CONSIDÉRATIONS DE SÉCURITÉ POUR LES MODÈLES DE DÉPLOIEMENT DE DISPOSITIFS MOBILES

JUIN 2020 **ITSAP.70.002**

Quand vous décidez d'une approche pour déployer des dispositifs mobiles dans votre organisme, vous pouvez choisir parmi différents modèles de déploiement ayant chacun leurs avantages et leurs risques. Pour ce qui est des dispositifs mobiles, la gestion des risques dépend en partie de la collaboration de l'employé (c.-à-d. sa volonté de permettre à l'organisme d'établir des restrictions d'utilisation ainsi que des modalités de surveillance et d'accès de sécurité) et en partie des risques et des vulnérabilités liés aux types de dispositifs offerts. Afin de choisir un modèle de déploiement qui équilibre le mieux ces éléments pour votre organisme, considérez l'expérience utilisateur, la confidentialité et les exigences de sécurité.

MODÈLES DE DÉPLOIEMENT

Voici votre appareil réservé au travail (VART) : Le dispositif appartient à votre organisme et peut seulement servir à des fins opérationnelles.

Voici votre appareil personnel (VAP) : Le dispositif appartient à l'organisme qui s'occupe de la surveillance et des contrôles du dispositif. Ce modèle permet à votre organisme de mettre en place des stratégies de sécurité plus strictes. Les employés peuvent utiliser leur dispositif à des fins personnelles, et vous pourriez les laisser choisir le type de dispositif utilisé.

Prenez vos appareils personnels (PAP) : Les employés utilisent leurs dispositifs à des fins opérationnelles, et vous pouvez décider de rembourser certains coûts associés aux dispositifs. Toutefois, puisque le dispositif n'appartient pas à votre organisme, vous avez peu d'emprise sur les contrôles de sécurité mis en place sur le dispositif.

AVANTAGES ET RISQUES

Il y a des avantages et des risques associés à chacun de ces modèles de déploiement. Les deux tableaux ci-dessous présentent des exemples d'avantages et de risques à considérer, et indiquent si ces exemples s'appliquent (✓) ou non (**x**) au modèle de déploiement.

Toutefois, ces avantages et ces risques peuvent différer selon les besoins et les exigences en sécurité de votre organisme ainsi que selon les utilisateurs. En ce qui concerne les avantages et les risques liés à chacun des modèles de déploiement, vous devriez aussi considérer le modèle qui permettra à votre organisme d'établir un équilibre entre la fonctionnalité, l'expérience utilisateur et la sécurité.

EXEMPLES D'AVANTAGES	VART	VAP	PAP
Améliore la satisfaction au travail	✓	✓	✓
Améliore l'efficacité et la flexibilité au travail (p. ex., travail à distance)	✓	✓	✓
Offre un dispositif pouvant être utilisé à des fins opérationnelles et personnelles	x	✓	✓
Réduit le coût du matériel	x	x	✓
Contrôle les mises à jour du dispositif	✓	✓	x
Offre l'option de travailler à distance	✓	✓	✓

EXEMPLES DE RISQUES	VART	VAP	PAP
Manque de contrôle de la gestion (p. ex., peu de contrôle sur les mises à jour et sur les téléchargements de logiciels)	x	x	✓
Télécharge des applications malveillantes (p. ex., les pirates informatiques peuvent obtenir l'accès à des données opérationnelles)	✓	✓	✓
Utilise des dispositifs de façon non sécuritaire (p. ex., l'employé accède à de l'information sur un Wi-Fi public ou il laisse d'autres personnes utiliser le dispositif)	✓	✓	✓
Permet la modification des fonctions de sécurité (p. ex., le débridage du dispositif permet de déverrouiller les restrictions de configuration)	x	x	✓
Perd des données (p. ex., le stockage de données personnelles et opérationnelles sur le même dispositif peut mener à des fuites de données)	x	✓	✓

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

MESURES D'ATTÉNUATION DES RISQUES

Il existe plusieurs façons d'atténuer les risques que représentent les dispositifs mobiles pour votre organisme. Certains modèles de déploiement permettent de mettre en œuvre un plus grand nombre de mesures d'atténuation que d'autres modèles.

La plupart des risques liés au modèle PAP sont incontrôlables puisque le dispositif appartient à l'employé. Les dispositifs appartenant à l'organisme permettent de mieux gérer les risques. Dans le modèle VART, le dispositif sert uniquement à des fins opérationnelles et votre organisme exerce un contrôle complet sur les données du dispositif et les stratégies de sécurité utilisées. Le modèle VAP offre une combinaison des points positifs du modèle PAP et du modèle VART : les employés peuvent utiliser les dispositifs à des fins personnelles, mais votre organisme contrôle les mesures de sécurité mises en place.

Le tableau ci-dessous énumère les exemples de mesures d'atténuation et indique si ces mesures s'appliquent (✓) ou non (**x**) au modèle de déploiement.

EXEMPLES DE MESURES D'ATTÉNUATION DES RISQUES	VART	VAP	PAP
Exige l'utilisation de mots de passe robustes et de mécanismes d'authentification	✓	✓	x
Veille à la mise en place de contrôles de sécurité (p. ex. gestion unifiée des terminaux [UEM pour *Unified endpoint management*])	✓	✓	x
Limite l'information partagée entre les dispositifs	✓	✓	x
Offre un soutien TI pour les dispositifs	✓	✓	x
Utilise des logiciels conçus et autorisés par l'organisme	✓	✓	x
Permet d'accéder aux applications de travail en utilisant l'infrastructure réseau de l'organisme	✓	✓	✓
Permet de mettre en place un plan de départ pour les employés (c.-à-d. les dispositifs et les données sont gérés quand un employé quitte l'organisme)	✓	✓	x

GESTION UNIFIÉE DES TERMINAUX

Votre organisme peut utiliser la gestion unifiée des terminaux (UEM pour *Unified Endpoint Management*) pour assurer la sécurité des dispositifs mobiles. Si votre organisme adopte le modèle PAP, vous pouvez utiliser l'UEM, mais votre capacité à gérer les dispositifs sera minime puisque ces derniers appartiennent aux employés. Dans les modèles VAP ou VART, vous pouvez utiliser l'UEM puisque vous avez le contrôle complet sur la surveillance et la sécurité des dispositifs.

L'UEM est une stratégie qui distribue, gère et contrôle les dispositifs de point de terminaison (p. ex., les dispositifs de bureau et les dispositifs mobiles) dans le lieu de travail. Elle combine des caractéristiques provenant des processus de gestion des dispositifs mobiles et de la mobilité d'entreprise afin de répondre aux préoccupations de sécurité liées à la gestion des données opérationnelles tout en augmentant la connectivité et la productivité. L'UEM inclut des fonctionnalités qui aident à assurer la sécurité de l'information opérationnelle et des données des employés. Ces fonctionnalités comprennent notamment :

- la surveillance continue des dispositifs (p. ex., sur place ou à distance);
- la séparation des plateformes d'application (p. ex., mise en bac à sable);
- l'application de justificatifs d'authentification robustes (p. ex., l'utilisation de clés différentes entre les dispositifs personnels et les ordinateurs de bureau);
- l'intégration de services de messagerie;
- la préparation des dispositifs pour la configuration et l'inscription;
- le chiffrement des données inactives et en transit;
- l'exécution à distance de la surveillance, du verrouillage et de la réinitialisation;
- la détection de dispositifs débridés;
- la mise à jour automatique des correctifs de sécurité et des antimaliciels;
- la mise sur liste blanche et la mise sur liste noire des applications.

CONSIDÉRATIONS POUR VOTRE ORGANISME

Votre organisme doit choisir le modèle de déploiement qui s'applique le mieux à ses besoins opérationnels en considérant les éléments suivants :

- le niveau de contrôle nécessaire selon la sensibilité des données traitées;
- le budget disponible pour chacun des modèles de déploiement (p. ex., l'approvisionnement en matériel et le soutien TI);
- le meilleur équilibre entre vie professionnelle et vie personnelle.

Il est important que votre organisme forme ses employés sur les meilleures pratiques de sécurité et de confidentialité afin d'assurer une utilisation sécuritaire selon le modèle de déploiement choisi par votre organisme.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.