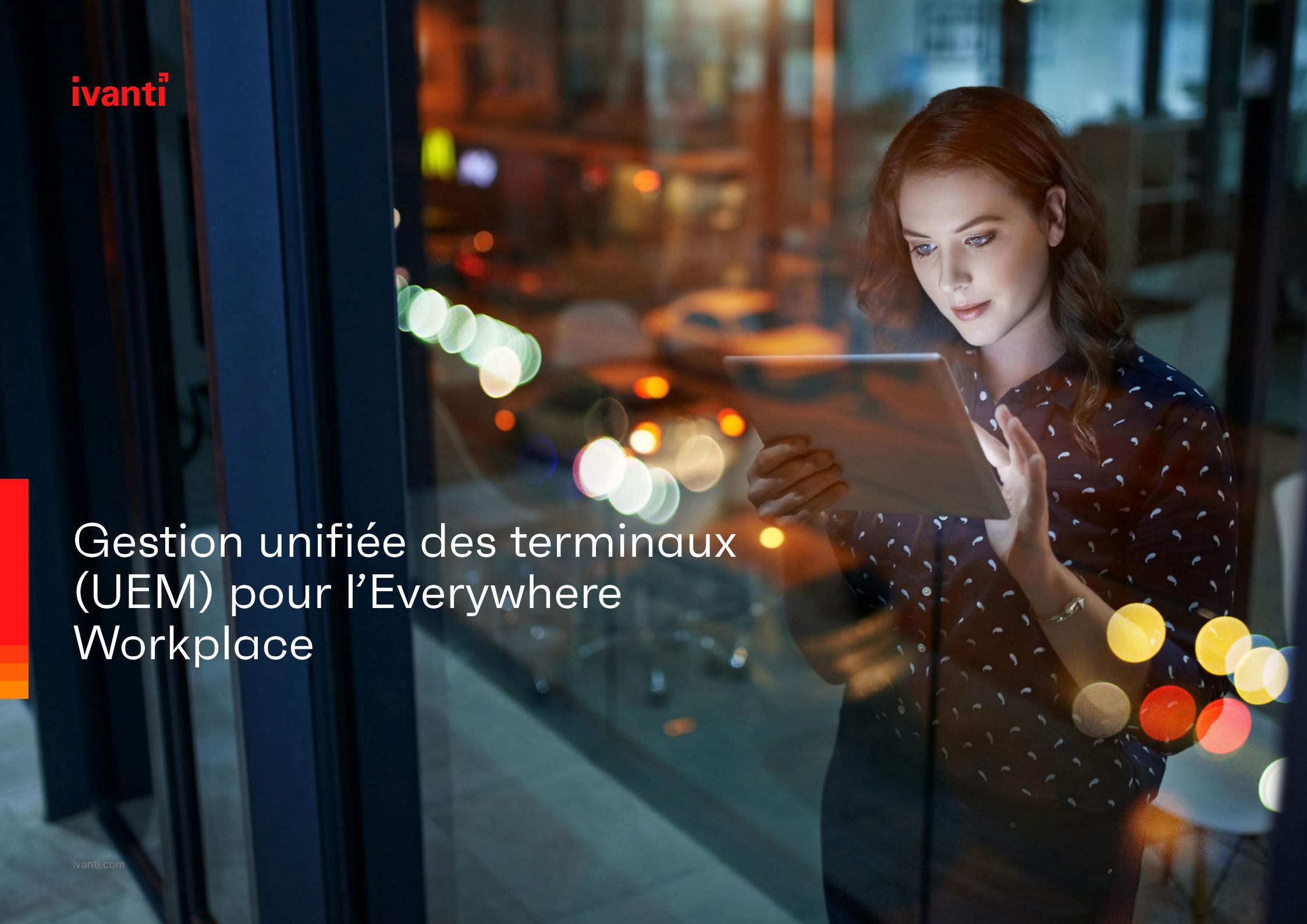


ivanti

# Gestion unifiée des terminaux (UEM) pour l'Everywhere Workplace

## Table des matières



## Introduction

La mobilité et la consumérisation de l'IT sont devenues la norme dans l'entreprise. Concrètement, les collaborateurs souhaitent pouvoir travailler partout et à tout moment sur différents périphériques : ordinateurs de bureau, ordinateurs portables, tablettes, smartphones. Et c'est encore plus vrai dans l'Everywhere Workplace. À une époque, les tâches « sérieuses » étaient réalisées sur un ordinateur de bureau ou portable, et les collaborateurs avaient une utilisation limitée de leurs périphériques mobiles. Ils les utilisaient par exemple pour traiter leurs emails lorsqu'ils étaient en déplacement ou en télétravail. Aujourd'hui, ils souhaitent pouvoir accéder aux mêmes informations, exécuter la plupart des applications et services, et traiter tout type de tâche sur leurs périphériques professionnels et personnels. La frontière entre PC et périphériques mobiles a bel et bien disparu.

Cette nouvelle donne représente un vrai défi pour l'entreprise, mais aussi une réelle opportunité. Commençons par le défi : le département IT doit mettre en place des stratégies de gestion et de sécurisation des applications et des informations sensibles pour chaque périphérique, sans que cela se fasse au détriment de la productivité de l'utilisateur et en respectant ses préférences en matière d'utilisation. Malgré les efforts entrepris par les entreprises, des disparités de traitement existent entre les terminaux mobiles et les postes traditionnels.

Quels sont les risques ? Les départements IT s'exposent à des menaces et à des fuites de données. Sans contexte sur l'identité de l'utilisateur, ses périphériques et leur emplacement, ses expériences Zero Trust et collaborateur, l'IT est contraint de mettre en place "un confinement" pour éviter les risques susceptibles d'impacter la productivité.

La meilleure façon d'anticiper ces risques est de doter l'IT d'une solution capable d'ajuster automatiquement la stratégie de sécurité pour chaque collaborateur, de surveiller proactivement le réseau et d'alerter sur des dangers potentiels.

## La gestion des périphériques à l'ère des fuites de données

Dans la plupart des entreprises, l'IT a mis en place un ou plusieurs systèmes de gestion pour les ordinateurs portables et de bureau. Les périphériques mobiles tels que les smartphones et les tablettes sont quant à eux traités avec un système de gestion séparés, relèvent de fournisseurs distincts et de stratégies différentes. Dans ce type de situation, le département IT désigne généralement deux personnes différentes, respectivement chargées de la gestion des périphériques mobiles et des postes de travail traditionnels.

Alors que les fuites de données gagnent en fréquence et en gravité, cette approche présente de sérieuses faiblesses. En effet, les périphériques mobiles ainsi que les applications et données d'entreprise qu'ils contiennent sont des vecteurs de risques. Les malwares mobiles constituent fréquemment un point d'entrée dans le réseau de l'entreprise. Vol ou perte de périphérique, infiltration de malwares : nombreux sont les dangers qui menacent les entreprises n'ayant pas mis en place une gestion uniformisée des terminaux.

### Une expérience utilisateur commune

La multiplicité de stratégies et d'applications de gestion ne permet pas d'offrir une expérience UX satisfaisante et commune sur l'ensemble des périphériques. Des opérations comme l'onboarding, le provisioning et le dépannage des périphériques multiples deviennent inutilement complexes et longues. C'est là qu'intervient la notion d'opportunité.

Sécurisez l'Everywhere Workplace avec une solution capable de découvrir et de gérer tous les périphériques de vos collaborateurs, du Cloud à la périphérie. Mettez en place un accès sécurisé Zero Trust avec automatisation contextuelle et fournissez une expérience personnalisée à chaque collaborateur, quel que soit l'endroit où il travaille. Les résultats : des gains significatifs en terme de productivité, vitesse opérationnelle, coûts et niveau de service.

### Des règles de stratégies communes à tous les utilisateurs

Protéger les informations sensibles et l'accès au réseau exige de définir des règles d'identification des utilisateurs et de sécurité strictes. La situation est d'autant plus complexe que les équipes IT sont confrontées à une utilisation accrue des périphériques mobiles.  En effet, l'IT doit créer et déployer un ensemble commun de règles pour gérer les identités et les accès, et définir une stratégie pour l'ensemble des systèmes de gestion des terminaux. Lorsque deux systèmes de gestion différents sont utilisés, le déploiement de règles communes est encore plus problématique. C'est pourquoi il est recommandé d'opter pour une approche plus simple, avec une seule solution UEM.

Par le passé, la gestion des postes de travail et des ordinateurs portables incombait aux équipes IT. Les smartphones, quant à eux étaient gérés par l'équipe chargée des télécommunications. Les deux équipes avaient donc des compétences, des priorités et des perspectives différentes.

La création et le déploiement de stratégies distinctes généraient des failles de sécurité insoupçonnées qui ouvraient la porte aux pirates et aux fuites de données.

Avec un système UEM unifié, vous définissez un jeu unique de stratégies d'accès utilisateur et de sécurité, qui sera ensuite déployé de manière cohérente sur tous les périphériques des collaborateurs.

### Coûts d'administration et ressources nécessaires

L'utilisation de deux plateformes de gestion distinctes avec des fournisseurs, des interfaces et des contrats de support différents requiert davantage de temps, de formation et de ressources qu'une plateforme unique. Non seulement l'onboarding des nouveaux collaborateurs, les coûts de support et les besoins en ressources augmentent, mais tous les changements de statut ou d'accès relatifs aux utilisateurs exigent de modifier les stratégies dans les deux systèmes. Les inconvénients sont connus : un risque d'erreur et la monopolisation des ressources humaines.

La gestion des périphériques requiert en effet du temps et des ressources qui pourraient être consacrées à d'autres activités plus stratégiques. En raison de la rapidité des changements technologiques et de leur rôle de plus en plus important dans la compétitivité des entreprises, les départements IT sont plus performants s'ils sont capables de réduire au maximum le temps passé sur des tâches de gestion quotidiennes.

## Le mythe de l'intégration

Face à l'adoption croissante des plateformes d'Enterprise Mobility Management (EMM), de plus en plus d'intégrations sont disponibles avec les plateformes de gestion des terminaux de bureau (mobiles ou PC). C'est une tendance encourageante, mais cette supposée intégration entre des systèmes très différents ne génère pas les mêmes économies ni la même facilité d'utilisation qu'un système UEM, avec une seule interface et une seule relation fournisseur. L'UEM présente l'avantage de pouvoir déployer un jeu de stratégies et de ressources cohérent pour chaque utilisateur sur tous ses périphériques, au lieu d'établir une séparation artificielle entre systèmes et périphériques mobiles et traditionnels. Ce type de système doit fournir les fonctions suivantes, sur tous les périphériques :

**Gestion du terminal** pour chaque périphérique d'un collaborateur, avec notamment la découverte et l'inventaire des périphériques, le provisioning du périphérique (déploiement d'OS/recensement du périphérique, distribution de logiciels/d'applis mobiles), support et contrôle à distance.

**Sécurisation** grâce à un renforcement de la sécurité opérationnelle, avec gestion des correctifs, sécurité du terminal, distribution de logiciels, mises à jour, et application de stratégies d'identité et d'accès. Pour les périphériques mobiles, verrouillage et réinitialisation à distance en cas de perte ou de vol sont des fonctions indispensables.

**Gestion des actifs** par le suivi des licences logicielles, des contrats, des garanties et des accords de bail.

**Provisioning**, incluant l'onboarding et l'offboarding des collaborateurs, la gestion des nouveaux périphériques et la création d'images de périphériques. De nombreuses solutions MDM incluent des fonctions d'autoprovisioning, que l'on doit également retrouver dans une solution complète de gestion des terminaux.

En intégrant dans un système UEM toutes ces fonctions de sécurisation des applications et des données, vous bénéficiez d'avantages non négligeables : une gestion centralisée des périphériques, des applications et des informations utilisateurs, un ensemble cohérent de stratégies et une équipe dédiée pour toutes ces tâches.

## La solution Ivanti

La solution Ivanti de gestion des périphériques utilisateur abolit la séparation artificielle entre les postes de travail traditionnels et leurs équivalents mobiles. Ivanti prône une gestion unifiée des terminaux par l'intermédiaire d'une solution unique permettant de déployer des règles de stratégies communes pour la gestion de l'intégralité du cycle de vie des périphériques. L'UEM cible l'utilisateur, pas le périphérique. Grâce à cette approche centrée sur l'utilisateur, Ivanti propose une solution de gestion complète fournissant une expérience utilisateur transparente et satisfaisante. Ivanti Endpoint Manager, solution leader du secteur, offre les fonctions suivantes :

**Découverte et inventaire**
Ivanti découvre et inventorie automatiquement tous les périphériques gérés et non gérés (PC, ordinateurs portables, smartphones, tablettes et autres périphériques mobiles) connectés au réseau, quel que soit leur système d'exploitation. Avec Ivanti Cloud Services Appliance, le département IT peut même découvrir et inventorier les périphériques distants et les gérer par connexion bas débit, sans avoir besoin de VPN.

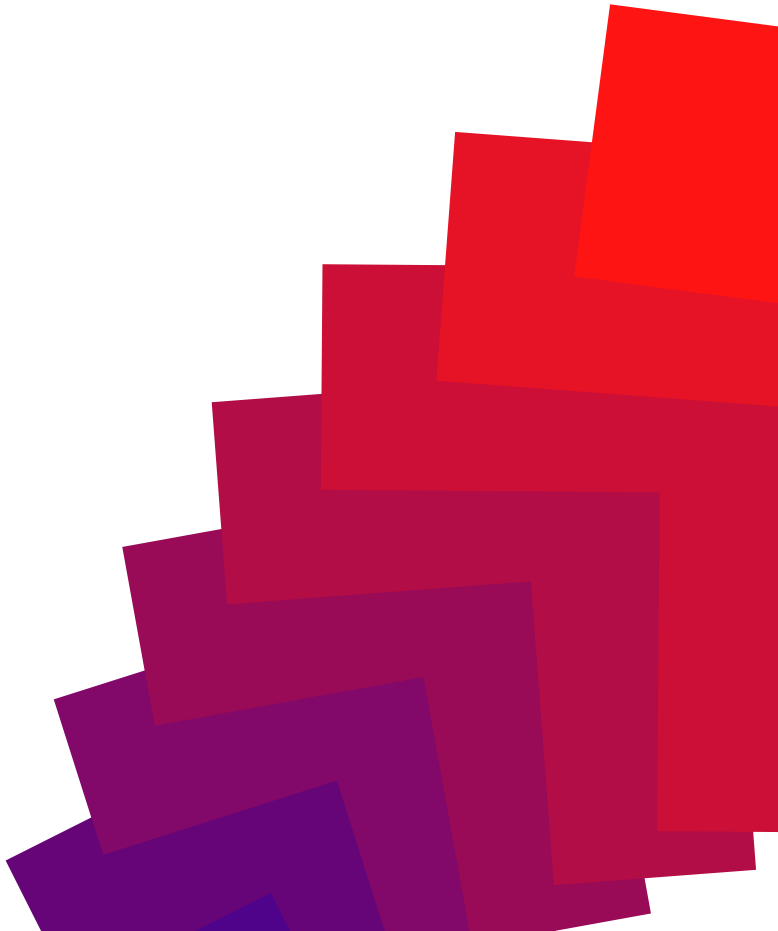
**Déploiement et distribution de systèmes d'exploitation**
Ivanti simplifie et automatise l'installation et la migration des systèmes d'exploitation Windows et macOS sur tous les systèmes utilisateur concernés, en conservant les utilisateurs, les applications, les paramètres et les fichiers afin de les restaurer sur une machine nouvelle ou existante.

**Distribution de logiciels**
Ivanti automatise la distribution de logiciels sur l'ensemble des périphériques : Windows, Mac, et périphériques mobiles iOS et Android. Les technologies brevetées de distribution permettent de diffuser des packages logiciels volumineux sur des milliers de périphériques en quelques minutes, avec une bande passante minimale.

**Administration simple basée sur l'utilisateur**
La solution permet au département IT d'implémenter une seule configuration utilisateur et la même stratégie de sécurité sur tous les périphériques d'un collaborateur. Grâce à cette fonction, la connexion et le provisioning du périphérique d'un nouveau collaborateur s'effectuent en quelques minutes via un seul déploiement de stratégie.

**Gestion des licences logicielles**
Ces outils permettent d'automatiser les audits et la surveillance des licences logicielles, afin d'aider les entreprises à acheter seulement ce dont elles ont réellement besoin et de leur fournir les informations nécessaires pour renégocier les accords de licence avec les fournisseurs et ainsi mieux contrôler leurs coûts. Une utilisation intelligente de la gestion des licences logicielles peut faire économiser à l'entreprise des milliers, voire des centaines de milliers de dollars.

**Les tableaux de bord système** et le reporting permettent d'avoir une visibilité sur le fonctionnement de tous les systèmes : PC, Mac, smartphones et tablettes. Avec Xtraction, les DSI et responsables IT disposent d'informations graphiques pertinentes facilitant la prise de décision. Ils pourront de plus les réutiliser dans des présentations et ainsi contribuer à la valorisation de leur département. Des outils permettant de mesurer votre ROI sont aussi disponibles. Ivanti inclut également des outils d'alerte et de surveillance des seuils, qui permettent au département IT de gérer proactivement les problèmes.



**Résolution des problèmes à distance avec Ivanti Remote Control**
Le département IT peut prendre le contrôle des périphériques afin de résoudre les incidents de support ou de transférer des fichiers d'un système à un autre.

**Gestion de l'alimentation**
Créez et déployez des stratégies de gestion de l'alimentation sur l'ensemble du réseau.

**Gestion complète de la mobilité informatique en entreprise**
Cette fonctionnalité couvre la gestion des applications mobiles, la gestion des périphériques mobiles et la gestion de la sécurité mobile (localisation, verrouillage et réinitialisation d'un périphérique à distance). Elle permet aussi de gérer les ordinateurs de bureau, les ordinateurs portables et les périphériques hybrides (en mode MDM ou pas) autorisant toutes les actions de gestion.

**Des espaces de travail basés sur les rôles**
Indépendamment du périphérique utilisé, chaque collaborateur accède depuis son espace de travail à l'ensemble des services IT, y compris au centre de support et aux mises à jour de sécurité.

Des modules facultatifs s'intègrent à Endpoint Manager pour assurer la gestion des actifs, la gestion du cycle de vie des logiciels et du matériel, et la gestion des services, avec des processus qui garantissent la productivité des utilisateurs et l'efficacité organisationnelle.

Ivanti UEM permet de prendre en charge tous les périphériques utilisés par les collaborateurs et d'améliorer la productivité des utilisateurs et du département IT. L'approche unifiée de la solution d'Ivanti présente plusieurs avantages pour le département IT : réduction des coûts de gestion des terminaux, libération des effectifs pour les allouer à d'autres tâches, renforcement de la sécurité et expérience utilisateur transparente pour les collaborateurs.

## Vers une approche IT centrée sur l'utilisateur

Il y a encore quelques années, deux mondes séparaient les PC et ordinateurs portables de leurs équivalents mobiles. Ils avaient des fonctions et des utilisations différentes. Il était alors relativement logique de développer et de déployer des systèmes de gestion différents pour chacun de ces univers. Dans l'Everywhere Workplace d'aujourd'hui, les collaborateurs peuvent utiliser tous ces périphériques. Dans un tel environnement, s'appuyer sur des systèmes de gestion distincts constituerait une entrave indue autant pour les utilisateurs que pour le département IT.

La solution UEM d'Ivanti allège la charge des équipes IT en leur permettant de se concentrer sur la sécurité et la gestion des utilisateurs. Elle offre non seulement une gestion unifiée, mais aussi une interface utilisateur unique, sur l'ensemble des périphériques, partout et à tout moment.



ivanti

ivanti.fr
+33 (0)1 49 03 77 80
contact@ivanti.fr