White Paper

10 essentiële elementen voor een strategie voor enterprise mobility

Best practices voor het beschermen van gevoelige bedrijfsgegevens terwijl mensen productief kunnen zijn waar ze ook zijn

CITRIX®

Mobiliteit en BYOD (Bring Your Own Device) veranderen de manier waarop mensen werken en waarop organisaties hen ondersteunen. Bij mobiliteit gaat het om meer dan alleen het beschikbaar maken van toegang op afstand, en mobiele devices kunnen tegenwoordig voor veel meer dan als beperkte gadgets gebruikt worden. Smartphones en tablets zijn geschikt voor het openen, opslaan en verzenden van applicaties en gegevens zoals traditionele computers en kunnen worden gebruikt voor vrijwel elke bedrijfstaak. Om het volledige potentieel van enterprise mobility te ontsluiten, moet IT mensen de vrijheid geven om al hun applicaties en gegevens naadloos en gemakkelijk te benaderen vanaf elk device.

Mobiele devices vragen ook om de juiste aanpak van beveiliging, zodat zakelijke informatie beschermd is, zelfs wanneer die op meerdere plaatsen en vaak via niet-vertrouwde netwerken gebruikt wordt, met kans op verlies of diefstal. IT moet compliancy onderhouden en gevoelige informatie beschermen waar en hoe die ook worden gebruikt en opgeslagen, zelfs wanneer zakelijke en persoonlijke applicaties samengaan op hetzelfde device. Opkomende mobiele trends van draagbare technologieën en “the internet of things” zorgen al voor nieuwe punten ter overweging. Het ontwikkelen van een zeer uitgebreide en beveiligingsbewuste mobiliteits-strategie is nu een topprioriteit voor elke organisatie.

In dit document staan 10 belangrijke punten om te overwegen wanneer u uw enterprise mobility strategie ontwikkelt met daarin beveiliging, gebruikerservaring, IT-werkzaamheden en BYOD. Als de leider in mobile workstyles biedt Citrix een complete oplossing voor beveiligde enterprise mobility, waaronder technologieën voor mobile device management (MDM), mobiel applicatiebeheer (MAM), applicatie- en desktopvirtualisatie, en totale beveiliging van datacenter tot device. Samen helpen deze richtlijnen, best practices en technologieën uw organisatie de volledige voordelen van mobiliteit te realiseren.

1. Beheer en bescherm datgene wat belangrijk is

Wanneer mensen gegevens en applicaties benaderen vanaf meerdere devices, inclusief eigen smartphones en tablets, is het niet meer realistisch voor IT om elk aspect van de omgeving te controleren en te beheren. In plaats daarvan moet u zich richten op wat echt belangrijk is voor uw organisatie en de mobiliteitsbeheermodellen kiezen die het meest zinvol zijn voor uw bedrijf en uw mobiele gebruiksscenario’s. Er zijn vier modellen om uit te kiezen, hetzij afzonderlijk of in combinatie.

Mobile device managment (MDM) – met MDM kunt u mobiele apparatuur die wordt gebruikt voor toegang tot zakelijke middelen beheren en controleren. Voordat een bedrijfs-device of een privé device toegang heeft tot het bedrijfsnetwerk, kunt u controleren of het voldoet aan de laatste beveiligingseisen en niet is aangetast. Encryptie, blokkeren en wissen op afstand, mobiele VPN, blacklists voor apps en de mogelijkheid om device-eigen mogelijkheden uit te schakelen, zorgen voor een hoog niveau van beveiliging.

Mobiele hypervisors en containers – Vooral nuttig ter ondersteuning van BYOD, met dit model kunt u apps, gegevens, beleid en instellingen beheren binnen een container op het device, zonder interactie met alle persoonlijke inhoud ervan. In feite wordt een mobile device twee afzonderlijke virtuele devices: een voor werk en een voor het persoonlijke leven.

Mobiel applicatiebeheer (MAM) – Voortbouwend op de containeraanpak kunt u met MAM voor elke mobiele app het beheer, de beveiliging en controle centraliseren als onderdeel van een container, en hetzelfde doen voor de gegevens en instellingen van de app. Beleid op app-niveau kan verificatie, netwerk, locatie, wachtwoorden en encryptie omvatten.

Applicatie- en desktopvirtualisatie – de inherente beveiliging van virtualisatie geldt ook in mobiele gebruiksscenario's. Bedrijfsapplicaties kunnen worden geoptimaliseerd voor mobiele devices en on-demand worden geleverd terwijl gegevens beschermd blijven in het datacenter.

2. Denken vanuit 'gebruikerservaring'

Mobiele devices zijn een belangrijke impuls voor bedrijfsmatig gebruik van consumentenapparatuur, waarmee er krachtige nieuwe manieren kwamen om te werken met apps en informatie in het privéleven. Daarmee is de inzet verhoogd voor IT, die nu moet zorgen voor een ervaring die gunstig afsteekt bij de vrijheid en het gemak geboden door bedrijven voor consumententechnologie. Het kan nuttig zijn om te informeren of onderzoek te doen naar gebruikersbehoeften en voorkeuren om ervoor te zorgen dat uw mobiliteitsstrategie resulteert in wat gebruikers echt willen.

Zoek, terwijl u werkt aan een optimale gebruikerservaring, naar manieren om mensen meer te geven dan ze verwachten en naar nuttige mogelijkheden waaraan zij misschien nog niet gedacht hebben. Bijvoorbeeld:

- Laat mensen toegang krijgen tot hun applicaties en gegevens op elk device dat ze gebruiken, compleet met hun persoonlijke instellingen, zodat ze direct aan het werk kunnen.
- Geef mensen self-service voorzieningen via een appstore voor de onderneming met enkelvoudige aanmelding voor elke app, gehost, mobiel of SaaS, die ze nodig hebben.
- Zorg voor gedeelde thin clients of andere bedrijfs-devices waarop mensen gemakkelijk kunnen overschakelen als ze bepaalde apps niet kunnen gebruiken op hun consumentendevice vanwege veiligheidseisen.
- Automatiseer controles op het delen en beheren van gegevens, zoals de mogelijkheid om gegevens tussen applicaties te kopiëren, zodat mensen geen specifiek beleid hoeven te onthouden.

- Definieer toegestane device-functies per app zodat mensen nog gebruik kunnen maken van functies zoals afdrukken, camera en lokale dataopslag in bepaalde apps als IT die uit moet schakelen voor andere apps.
- Maak het eenvoudig voor mensen om bestanden te delen en synchroniseren vanaf elk device en om bestanden eenvoudig te delen met externe partijen door het sturen van een link.

Door uw mobiliteitsstrategie in de geest van en samenwerking met gebruikers te ontwikkelen, kunt u beter aan hun behoeften voldoen, terwijl u een waardevolle gelegenheid krijgt om de verwachtingen bij te stellen en te zorgen dat ze de behoeften van IT omtrent compliancy begrijpen, zoals de noodzaak om apps en gegevens te beveiligen, netwerktoegang te controleren en devices naar behoren te beheren.

3. Vermijd de viervoudige bypass

De viervoudige bypass vertegenwoordigt het slechtste scenario voor bedrijfsmobiliteit: een BYOD-gebruiker op een consumenten-device die gevoelige bedrijfsgegevens gebruikt en direct naar de cloud gaat. Deze aanpak omzeilt volledig de controle en zichtbaarheid voor IT en het is schrikbarend gebruikelijk in moderne organisaties. Daar zijn natuurlijk goede redenen voor. Cloud apps kunnen mensen helpen tijd te besparen en hun werk gemakkelijk gedaan te krijgen, en ze kunnen ook waarde opleveren voor het bedrijf. Het probleem ontstaat wanneer cloud apps op de verkeerde manier worden gebruikt met gevoelige gegevens van de organisatie en daarmee afbreuk doen aan beveiliging en naleving.

IT-beleid en het onderrichten van gebruikers kan de viervoudige bypass maar ten dele voorkomen, want als het de beste oplossing is voor iemands behoeften en het onwaarschijnlijk lijkt dat IT erachter komt, zal het gebeuren. Dat maakt het essentieel om mensen een stimulans te geven om met IT mee te werken en de infrastructuur van IT te gebruiken, vooral als het gaat om gevoelige gegevens en apps. De beste stimulans is een optimale gebruikerservaring, proactief geleverd en ontworpen om beter aan de behoeften te voldoen dan het onbeheerde alternatief.

4. Schenk aandacht aan uw dienstverleningsstrategie

Mobiele gebruikers rekenen op een verscheidenheid aan applicaties, niet alleen aangepaste mobiele apps, maar ook mobiele apps van derden, gemobiliseerde Windows-apps en SaaS-oplossingen. Bij het ontwikkelen van uw mobiliteitsstrategie moet u nadenken over de mix van apps die de personen en groepen in uw organisatie gebruiken, en hoe deze moeten worden benaderd op mobiele devices.

Er zijn vier benaderingswijzen voor apps op mobiele devices:

Device-eigen ervaring – in dit scenario blijft het device van de gebruiker volledig onbeheerd. Mensen kopen hun eigen apps, kunnen zakelijke en persoonlijke gegevens vrijuit vermengen en via elk netwerk werken. Net als de hierboven beschreven viervoudige bypass is dit een risicovolle en niet-veilige aanpak die nooit mag worden toegestaan voor gevoelige gegevens.

Gevirtualiseerde toegang – virtuele applicaties en gegevens, en ook virtuele desktops indien gewenst, worden gehost in het datacenter en gepresenteerd via een protocol voor weergave op afstand. IT kan toegang beheren en volledige beveiliging garanderen en ondertussen mensen met Windows apps laten werken op mobiele platforms. Gegevens verlaten het datacenter nooit, wat de noodzaak van gegevensbescherming op het device zelf verlicht. Deze methode hangt af van connectiviteit, wat offline gebruiksscenario's beperkt.

Ervaring met containers – de organisatie zorgt voor een container op het device waarmee alle zakelijke mobiele apps, inclusief aangepaste en mobiele apps van derden, gescheiden van andere inhoud worden bewaard. IT kan de apps en data beheren die in de container gaan, terwijl gebruikers zich kunnen voorzien van hun eigen apps via een appstore voor de onderneming. Applicaties kunnen automatisch worden bijgewerkt, bevoorraad en gewijzigd op basis van het IT-beleid. Netwerkinstellingen zoals SSL-encryptie en applicatie-specifieke VPN's zijn mogelijk in de container, zodat mensen eenvoudig op de juiste manier verbinding kunnen maken in elke omgeving. De container kan op afstand worden gewist in geval van verlies, diefstal, upgraden van het device of vertrek van de werknemer.

Volledig beheerde bedrijfservaring – in deze aanpak is er volledige controle over het mobiele device met geïntegreerd beleid voor wissen op afstand, geografische beperkingen, verlopen van gegevens en andere veiligheidsmaatregelen. Alle mobiele apps worden expliciet gekozen en verstrekt door IT zonder mogelijkheid voor personalisatie. Hoewel deze aanpak zeer veilig en geschikt is voor een aantal organisaties en scenario's, betekent dit een restrictieve gebruikerservaring en geen compatibiliteit met BYOD.

Voor de meeste organisaties ondersteunt een combinatie van gevirtualiseerde toegang en een containerervaring het volledige scala van apps en scenario's waarvan mensen afhankelijk zijn. Dit maakt het ook mogelijk voor IT de zichtbaarheid en controle te behouden en tevens een optimale gebruikerservaring te bieden. Mensen kunnen toegang krijgen tot gehoste applicaties, tot mobiele apps op hun device en ook tot SaaS-applicaties zoals Salesforce en NetSuite via een single sign-on. Wanneer een medewerker de organisatie verlaat, kan IT onmiddellijk het account van die persoon uitschakelen om toegang tot alle bedrijfsapps op het device en tot gehoste en SaaS-apps onmogelijk te maken.

5. Automatiseer gewenste uitkomsten

Automatisering vereenvoudigt niet alleen de dingen voor IT, het helpt u ook een betere ervaring te leveren. Bedenk welk verschil automatisering kan maken voor de aanpak van gemeenschappelijke mobiliteitsbehoeften zoals deze:

- Een werknemer vervangt een verloren device of voert een upgrade uit naar een nieuwe. Met een klik op een URL zijn alle afzonderlijke bedrijfsapps plus werkinformatie beschikbaar op het nieuwe device, volledig geconfigureerd en gepersonaliseerd en klaar voor het werk. Een nieuwe werknemer en een contractant kunnen even gemakkelijk worden toegelaten en voorzien van alle zakelijke mobiele apps in een container op elk privé- of bedrijfs-device. Single sign-on (SSO) maakt naadloze toegang tot gehoste en SaaS-applicaties mogelijk.

- Terwijl een medewerker van locatie naar locatie en van netwerk naar netwerk gaat, herconfigureren situationele en adaptieve toegangscontroles de apps automatisch om te zorgen voor een adequate beveiliging met volledige transparantie voor de gebruiker.
- Een bestuurslid arriveert voor een vergadering, tablet in de hand. Alle documenten voor de vergadering worden automatisch geladen op het device, selectief geconfigureerd door IT voor alleen-lezentoegang en beperkt tot een app in een container indien nodig. Vooral gevoelige documenten kunnen zo worden ingesteld dat ze automatisch worden gewist op het device zodra het bestuurslid de ruimte verlaat.
- Wanneer werknemers veranderen van rol in de organisatie, worden de relevante apps voor hun huidige functie automatisch ter beschikking gesteld en apps die niet meer nodig zijn, verdwijnen. SaaS-licenties van derden worden direct teruggevorderd voor hertoewijzing.

Een manier om deze vorm van automatisering uit te voeren is via Active Directory. Koppel allereerst een specifieke rol aan een bijbehorende container. Iedereen met die rol zal automatisch de container en alle apps, gegevens, instellingen en privileges die erbij horen erven. Op het device zelf kunt u MDM gebruiken om centraal WiFi-pincodes en -wachtwoorden, gebruikerscertificaten, dubbele verificatie en andere elementen instellen die nodig zijn om deze geautomatiseerde processen te ondersteunen.

6. Het netwerk expliciet maken

Verschillende applicaties en scenario's kunnen verschillende netwerkvereisten hebben, variërend van een intranet of Microsoft SharePoint-site tot een extern partnerportaal, tot een gevoelige app die wederzijdse SSL-authenticatie vereist. Handhaving van de hoogste beveiligingsinstellingen op het device-niveau degradeert de gebruikerservaring onnodig. Aan de andere kant kan verlangen van mensen om verschillende instellingen toe te passen voor elke app nog vermoeiender zijn voor hen.

Door netwerken in specifieke containers of apps met aparte instellingen voor elk ervan te vergrendelen, kunt u voor elke app een specifiek netwerk maken, zonder extra stappen van de gebruiker. Mensen kunnen gewoon klikken op een app en aan de slag gaan, terwijl taken, zoals het aanmelden, certificaten aanvaarden of openen van een app-specifieke VPN, automatisch door het beleid worden gestart op de achtergrond.

7. Gevoelige gegevens boven alles beschermen

In veel organisaties weet IT niet waar zich de meest gevoelige gegevens bevinden en moet daarom alle gegevens behandelen op hetzelfde hoogste beveiligingsniveau, wat een inefficiënte en dure benadering is. Mobiliteit biedt een kans voor u om gegevens selectiever te beschermen op basis van een classificatiemodel dat voldoet aan uw unieke bedrijfs- en beveiligingsbehoeften.

Veel bedrijven werken met een relatief eenvoudig model met gegevensclassificatie in drie categorieën (publiek, vertrouwelijk en beperkt) dat ook rekening houdt met het gebruikte device en platform, terwijl andere organisaties een complexer classificatiemodel hebben en rekening houden met veel meer factoren, zoals de gebruikersrol en -locatie. Een manier om een eenvoudig model te implementeren is als volgt:

Publieke gegevens zonder implicaties voor vertrouwelijkheid, privacy of naleving kunnen overal en op elk device ongelimiteerde gegevensmobiliteit en onbeperkt gebruik hebben. Er is geen noodzaak voor gebruikers om de bedrijfsinfrastructuur te doorgronden, u kunt app-specifieke netwerkinstellingen configureren om hen te verbinden zoals dat het beste uitkomt.

Vertrouwelijke gegevens die niet publiek bedoeld zijn en een minimaal risico vormen in geval van lekken, vragen om een hoger beveiligingsniveau. In dat geval kunt u via het bedrijfsnetwerk gevirtualiseerde toegang verlenen op BYOD- of consumenten-devices, terwijl alleen volledige gegevensmobiliteit wordt toegestaan op bedrijfs-devices met MDM-functies zoals encryptie en wissen op afstand, of op hulpmiddelen op missieniveau die speciaal ontworpen zijn om gegevens te beschermen in vijandige situaties.

Sommige bedrijven kunnen besluiten dat een containerbenadering voldoende is voor dit soort gegevens. In dit geval kunnen de gegevens volledig voor mobiele apparatuur worden gemobiliseerd, zolang ze maar in een afzonderlijke container opgeslagen worden die beveiligd en gecontroleerd kan worden door IT.

Beperkte gegevens die een aanzienlijk risico van niet-naleven, reputatieschade, verloren business en andere materiële impact vormen, moeten uw grootste aandacht krijgen. Volledige gegevensmobiliteit moet worden beperkt tot missiegraads-devices met toegestane gevirtualiseerde toegang op bedrijfs-devices. BYOD- en andere consumenten-devices mogen helemaal geen toegang krijgen, of moeten zorgvuldig worden onderzocht en overwogen voor virtualisatie en containergebaseerde benaderingen in bepaalde omstandigheden.

In het bovenstaande model wordt rekening gehouden met zowel gegevensclassificatie als met device-soort. Het kan ook zijn dat u extra overwegingen wilt opnemen in uw beveiligingsbeleid, zoals het device-platform, de locatie en gebruikersrol. Sommige bedrijven en vele overheidsorganisaties maken een grotere set van specifiekere gegevenscategorieën, elk met eigen regels.

Door toegang tot het netwerk via uw bedrijfsinfrastructuur te configureren voor vertrouwelijke en niet-openbare gegevens, kunt u nagaan hoe mensen informatie gebruiken en de effectiviteit van uw gegevensgevoeligheidsmodel en beleid voor mobiele controle beoordelen.

8. Wees duidelijk over rollen en eigenaarschap

Op wiens bordje ligt bedrijfsmobiliteit in uw organisatie? In de meeste bedrijven wordt mobiliteit nog steeds aangepakt via een ad hoc-aanpak, vaak door een commissie die toezicht houdt op IT-functies van infrastructuur en netwerken tot apps. Gezien de strategische rol van mobiliteit in het bedrijfsleven en de complexe matrix van gebruikers en IT-vereisten die moeten worden aangepakt, is het cruciaal om de organisatiestructuur, rollen en processen rond mobiliteit duidelijk vast te leggen. Men moet begrijpen wie verantwoordelijk is voor de mobiliteit en hoe deze die holistisch zal beheren in verschillende IT-functies.

Het eigendom moet even duidelijk zijn wat betreft mobiele devices zelf, vooral in organisaties waar mobiliteit en BYOD hand in hand gaan. Uw BYOD-beleid moet bijvoorbeeld het grijze gebied tussen volledig beheerde hulpmiddelen van het bedrijf of van devices van gebruikers strikt voor persoonlijk gebruik aanpakken:

- Wie is verantwoordelijk voor back-ups van een BYOD-device? Wie biedt ondersteuning en onderhoud voor het device en hoe wordt daarvoor betaald?
- Hoe zal ontdekking worden behandeld bij dagvaarding voor gegevens of logs van een persoonlijk device?
- Wat zijn de gevolgen voor de privacy van persoonlijke inhoud wanneer iemand gebruik maakt van hetzelfde device voor werk?

Zowel gebruikers als IT moeten hun rol en verantwoordelijkheden begrijpen om misverstanden te voorkomen. Leg uw BYOD-programma expliciet vast en laat deelnemers tekenen voordat ze persoonlijke devices voor werk gaan gebruiken.

9. Bouw naleving in bij uw oplossingen

Wereldwijd hebben organisaties te maken met meer dan 300 beveiligings- en privacy-gerelateerde normen, voorschriften en wetten, met meer dan 3.500 specifieke controles. Het is niet genoeg alleen aan deze eisen voldoen, u moet uw naleving ook kunnen documenteren en volledig controleerbaar maken. En dan hebben we het nog niet over uw interne bedrijfsbeleid. U hebt misschien al de nalevingsuitdaging binnen uw netwerk opgelost. Het laatste wat u wilt, is bedrijfsmobiliteit een groot nieuw op te lossen probleem laten creëren. Zorg ervoor dat uw mobiele devices en platforms naadloze compliancy van de overheidsmandaten, industrienormen en beveiligingsbeleid van het bedrijf ondersteunen, van toegangscontrole op basis van beleid en classificatie tot beveiligde gegevensopslag. Uw oplossing moet voorzien in volledige logging en rapportage om u te helpen snel, efficiënt en met succes te reageren op controle.

10. Wees voorbereid op “the internet of Things”

Stel uw beleid niet alleen op voor nu maar houd er rekening mee hoe bedrijfsmobiliteit er in de komende jaren gaat uitzien. Draagbare technologieën zoals Google Glass en smart watches veranderen de manier waarop mensen mobiele technologieën gebruiken, met een meer menselijke, intuïtieve ervaring en tegelijk nieuwe gebruiksmogelijkheden. Aangesloten voertuigen, inclusief onbemande auto’s, gebruiken gegevens- en cloud-diensten op nieuwe manieren om mensen te helpen gemakkelijker en efficiënter op plaats van bestemming te komen. Industriële controlesystemen (ICS) gebruiken bedrijfsgegevens en wisselen die uit als onderdeel van

menselijke werkstromen en achter de schermen. Ontwikkelingen als deze blijven het potentieel van mobiliteit uitbreiden, maar zullen ook nieuwe implicaties introduceren voor beveiliging, compliancy, beheersbaarheid en gebruikerservaring.

Besteed aandacht aan de lopende discussies in de industrie over opkomende technologieën zoals deze en ontwerp uw mobiliteitsstrategie rond kernprincipes die toepasbaar zijn op elk type mobiel device en gebruiksscenario. Op die manier kunt u de frequente veranderingen in het beleid en iteraties die kunnen verwarren en frustreren minimaliseren.

De Citrix-oplossing voor beveiligde enterprise mobility

Als de leider in mobiele werkstijlen, biedt Citrix een complete oplossing voor beveiligde bedrijfsmobiliteit met de eenvoudige, handige gebruikerservaring die uw medewerkers vragen. Via integratie van volledige technologieën voor MDM, MAM, containerisatie, applicatie- en desktopvirtualisatie, brengt de oplossing voldoende flexibiliteit om veilige mobiliteit op de juiste manier te ondersteunen voor elke soort informatie, gebruiksscenario en rol in uw organisatie.

De Citrix-oplossing voor beveiligde enterprise mobility omvat de volgende producten:

XenMobile – XenMobile levert complete MDM- en MAM-mogelijkheden voor beheer van beveiligde bedrijfsmobiliteit. IT kan via een enkele klik toegang geven tot mobiele-, web-, datacenter- en Windows-apps vanaf een uniforme app store, inclusief geïntegreerde productiviteitsapps met een geweldige gebruikerservaring. XenMobile biedt ook beveiligde e-mail-, browser- en agenda-apps op bedrijfsniveau om de leemten in de beveiliging, die door de consument-apps geïntroduceerd kunnen worden, te voorkomen. IT krijgt op identiteit gebaseerde voorzieningverstrekking en controle over apps, gegevens en devices, automatische terugname van voorzieningen van accounts voor vertrokken gebruikers en selectief wissen van verloren devices. Met de geïntegreerde Citrix MDX-appcontainertechnologie zijn gegevensversleuteling, wachtwoordverificatie, veilig vergrendelen en wissen, beleid tussen apps en micro-VPN's voor mobiele apps mogelijk.

XenDesktop en XenApp – met XenDesktop en XenApp kan IT apps en volledige desktops veranderen in on-demand diensten die beschikbaar zijn op alle devices. Omdat apps en gegevens beheerd worden binnen het datacenter, behoudt IT een centrale gegevensbeveiliging, naleving, toegangscontrole en gebruikersadministratie op zowel persoonlijke devices als op zakelijke eindpunten binnen dezelfde uniforme omgeving. XenApp maakt het ook eenvoudig om Windows-applicaties te mobiliseren voor gebruik op smartphones en tablets, en de interfaces aan te passen zodat die zich gedragen als mobiele apps op een mobiel device voor een optimale gebruikerservaring.

ShareFile – met ShareFile kunt u een beveiligde en robuuste service bieden voor synchronisatie en delen van gegevens die voldoet aan alle eisen voor personeelsmobiliteit en samenwerking. De rijke ervaring in consumentenstijl maakt het voor mensen eenvoudig gegevens op te slaan en te synchroniseren op hun devices vanuit elke netwerklocatie. IT kan een hoog niveau van beheer en controle handhaven over het delen van bestanden en gegevens, met absolute flexibiliteit om te kiezen waar gegevens opgeslagen worden, een robuust beveiligingsbeleid voor devices, uitgebreide controlemogelijkheden en integratie met Microsoft Active Directory.

NetScaler – NetScaler is een compleet app-leveringsmechanisme voor beveiliging, controle en optimalisering van de levering van apps, desktops en services op elk device. Brede ondersteuning van mobiele OS met volledige SSL VPN-toegang voor leidende leveranciers van mobiele OS en toestellen, waaronder Apple, Google en Microsoft. Met Micro SSL VPN-ondersteuning kunt u specifieke verbindingen instellen voor afzonderlijke apps zonder dat de gebruiker extra stappen moet uitvoeren. Toegangscontrole, controle en rapportage ondersteunen naleving en gegevensbeveiliging. Volledige zichtbaarheid en controle geven u een betere orkestratie van uw gehele infrastructuur en maakt effectieve verdeling van de belasting mogelijk over meerdere onderdelen van de Citrix-mobiliteit.

Conclusie

Enterprise mobility heeft zich snel verder ontwikkeld dan bepaalde groepen en scenario's en is een fundamenteel element van bedrijfs-IT geworden. Zorg er bij het ontwikkelen van uw bedrijfsmobiliteitsstrategie voor dat u rekening houdt met alle vereisten van zowel gebruikers als IT. Mensen verwachten naadloze, gemakkelijke toegang tot hun gegevens en apps op elk device dat zij gebruiken, met een gebruikerservaring die beter is dan zij gewend zijn in hun privéleven. IT moet in staat zijn het juiste niveau van controle, bescherming en naleving te leveren voor elke gegevenssoort, zonder onnodige beperkingen voor de manier waarop mensen willen werken. Citrix-oplossingen bieden de uitgebreide functionaliteit die u nodig hebt ter ondersteuning van uw bedrijfsmobiliteitsstrategie, met XenMobile voor MDM, MAM en containerisatie; XenDesktop en XenApp voor virtualisatie; ShareFile voor veilig synchroniseren en delen van gegevens; en NetScaler voor het beveiligen, controleren en optimaliseren van de dienstverlening aan mobiele devices. Door effectief gebruik te maken van de beschikbare modellen en technologieën voor beveiliging en toegang tot applicaties en gegevens op mobiele devices bereikt u de uitgebreide mobiliteitsstrategie die uw organisatie vandaag en in de komende jaren nodig heeft.

Aanvullende bronnen

- Casestudie: Hoe 4 klanten van Citrix de enterprise mobility voor bedrijven oplossen
- Bedrijfsinformatie beveiligd leveren aan Android- en Apple iOS-devices
- De 10 essentiële zaken voor beveiligde bedrijfsmobiliteit
- Beheer van bedrijfsmobiliteit: BYOD verwelkomen met beveiligde levering van apps en gegevens

Hoofdkwartier
Fort Lauderdale, FL, Verenigde Staten

Hoofdkwartier Silicon Valley
Santa Clara, CA, Verenigde Staten

Hoofdkwartier EMEA
Schaffhausen, Zwitserland

India Development Center
Bangalore, India

Hoofdkwartier Online Division
Santa Barbara, CA, Verenigde Staten

Hoofdkwartier Pacifisch gebied
Hongkong, China

Hoofdkwartier Latijns-Amerika
Coral Gables, FL, Verenigde Staten

VK Development Center
Chalfont, Verenigd Koninkrijk

CITRIX®

Over Citrix
Citrix (NASDAQ:CTXS) geeft de toon aan in softwaregedefinieerde werkplekken op basis van geavanceerde virtualisatie-, mobility-, netwerk- en SaaS-oplossingen, die nieuwe manieren creëren om organisaties en mensen beter te laten werken. Citrix-oplossingen maken zakelijke mobility mogelijk in de vorm van beveiligde, mobiele werkplekken die mensen directe toegang bieden tot apps, desktops, data en communicatievoorzieningen op elk device, over elk netwerk en in elke cloud. Citrix boekte in 2014 een jaaromzet van 3,14 miljard dollar. Citrix-oplossingen worden gebruikt in meer dan 330.000 organisaties en door meer dan 100 miljoen mensen wereldwijd. Lees meer op www.citrix.nl.