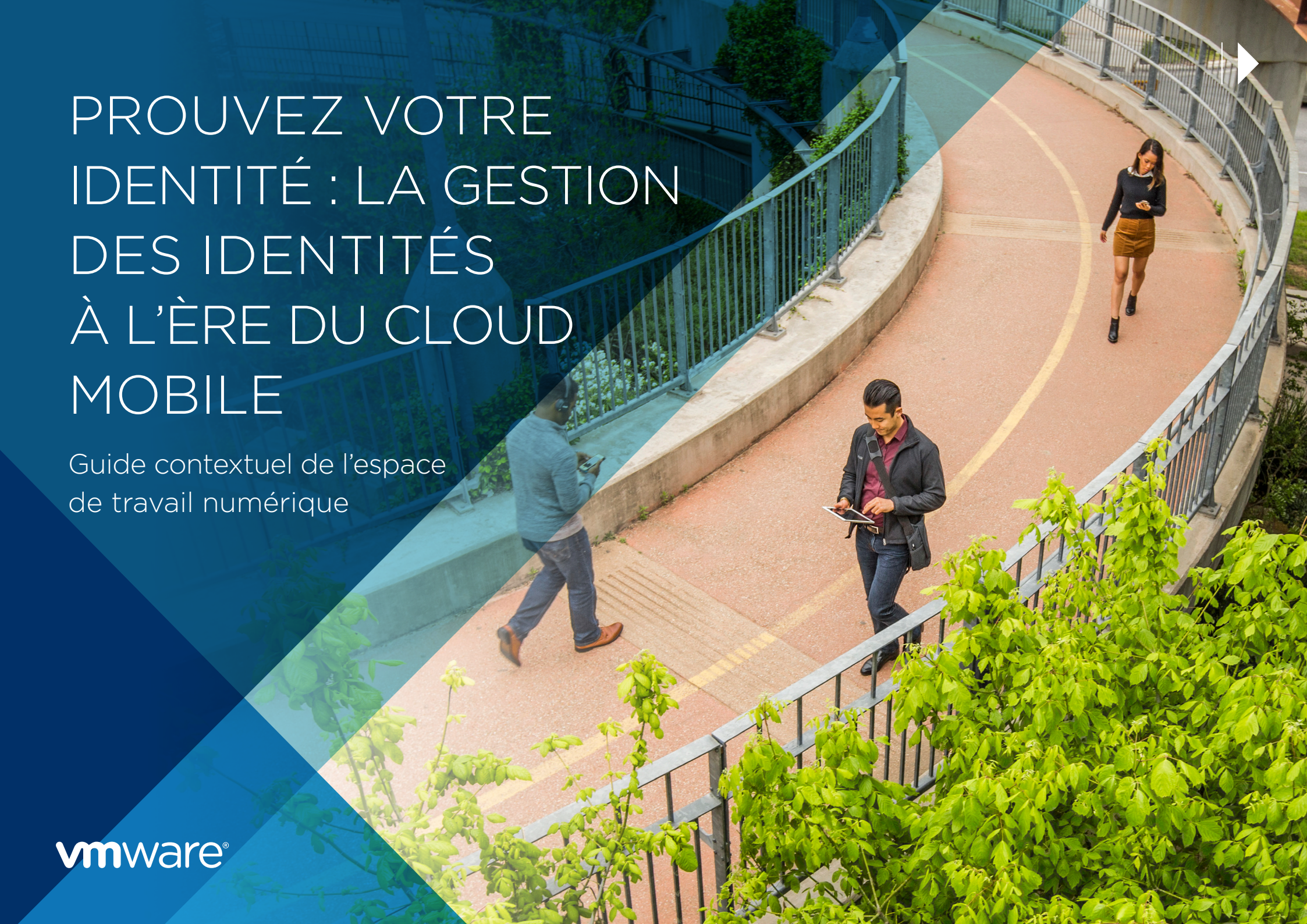
PROUVEZ VOTRE IDENTITÉ : LA GESTION DES IDENTITÉS À L'ÈRE DU CLOUD MOBILE

Guide contextuel de l'espace de travail numérique



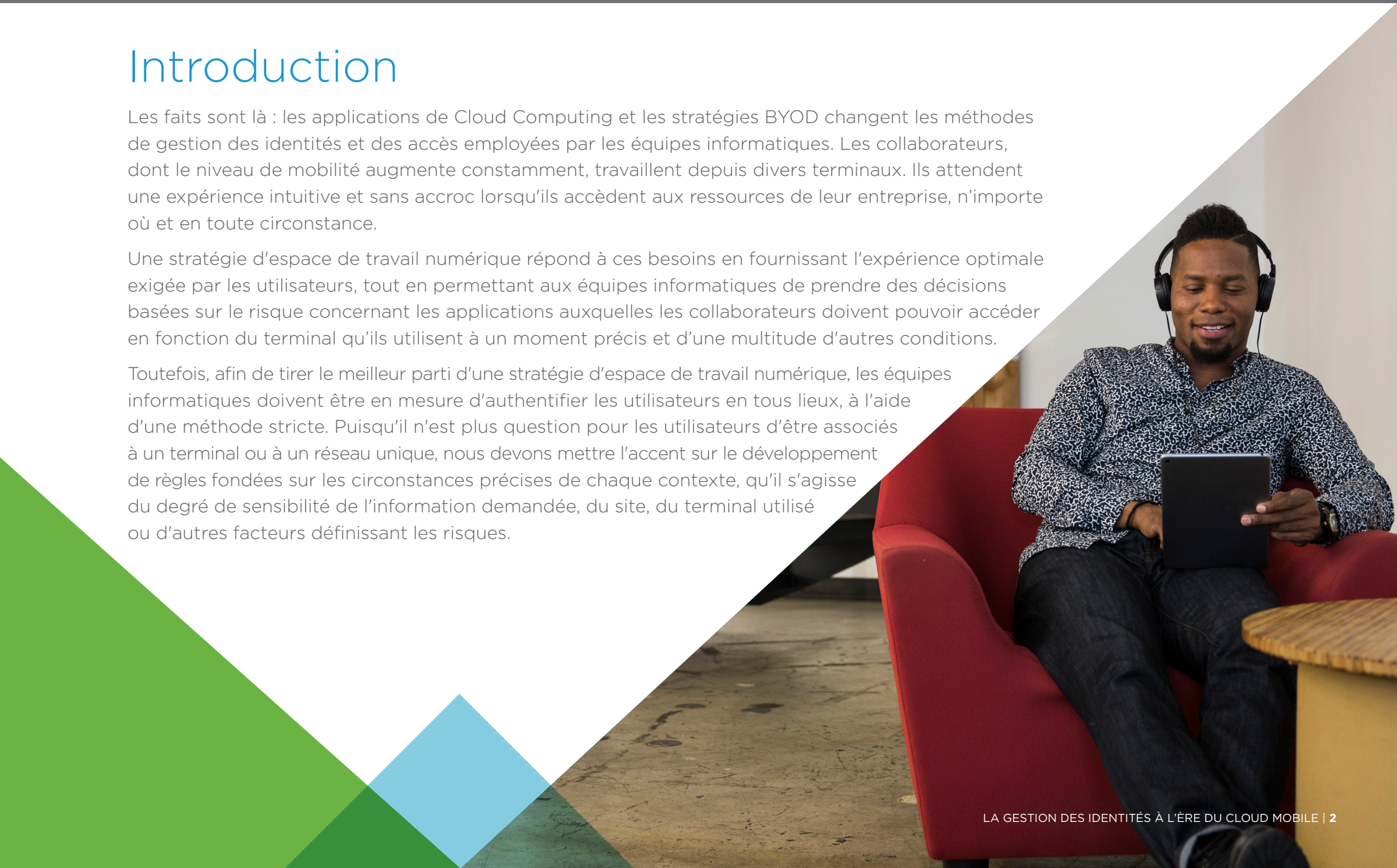
vmware®

Introduction

Les faits sont là : les applications de Cloud Computing et les stratégies BYOD changent les méthodes de gestion des identités et des accès employées par les équipes informatiques. Les collaborateurs, dont le niveau de mobilité augmente constamment, travaillent depuis divers terminaux. Ils attendent une expérience intuitive et sans accroc lorsqu'ils accèdent aux ressources de leur entreprise, n'importe où et en toute circonstance.

Une stratégie d'espace de travail numérique répond à ces besoins en fournissant l'expérience optimale exigée par les utilisateurs, tout en permettant aux équipes informatiques de prendre des décisions basées sur le risque concernant les applications auxquelles les collaborateurs doivent pouvoir accéder en fonction du terminal qu'ils utilisent à un moment précis et d'une multitude d'autres conditions.

Toutefois, afin de tirer le meilleur parti d'une stratégie d'espace de travail numérique, les équipes informatiques doivent être en mesure d'authentifier les utilisateurs en tous lieux, à l'aide d'une méthode stricte. Puisqu'il n'est plus question pour les utilisateurs d'être associés à un terminal ou à un réseau unique, nous devons mettre l'accent sur le développement de règles fondées sur les circonstances précises de chaque contexte, qu'il s'agisse du degré de sensibilité de l'information demandée, du site, du terminal utilisé ou d'autres facteurs définissant les risques.



La gestion des identités et des accès renforce la sécurité en toute simplicité

Alors que les collaborateurs utilisent toujours plus de terminaux et d'applications hors de l'espace de bureau traditionnel, il n'a jamais été aussi important de pouvoir identifier et faire confiance aux utilisateurs qui accèdent aux actifs sensibles de l'entreprise. La gestion des identités et des accès permet d'offrir un accès mobile sécurisé aux utilisateurs spécialistes du Cloud actuels, sans pour autant compromettre la sécurité ou la conformité.

Cette gestion permet de savoir qui vous êtes et à quoi vous avez accès, et elle peut utiliser ce qu'elle sait sur vous et votre terminal, ainsi qu'une multitude d'autres informations nécessaires, pour accorder, refuser ou fournir un accès limité aux ressources de l'entreprise. Étant donné que les utilisateurs se séparent rarement de leur téléphone, la gestion des identités et des accès peut exploiter la propriété d'un terminal unique et même les empreintes digitales d'un individu (ou d'autres facteurs biométriques) pour assurer une authentification plus forte. Les technologies d'authentification mobile deviennent de nouveaux moyens pour les utilisateurs de prouver qu'ils sont bien la personne qu'ils prétendent être, et elles renforcent la sécurité de l'entreprise tout en garantissant une grande simplicité d'utilisation.

Authentification

Les problèmes d'authentification courants qui entraînent des problèmes de sécurité sont notamment la faiblesse inhérente aux mots de passe, la lourdeur et le coût de l'authentification matérielle ou logicielle à deux facteurs basée sur jeton, et les conflits qui se produisent entre plusieurs identités utilisateur dans plusieurs applications.

Gouvernance

Dans un environnement de Cloud mobile, la possibilité d'accorder et de refuser l'accès de manière précise est impérative. Les délais sont également essentiels dans le monde de la technologie d'entreprise en constante évolution. Combien de temps prennent les mises à jour et modifications des utilisateurs ? Par exemple, pouvez-vous vérifier immédiatement et avec exactitude à quels programmes Bob a accédé à 8 h 30 ce matin ?

Accès contextuel

Une fois que vous êtes authentifié, le département informatique peut déterminer qui vous êtes et les applications auxquelles vous avez accès. Mais d'autres éléments doivent encore être pris en considération pour limiter l'accès en fonction d'une multitude de conditions. À l'ère du Cloud mobile, l'accès contextuel signifie que l'accès aux applications ne se fait plus selon le modèle du « tout ou rien », mais qu'il est fluide et dynamique. De plus, l'accès doit être surveillé après l'authentification initiale, afin que le département informatique puisse révoquer ou forcer une authentification basée sur le risque en fonction des besoins.

La multitude d'applications et de terminaux utilisés pour assurer une productivité optimale, ainsi que la nécessité de disposer d'un moyen crédible de gérer les risques en continu, conduisent directement à la nécessité de disposer d'une plate-forme unique capable de capturer des informations détaillées pour la surveillance du système tout en offrant une parfaite visibilité en temps réel grâce à des analyses avancées.

L'authentification unique transforme l'expérience mobile

L'ancien système de gestion des identités impliquait des comptes individuels, et bien souvent, par facilité, les mots de passe étaient écrits à la main et scotchés sur l'écran. De nombreuses entreprises ont également investi dans la fédération des identités pour les applications d'entreprise on premise à l'aide de services logiciels personnalisés impliquant l'utilisation d'une infrastructure d'annuaires complexe. Le Cloud et les terminaux mobiles ont cependant entraîné une augmentation phénoménale du nombre d'options et de types de comptes.

ÉTUDIONS L'EXPÉRIENCE UTILISATEUR STANDARD ACTUELLE...	...PAR RAPPORT AUX POSSIBILITÉS OFFERTES PAR UNE STRATÉGIE D'ESPACE DE TRAVAIL NUMÉRIQUE.
Vous téléchargez une application (par exemple, Microsoft OneDrive) depuis l'App Store d'Apple ou Google Play. Vous la lancez depuis votre écran d'accueil.	Plus qu'une simple connexion en un clic, les systèmes SSO se présentent sous trois formes :
Vous répondez à la demande d'adresse e-mail de l'application, puis à l'invite vous demandant de saisir votre nom d'utilisateur et votre mot de passe.	Vous devez saisir les mêmes nom d'utilisateur et mot de passe pour chaque application, à chaque fois.
Vous saisissez un mot de passe excessivement compliqué comprenant des majuscules, des chiffres et des symboles. Vous recevez un message d'erreur signalant que le nom d'utilisateur et/ou le mot de passe sont incorrects. Vous maudissez l'application et saisissez à nouveau le mot de passe complexe susmentionné.	–ou– Vous devez saisir vos nom d'utilisateur et mot de passe une seule fois pour lancer plusieurs applications.
Vous vérifiez que vous utilisez l'authentification à deux facteurs. Vous réalisez que vous devez aller dans une autre pièce, où se trouve actuellement l'autre terminal qui contient le code de vérification.	–ou–
Vous obtenez enfin l'accès à l'application.	Le nom d'utilisateur et le mot de passe ne sont pas importants car votre identité est certifiée via un certificat géré et un code PIN simple, installés sur votre terminal personnel.
Vous devez répéter ce processus à chaque fois que vous devez accéder à une application différente.	

La gestion des identités peut révolutionner l'expérience mobile lorsque l'utilisateur n'a plus à se souvenir et à saisir son nom d'utilisateur et son mot de passe pour aucune des applications installées. À la place, la fédération des identités sur les terminaux mobiles offre un système d'authentification unique (SSO) qui permet un accès aisé aux programmes nécessaires.

Avec VMware Workspace ONE™, le terminal est provisionné avec un jeton cryptographique sécurisé sous la forme d'un certificat qui vérifie l'identité de l'utilisateur. Une fois l'authentification réussie, le système peut décider si le terminal est fiable ou non en fonction de critères de gestion et de conformité provenant de VMware AirWatch® Unified Endpoint Management™. Si les conditions sont réunies, la plate-forme Workspace ONE autorise ou refuse l'accès à l'application.

Il s'agit d'une forme de la technologie en instance de brevet appelée « Secure App Token System » (système SATS), conçue pour les terminaux natifs iOS et Android qui n'autorisent pas les navigateurs à partager des informations telles que les cookies utilisés dans Windows ou Mac OS. Elle permet à une entreprise d'établir la confiance entre une application de Cloud back-end (interne ou externe) où résident les données des applications, le terminal de l'utilisateur (qu'il s'agisse d'un terminal personnel ou appartenant à l'entreprise) et la solution d'espace de travail numérique de l'entreprise (telle que VMware Workspace ONE). Grâce à l'association de jetons et de la gestion de certificats, la solution d'espace de travail numérique intercepte le flux d'authentification et fournit à l'utilisateur une solution d'authentification unique directe via un certificat unique sur son terminal.

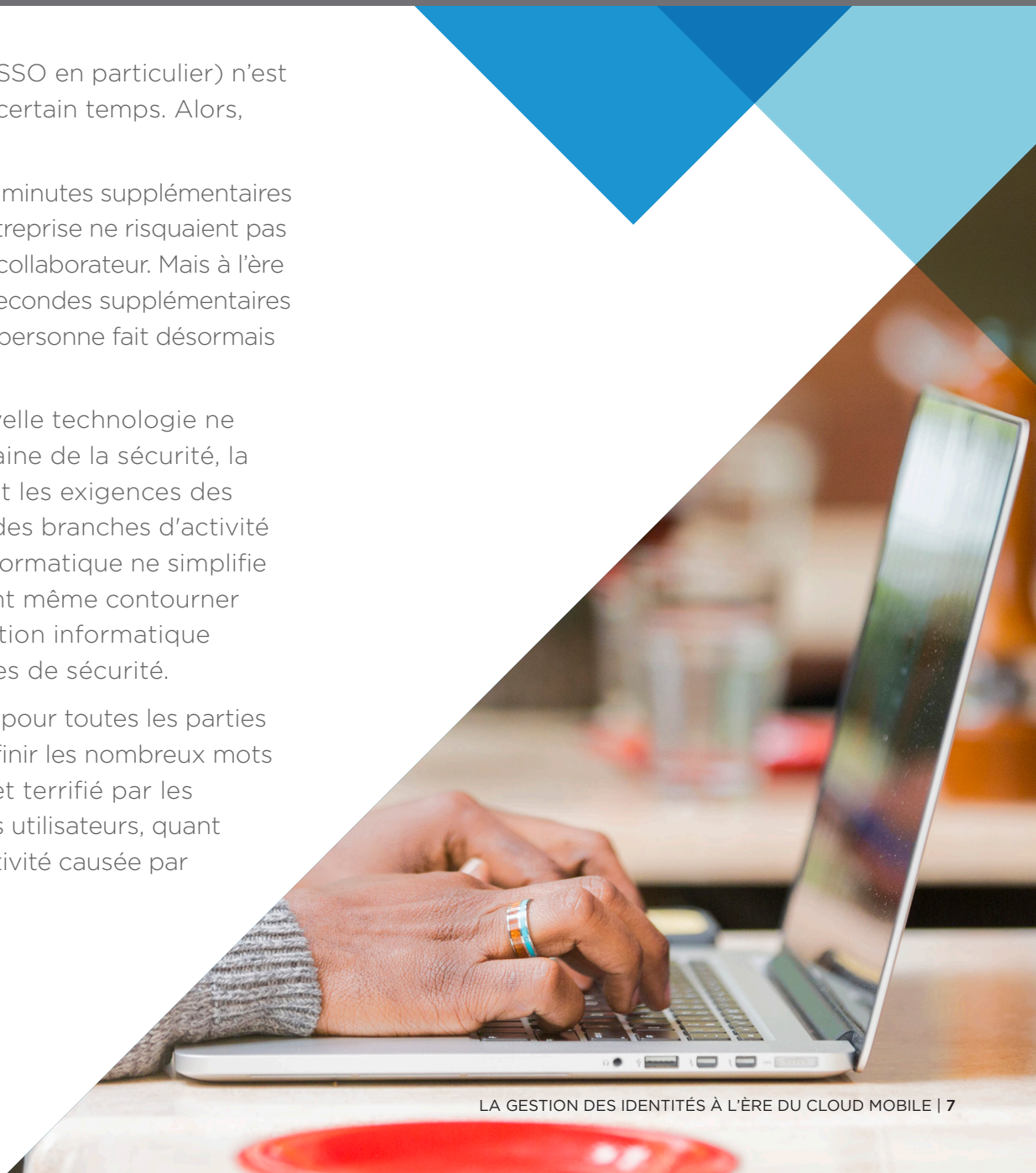
Pour résumer, cela signifie que l'utilisateur bénéficie d'une bien meilleure expérience qu'en essayant de négocier un mot de passe très long comportant des chiffres, des lettres et des caractères. Plus important encore, ce mot de passe peut facilement être usurpé. Et toute personne disposant de ce mot de passe peut l'utiliser sur n'importe quel terminal. L'importance des certificats réside dans le fait qu'ils sont étroitement associés à leur utilisateur individuel, qui peut maintenant accéder à une application à l'aide d'un simple identifiant PIN ou biométrique, avec la même facilité que pour n'importe quelle application grand public.

La gestion des identités et des accès (et la technologie SSO en particulier) n'est pas une nouveauté. Elle existe en réalité déjà depuis un certain temps. Alors, comment expliquer ce brusque pic d'intérêt ?

À l'époque de la suprématie des postes de travail, les trois minutes supplémentaires nécessaires pour lancer un réseau privé virtuel (VPN) d'entreprise ne risquaient pas d'avoir une incidence sur la productivité quotidienne d'un collaborateur. Mais à l'ère du Cloud mobile, le fait de prendre ne serait-ce que cinq secondes supplémentaires pour accéder à une tâche essentielle sur le terminal d'une personne fait désormais une énorme différence au niveau de l'efficacité.

Pour un département informatique, l'intérêt d'une nouvelle technologie ne compte jamais réellement. Si l'entreprise n'est pas certaine de la sécurité, la technologie n'est pas mise en œuvre, quelles que soient les exigences des utilisateurs. Du côté des collaborateurs, ou même pour des branches d'activité entières, si la technologie fournie par le département informatique ne simplifie pas le travail, personne ne va l'utiliser. Ou pire, ils peuvent même contourner les équipes informatiques et mettre en œuvre une solution informatique « fantôme » potentiellement source de nouveaux risques de sécurité.

La gestion des identités et des accès moderne est idéale pour toutes les parties impliquées. Le département informatique est las de redéfinir les nombreux mots de passe avec lesquels les utilisateurs doivent jongler, et terrifié par les conséquences éventuelles d'une violation de sécurité. Les utilisateurs, quant à eux, ne peuvent pas se permettre une perte de productivité causée par des processus de connexion incommodes et laborieux.



Prise en charge d'applications diverses à l'aide de la gestion des identités et des accès

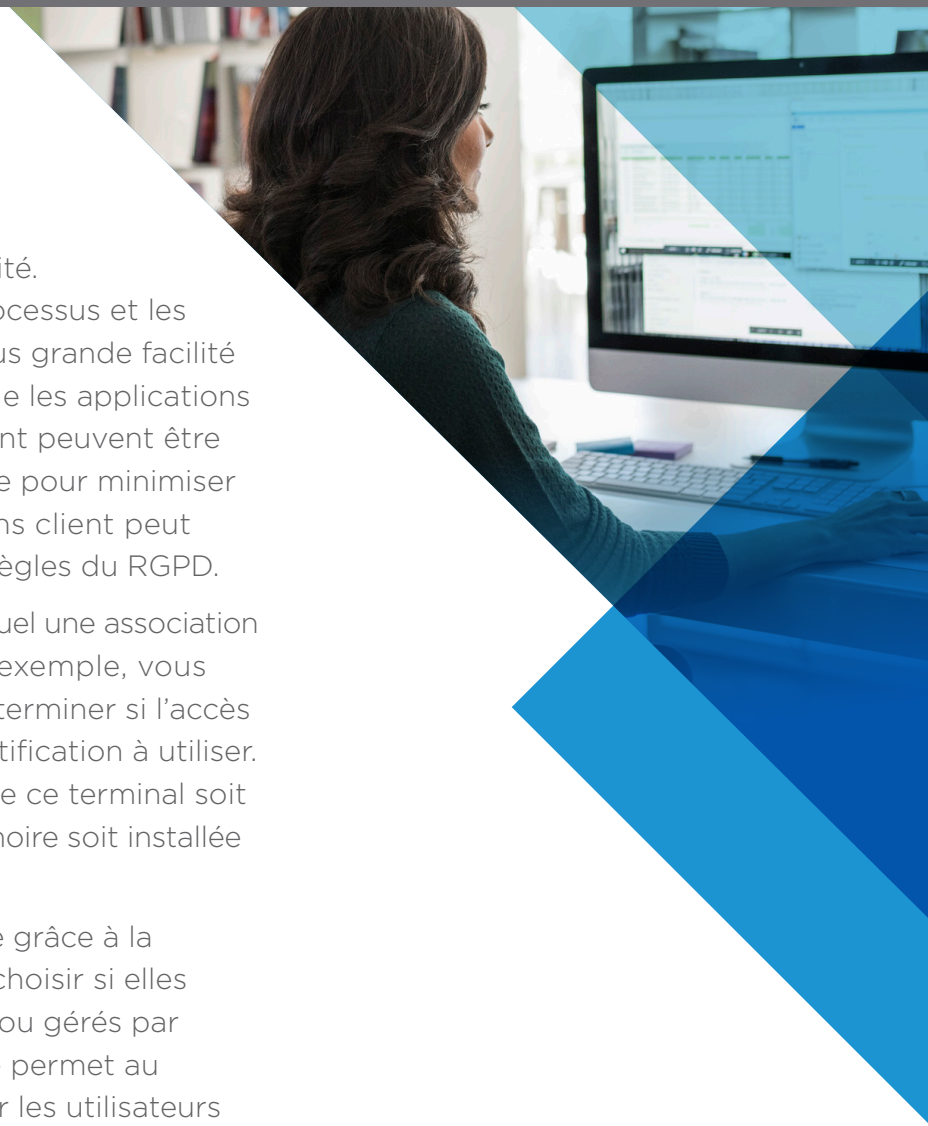
Le point critique imposant le recours à une solution de gestion des accès pour les applications Web et mobiles, c'est lorsque l'entreprise commence à développer ses propres applications ou à intégrer des applications tierces qui peuvent avoir des architectures mixtes. Quels éléments définissent les priorités de la gestion des identités et des accès ?

L'arrivée à maturité des applications SaaS (logiciel sous forme de service)

L'utilisation de la gestion des accès pour soutenir la transition vers des applications SaaS (logiciel sous forme de service) suscite un vif intérêt. Chaque application placée dans le Cloud a ses propres besoins en matière d'administration des identités, de contrainte d'accès et de création de rapports. Lorsque vous utilisez un mélange éclectique de terminaux mobiles et non mobiles incluant des architectures applicatives natives, vous avez besoin d'une solution de gestion des accès capable de prendre en charge les applications natives, l'accès classique via un navigateur en exploitant des protocoles tels que le langage SAML, ou les applications existantes qui nécessitent très probablement une passerelle les reliant aux solutions existantes de fédération et de gestion des mots de passe.

Les utilisateurs sont de plus en plus mobiles

La sécurité des applications n'est plus simplement question d'authentification utilisateur. Les entreprises doivent maintenant déterminer dans quelles circonstances l'accès doit être accordé à des utilisateurs spécifiques. Même une fois que vous êtes en mesure de confirmer qui est un utilisateur, il reste des questions concernant certains points, notamment le lieu. Par exemple, ces questions peuvent concerner les locaux d'un hôpital où les informations sont accessibles, ou bien le pays dans lequel le directeur commercial doit se rendre pour rencontrer un client.



Applications différentes, sécurité différente

Certaines applications ne nécessitent pas un accès aussi limité que d'autres. Par exemple, si vous êtes en déplacement et utilisez une application telle que Concur pour effectuer la gestion de vos dépenses, vous devez constamment prendre des photos de vos justificatifs pour les envoyer au service Comptabilité. Dans le cas d'informations aussi peu sensibles, l'entreprise souhaite que le processus et les règles d'authentification soient aussi libéraux que possible pour garantir la plus grande facilité d'utilisation. D'autres activités peuvent être beaucoup plus sensibles, telles que les applications ERP ou de gestion de la relation client (CRM ou GRC) où les informations client peuvent être réglementées, exigeant une gestion de l'authentification beaucoup plus stricte pour minimiser le risque de perte de données. Dans l'UE, par exemple, la perte d'informations client peut constituer une violation de la confidentialité réglementée selon de nouvelles règles du RGPD.

Une fonction clé de Workspace ONE est le contrôle d'accès contextuel, dans lequel une association de contextes d'identité et de terminal est utilisée pour réguler l'accès. Par exemple, vous pouvez vous fonder sur l'emplacement réseau ou le type de terminal pour déterminer si l'accès doit ou non être accordé et, dans l'affirmative, pour décider du type d'authentification à utiliser. De même, selon le contexte ou la position du terminal (par exemple, le fait que ce terminal soit géré ou non, qu'il soit débloqué ou non ou qu'une application figurant en liste noire soit installée ou non), l'accès à une application spécifique peut être autorisé ou refusé.

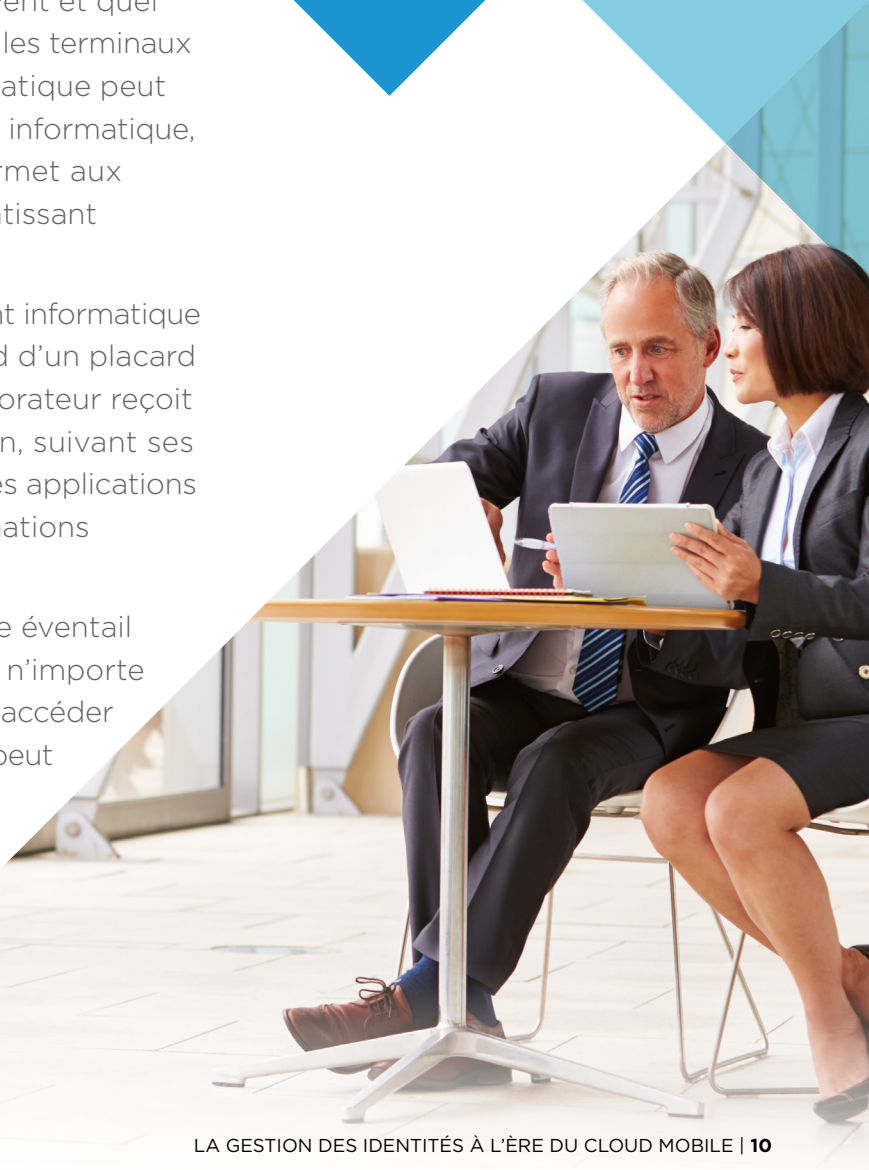
De plus, avec la détection des terminaux et le contrôle de l'état de conformité grâce à la gestion unifiée des terminaux via VMware AirWatch, les entreprises peuvent choisir si elles souhaitent autoriser l'accès aux terminaux non gérés, gérés personnellement ou gérés par l'entreprise. La connaissance de la position du terminal et de l'identité globale permet au département informatique d'assurer l'équilibre entre la flexibilité souhaitée par les utilisateurs et les règles de conformité de l'entreprise. Enfin, cela donne au département informatique la possibilité de faire évoluer les fonctionnalités du magasin d'applications de l'entreprise en fonction des besoins de l'activité.

Donner la liberté de choix de terminal aux utilisateurs

Les collaborateurs souhaitent désormais pouvoir être productifs où qu'ils se trouvent et quel que soit le terminal qu'ils utilisent. L'innovation et la facilité d'utilisation offertes par les terminaux grand public ont dépassé l'expérience et l'équipement que le département informatique peut provisionner dans un modèle d'entreprise traditionnel. Ce qu'il faut au département informatique, et que les utilisateurs attendent, c'est un modèle en libre-service évolutif qui permet aux utilisateurs de faire un travail de qualité sur le terminal de leur choix tout en garantissant le respect des normes de gestion et de sécurité de l'entreprise.

Étudions le cas d'une nouvelle embauche. Au lieu de devoir se rendre au département informatique pour récupérer un ordinateur portable reconfiguré qui avait été entreposé au fond d'un placard (et qui n'a pas forcément fait l'objet d'une création d'image récemment), le collaborateur reçoit un terminal livré directement et prêt à l'emploi qu'il peut emporter avec lui. Sinon, suivant ses préférences, il peut tout simplement utiliser son propre terminal en téléchargeant les applications nécessaires configurées par le département informatique et en utilisant les informations d'authentification utilisateur fournies.

Il est important de noter que cette idée de gestion d'un terminal recouvre un large éventail d'applications. Dans certains cas, elle signifie qu'un utilisateur doit pouvoir utiliser n'importe quelle machine (à la maison, chez son voisin, à la bibliothèque) et être en mesure d'accéder à un site Web, de se connecter et d'obtenir un certain niveau d'accès. À l'inverse, on peut avoir un terminal totalement supervisé ou verrouillé appartenant à un service de l'entreprise. Cela peut signifier qu'un utilisateur ne dispose d'aucun droit d'administration ou n'a pas la possibilité de modifier la configuration de ce terminal, car l'entreprise souhaite s'assurer qu'il reste toujours homéostatique. Cette approche est certainement la plus sécurisée, mais elle ne laisse pas beaucoup de place à la flexibilité utilisateur.



Quels sont les points essentiels d'une solution efficace ?

Lorsqu'il s'agit de déterminer quelle solution de gestion des identités et des accès est la mieux adaptée à vos besoins, voyez si elle peut fournir l'expérience intuitive et sans accroc recherchée par vos utilisateurs tout en proposant la sécurité et la gérabilité solides nécessaires à l'équipe informatique.

SIX CRITÈRES ESSENTIELS DE LA SOLUTION

- ✔ Authentification unique
- ✔ Intégration des services d'annuaire
- ✔ Authentification multifacteur
- ✔ Gestion des règles
- ✔ Lanceur et catalogue multiterminaux
- ✔ Analyses et rapports

LA SOLUTION PERMET-ELLE DE...

- Automatiser et simplifier l'intégration et la révocation ?
- Accroître la productivité ?
- Réduire la complexité grâce à sa facilité d'utilisation ?
- Répondre aux exigences de sécurité et de conformité ?
- Prendre en charge tout type de terminal et de système d'exploitation ?
- Prendre en charge tout type d'application ?

Couches de gestion d'accès des identités

L'application Workspace ONE offre aux collaborateurs un accès instantané à leur catalogue d'applications d'entreprise personnalisé. L'intégration de VMware Identity Manager™ offre un grand choix de couches de gestion d'accès des identités.

Création d'un catalogue d'applications

- Installation directe des applications sur le tableau de bord ou accès par le biais d'un portail d'applications HTML5 réactif
- Provisionnement automatique des workflows

Fédération de l'identité utilisateur

- Authentification unique (SSO) avec connexion au domaine
- Authentification forte avec provisionnement et révocation instantanés de l'accès

Authentification en une seule étape

- Aucune configuration ni connexion requise
- Utilisation de la propriété et du déblocage des terminaux pour établir une authentification

Authentification multifacteur

- Sécurité renforcée à l'aide de plusieurs composants d'identification
- Prise en charge de l'authentification biométrique ou d'autres méthodes multifacteur pour les applications plus stratégiques

Accès conditionnel

- Terminaux gérés ou non, portée du réseau, niveau de sécurité de l'authentification
- Définition des niveaux de règles par application

Conclusion

La gestion des identités et des accès ne se limite pas à prouver que vous êtes bien la personne que vous prétendez être. Du point de vue de l'entreprise, la gestion et le contrôle d'accès établissent l'équilibre délicat entre ce que les collaborateurs toléreront simplement et ce qu'ils utiliseront réellement.

La plupart des entreprises ont acheté des services SaaS et des applications mobiles. La plupart de ceux-ci contribuent à l'informatique « fantôme », et certains peuvent même être intégrés au système de tickets de support pour la création de compte et la réinitialisation des mots de passe. Cependant, de nombreuses entreprises atteignent maintenant le point de rupture. La nécessité de disposer d'une solution de gestion des identités et des accès dans le Cloud mobile devient évidente pour l'équipe informatique dans les situations suivantes :

- Elles en sont à la quatrième ou cinquième application et les tickets de support s'accumulent.
- Une « violation » par un ancien collaborateur disposant toujours des droits d'accès est signalée.
- La branche d'activité pousse le département informatique à simplifier l'expérience utilisateur, car l'accès mobile, bien que stratégique, est trop fastidieux.

GESTION DES IDENTITÉS ET DES ACCÈS

✓ **Permet aux collaborateurs d'être productifs en levant les obstacles traditionnels liés à la mobilité (VPN, mots de passe multiples, jetons et utilisation d'ordinateurs portables et de terminaux mobiles non gérés ou non joints au domaine).**

✓ **Améliore la sécurité en renforçant l'authentification pour les applications au-delà des mots de passe tout en simplifiant l'expérience utilisateur.**

✓ **Permet à l'entreprise de déployer de nouveaux services et applications et de se développer en toute confiance, de façon naturelle ou non, en ayant l'assurance que les systèmes informatiques peuvent immédiatement prendre en charge les nouveaux utilisateurs.**

Vous souhaitez en savoir plus ?

VMware Workspace ONE vous permet de libérer le potentiel d'un espace de travail numérique en conjonction avec une gestion des identités et des accès totalement intégrée. Cette solution met en œuvre l'accès évolutif et conditionnel dont vous avez besoin pour garantir le niveau de sécurité approprié, basé sur le niveau de sécurité de l'authentification, la sensibilité des données, l'emplacement des utilisateurs et la position des terminaux. L'intégration parfaite de la gestion des identités et des accès dans la solution Workspace One vous permet de facilement moderniser vos opérations informatiques pour l'ère du Cloud mobile.

La création d'une stratégie complète d'espace de travail numérique est la solution qui permet de gérer l'accès des utilisateurs depuis un même emplacement, en permettant à ceux-ci de s'abonner aux applications dont ils ont besoin, tandis que le département informatique conçoit des règles d'accès centralisées en fonction de l'utilisateur et du type de terminal.

Chez VMware, nous rejetons l'idée que la sécurité et l'utilisabilité s'excluent mutuellement. Il ne faut pas opposer les utilisateurs au département informatique, mais plutôt associer la simplicité d'utilisation et la sécurité de l'entreprise dans l'espace de travail numérique.

Essayez le laboratoire d'essai en ligne VMware pour la simplification de la gestion des accès et des applications

Rejoignez-nous en ligne :

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin 100-101 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.fr