Smart Containerization

Une technologie unique de gestion des caractéristiques de sécurité, de performances, de conformité et de support de tout type de périphérique, d'application, de contenu ou de courriel, qui préserve la qualité de l'expérience utilisateur mobile

Nagi Prabhu
James Rendell

ca technologies

Introduction : qu'est-ce que la « conteneurisation » ?

con·te·neu·ri·sa·tion [kɔ̃·t(ə)·nœ·ʀi·za·sjɔ̃]

N. f. *Transport*.
Méthode de transport des marchandises dans des conteneurs relativement uniformes, scellés et mobiles dont le contenu ne doit pas être déchargé à chaque point de transit.

La technique de la conteneurisation a été inventée au XXe siècle dans le transport maritime afin de rendre le transport de marchandises plus simple, plus rapide, plus sûr et plus efficace. Cette technique implique de séparer les marchandises par type pour ensuite les placer dans des conteneurs de taille uniforme et les transporter à l'aide de différentes méthodes. Bien qu'ils soient de taille uniforme, chaque conteneur est traité différemment en fonction de son contenu. Par exemple, certains conteneurs peuvent être réfrigérés, tandis que d'autres peuvent nécessiter le contrôle de l'humidité. Un conteneur peut quitter une usine par camion et être transféré sur un wagon, puis sur un bateau et enfin sur une péniche. Le transfert de marchandises non conteneurisées peut avoir comme conséquences le vol, une perte d'efficacité et un accroissement considérable des coûts de transport.

Ces principes ont été adoptés dans la mobilité en entreprise afin d'isoler les données de l'entreprise sur un périphérique mobile. Ainsi, toutes les données de l'entreprise sont placées dans un « conteneur » de manière à les séparer des données propres aux utilisateurs. De cette façon, les entreprises peuvent autoriser leurs employés à utiliser leurs appareils, applications et données comme bon leur semble, en appliquant cependant des règles de sécurité sur le conteneur afin d'assurer la protection permanente des données qui s'y trouvent.

Plusieurs fournisseurs de solutions de mobilité ont tenté d'implémenter cette technique en apparence simple de différentes manières et avec plus ou moins de succès, sans toutefois que l'une de ces solutions parvienne à vraiment s'imposer. Certaines de ces technologies sont décrites ci-dessous.

A. Utilisation d'une application unique sur le périphérique

Cette implémentation implique le recours à une application propriétaire spécialisée unique pour l'accès à toutes les applications de l'entreprise, avec des applications PIM (Personal Information Management, gestion des informations personnelles) mobiles fondamentales communes, telles que le courrier électronique, le calendrier, les contacts, etc., dupliquées dans un format propriétaire au sein de l'application-conteneur. Ces applications « parallèles » obligent l'utilisateur final à se familiariser avec de nouvelles interfaces utilisateur non natives pour les fonctions mobiles de base de messagerie, de courriel et de navigation sur le Web, ce qui rend cette forme de solution conteneurisée extrêmement impopulaire auprès des utilisateurs finaux.

Toutes les applications, quel que soit le type ou la sensibilité des données auxquelles elles ont accès, sont placées à l'intérieur de cette application-conteneur. Les applications intégrées au périphérique mobile ou d'autres applications tierces ne peuvent pas accéder au conteneur ni à son contenu. Une telle approche à l'aide d'un conteneur spécialisé est commercialisée comme une solution de sécurité se fondant sur la séparation des données de l'entreprise des données personnelles sur le périphérique, ce qui permet à l'entreprise la suppression du conteneur, et donc de toutes les données qu'il contient, en fonction des besoins.

Pour reprendre l'analogie du transport maritime, cette approche revient à créer un conteneur unique géant et à y placer tous les types de marchandises, qu'elles nécessitent un traitement spécial, soient périssables, requièrent une réfrigération, etc. Dans une telle approche, ce conteneur unique devient rapidement ingérable en raison de sa taille, est extrêmement difficile à charger et décharger et ne permet pas de prendre en charge les différents types de traitements exigés selon les marchandises. Par conséquent, les marchandises ne sont pas expédiées de cette façon dans le monde réel. De manière similaire, dans la mobilité en entreprise, cette approche ne permet pas de gérer les données et les applications de l'entreprise de manière flexible et granulaire.

B. Utilisation d'un accès à distance

Plusieurs éditeurs de logiciels se sont spécialisés dans la technologie d'accès à distance afin d'offrir une solution dans laquelle les données et les applications sont exécutées sur un ordinateur de bureau ou un serveur dans le data center et l'accès est fourni à l'ordinateur à travers le réseau en affichant l'interface utilisateur du PC natif sur l'écran mobile. La simple reproduction de l'interface utilisateur de l'ordinateur ou du serveur sur le périphérique mobile engendre la perte de tous les avantages et de la puissance de l'interface utilisateur native du périphérique mobile. De plus, la qualité de l'expérience utilisateur dépend entièrement de la qualité de la connexion réseau qui doit rester disponible durant toute l'utilisation de l'application distante. Du point de vue de la sécurité, l'hypothèse est qu'en exécutant les données et les applications uniquement au sein du data center et en ne transférant pas les données sur le périphérique mobile, tout risque de perte ou de vol de données disparaît.

En considérant encore une fois l'analogie avec le conteneur de transport maritime, cette solution équivaudrait à placer le chargement dans des conteneurs et à fournir un flux vidéo par webcam montrant le contenu du conteneur ainsi qu'un bras robotisé contrôlé à distance pour accéder aux marchandises. Cette solution n'apporte aucune valeur, les marchandises n'étant pas effectivement envoyées vers la destination où elles doivent être consommées.

C. Utilisation d'une solution « dual persona »

Certains fabricants de périphériques ont tenté d'implémenter la conteneurisation à l'aide d'une technologie connue sous le nom de « dual persona ». Dans cette méthode, les courriels, les applications et le contenu sont sécurisés en créant un conteneur sous la forme d'un environnement dupliqué sur le téléphone. Les utilisateurs sont contraints de conserver tous leurs courriels, applications et données personnels dans un environnement, tandis que l'entreprise utilise le deuxième environnement pour y stocker ses applications et données. Aucune interaction n'est permise entre les deux environnements. L'entreprise peut supprimer le deuxième environnement et, ce faisant, toutes les données et applications qu'elle a placées sur le périphérique.

Dans le cadre de notre analogie avec le transport maritime, cette solution revient à diviser un bateau en deux à l'aide d'une cloison épaisse et impénétrable. Le chargement est réparti des deux côtés de la cloison qui empêche tout déplacement entre les deux moitiés. Bien que la séparation semble être bénéfique, si une tâche requiert des marchandises des deux côtés, une personne devra faire la navette entre les deux parties pour réaliser la tâche.

D. Utilisation de la virtualisation

Les fournisseurs de services de virtualisation créent un conteneur sous la forme d'un « téléphone dans un téléphone ». Dans le système d'exploitation présent sur le périphérique mobile, un autre périphérique virtuel est créé afin d'héberger l'application et les données de l'entreprise. En supprimant le périphérique virtuel, l'application et les données de l'entreprise peuvent aisément être supprimées. Il était supposé que la virtualisation pourrait être appliquée à tous les périphériques et à tous les systèmes d'exploitation. Il s'avère toutefois que cette technique est incompatible avec la majorité des périphériques, tels que la plupart des implémentations Android et iOS Apple, où les fabricants correspondants empêchent les modifications de bas niveau nécessaires à la mise en œuvre de la virtualisation.

L'approche de la virtualisation peut être comparée au fait de placer un bateau à l'intérieur d'un autre plus grand. Outre les désagréments de devoir se déplacer entre les deux bateaux pour la réalisation de toute tâche, il s'agirait d'une utilisation très inefficace de l'espace. Le bateau hébergé à l'intérieur utiliserait de l'espace de chargement précieux du bateau principal. Il n'existe presque pas de bateaux conçus pour en abriter un autre et la plupart des bateaux ne disposeraient pas d'un excédent de puissance moteur suffisant pour déplacer la masse d'un bateau supplémentaire. Cette analogie s'applique également aux périphériques mobiles : rares sont ceux adaptés à la virtualisation et les répercussions sur la consommation des ressources du fait d'avoir un « téléphone dans un téléphone » sont trop importantes pour la plupart des appareils.

Bien que chacune des techniques de conteneurisation ci-dessus semble en apparence fondée sur un principe simple et direct, aucune d'entre elles n'offre une solution de gestion de la mobilité globale pour l'entreprise. En plus des points susmentionnés, les techniques de conteneurisation existantes présentent une multitude d'autres inconvénients inhérents :

Trop peu d'attention accordée à l'utilisateur : les solutions de conteneurisation existantes sont conçues uniquement pour répondre aux défis en matière de sécurité, passant complètement à côté de l'occasion de résoudre d'autres problèmes, tels que la gestion des performances, le support des applications et la gestion de l'expérience utilisateur. Une approche stratégique d'avenir pour la gestion de la mobilité garantit que les utilisateurs ont non seulement accès aux applications et aux données en toute sécurité, mais jouissent également d'une formidable expérience. Une étude de marché indique une tendance à la hausse des particuliers à posséder 2 voire 3 appareils simultanément. L'adaptation de l'expérience utilisateur n'en devient qu'encore plus critique lorsque les applications mobiles sont déployées sur des millions de périphériques sur plusieurs plates-formes.

Absence de granularité : le stockage de toutes les données dans un unique conteneur implique que toutes sont traitées de la même façon. Il n'existe ainsi qu'une seule règle de sécurité : celle appliquée au conteneur et par le conteneur. Étant donné que l'entreprise traite de nombreux types de données différents, chacun présentant des besoins de gestion et de sécurité spécifiques, l'approche basée sur une règle « passe-partout » est trop rigide pour une utilisation à l'échelle de l'entreprise.

Caractère non multicanal : les solutions actuelles de conteneurisation qui ne fonctionnent que sur des périphériques mobiles tels qu'iOS et Android ne sont généralement pas de nature multicanal. Dans une entreprise imaginaire où seuls les périphériques mobiles seraient autorisés, cela aurait pu ne pas représenter un problème. Toutefois, de plus en plus, les équipements mobiles ne sont qu'un des nombreux types de périphériques utilisés pour accéder aux applications et données de l'entreprise. Étant donné qu'elles fonctionnent dans un « silo mobile », ces solutions obligent l'entreprise a trouvé des solutions de sécurités supplémentaires séparées pour les autres types de périphériques utilisés dans l'entreprise, à savoir les ordinateurs portables, les PC de bureau, les compteurs intelligents, les caméras IP, etc.

Existence de frontières : dans notre monde de connexion en ligne permanente, caractérisé par une omniprésence des périphériques mobiles, la capacité de contrôler l'utilisation de données au sein et en dehors de l'entreprise revêt une importance capitale, car c'est précisément en dehors de l'entreprise que les données confidentielles sont exposées aux plus grands risques. En bref, les solutions de sécurité ne doivent pas connaître de frontières.

Donc, malgré le fait que ces solutions de conteneurisation de première génération soient commercialisées comme des outils de sécurité, leur gestion de la mobilité en entreprise manque singulièrement d'efficacité.

CA Smart Containerization™

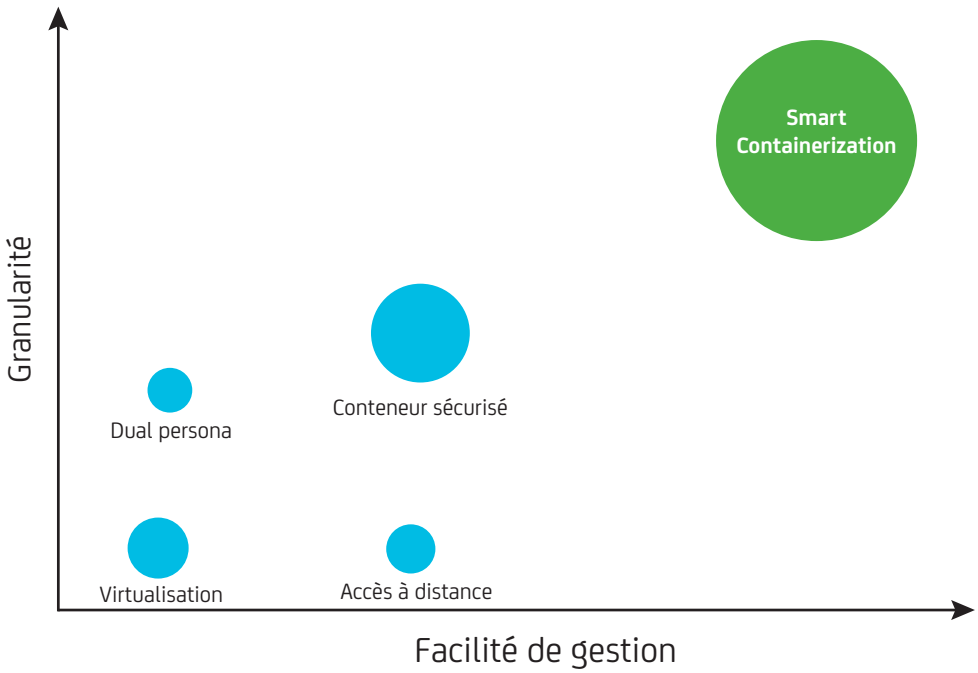
CA Management Cloud for Mobility utilise la technologie « Smart Containerization » de CA Technologies. Celle-ci associe une règle décrivant les exigences de sécurité, de performances et de support à du contenu, des courriels, des applications ou des périphériques spécifiques. Un fichier, un courriel, une application ou un périphérique unique est ainsi protégé dans un conteneur intelligent qui applique des règles appropriées au type de contenu géré. Par exemple :

- Une application mobile peut disposer d'une règle contrôlant où elle peut être exécutée (c.-à-d. un emplacement géographique ou un réseau Wi-Fi).
- Un courriel particulier peut se voir appliquer une règle de chiffrement sur la base de son contenu ou une règle l'empêchant d'être transféré en dehors de l'entreprise.
- Une règle peut être attribuée à un document pour que celui-ci ne puisse pas être stocké localement sur le périphérique.
- Une application peut être soumise à une règle recueillant et présentant les caractéristiques de performances du périphérique ou de ses propres performances.

La Smart Containerization résout les problèmes critiques des solutions de conteneurisation de première génération de la manière suivante :

- La Smart Containerization assure une *forte acceptation par l'utilisateur final* en fournissant une expérience utilisateur native sur le périphérique. L'application d'un traitement unique sur toutes les données et applications rend le conteneur très intrusif du point de vue de l'expérience utilisateur sur le périphérique. Le conteneur intelligent est transparent et maintient l'expérience utilisateur du périphérique dans sa forme native.
- La technologie CA Smart Containerization est par essence *multicanal*, couvrant tant les PC et les ordinateurs portables que les périphériques mobiles.
- La Smart Containerization est intrinsèquement dénuée de frontières car les règles suivent le flux des données, du contenu, des applications et des périphériques.

Ce graphique présente les performances des techniques de conteneurisation décrites ci-dessus par rapport aux critères énoncés.



La taille des bulles représente la diversité des éléments que le conteneur peut gérer.

- La Smart Containerization fournit le *contrôle granulaire* requis par les entreprises car le contenu, les courriels, les applications ou les périphériques sont en mesure de « se défendre eux-mêmes » et communiquent leurs propres exigences en matière de sécurité et de support au conteneur.
- Un conteneur intelligent permet tous les *domaines de gestion IT* qu'une entreprise souhaite exécuter sur le périphérique mobile, les données et les applications, qu'il s'agisse de la gestion des performances, de la sécurité, du support, de l'expérience utilisateur ou autres.

Si nous appliquons notre analogie de conteneur de transport maritime à la Smart Containerization, cette technologie équivaut à créer de multiples conteneurs, chacun optimisé pour différents chargements. De la sorte, les exigences de transport des marchandises peuvent être appliquées aux conteneurs spécifiques avec des attributs appropriés. Par exemple, de la crème glacée et de la viande peuvent être placées dans le même conteneur, puisqu'elles doivent toutes les deux être congelées, tandis que des légumes peuvent requérir un conteneur dont la température est contrôlée sans congeler les marchandises, puisque cela pourrait détruire les légumes, etc.

Les conteneurs intelligents offriraient de nombreux avantages au-delà de la simple protection du contenu :

- Ils pourraient fournir des contrôles de l'environnement adaptatifs, en matière notamment d'humidité, d'intensité lumineuse et de température sur la base de leur contenu.
- Les conteneurs intelligents pourraient optimiser leur consommation d'énergie en fonction des circonstances, telles que la température ambiante ou l'heure du jour.
- Les conteneurs intelligents pourraient déterminer les personnes autorisées à accéder à leur contenu, facilitant l'entrée des personnes autorisées dans les conteneurs tout en en refusant l'accès à toute autre personne.

De par leur caractère adaptatif, les conteneurs intelligents permettraient au transporteur de simplement placer le contenu dans le conteneur et de laisser à ce dernier le soin de se charger du contenu.

Les sections suivantes décrivent la manière dont les produits au sein de CA Management Cloud for Mobility implémentent et appliquent leurs responsabilités particulières en matière de règles à l'aide de la technologie Smart Containerization.

Périphériques : CA Mobile Device Management (MDM)

CA MDM gère l'inventaire et la configuration d'une multitude d'équipements mobiles, ainsi que de PC Windows, et assure une gestion distante de ces périphériques de manière sûre et évolutive. La Smart Containerization pour CA MDM commence au niveau du matériel du périphérique et de sa pile logicielle, en passant par un contrôle des règles granulaire centralisé et la configuration d'une multitude de fonctionnalités de périphérique, telles que caméra, accès réseau, contrôle GPS, etc.

Fonctionnalités des plates-formes des périphériques mobiles : une évolution intéressante dans l'univers de la mobilité réside dans le fait que les fabricants de périphériques mobiles assument de plus en plus leurs responsabilités en matière de sécurité, d'intégrité et de robustesse de la plate-forme qu'ils fournissent. Tout comme nous attendons d'une voiture qu'elle présente des caractéristiques de sécurité et de sûreté intégrées, les fabricants de périphériques mobiles répondent aujourd'hui aux attentes des consommateurs afin que ces périphériques fournissent également des fonctionnalités de sécurité appropriées.

Parmi celles-ci, il convient en particulier de citer les fonctionnalités de sécurité d'Apple dans l'iOS 7 et de Samsung For Enterprise (SAFE) et KNOX pour les appareils Android de Samsung.

La prise en charge par CA MDM des fonctionnalités de sécurité de l'iOS 7 d'Apple et des extensions de sécurité d'Android de Samsung permet d'appliquer la protection Smart Containerization à ces périphériques. Cela offre une base solide sur laquelle déployer des fonctionnalités de sécurité supplémentaires afin de contrôler l'utilisation des applications, du contenu et des courriels. Les fonctionnalités typiques proposées par ces plates-formes et pouvant être contrôlées de manière centrale via CA MDM sont notamment les suivantes.

Gestion de l'ouverture : dans l'iOS 7, CA MDM peut contrôler de manière centrale la liste des applications autorisées à ouvrir du contenu d'un type déterminé, que des applications complémentaires soient à la disposition de l'utilisateur ou non. Par exemple, si les normes de l'entreprise prévoient l'utilisation d'un logiciel de lecture de fichiers PDF spécifique, celui-ci peut être défini comme le seul logiciel de lecture pouvant ouvrir les fichiers PDF joints aux courriels, téléchargés via Safari, etc. Cela permet au périphérique iOS 7 de « conteneuriser de manière intelligente » des données sélectionnées dans des applications spécifiques contenues sur le périphérique.

Fonctionnalité VPN par application : permet de « conteneuriser de manière intelligente » une application dans un réseau déterminé sur iOS 7 et Android de Samsung. Par exemple, une application professionnelle peut être configurée pour démarrer automatiquement et ne s'exécuter que si une connexion VPN spécifique est disponible, empêchant de la sorte une application professionnelle sensible d'utiliser Internet de manière illimitée.

Contrôles d'applications avancés : les contrôles d'applications avancés sur Android de Samsung permettent à CA MDM de contrôler de manière centralisée l'installation et la suppression d'applications, ainsi que d'inclure des applications sur la liste noire et sur la liste blanche et de supprimer de manière centralisée les données d'une application.

Contrôles de provisioning des messageries : permettent la configuration et la suppression centralisées de comptes de messagerie.

Contrôles de fonctionnalités des périphériques : permettent l'administration centrale de composants matériels spécifiques, tels que le Bluetooth, le Wi-Fi et la caméra, de même que le chiffrement de stockage.

Authentification unique pour l'entreprise : permet l'intégration du périphérique mobile à Microsoft ActiveDirectory ou à un autre environnement d'authentification basé sur Kerberos.

Fonctionnalités de navigation sécurisée sur le Web : permettent l'établissement de listes noires et blanches pour les URL, ainsi que le contrôle centralisé des options de confidentialité du navigateur et l'application d'un proxy HTTP pour la navigation sécurisée sur Internet à partir du périphérique mobile.

CA MDM peut contrôler la distribution d'applications vers des périphériques mobiles via un magasin d'applications de l'entreprise. En association avec CA Mobile Application Management, CA MDM peut distribuer des applications d'entreprise conteneurisées de manière intelligente vers des périphériques mobiles.

CA MDM prend également en charge de nombreuses autres plates-formes de périphériques, dont Windows Phone 8, BlackBerry et tous les autres périphériques génériques basés sur Android (Android 2.2 et supérieur).

La technologie Smart Containerization via CA MDM permet à une entreprise d'appliquer des règles de sécurité robustes et granulaires, quel que soit le type de périphérique utilisé.

Applications : CA Mobile Application Management (MAM)

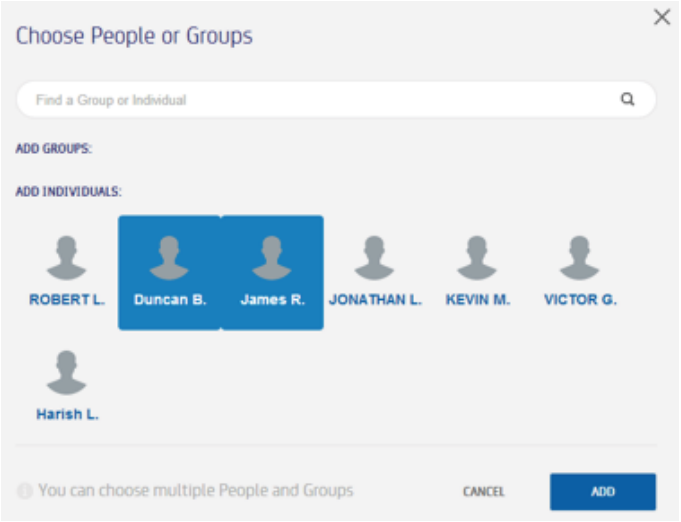
CA MAM permet un contrôle avancé et granulaire de l'utilisation des applications sur le périphérique mobile et de la disponibilité de fonctionnalités de périphériques spécifiques pour chaque application mobile. Chaque application est « encapsulée » à l'aide d'un conteneur intelligent qui lui applique un contrôle de règle granulaire.

Le diagramme de droite illustre la manière dont la technologie Smart Containerization est appliquée de façon sélective aux deux applications sur un périphérique mobile :

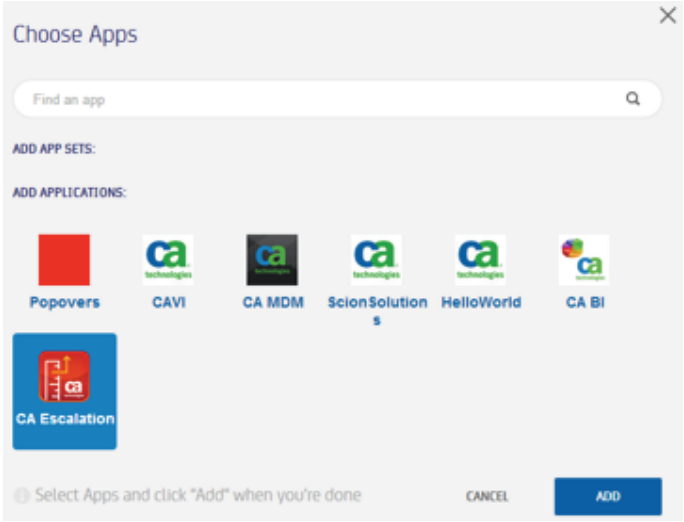
- L'application CA Corporate Escalation est munie d'une règle spécifiant qu'elle ne peut être exécutée que lorsque le périphérique se trouve au siège de CA Islandia ou au siège de CA Ditton Park EMEA et que l'accès à la caméra est autorisé mais pas le copier/coller à partir de l'application.
- L'application CA Business Intelligence, une application d'analyse et de reporting, est équipée d'une règle précisant qu'elle ne peut être exécutée que durant les jours ouvrables, peut accéder à Internet et que ses données peuvent faire l'objet d'un copier/coller.

Les règles de conteneurisation intelligente de la gestion des applications mobiles permettent de nombreux contrôles granulaires des applications :

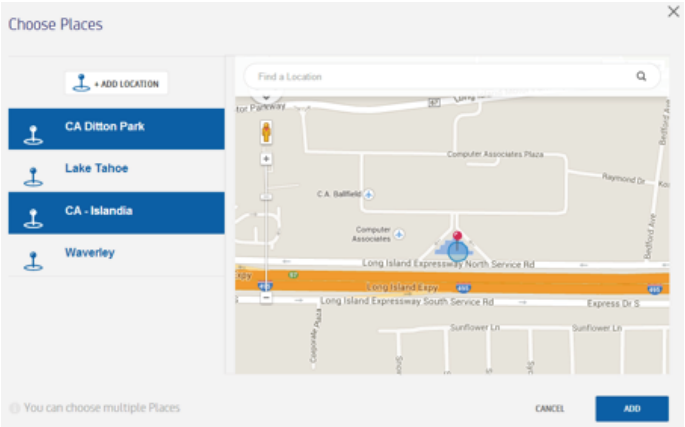
Identité : les utilisateurs et groupes spécifiques autorisés à exécuter une application ou auxquels l'exécution en est interdite.



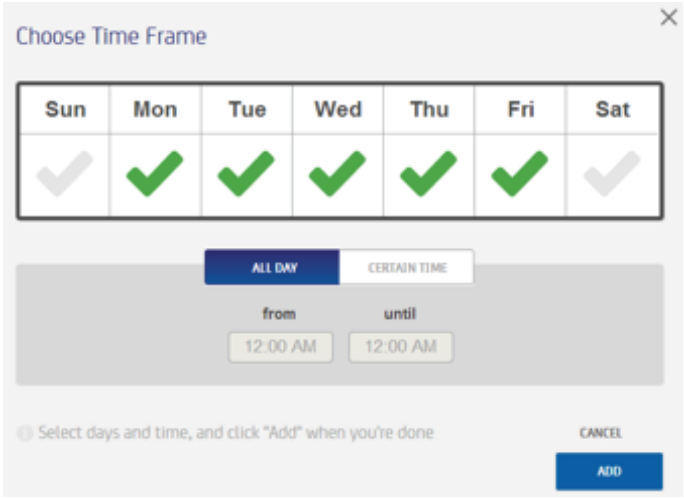
Applications : les applications spécifiques auxquelles la règle est liée.



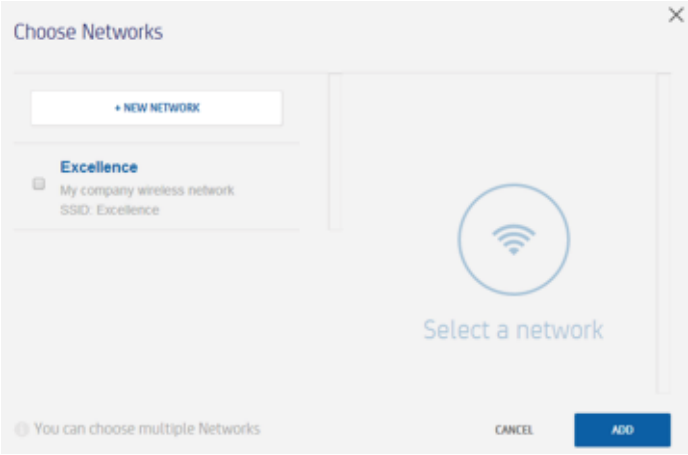
Géolocalisation : une application peut être configurée pour ne s'exécuter que lorsque le périphérique se trouve à un endroit spécifique ou pour empêcher son exécution lorsque le périphérique se trouve à un endroit spécifique.



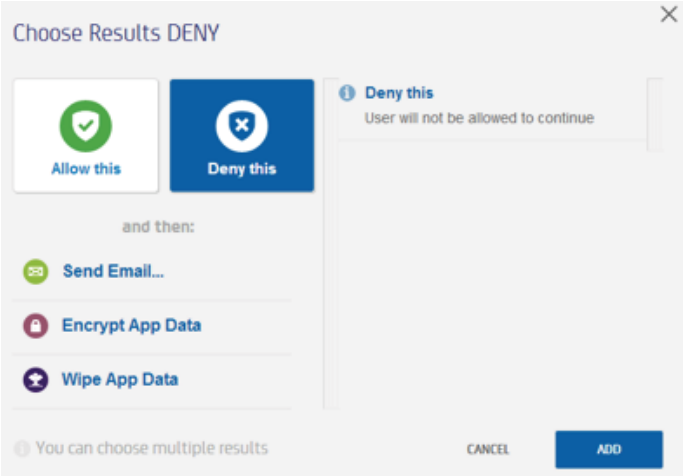
Fenêtres horaires : les périodes durant lesquelles une application peut ou ne peut pas être exécutée.



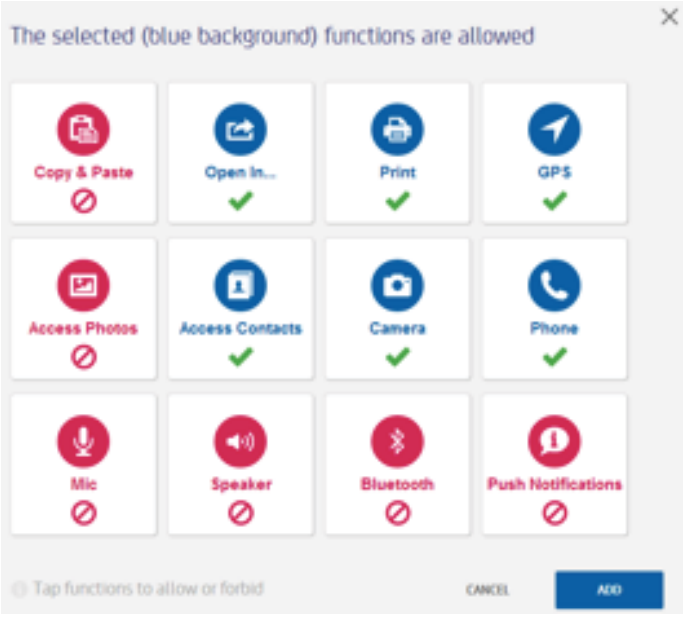
Réseau : une application peut être « verrouillée » de manière explicite sur un segment de réseau Wi-Fi spécifique, p. ex. une application ne peut être utilisée que lorsqu'elle se trouve sur le réseau Wi-Fi de l'entreprise.



Suppression sélective : lorsque l'accès à une application est interdit, il existe des options supplémentaires pour verrouiller l'accès à l'application et pour supprimer de manière permanente, mais sélective, toute donnée stockée sur le périphérique par l'application.



Fonctionnalités : l'accès d'une application à de nombreuses fonctionnalités du périphérique peut être activé ou désactivé, p. ex. copier/coller, GPS, caméra, contacts, etc.

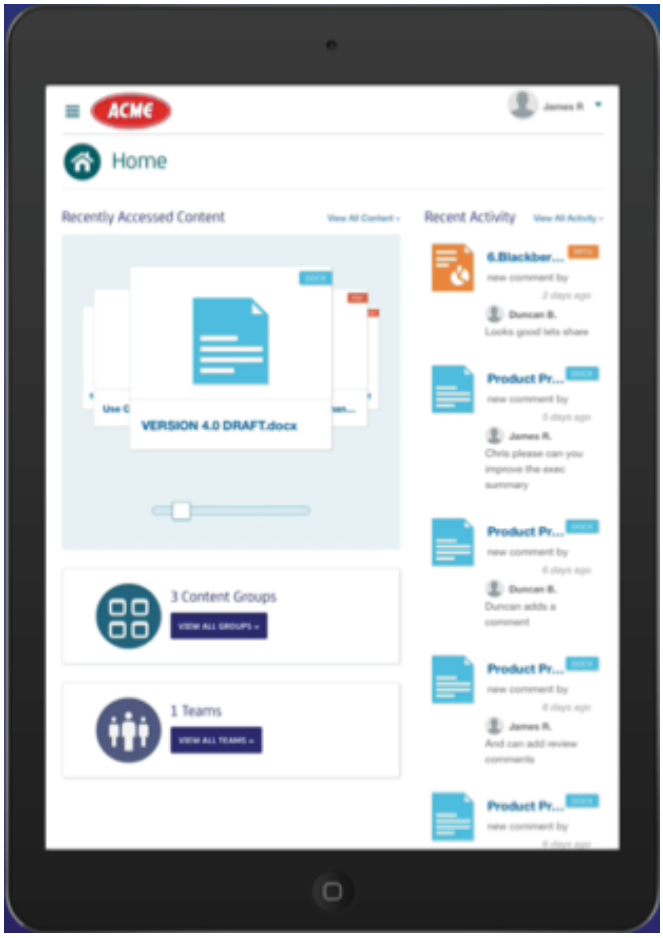


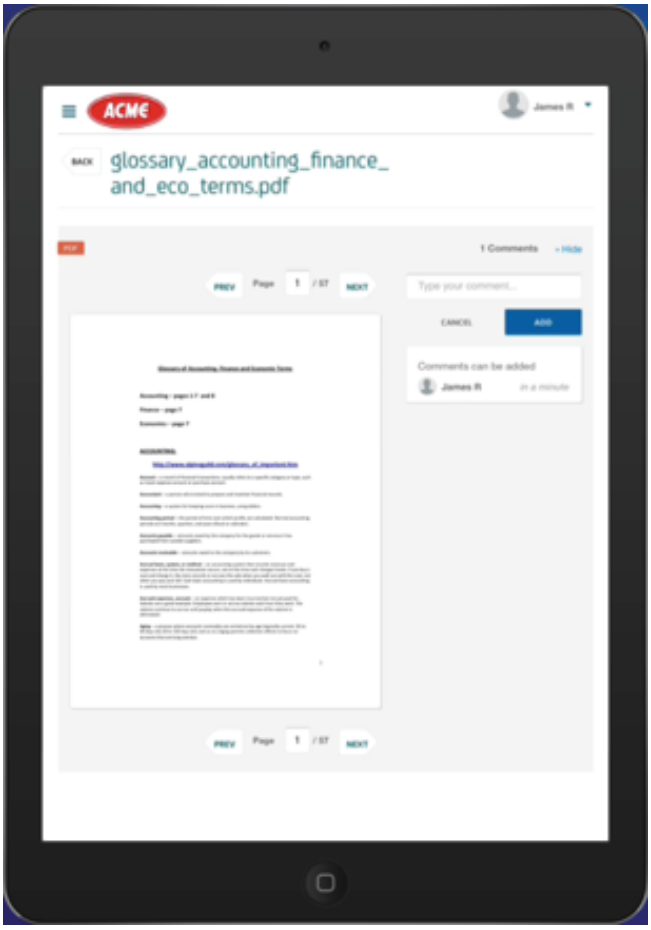
La technologie Smart Containerization par encapsulation d'application à l'aide de CA MAM est un complément idéal aux fonctionnalités de sécurité des périphériques. Lorsque le périphérique utilisé *ne fournit pas* de fonctionnalités de sécurité de plate-forme spécifiques, CA MAM ajoute une couche de contrôle bien nécessaire. Lorsque le périphérique fournit des fonctionnalités de sécurité intégrées, CA MAM ajoute à l'application des contrôles de sécurité non proposés via les fonctions de sécurité propres à l'appareil.

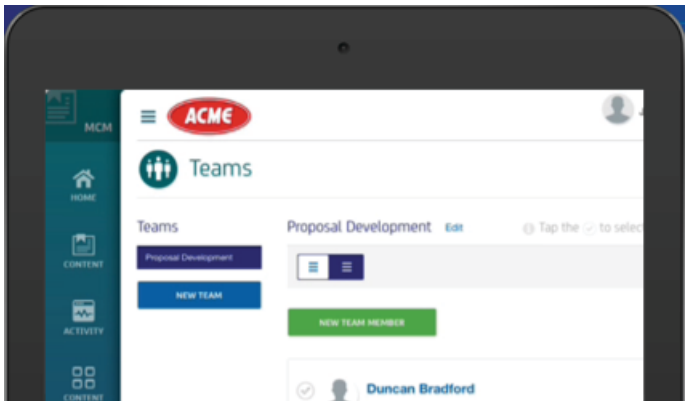
Contenu : CA Mobile Content Management (MCM)

CA MCM fournit une plate-forme afin de permettre une collaboration sécurisée où le contenu est partagé entre des utilisateurs avec des périphériques mobiles et non mobiles.

CA MCM applique la protection Smart Containerization aux données sur le périphérique mobile pour garantir que seuls les utilisateurs autorisés peuvent consulter le contenu et pour empêcher l'utilisation non autorisée de contenu sensible en interdisant la copie locale et le copier/coller de contenu.







Le propriétaire du contenu peut contrôler les personnes pouvant y accéder. Les utilisateurs autorisés du contenu ont la possibilité de faire des commentaires sur le contenu en temps réel. Les mises à jour du contenu sont disponibles instantanément aux utilisateurs autorisés.

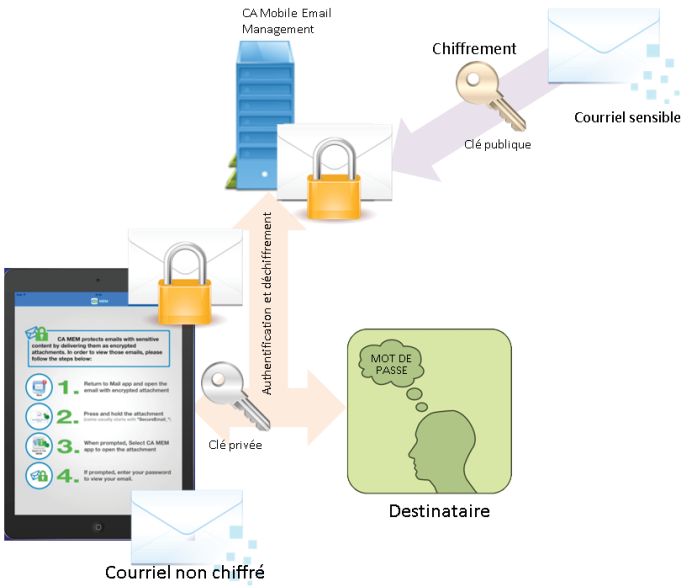
CA MCM gère les connexions back-end à de multiples magasins et référentiels de données, tels que des services de partage de fichiers dans le Cloud, des systèmes de gestion de contenu de l'entreprise comme SharePoint et des applications SaaS courantes comme Salesforce.com.

La technologie Smart Containerization résout un problème traditionnel obligeant à sécuriser séparément différents référentiels back-end (messagerie, partage de fichiers, téléchargement Web, etc). Dans cet environnement hérité, les attributs de sécurité étaient définis en fonction du canal (messagerie, autorisations de partage de fichiers, autorisations d'applications Web, etc.) et peuvent ne pas être cohérents entre les canaux ou appropriés au contenu. La technologie Smart Containerization via CA Mobile Content Management rend les référentiels back-end abstraits pour l'utilisateur et applique une règle de sécurité directement à l'élément de contenu spécifique, plutôt que de déterminer la règle sur la base du référentiel dans lequel il a été stocké.

Bien que CA MCM offre aux utilisateur un moyen plus sûr de partager du contenu sensible et de collaborer qu'en envoyant celui-ci par courriel, la messagerie électronique conserve naturellement un rôle vital au sein de l'entreprise. C'est pourquoi la gestion sécurisée de contenu via la plate-forme CA MCM est complétée par CA Mobile Email Management, une plate-forme permettant la protection des courriels sensibles.

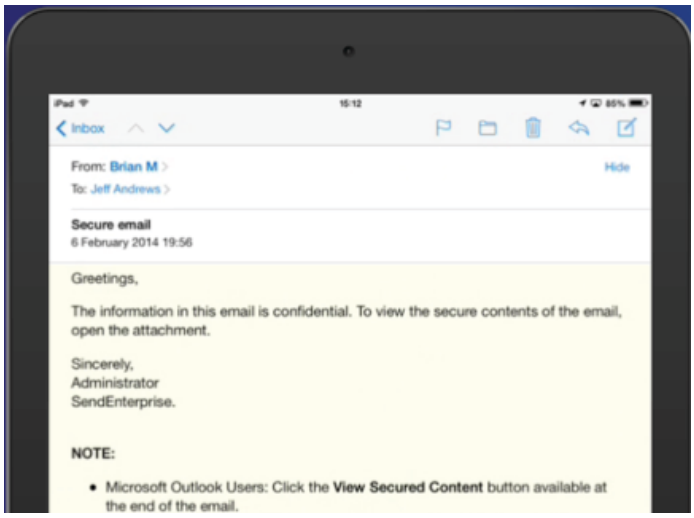
Courriel : CA Mobile Email Management (MEM)

Comme nous l'avons fait remarquer dans l'introduction, la technologie Smart Containerization peut être appliquée à un courriel unique, ainsi qu'à une application ou à un document unique. CA MEM applique le chiffrement par clé publique basé sur des règles aux courriels ayant été identifiés comme contenant des données sensibles. De nombreux courriels échangés par des utilisateurs ne sont pas effectivement sensibles. Un courriel contient souvent des informations non sensibles, insignifiantes ou disponibles publiquement et l'application de protection à de tels courriels est un gaspillage de ressources et est gênante pour l'utilisateur. Par exemple, dans le modèle de conteneurisation simple, il peut arriver qu'un utilisateur ouvre un client de messagerie spécial afin d'accéder à ses courriels professionnels juste pour découvrir un nouveau message portant sur un événement social d'équipe !



En revanche, CA MEM chiffre uniquement les courriels sensibles. Le chiffrement est fondé sur la clé publique des destinataires et le destinataire doit s'authentifier à l'aide de la clé privée correspondante pour déchiffrer le courriel.

La technologie Smart Containerization à l'aide de CA MEM résout des problèmes critiques posés par la conteneurisation simple de différentes façons :

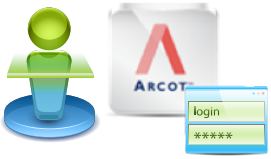


Expérience client native : comme mentionné dans l'introduction, les utilisateurs finaux sont très réticents envers les solutions de sécurité qui les obligent à utiliser un client propriétaire séparé dupliquant les fonctions de base du périphérique mobile. CA Mobile Email Management s'intègre au client de messagerie natif du périphérique mobile, qui fournit une expérience utilisateur bien plus satisfaisante.

Interplate-forme : CA Mobile Email Management s'intègre aux services de messagerie Web et aux clients de messagerie Outlook, fournissant de la sorte une fonctionnalité de conteneurisation intelligente des courriels sur tout périphérique à la disposition de l'utilisateur pour l'accès aux courriels. Si le périphérique est connecté à Internet, CA MEM peut le prendre en charge.

Sans frontières : CA MEM peut chiffrer des courriels pour les utilisateurs qui ne sont pas encore enregistrés, générant une paire de clés publique/privée et maintenant les clés en dépôt, ainsi que le courriel chiffré, jusqu'à l'enregistrement de l'utilisateur. De plus, la solution fonctionne de manière transparente au sein et en dehors de l'entreprise. Les utilisateurs externes sont tout aussi capables de s'inscrire sur le système pour la gestion de contenu de courriel sensible que les utilisateurs de l'entreprise. La capacité de fournir des règles de protection qui s'appliquent au courriel indépendamment de l'appartenance de l'utilisateur à l'entreprise afin que la règle de sécurité soit appliquée est un avantage clé de la technologie Smart Containerization.

Authentification multifacteur : comme illustré ci-dessus, le périphérique mobile devient donc un facteur d'authentification à part entière. Cela constitue une preuve d'identité robuste lors de l'accès à du contenu électronique sensible.



Résumé

La conteneurisation a vu le jour en tant qu'approche simple pour la sécurisation des données de l'entreprise sur le périphérique mobile. Toutefois, sa simplicité s'est également accompagnée d'un certain nombre de points faibles critiques en termes de granularité pour les exigences de l'entreprise d'aujourd'hui et de robustesse vis-à-vis des menaces avancées émergentes. De plus, sa portée limitée à la gestion de données uniquement sur des périphériques mobiles au sein de l'entreprise représentait une restriction trop importante pour les exigences stratégiques des entreprises modernes. En ajoutant à ces problèmes d'entreprise le fait que les utilisateurs finaux détestent la façon dont ces technologies de conteneurisation les forcent à abandonner l'expérience utilisateur native des périphériques mobiles, il n'est pas difficile de comprendre pourquoi les entreprises attendent avec impatience l'émergence d'une technologie de remplacement.

La technologie Smart Containerization par CA Technologies est la seule à fournir la meilleure expérience d'interface utilisateur que réclament les utilisateurs finaux et propose des fonctionnalités de sécurité avancées telles que le support des dernières fonctionnalités de sécurité de plates-formes, des avantages de gestion complète au-delà de la sécurité et l'authentification multifacteur robuste. Elle est en outre véritablement dénuée de frontières et multicanal, prenant en charge des périphériques mobiles, ainsi que non mobiles.

Pour plus d'informations sur la technologie Smart Containerization de CA Technologies, prenez contact avec votre équipe de gestion de compte CA ou rendez-vous sur le site **ca.com/fr/mobility**.

ca technologies

Restez connecté à CA Technologies sur ca.com/fr

Avantages de CA Technologies

CA Technologies (NASDAQ : CA) fournit des solutions de gestion des systèmes d'information qui aident les clients à gérer et à sécuriser des environnements informatiques complexes pour supporter des services métier agiles. Les organisations s'appuient sur les logiciels et les solutions SaaS de CA Technologies pour accélérer l'innovation, transformer leur infrastructure et sécuriser les données et les identités, du cœur des data centers jusqu'au Cloud. CA Technologies s'engage à ce que ses clients atteignent les résultats souhaités et la valeur métier attendue **ca.com/fr/customer-success**. Pour plus d'informations sur CA Technologies, rendez-vous sur le site **www.ca.com/fr**.

 CS200-65290_0414