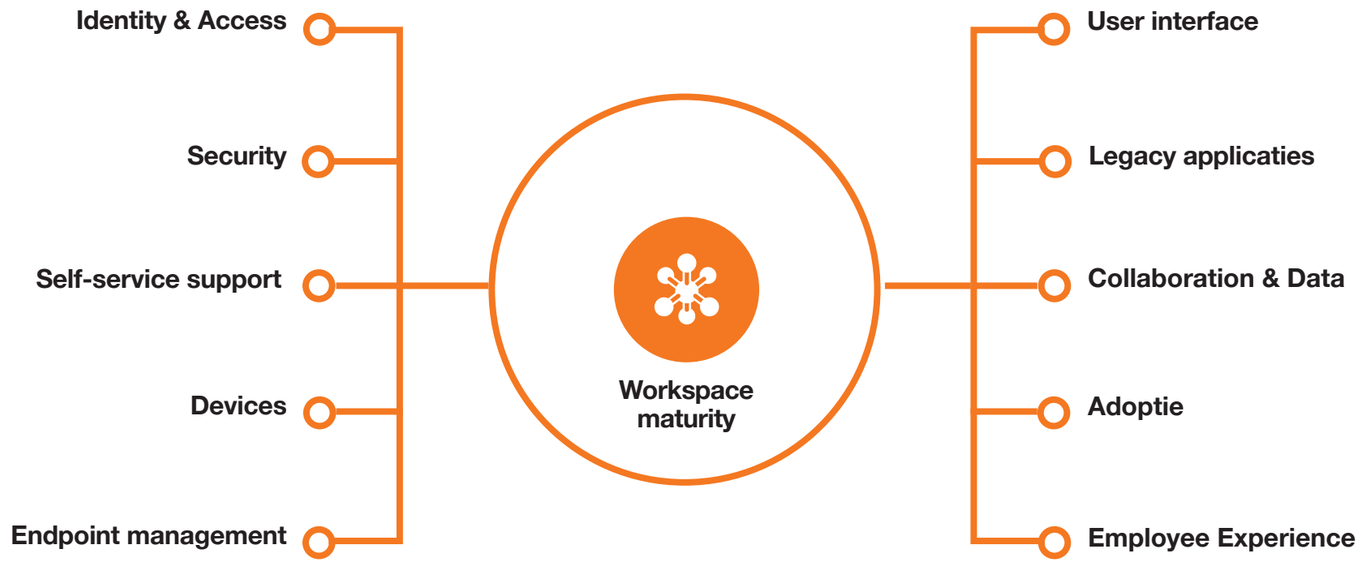
Een maturity assessment biedt niet alleen inzicht in de huidige stand van zaken, maar ook in de mogelijkheden tot verbetering, specifiek gericht op het vergroten van de medewerkerstevredenheid en het optimaliseren van hun werkervaring.

Door het aanpakken van uitdagingen zoals gebruiksvriendelijkheid, samenwerkingsmogelijkheden en het waarborgen van digitale veiligheid, kunnen organisaties niet alleen hun concurrentiepositie versterken, maar ook aantrekkelijker worden voor potentiële werknemers, zelfs in een competitieve arbeidsmarkt.

“Een effectieve digitale werkplek is cruciaal om succes te behalen in de digitale economie.”
– Gartner

Roadmap naar de optimale digitale werkplek

Om de roadmap naar de optimale digitale werkplek voor je organisatie te maken, is het van groot belang om inzicht te hebben in de volwassenheid van de tien belangrijkste werkplekcomponenten.



Identity & Access Management. Essentieel voor security én medewerkers-tevredenheid

Identity en Access Management (IAM) is een raamwerk van beleidsmaatregelen, processen en technologieën dat ervoor zorgt dat de juiste personen op het juiste moment en om de juiste redenen toegang hebben tot de juiste middelen. Dat klinkt als een technisch feestje, maar in de krappe arbeidsmarkt van vandaag de dag brengt IAM je nog veel meer voordelen.

Minder risico op ongeautoriseerde toegang

Het applicatielandschap in veel organisaties is behoorlijk complex. Systemen die – nog – niet met elkaar zijn geïntegreerd zorgen voor een veelheid aan gebruikersnamen en wachtwoorden. Dat brengt allerlei risico’s met zich mee. Identity en Access Management (IAM) kan organisaties helpen te voldoen aan wet- en regelgeving en beveiligingsnormen door een gecentraliseerde, consistente aanpak voor het beheren van identiteiten en toegangsrechten over verschillende toepassingen en systemen. Zo verminder je het risico op ongeautoriseerde toegang of gegevensinbreuken.

80%

van de IT-beslissers heeft al cloud gebaseerde Identity & Access Management oplossingen geadopteerd, of is van plan om dit in de komende twee jaar te doen. (Forrester)

Hogere medewerkerstevredenheid

Dat klinkt in eerste instantie misschien als een technisch ‘feestje’, maar vergis je niet. Vandaag de dag is het enorm moeilijk om talent te vinden – en te behouden. Dat maakt dat er steeds meer aandacht is voor het indiensttredingsproces. Een vlekkeloos Joiners-Movers-Leavers-proces kan helpen frustraties te voorkomen en je talent binnen te houden. Door goed grip te hebben op dit proces kun je medewerkers, al in de kritische fase waarin ze nog niet die loyaliteit voelen, het gevoel geven dat ze belangrijk zijn. Zo blijkt maar weer dat iets technocratisch als het verlenen van rechten ook enorm belangrijk kan zijn voor de medewerker-stevredenheid.

Evolutie van IAM binnen organisaties

On-premise accounts

Op het basisniveau bevinden de accounts van je medewerkers zich in het eigen – on premise – datacenter, meestal via Microsoft Active Directory (AD).

SSO in de cloud

Zodra een organisatie overstapt naar de cloud, bijvoorbeeld naar Microsoft 365, moeten de identiteiten en accounts worden gesynchroniseerd naar een andere identiteitendirectory genaamd Azure AD, de cloudvariant van het klassieke AD. Op Azure AD kunnen andere applicaties worden gekoppeld, waardoor Single Sign-On (SSO) mogelijk is. Bijvoorbeeld voor Salesforce of AFAS voor HR, die ook als SaaS-dienst in de cloud draaien. Door deze koppeling hoeven medewerkers niet steeds opnieuw in te loggen, en wordt authenticatie uitbesteed aan Azure AD, de zogenaamde federated identity. Het opzetten van zo'n SSO-koppeling is een vrij ingewikkeld traject, vooral als een organisatie veel applicaties heeft, in zowel de cloud als in het eigen datacenter. Om tot een bepaald volwassenheidsniveau te komen, moeten alle applicaties zijn gekoppeld aan Azure AD.

Centraal beheer

Daarna komt het volgende volwassenheidsniveau. Daarbij gaat het niet alleen over de identiteit van de gebruiker, maar ook over de rechten die een gebruiker heeft binnen verschillende applicaties. Een identiteit gaat over het bewijzen van wie je bent, terwijl access rights gaan over wat je mag doen binnen een applicatie. Zo kan een HR-medewerker bijvoorbeeld toegang hebben tot alle HR-gegevens, terwijl 'gewone' medewerkers alleen hun eigen gegevens kunnen inzien. Op dit allerhoogste niveau van IAM is het mogelijk om vanuit een centrale plek alle rechten te beheren. Op lagere niveaus gebeurt dit vaak nog handmatig door functioneel beheerders.

Role Based Access Control

Er zijn maar weinig organisaties die al op dat hoogste niveau zijn. En zelfs op het hoogste niveau zijn er nog wel eens legacy-applicaties waar handmatig rechten aan moeten worden toegewezen. Het ideaal is om op basis van functieomschrijving, afdeling en manager rechten toe te wijzen, ook wel bekend als Role Based Access Control (RBAC). Op basis van de rol van de medewerker worden specifieke rechten toegekend, zoals het al dan niet kunnen bekijken of betalen van binnenkomende facturen in de boekhouding. Zodra bijvoorbeeld een HR-manager naar een andere afdeling verhuist, verliest hij automatisch de rechten om HR-gegevens in te zien. De nieuwe HR-manager krijgt automatisch die rechten toebedeeld. Het goed opzetten van IAM zorgt voor een vloeiend Joiners-Movers-Leavers-proces. Zo neem je frictie weg voor medewerkers en zorg je ervoor dat ze snel productief kunnen zijn, terwijl je als organisatie volledig voldoet aan wet- en regelgeving en voorkomt dat medewerkers te veel rechten krijgen.

De beveiligingsrisico's van hybride werken

Hybride werken is uitgegroeid tot het nieuwe normaal. Naast dat het voor zowel organisaties als werknemers tal van voordelen biedt wat betreft flexibiliteit en gemak, zorgt het ook voor terechte bezorgdheid met het oog op cyberdreigingen en beveiligingsrisico´s.

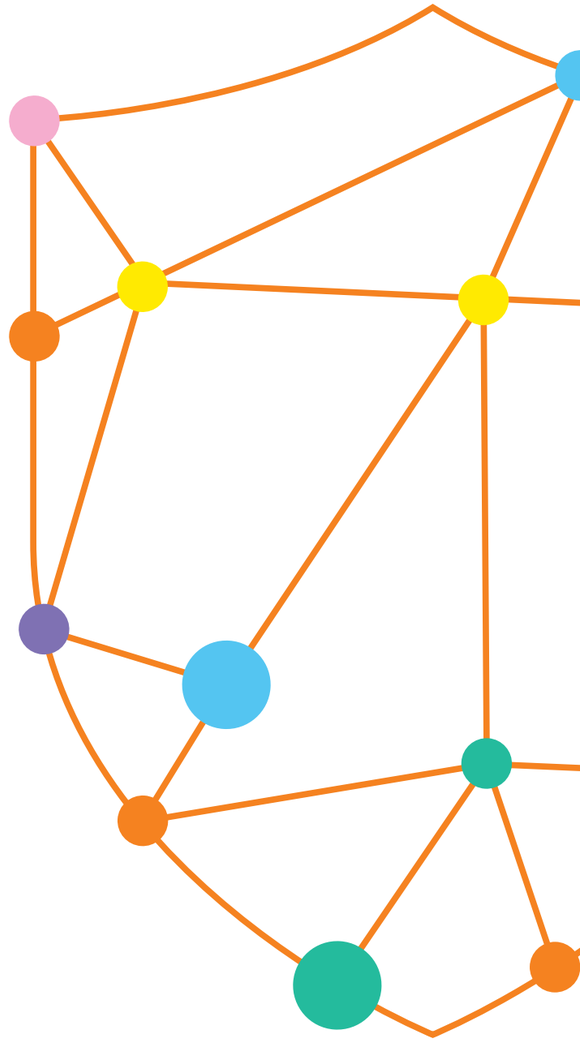
Nu medewerkers vaker dan ooit van omgeving veranderen, kan het managen van de veiligheid een complexe opgave zijn. Traditionele maatregelen, gebaseerd op het beveiligen van apparaten binnen het kantoor die zijn aangesloten op het bedrijfsnetwerk, voldoen inmiddels niet meer. Omdat steeds vaker op afstand wordt gewerkt zijn de methoden en maatregelen voor informatiebeveiliging complexer geworden.

Hybride werken bezorgt veel IT´ers dan ook de nodige kopzorgen, maar met behulp van moderne digitale werkplektechnologieën en aandacht voor het menselijk gedrag kan aan alle uitdagingen worden voldaan.

Endpointbeveiliging is cruciaal

Omdat het endpoint dé cruciale schakel is in de automatiseringsketen, moet beveiliging hiervan voor elke organisatie prioriteit nummer één zijn. Endpoints zijn een belangrijke schakel binnen het systeem waar menselijk gedrag een belangrijke impact op heeft, mede omdat hier ook buiten het bedrijfsnetwerk gebruik van wordt gemaakt. Dat betekent dat menselijke fouten zoals per ongeluk op verdachte links klikken of software met kwetsbaarheden downloaden vaak de oorzaak zijn van een beveiligingslek.

Volgens Verizon (2023 Data Breach Investigation Report) was in 2022 de menselijke factor verantwoordelijk voor 78 procent van alle lekken. Of het nu gaat om het gebruik van gestolen inloggegevens, phishing, misbruik, of gewoon een fout: de mens blijft een erg grote rol spelen bij het ontstaan van incidenten en lekken.



Het risico beheersen

Om hun organisatie te beveiligen moeten IT-teams door middel van een holistische aanpak de risico's voor endpointbeveiliging verlagen die samenhangen met werken op afstand. Bij het opzetten van een passende strategie voor endpointbeveiliging moet rekening worden gehouden met zowel mensen als met technologie.

Endpointbeveiliging

Mensen

Informeer je medewerkers
Medewerkers krijgen steeds vaker te maken met cyberdreigingen. Het is inmiddels heel normaal om dezelfde laptop op verschillende locaties te gebruiken, zoals op kantoor, thuis of onderweg, en dat brengt de nodige uitdagingen voor de veiligheid met zich mee.

Het is van cruciaal belang dat al je medewerkers zich bewust zijn welke risico's ze lopen en weten hoe ze daarmee moeten omgaan. Medewerkers moeten weten hoe ze bedreigingen kunnen herkennen, welke risicobeperkende maatregelen ze moeten toepassen, en hoe ze cyberaanvallen en -dreigingen moeten melden.

Hoewel we nog maar aan het begin staan van cyberbewustzijn, moeten medewerkers zowel in hun werk als privé cyberveilig gedrag omarmen én toepassen. Het doel is om dit bewustzijn verder op te bouwen tot een veiligheidscultuur. Organisaties met een sterke cybersecuritycultuur profiteren van meer inzicht in mogelijke bedreigingen, minder cyberincidenten, en betere veerkracht na een eventuele aanval.

Technologie

Vertrouw op technologie om je te ondersteunen
Het goede nieuws is dat er beveiligingsoplossingen bestaan die alle gebruikers beveiliging kunnen bieden voor hun specifieke niveau binnen de organisatie. Om de beste resultaten te bereiken maken deze systemen gebruik van geavanceerde beveiligingstechnologieën.

Endpoint Protection Platforms, oftewel EPP's, maken gebruik van geïntegreerde toegangspunttechnologieën voor het detecteren en voorkomen van verdachte activiteit op het endpoint. Een EPP controleert elk bestand dat het systeem binnenkomt op kwaadaardige kenmerken.

Endpoint Detection and Response, ook bekend als EDR, vormt een aanvulling op het basale EPP. Dit systeem detecteert potentiële risico's en triggert een geautomatiseerde respons. Dankzij krachtige functionaliteiten kan EDR-dreigingen van een hoog niveau onschadelijk maken, zoals zero-day exploits en fileless threats.

Zoals de naam al aangeeft reikt **XDR** (Extended Detection and Response) verder dan normale EDR. XDR verzamelt en combineert enorme hoeveelheden data van talloze netwerktoegangspunten om bedreigingen beter te detecteren en te voorkomen. Vergeleken met EDR biedt deze technologie bredere bescherming en complexere features.

Zero trust als antwoord op digitale complexiteit en constante dreigingen

Zero Trust is een cybersecuritybenadering die draait om het idee dat organisaties niet automatisch vertrouwen mogen toekennen aan gebruikers, apparaten, applicaties of systemen, zelfs niet als ze zich binnen het interne netwerk bevinden. In plaats daarvan gaat Zero Trust ervan uit dat er altijd sprake kan zijn van dreigingen, zowel van interne als externe bronnen, en stelt het veiligheidsmaatregelen voor die gericht zijn op continue verificatie en beperking van toegang, ongeacht de locatie van de gebruiker of het apparaat.

Microsoft heeft drie kernprincipes gedefinieerd voor zero trust beveiliging.

- Uitdrukkelijk verifiëren: benadrukt de noodzaak om gebruikers en apparaten expliciet te identificeren en verifiëren, in plaats van automatische toegang te verlenen.
- Gebruik toegang met minimale machtigingen: beperkt privileges tot het strikt noodzakelijke, waardoor potentiële aanvalspunten worden verminderd.
- Ga uit van een lek: erkent de realiteit van aanvallen en lekken en moedigt aan tot strategieën die de impact minimaliseren en kwetsbare systemen beschermen.

Hoewel er duidelijke voordelen verbonden zijn aan hybride werken, mag dit niet ten koste gaan van de veiligheid. Moderne bedrijven moeten daarom hun medewerkers voorlichten op het gebied van cybersecurity en kiezen voor het juiste beveiligingstechnologieniveau om hen te ondersteunen.

Self-service support. Wat, hoe en waarom?

Of je nu vooroploopt in de digitalisering of niet zo'n fan bent van technologie, we hebben allemaal weleens met een helpdesk gebeld. Die ervaringen zijn niet onverdeeld positief, zullen we maar zeggen. Gelukkig verandert ook de wereld van IT-support.

Self-service support, wat is het?

Als je hulp nodig hebt met een computer, printer, een ander device of een digitale dienst, bel je in de klassieke situatie naar de helpdesk. Bij self-service support zijn er meerdere manieren waarop een medewerker ondersteuning kan krijgen. Eén zo'n methode is bijvoorbeeld het self-service portaal om een wachtwoord te resetten. Dat kennen we allemaal wel, al was het maar van online webshops als Bol.com of Coolblue. Maar het is ook mogelijk om medewerkers zelf de status van hun ticket op te laten vragen of een workflow te laten doorlopen als ze een applicatie nodig hebben of toegang willen tot een bepaalde gegevensbron. Self-service support bij een IT-helpdesk geeft medewerkers de mogelijkheid om problemen en issues op te lossen en ondersteuning te krijgen zonder tussenkomst van een helpdesk-medewerker.

Zo veel mensen, zo veel voorkeuren

Medewerkers hebben verschillende voorkeuren als het gaat om communicatie en ondersteuning. De één wil een persoon van vlees en bloed spreken – telefonisch of misschien zelfs in levenden lijve – die je aan de denkbeeldige hand door het hele proces begeleidt. Dat gaat dan vooral om medewerkers die wat hulp nodig hebben met het stellen van de juiste vraag. Medewerkers die al wat meer digitaal onderlegd zijn en weten hoe ze hun vraag kunnen formuleren, kunnen vaak prima uit de voeten met self-service support. Denk daarbij aan een self-service portaal met geautomatiseerde workflow, een chatbot of een persoonlijke assistent à la Siri of Alexa.

Steeds meer geïntegreerd

In steeds meer apps en diensten zijn self-service opties geïntegreerd. Als je een aantal jaar geleden een document of folder benaderde waar je geen toegang toe had, kreeg je de melding: Je hebt geen toegang. Dan moest je de helpdesk bellen, uitleggen om welke data het ging. Vervolgens moest de helpdesk achterhalen wie de eigenaar van die gegevens was, toestemming vragen en de aanvrager toegang geven. Vandaag de dag is de mogelijkheid om rechten aan te vragen geïntegreerd in veel oplossingen, zoals bijvoorbeeld Microsoft 365. Naast de melding dat je geen toegang hebt, wordt direct de mogelijkheid geboden om toegang aan te vragen en met een druk op de knop komt de aanvraag direct bij de juiste persoon, die vervolgens ook met een druk op de knop de aanvrager toegang kan geven – of niet.

Self-service centraal toepassen binnen je organisatie

Wil je binnen je organisatie self-service centraal inzetten, dan is het noodzakelijk om alle functies van alle verschillende diensten, zoals bijvoorbeeld Microsoft 365, de digitale werkomgeving en de belangrijkste zakelijke applicaties op een slimme manier te bundelen. De meeste vergaande vorm hierbij is multichannel. Daarbij geef je medewerkers toegang tot verschillende kanalen om tot een antwoord te komen. Dat kunnen vooruitstrevende oplossingen, zoals AI-chatbots en een online assistent zijn, maar natuurlijk ook nog klassiekere middelen zoals een self-service portaal of een helpdeskmedewerker.

Als je deze kanalen dan ook nog eens naadloos met elkaar integreert, krijg je een uniforme en consistente medewerkerservaring en kan iedere medewerker kiezen voor het kanaal wat het beste aansluit bij de persoonlijke behoefte.

Voordelen van een centrale aanpak

De voordelen van een centrale, multichannel self-service aanpak zijn talrijk. Zo kun je een medewerker sneller helpen via een kanaal naar keuze, wat weer een positieve bijdrage levert aan de medewerkerservaring. Daarnaast vermindert het de druk op de helpdesk en kun je deze dus runnen met minder mensen.

Waar moet je voor waken?

Er zijn ook zeker dingen waar je voor moet waken als je met self-service support aan de slag gaat. Dat heb ik laatst zelf ervaren. Op mijn toetsenbord ontbrak een toets. Een relatief eenvoudig probleem, zou je denken. Een helpdeskmedewerker had me direct begrepen, daar durf ik heel wat onder te verwedden. Maar de self-service portal begreep mijn probleem niet. Ik kreeg het advies om telefonisch contact op te nemen. Dat wilde ik best doen, ware het niet dat ik een menuutje kreeg waar ik me doorheen moest worstelen. Ik nam allerlei afslagen en kreeg talloze opties, maar 'toets ontbreekt' zat er niet bij. Uiteindelijk kreeg ik een medewerker aan de lijn, alleen van de verkeerde afdeling. Het is goed gekomen, maar het geeft wel aan dat het persoonlijke contact verloren kan gaan. Zeker mensen die het moeilijk vinden om de juiste vraag te formuleren, kunnen de weg kwijtraken. Of stel dat het om een complexer probleem gaat. Een scherm dat de ene keer wel knippert en de andere keer niet, hoe moet je dat uitleggen aan een systeem. Dan is het nog steeds fijn als iemand je te woord kan staan.

Device-as-a-Service:
De toekomst van efficiënt hardwarebeheer?

Vandaag de dag hebben medewerkers op z'n minst één apparaat nodig om hun werk te kunnen doen. Dat kan een laptop zijn, maar ook een tablet of een smartphone. Het aanschaffen, beheren en onderhouden van deze apparaten kan een tijdrovend en complex logistiek proces zijn voor organisaties.

Hardware zelf aanschaffen is een fikse logistieke uitdaging

Vrijwel elke medewerker heeft een apparaat nodig om te kunnen werken. Vaak is dat een laptop, maar er zijn ook veel medewerkers die afhankelijk zijn van een tablet of smartphone. Denk aan zorgmedewerkers, kantoormedewerkers, politieagenten, of mensen in de buitendienst van een bedrijf. Natuurlijk kun je deze devices als organisatie zelf allemaal aanschaffen en beheren. Google 'computer kopen' en je krijgt zo'n 28 miljoen resultaten. Leveranciers als HP of Dell, maar ook de Coolblue's, Bol.coms en Amazons van deze wereld ontvangen zakelijke klanten met open armen. Maar het zelf aanschaffen en beheren van alle devices brengt voor een organisatie wel een fikse logistieke uitdaging met zich mee. Van aanschaf tot levering en van installatie tot afvoer, er is altijd wel wat te regelen. En is het apparaat stuk of heeft het een storing? Dan ben je afhankelijk van de servicedesk van je leverancier en zul je af moeten wachten tot er iemand langskomt. In de tussentijd zit je medewerker duimen te draaien. Het is dan ook niet verrassend dat Device-as-a-Service (DaaS) steeds populairder wordt.

Device-as-a-Service

Device-as-a-Service is een oplossing voor het beheren van de complete hardware-cyclus binnen een organisatie. Door je hardware als een dienst af te nemen, zorgt je IT-partner voor de aanschaf, levering, onderhoud en uiteindelijk het milieuvriendelijk verwerken van de hardware, inclusief het veilig verwijderen van data. Dit maakt het hele proces efficiënter, veiliger en kosteneffectief.

DaaS van Orange Business

Als je kies voor Device-as-a-Service van Orange Business, ontzorgen we je over de hele keten. Een nieuwe medewerker in dienst? Wij leveren de laptop op het huisadres af, de medewerker pakt de laptop uit, logt in en het systeem wordt helemaal volgens jouw IT-beleid ingericht. En dat voor een vaste prijs per maand per medewerker. Hoe transparant en flexibel wil je het hebben? Bovendien kun je in je duurzaamheidsverslag precies laten zien hoe groen je – op hardware-gebied – bent. Voor elk afgevoerd apparaat krijg je een certificaat dat het milieuvriendelijk is verwerkt. Ook kun je voldoen aan alle wet- en regelgeving op het vlak van security. Met een certificaat kun je aantonen dat alle data veilig van het apparaat is verwijderd. Zo loop je nooit het risico dat er ineens ergens data tevoorschijn komt waar je het niet had verwacht.

De 5 grootste voordelen van DaaS

Ontzorging
Als je DaaS onderbrengt bij de juiste partner, neemt deze de volledige verantwoordelijkheid voor het beheren van de hardware-cyclus van je over. Werkt iets niet, dan krijg je een vervangend apparaat zodat je in ieder geval door kunt werken. Zo neemt de druk op je servicedesk af en kunnen jouw medewerkers zich concentreren op hun kernactiviteiten.

Flexibiliteit
Je kunt zelf kiezen welke apparaten je beschikbaar stelt voor je medewerkers. Wil je dat medewerkers helemaal zelf een apparaat kunnen kiezen via een online portal, of wil je dat ze op basis van hun persona, bepaalde apparaten voorgeschoteld krijgen?

Soepele start
Door te kiezen voor DaaS, kun je er ook voor kiezen dat nieuwe medewerkers hun apparaten thuis geleverd krijgen, compleet met een welkomstbericht en instructies voor gebruik. Dit zorgt voor een soepele start en draagt bij aan de medewerkerstevredenheid. Immers: hoe welkom voel je je als je ergens binnenkomt en er is niets geregeld? Geen slimme zet in de huidige krappe arbeidsmarkt.

Duurzaamheid
Een goede DaaS-partner zorgt voor milieuvriendelijke verwerking van afgedankte apparaten en voorziet je van certificaten die aantonen dat de hardware op een verantwoorde manier is afgevoerd.

Veiligheid
DaaS garandeert dat alle data van afgeschreven apparaten wordt verwijderd, waardoor het risico op datalekken wordt verminderd. Vervolgens kun je de devices laten afvoeren, opnieuw in gebruik nemen, maar je kunt er ook voor kiezen om ze – helemaal opgeschoond en wel – te doneren aan een goed doel.

Endpoint management is het proces van het beheren en beveiligen van apparaten, zoals desktops, laptops en andere mobiele apparaten, binnen een bedrijfsnetwerk.

Van bedreiging naar bescherming: waarom endpoint management essentieel is voor jouw organisatie

Endpoint management is de onmisbare hoeksteen in jouw organisatie als je in controle wilt zijn over je (gevoelige) data.

Waarom endpoint management?

Het doel van endpoint management is ervoor te zorgen dat alle endpoints, hun besturingssystemen en de applicaties die erop draaien, goed geconfigureerd zijn en voorzien zijn van de laatste beveiligingspatches en beleidsmaatregelen. Het geeft je als organisaties controle over je apparaten, zodat je je ervan kunt verzekeren dat ze veilig en compliant zijn. Zo kun je bijvoorbeeld op afstand een laptop wissen als deze gestolen wordt en ervoor zorgen dat de dief geen toegang heeft tot het systeem en de data. Daarnaast geeft het je inzicht welke software op welke apparaten draait en of er updates nodig zijn. Met endpoint management kunnen organisaties in controle zijn over hun apparaten en applicaties.

TikTok van telefoons ambtenaren

Eind maart riep het kabinet ambtenaren op om apps als TikTok van hun werktelefoon te verwijderen. Het is op zich al opmerkelijk dat overheidspersoneel überhaupt een dergelijke app kan installeren, maar vervolgens vertrouwen ze blijkbaar ook nog eens op de bereidwilligheid van hun ambtenaren om ongeoorloofde apps te verwijderen. Met endpoint management kun je dit soort situaties voorkomen en zorgen dat ongewenste applicaties niet geïnstalleerd kunnen worden of dat ze zijn afgescheiden van de zakelijke gegevens op het apparaat.

In controle, ook buiten het kantoor

Een belangrijk voordeel van endpoint management is de controle die het je geeft over de apparaten en applicaties van je medewerkers. Zo kun je compliancy en beveiliging waarborgen. Een ander voordeel is dat endpoint management ook kan worden toegepast op apparaten die buiten het kantoornetwerk worden gebruikt, wat voorheen heel ingewikkeld was. Moderne oplossingen als Microsoft Intune zijn toegankelijk via het internet hiermee kun je apparaten van over de hele wereld bereiken, beheren en updaten.

Trends en ontwikkelingen

Endpoint management is voortdurend in ontwikkeling. Zo worden er steeds betere toolsets ontwikkeld en wordt er meer en meer aandacht besteed aan de beveiliging van endpoints buiten het kantoornetwerk. Een nieuwe trend is de focus op de eindgebruiker en het creëren van een goede gebruikerservaring, terwijl de veiligheid van de endpoints gewaarborgd blijft.

Maken je medewerkers zich zorgen over de privacy van hun persoonlijke gegevens op hun zakelijk beheerde apparaten? Je kunt de privégegevens afschermen, terwijl je toch ‘in control’ blijft over de endpoints.

De evolutie van de werkplek user interface

In het snel evoluerende digitale landschap van vandaag kan de toegevoegde waarde van user interfaces (UI) van de digitale werkplek niet genoeg worden benadrukt. Deze interface is de brug tussen menselijke interactie en technologie. Van het Windows startmenu - wat met Windows 95 werd geïntroduceerd - tot de geavanceerde wereld van aanpasbare portalen van vandaag, het UI-ontwerp bepaalt hoe wij toegang krijgen tot onze data en applicaties.

Device-gebaseerde menustructuren en gebruikersprofielen

Het hart van veel besturingssystemen wordt gevormd door de device-gebaseerde menustructuur, geïllustreerd door het iconische Windows startmenu. Deze structuur geeft de gebruikers toegang tot applicaties, instellingen en bestanden. Daarnaast zorgen gebruikersprofielen, beheerd via group policies, voor een mechanisme om persoonlijke instellingen en toegangsrechten te behouden over netwerken of domeinen. In zakelijke omgevingen waarborgt deze aanpak uniformiteit, security en het bevordert efficiënt IT-beheer.

UEM/MDM-oplossingen voor beheer van gebruikersprofielen

In het domein van gebruikers-profielbeheer zijn Unified Endpoint Management (UEM) en Mobile Device Management (MDM) de belangrijkste ontwikkelingen. Deze oplossingen stellen beheerders in staat om gebruikersprofielconfiguraties te stroomlijnen, wat de handhaving van beveiligingsbeleid, applicatiedistributie en beheer op afstand van apparaten vergemakkelijkt. Hierdoor kunnen organisaties consistentie bevorderen over verschillende apparaten en hebben ze meer flexibiliteit in het beheren van gebruikersprofielen en menustructuren, wat de eindgebruiker een betere ervaring biedt.

Aanpasbare werkplekportalen

Een recente innovatie die prominent in beeld is gekomen, is het concept van aanpasbare werkplekportalen. Deze portalen fungeren als één centrale hub voor toegang tot applicaties en gegevens op verschillende soorten apparaten (zoals laptops, desktops of mobiele telefoons) en verschillende platformen (zoals Windows of macOS). De werkplekportalen bieden een uniforme ervaring die is afgestemd op de rol van de gebruiker en zijn persoonlijke voorkeuren. Gebruikers kunnen elementen binnen de omgeving rangschikken en organiseren wat bijdraagt aan een efficiëntere digitale werkplek en aan een hogere medewerkers tevredenheid over de digitale werkplek.

Apps met low code en directe toegang tot functies

In de zoektocht naar het verbeteren van de gebruikerservaring heeft de integratie van apps met low code zich geprofileerd als een gamechanger. Deze apps bieden gebruikers directe toegang tot vaak gebruikte functies en gegevens binnen de digitale werkomgeving tegen lage ontwikkelkosten. Met minimale programmeervereisten kunnen gebruikers op maat gemaakte oplossingen creëren om specifieke behoeften aan te pakken, wat zelfredzaamheid en snelle innovatie bevordert, zoals een geautomatiseerd proces voor onboarding van werknemers of een portaal voor samenwerking met leveranciers.

De evolutie van de gebruikersinterface voor de digitale werkplek weerspiegelt onze voortdurende zoektocht naar intuïtievere en efficiëntere interacties met technologie. Van de traditionele device-gebaseerde menustructuren die worden beheerd via groepsbeleid of UEM/MDM-oplossingen tot de introductie van aanpasbare werkplekportalen en de integratie van apps met minimale code. Elke ontwikkeling betekent een sprong naar verbeterde gebruikerservaring en productiviteit. Terwijl technologie blijft evolueren, blijft UI-ontwerp een sleutelfactor in het vormgeven van de toekomst van de digitale werkplek. Het streven blijft om medewerkers een intuïtieve, efficiënte en zelf aanpasbaar toegang tot applicatie, informatie en werkprocessen te geven zodat zij hun werk optimaal kunnen verrichten met een hoge tevredenheid.

Dit is hoe je legacy-applicaties integreert in je SaaS-landschap

Het beheer en onderhoud van legacy-applicaties is vaak tijdrovend en kostbaar. Het liefst wil je er dan ook zo snel mogelijk vanaf, maar meestal is afscheid nemen van deze applicaties niet zo maar mogelijk.

Legacy-applicaties, wat zijn het?

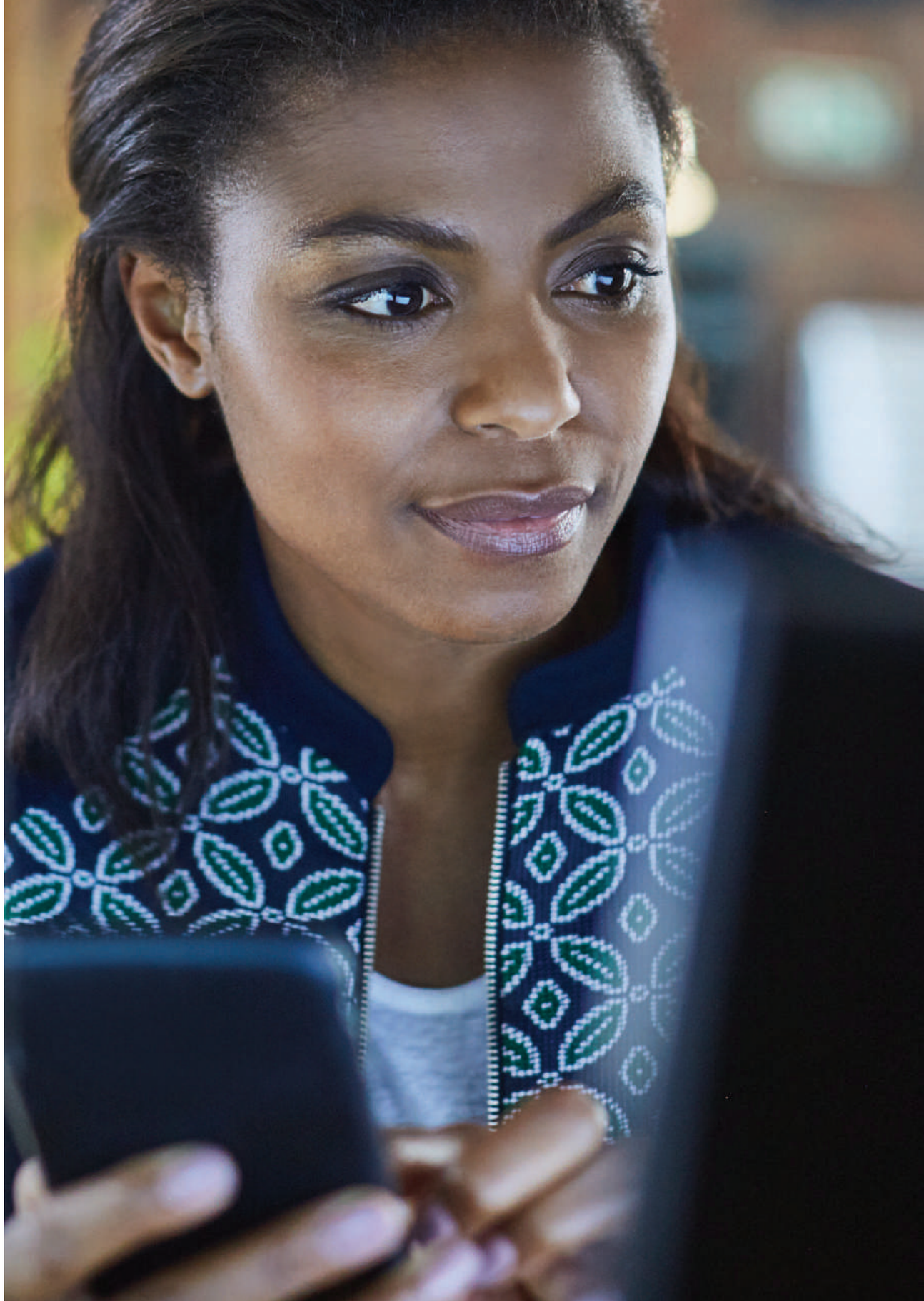
Legacy-applicaties zijn oude Windows-applicaties die nog steeds in gebruik zijn binnen een organisatie. Vaak zijn ze in het verleden ontwikkeld en is het niet eenvoudig om ze te vervangen of te upgraden. Het is nu eenmaal zo dat niet elke applicatie kan worden vervangen door een SaaS-oplossing. Legacy-applicaties worden vaak gezien als verouderd en zijn mogelijk niet compatibel met nieuwe systemen of technologieën. Vaak zijn ze geschreven in achterhaalde programmeertalen en kunnen ze voor beveiligings- en prestatieproblemen zorgen. Het beheer en onderhoud van legacy-applicaties kan tijdrovend en kostbaar zijn, maar organisaties kunnen er toch voor kiezen om ze te blijven gebruiken vanwege hun historische waarde of omdat specifieke bedrijfsprocessen er afhankelijk van zijn. Vooral grote organisaties kampen nog met legacy-applicaties.

Centraal onderhoud via Azure Virtual Desktop, Citrix of VMware

Het beheer en onderhoud van legacy-applicaties kan een fikse uitdaging vormen. Om ze te onderhouden heb je de juiste tools nodig en ook om ‘future-proof’ te zijn moet je passende middelen hebben. Binnen de meeste organisaties bestaan legacy- en SaaS-applicaties naast elkaar, wat het voor medewerkers lastig kan maken om bij te houden waar een applicatie vandaan komt. Dankzij oplossingen zoals Azure Virtual Desktop, Citrix of VMware kun je applicaties toch op een geïntegreerde en toegankelijke manier aanbieden, zonder dat deze op de lokale laptop hoeven te worden geïnstalleerd. Dit betekent in ieder geval dat er maar één centraal punt is waar onderhoud moet worden gepleegd. Met elke legacy-applicatie waarvan je afscheid neemt, kun je de Azure Virtual Desktop, Citrix of VMware oplossing afschalen. Met name in de zorg gebeurt dit veel. Daar wordt met tientallen applicaties gewerkt, die een voor een vervangen kunnen worden door een cloudoplossing.

SaaS-only

De meeste organisaties hanteren tegenwoordig een SaaS-only strategie. Hoewel dit ideaal zou zijn, is het voor veel bedrijven nog niet haalbaar. Het is zeker goed om SaaS-only na te streven, maar het tempo waarin je dit kunt bereiken zal behoorlijk verschillen en hangt af van de exacte situatie.



Samenwerken en data delen, de voordelen van de cloud

De meeste organisaties gebruiken Microsoft 365 als hun digitale werkomgeving voor kantoortoepassingen. Daarin werken medewerkers niet alleen samen, er wordt ook een heleboel data verzameld. De manier waarop je daarmee omgaat, is afhankelijk van het volwassenheidsniveau waarin je organisatie zich bevindt.

Data in eigen datacenter

In traditionele werkomgevingen wordt data opgeslagen op eigen systemen, servers, mailboxen en fileshares, en wordt deze ontsloten via persoonlijke schijven en groepsshares. Om toegang te krijgen tot deze data, moet je toegang hebben tot het datacenter. Sommige organisaties stellen nog steeds als voorwaarde dat medewerkers op de locatie moeten zijn of eerst een VPN-verbinding moeten openen voordat ze toegang krijgen. Het is echter ook mogelijk om op afstand bij deze data te komen, bijvoorbeeld via een remote desktop.

Data in de cloud

Op het moment dat organisaties de data niet alleen binnen hun eigen netwerk ontsluiten, maar ook via de cloud, kan er ofwel een koppeling worden gelegd met de cloud, ofwel kan de data worden overgebracht naar de cloud. Dit geldt ook voor mail, dat er een koppeling kan worden gelegd tussen de mailsystemen in het eigen datacenter en de clouddienst, of de hele afhandeling naar de cloud kan worden verplaatst. Als je ervoor kiest alles naar de cloud te verplaatsen, hoef je minder te beheren en hoef je geen hardware aan te schaffen. Tegelijkertijd kun je profiteren van de optimalere samenwerkingsmogelijkheden en betere beschikbaarheid. Immers, de cloud is 24/7 bereikbaar, waar je medewerkers ook zijn.

Samenwerken in de cloud

Het vervangen van fileshares naar een cloudoplossing is iets uitdagender, omdat dit veranderingen met zich meebrengt in de manier van werken. Immers, als je gegevens op een fileshare staan, kun je niet – of in ieder geval niet eenvoudig – samenwerken in documenten. Als de data wordt verplaatst naar SharePoint Online, OneDrive for Business of Teams, kunnen medewerkers wel eenvoudig samenwerken met collega's, documenten delen en gebruikmaken van geavanceerdere collaboratiemogelijkheden zoals de mogelijkheid tegelijkertijd in een document te werken of in een Loop object (een samenwerkingsobject dat in meerdere documenten en applicaties aanwezig kan zijn). Dit soort mogelijkheden heb je alleen als je naar de cloud verhuist.

Moderne cloudwerkplek

De voordelen van een cloud-werkplek zijn onder andere betere samenwerkingsmogelijkheden, meer beschikbaarheid, betere toegankelijkheid en minder beheer. Een – tijdelijk – nadeel kan zijn dat het een verandering met zich meebrengt in de manier van werken. Alleen als je medewerkers de tools omarmen, wordt digitalisering een succes. Vergeet dus niet te investeren in een goed adoptieproces.

47%

van de organisaties geeft aan dat een gebrek aan digitale vaaardigheden een belangrijk obstakel is voor succesvolle digitale transformatie. (IDC)

Zonder adoptie geen succesvolle digitalisering

Ongeacht de branche waar je in werkt, digitalisering is niet meer te stoppen. Maar om daadwerkelijk het beste uit technologie te halen, moet je wel actie ondernemen. Alleen als je medewerkers de tools omarmen, wordt digitalisering een succes.

Medewerkers toerusten

Bij adoptie gaat het om de vraag hoe je medewerkers toerust in de omgang met digitale middelen. Het is niet genoeg om die digitale tools te introduceren en te denken dat alles vanzelf gaat. Je moet ook je medewerkers trainen zodat ze weten hoe ze ermee moeten omgaan. Alleen als ze de tools omarmen en weten hoe ze er waarde uit kunnen halen, wordt digitalisering een succes.

Trends en ontwikkelingen

De medewerker staat steeds vaker centraal. Dat klinkt misschien als een holle frase, maar het is wel wat we in de praktijk zien gebeuren bij organisaties. Vroeger lag de focus heel erg op de technologie. Niet omdat de medewerker niet belangrijk was, maar simpelweg omdat het voor de meeste organisaties heel complex was om de technologie aan de praat te krijgen. Nu de technologie steeds vaker ‘gewoon’ doet wat het moet doen, gaan we ons realiseren dat we er daarmee nog niet zijn. Medewerkers krijgen een tsunami aan informatie over zich heen. Om daar vervolgens waarde uit te halen, daar moet je ze bij helpen. Kijk alleen maar naar de Microsoft 365-suite. Je kunt misschien wel op tien verschillende manieren bij je documenten komen, maar wat is nu de meest optimale manier voor jouw organisatie, jouw team? Daar moet je mensen bij begeleiden.

Persona’s als archetypen

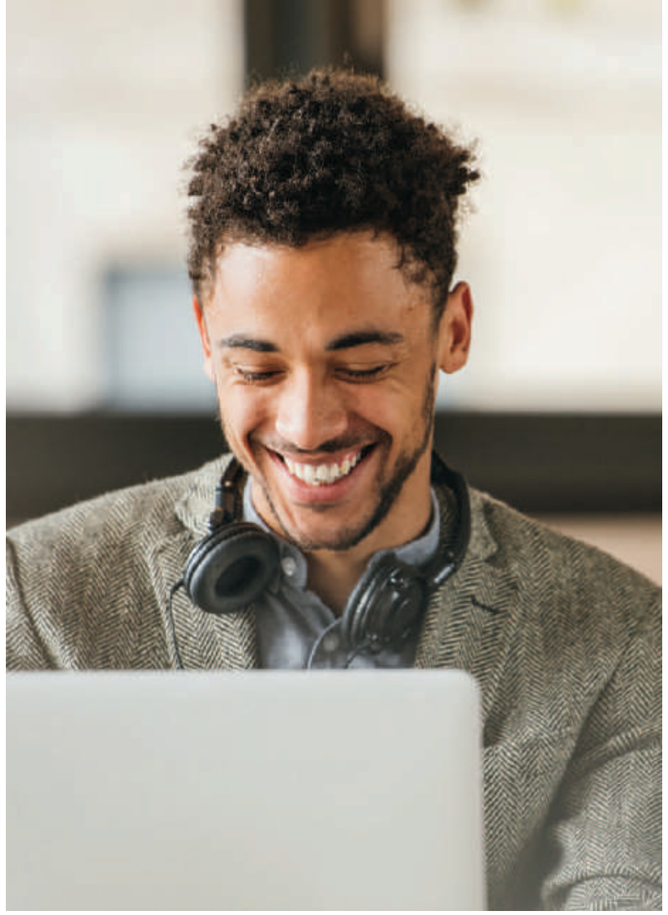
Een logisch gevolg daarvan is dat organisaties het adoptietraject steeds serieuzer gaan nemen. Welke digitale middelen zijn er, welke verschillende groepen medewerkers zijn er en wat hebben zij nodig om de meeste waarde uit die middelen te halen? Het definiëren van persona’s kan daarbij helpen. Zo’n persona kun je zien als een archetype medewerker. In een adoptiecampagne worden die persona’s geïnformeerd over wat voor hen een belangrijke verandering is. Dat kan op de klassieke manier gaan: via het intranet of een old skool flyer op het bureau of via meer moderne middelen, zoals het aanbieden van een instructiefilmpje op het moment dat je voor het eerst een applicatie opstart, of bijvoorbeeld het inzetten van digitale assistenten.

Voorkom een kloof tussen mens en technologie

Door je medewerkers een goed adoptietraject aan te bieden, voorkom je dat er een kloof ontstaat tussen medewerker en technologie. Natuurlijk is er altijd een groep mensen die affiniteit heeft met IT en er zelf wel uitkomt. Maar laat je daar niet door leiden. Het zijn de mensen die die feeling niet hebben, die je een steuntje in de rug moet geven. Doe je dat niet, dan lopen ze een achterstand op en gaan daardoor mogelijk minder arbeidsvreugde beleven. En dat wil je natuurlijk voorkomen.

Gedeelde verantwoordelijkheid

Adoptie is een relatief nieuw fenomeen waar je als organisatie in moet investeren. Hoe sneller de digitalisering gaat, hoe meer je moet nadenken over hoe je écht toegevoegde waarde haalt uit de oplossingen die je aankoopt. Ga je een adoptietraject opzetten? Onthoud dan dat het een gedeelde verantwoordelijkheid is, die op het snijvlak van IT, HR, L&D en Communicatie ligt.



24%

van de werknemers heeft overwogen om hun baan op te zeggen omdat de apps en software die ze gebruiken niet goed aansluiten op hun behoeften. (G2)

Next level employee experience: van DEX tooling tot XLA's

Een positieve employee experience is niet langer een optionele luxe, maar een cruciale factor voor het aantrekken, behouden en motiveren van werknemers.

Employee experience?

Employee experience omvat alle percepties die een medewerker heeft over de interacties met zijn of haar organisatie. Dit omvat niet alleen de relaties met leidinggevenden, collega's en klanten, maar ook de ervaringen met de digitale werkplek. Zeker voor de moderne kenniswerker is de werkplek het startpunt bij het uitvoeren van hun taken.

Een goed ontworpen digitale werkplek draagt dan bij aan hogere productiviteit, een verbeterde werk-privébalans, meer betrokkenheid bij het werk en een gevoel van waardering vanuit de organisatie. Daarentegen kan een negatieve ervaring met de digitale werkplek leiden tot frustratie, verminderde productiviteit en een minder positieve werkomgeving.

Relatie met de digitale werkplek

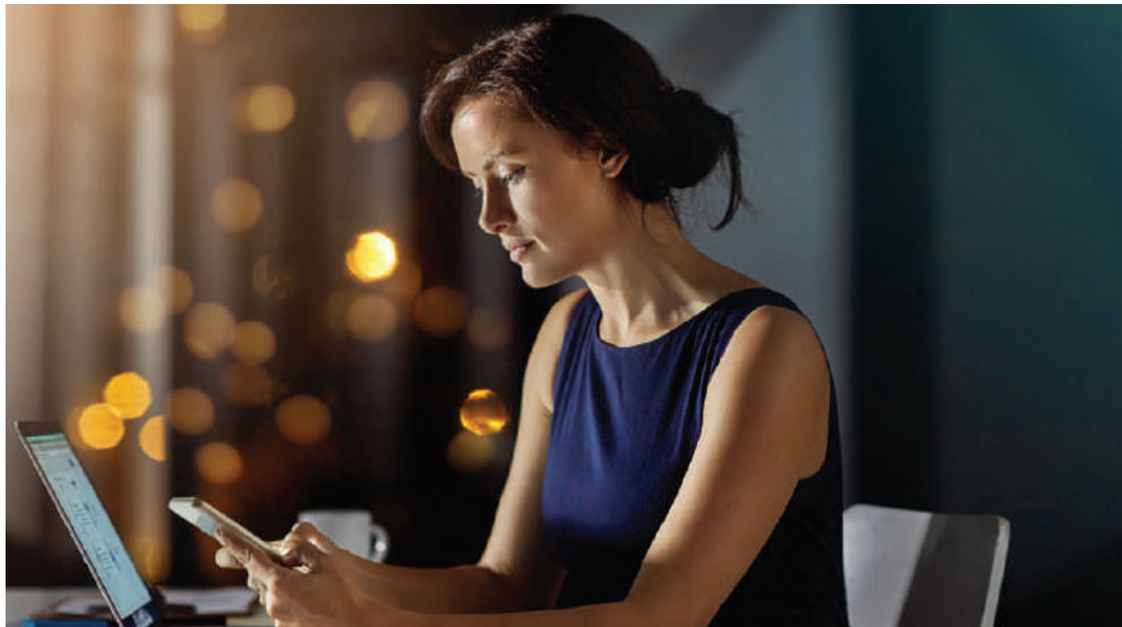
Als we het hebben over de employee experience in relatie tot de digitale werkplek, hebben we het over meer dan alleen de technische aspecten. Natuurlijk is het belangrijk dat applicaties snel opstarten en probleemloos werken, maar beleving gaat over meer dan dat. Het omvat alle aspecten van hoe werknemers de digitale werkplek ervaren, zoals de gebruiksvriendelijkheid van de software, de efficiëntie van de systemen, de toegankelijkheid van informatie en de mogelijkheid om effectief samen te werken met collega's, ongeacht hun fysieke locatie.

Hoe meet je employee experience?

In de krappe arbeidsmarkt van vandaag de dag is een positieve employee experience cruciaal voor het aantrekken én behouden van talent. Om je werknemers tevreden en productief te houden, is het slim om inzicht te hebben in de ervaring met de digitale werkplek, zodat je vanuit IT continu verbeteringen kunt doorvoeren op basis van feedback en behoeften van de medewerker. Dit inzicht kun je op de klassieke manier verkrijgen met een enquête of door middel van het invullen van een korte poll na bijvoorbeeld een helpdeskervaring. Er zijn echter ook tools die feedback kunnen ophalen. Dit wordt ook wel Digital Employee Experience (DEX) management genoemd: het verzamelen van data over hoe de digitale werkomgeving functioneert in een bepaalde context, bijvoorbeeld als een medewerker thuis op een laptop met een ERP-applicatie werkt. Dit kan ook om subjectieve data gaan, bijvoorbeeld in de vorm van sterren of een duimpje omhoog of omlaag. De sterretjes die je kunt toekennen na een Microsoft Teams-meeting, dat is zo'n typisch voorbeeld van het digitaal meten van de employee experience.

Van SLA naar XLA

Digital Employee Experience (DEX) tools geven organisaties de kans om anders te kijken naar hun prestaties op het gebied van IT. Door niet alleen te kijken naar de klassieke KPI's, maar ook subjectieve en objectieve informatie te verzamelen, krijg je een veel beter totaalbeeld. Dat betekent ook dat IT een omslag moet maken in de wijze waarop zij hun producten en diensten leveren: service level agreements (SLA's) zijn niet meer voldoende, experience level agreements (XLA's) moeten de nieuwe standaard worden. Door employee experience-tooling in je dienstverlening te integreren, kun je data ophalen en analyseren. Zo kun je continu je dienstverlening verbeteren en gaan medewerkers hun werkplek steeds beter waarderen.



De Workspace Maturity Index als strategisch hulpmiddel bij innovatie

Op basis van twee decennia aan expertise in digitale werkplekken heeft Orange Business de Workspace Maturity Index ontwikkeld. Deze tool biedt een gestructureerde evaluatie van de huidige staat van de digitale werkplek binnen jouw organisatie door het volwassenheidsniveau van de tien belangrijkste werkplekcomponenten te meten.

De Workspace Maturity Index identificeert sterke punten en zwakke punten, evenals kansen voor groei en ontwikkeling. Het resultaat helpt je om strategische besluiten te nemen en gerichte verbeteringen door te voeren in de reis naar de best passende digitale werkplek, waarmee medewerkers het beste uit zichzelf kunnen halen.

Van A naar Beter: een persoonlijke roadmap voor jouw organisatie

Het gewenste volwassenheidsniveau van de digitale werkplek verschilt per organisatie en per branche. Een financiële instelling stelt ongetwijfeld hogere eisen aan security dan een facilitair dienstverlener. Het gaat niet om goed of fout maar of de werkplek het volwassenheidsniveau heeft wat voor jouw organisatie wenselijk is. De Workspace Maturity Index maakt dit eenvoudig inzichtelijk. Op basis van het verschil tussen de huidige situatie en het gewenste niveau – de ‘gap’ kun je een actieplan opstellen. Dit kun je zelf doen, maar je kunt ook de ondersteuning van onze architecten inschakelen die je helpen om de gap te vertalen naar een roadmap met concrete projecten.

De voordelen van de Workspace Maturity Index

De Workspace Maturity Index biedt waardevolle inzichten voor elke organisatie. Het dient als input voor de roadmap en het budget, omdat je op basis hiervan kunt bepalen wat er nodig is om de digitale werkplek op het gewenste niveau te brengen. Het helpt je bij het stellen van prioriteiten, zodat je je kunt focussen op de juiste zaken. Daarnaast biedt het inzicht in risicomanagement. Als je ziet dat je ergens onder het gewenste niveau zit, loop je risico’s. Met de Workspace Maturity Index kun je die zwakke plekken identificeren. Het stimuleert ook het continu verbeteren van de digitale werkplek. Je kunt meten, evalueren, doelen stellen, actie ondernemen en vervolgens werken aan de volgende stap. Dit is overzichtelijker dan een enorm project zonder einde. Bovendien maakt het voor IT-managers het opstellen van budgetten en het verkrijgen van goedkeuring van het management eenvoudiger.

Meten op vier volwassenheidsniveaus

Weten hoe jouw organisatie scoort op de digitale werkplek?

Ben je benieuwd hoe jouw organisatie scoort op het gebied van de digitale werkplek? Vul dan nu onze Workspace Maturity Index in en ontvang een persoonlijk rapport dat inzicht geeft op welke van de tien onderwerpen je vooroploopt en waar jouw verbeterkansen liggen.

Ben jij klaar voor de volgende stap?

Naar de test >

Orange Business Services B.V.

Radarweg 60
1043 NT Amsterdam
+31 88 594 9000

cloud.orange-business.com/nl

Business