

Évaluer de la gestion des terminaux :

pourquoiles solutions
traditionnelles ne répondent
pas aux besoins modernes



Introduction

Mobiles et dispersées, les équipes d'aujourd'hui ont plus que jamais besoin de flexibilité.

Que votre organisation mise entièrement sur le télétravail, ait choisi une approche hybride ou soit entièrement de retour au bureau, les appareils mobiles sont devenus indissociables des opérations commerciales. Smartphones, tablettes et autres terminaux mobiles sont incontournables dans tous les secteurs. Ils unifient les workflows, permettent d'accéder aux données en temps réel et dopent la productivité partout où se trouvent vos collaborateurs.

Avec l'accélération de l'adoption du mobile, la question n'est plus de savoir si ces appareils ont leur place dans l'entreprise, mais si celle-ci a les moyens de les gérer et les sécuriser efficacement.

Devenue incontournable dans des secteurs tels que la santé, la finance, le bâtiment et les transports, la mobilité introduit une complexité nouvelle. Le service informatique est amené à gérer un paysage d'appareils fragmenté et assurer la conformité d'un parc combinant différents modèles de propriété. Il doit soutenir la productivité des utilisateurs sans compromettre leur sécurité ni la protection de leur vie privée, tout en alignant la technologie mobile et les processus informatiques sur les objectifs et les résultats de l'entreprise.

En explorant le changement de paradigme qui touche la gestion et la sécurité de la mobilité en entreprise, cet e-book cherche à expliquer pourquoi les outils traditionnels ou généralistes ne répondent plus aux besoins des entreprises modernes. Il souligne l'intérêt de solutions évolutives et intégrées, capables de prendre en charge les workflows modernes et d'autonomiser les utilisateurs finaux, mais aussi de fournir au service informatique le contrôle et la visibilité indispensables pour maintenir le parc mobile en phase avec les priorités stratégiques.

Si vos outils actuels n'ont pas été pensés pour le travail et la mobilité, ce guide vous aidera à déterminer s'ils servent encore vos intérêts ou si le moment est venu de repenser votre approche.

Travailler sans frontières

Que vos équipes soient toutes en télétravail ou que votre entreprise ait misé sur le retour au bureau, les appareils mobiles sont omniprésents. Ils se sont naturellement imposés dans de nombreux secteurs grâce à leur polyvalence, leur performance, leur portabilité et leur efficacité. Mais ils tendent également à brouiller la frontière entre usage personnel et utilisation professionnelle.

Quelle est l'importance de la mobilité pour la continuité des activités ?

Selon l'**indice de sécurité mobile Verizon 2024**,



« 80 % des personnes interrogées reconnaissent que les appareils mobiles sont indispensables au bon fonctionnement de leur organisation. »

La mobilité est aujourd'hui un outil essentiel pour les opérations commerciales, la fourniture de produits et la prestation de services. Dans ce contexte, les organisations ne doivent pas seulement veiller à ce que les terminaux mobiles soient gérés et sécurisés, il faut aussi qu'ils soient en phase avec les objectifs commerciaux. C'est le seul moyen de garantir que la mobilité reste conforme, flexible face à l'évolution des besoins de l'organisation et de ses opérations, et protégée contre les menaces actuelles et à venir.

Les rôles et les pratiques évoluent

Ces dernières années, de nombreux secteurs se sont tournés vers les appareils mobiles pour dynamiser leurs activités et leur croissance en explorant des pistes inédites que seule la mobilité permet. Voici quelques exemples des bénéfices et des gains d'efficacité que tirent différents secteurs de la mise en place d'appareils mobiles :

Aviation

Les appareils mobiles simplifient la maintenance des avions, les opérations de vol et le service aux passagers en **facilitant l'accès aux données et la communication en temps réel**, de la porte d'embarquement au poste de pilotage. En passant des nécessaires de vol classiques à leur équivalent électronique, les pilotes de ligne ne s'encombrent plus de cartes, de manuels de vol et de guides. Tous ces documents, qui pèsent plus de 18 kg, sont condensés dans un iPad de 800 grammes, pour une efficacité et une conformité maximales.

Bâtiment

Les tablettes et les smartphones fluidifient la collaboration, **réduisent les retards et renforcent la supervision des chantiers** en facilitant l'accès à la documentation et aux outils de gestion de projet sur le terrain comme au bureau. Sur leur iPad, les employés peuvent consulter les plans tandis que leurs superviseurs vérifient et signent les documents administratifs sans perdre un instant. Enfin, les équipes restent en communication constante avec tous les acteurs et les partenaires du chantier.

Services financiers

Les smartphones améliorent le service à la clientèle, augmentent la productivité et favorisent la conformité en donnant accès à différentes plateformes de communication chiffrée. Les professionnels de la finance, analystes en tête, bénéficient d'un accès sécurisé aux données de leurs clients et peuvent suivre l'activité du marché à tout moment. De la même façon, les courtiers sont libres d'exécuter des transactions où qu'ils se trouvent et en toute sécurité sur leur iPhone géré, **pour offrir à leurs clients un soutien sur mesure** (article en anglais).

Hôtellerie

Grâce aux smartphones et aux tablettes, les hôtels **enrichissent l'expérience des clients et unifient les workflows des différentes équipes** à l'aide de systèmes mobiles connectés, pour leur permettre d'offrir des services plus rapides et personnalisés. Les clients peuvent s'enregistrer eux-mêmes sur iPad en mode kiosque pour profiter de leur séjour sans perdre une seconde. Dans les chambres, les iPad gérés et les applications dédiées facilitent l'accès aux informations et aux services de conciergerie.

Commerce de détail

Les appareils mobiles sont aussi pratiques pour les détaillants que pour les clients : ils permettent d'effectuer rapidement des transactions, améliorent l'engagement et **fluidifient les opérations, en boutique comme en ligne**. En troquant les systèmes de caisse traditionnels pour des points de vente mobiles, les vendeurs peuvent aisément gérer l'inventaire tout en conseillant les clients en boutique. Toutes les informations utiles sont accessibles en un coup d'œil. Ils peuvent mettre à jour les données des clients et traiter des paiements sur leur iPhone ou leur iPad.

Les défis pour les entreprises

L'approche traditionnelle, qui consiste à utiliser une même solution de gestion pour superviser un parc d'appareils homogène, n'est plus en phase avec la réalité des entreprises orientées mobile d'aujourd'hui. Face à la diversité des formats d'appareils, des modèles de propriété et des systèmes d'exploitation, le service informatique a fort à faire pour maintenir l'alignement du parc, assurer sa conformité et stimuler la productivité des employés dans des environnements extrêmement fragmentés. À cela s'ajoute l'évolution rapide du paysage des menaces ; les organisations ne doivent pas attendre pour déterminer si leur solution de gestion actuelle peut encore répondre – ou s'adapter – à des exigences de plus en plus complexes tout en continuant à apporter de la valeur à leur entreprise.

Il n'y a pas de solution générique

Traditionnellement, le service informatique a pris pour acquis qu'il était possible de gérer un seul type d'appareil, fonctionnant sous un seul OS, à l'aide d'une seule solution de gestion. Qu'il s'agisse de gérer 100 appareils, 1 000 ou des dizaines de milliers, il y avait une certaine logique dans cette croyance, et cela permettait au service informatique de gérer et de sécuriser des terminaux homogènes.

Prenons un instant pour faire l'inventaire de tous les types d'appareils qui entrent dans la catégorie « mobile » :

- Smartphones
- Tablettes
- Ordinateurs portables
- Dispositifs corporels
- Internet des objets (IoT)
- Liseuses électroniques
- Consoles de jeux portables
- Appareils photo numériques

Considérez l'incroyable diversité des appareils et le **nombre moyen d'appareils possédés** par habitant dans le monde (3,6), puis pensez maintenant aux entreprises traditionnelles. Leur réalité est bien loin du paysage informatique moderne et, par extension, du paysage des menaces d'aujourd'hui.



« 85% des personnes interrogées affirment que les risques liés aux menaces mobiles ont augmenté au cours de l'année écoulée. »

– Indice de sécurité mobile Verizon 2021

La question est donc la suivante : votre solution de gestion et de sécurité est-elle toujours en phase avec les objectifs de l'entreprise, ses exigences de conformité et ses impératifs de productivité ?

Garantir la conformité sur différents modèles de propriété

Avant de tenter de répondre à la question, nous aurions tort de ne pas nous intéresser à l'impact de la diversité des modèles de propriété sur l'usage des appareils mobiles en entreprise.

Cette section porte sur le **maintien d'une sécurité homogène dans l'entreprise** lorsqu'une partie des appareils utilisés pour le travail appartient à l'entreprise et que l'autre est composée d'appareils personnels. En effet, il est particulièrement complexe de devoir prendre en charge :

- **différents types d'appareils** (ordinateurs portables, smartphones, tablettes, dispositifs corporels)
- **différents constructeurs** (Apple, Microsoft, Samsung, etc.)
- **plusieurs systèmes d'exploitation** (Apple, Android, ChromeOS et Windows)
- **différentes versions des logiciels** (applications et OS)
- **des équipes distribuées** (retour au bureau, télétravail et environnements hybrides)

C'est une réalité : les entreprises modernes sont un véritable pot-pourri d'appareils, de modèles de propriété et de systèmes d'exploitation, et toute cette diversité affecte leurs besoins de mille façons. Pour le service informatique, tout le défi consiste à veiller à ce que les terminaux, qu'ils appartiennent ou non à l'entreprise, permettent à leur utilisateur final d'accéder aux ressources professionnelles et de travailler. La productivité des utilisateurs d'appareils mobiles doit être protégée de manière globale dans l'entreprise. Enfin, ces précieux outils professionnels doivent être utilisés conformément aux objectifs de l'entreprise afin de soutenir les opérations et la croissance de l'organisation.



« 87 % des participants du secteur des infrastructures critiques estiment qu'une faille de sécurité impliquant des appareils mobiles et IoT aurait un impact significatif sur leur activité. »

– Indice de sécurité mobile Verizon 2021

L'équation à une inconnue

Les outils traditionnels n'ont pas été conçus pour prendre en charge les environnements de travail hybrides et mobiles d'aujourd'hui. Les équipes informatiques ont besoin de solutions intégrées pour sécuriser et simplifier la gestion à grande échelle. Les solutions de gestion modernes aident les organisations à atteindre leurs objectifs commerciaux en simplifiant le déploiement à distance, en automatisant l'application des correctifs et en établissant des profils de conformité sur toutes les plateformes. Par ailleurs, une intégration étroite avec les fournisseurs d'identité permet de mettre en place une architecture « zero trust » et de sécuriser les accès à partir de n'importe quelle connexion réseau. La détection comportementale des menaces et la surveillance des points de terminaison en temps réel améliorent la réponse aux incidents. La prise en charge des critères du CIS offre au service informatique la possibilité d'auditer et de démontrer la conformité de son environnement en permanence, tout en préservant la productivité des utilisateurs et les performances de tous les types d'appareils, quels que soient le modèle de propriété et l'environnement de travail.

Aligner les processus techniques sur les objectifs de l'entreprise

Le service informatique, comme toute autre fonction de l'entreprise, est essentiel à sa réussite. Pour qu'il puisse mener à bien sa mission, ses processus doivent repousser les limites de la gestion des appareils traditionnelle, mise à l'épreuve par la diversité des appareils mobiles, la fragmentation de l'environnement de travail et l'évolution des menaces de sécurité.

Pour rester compétitif, le service informatique doit s'aligner sur les objectifs principaux de l'entreprise pour apporter une contribution directe à :

1. la croissance stratégique
2. l'efficacité des opérations
3. la résilience à long terme

et autonomiser l'entreprise en maximisant son agilité, en soutenant la productivité et en atténuant les risques sans sacrifier l'expérience utilisateur.

En mettant en place une solution de gestion compatible avec la diversité mobile et capable de soutenir la stratégie d'entreprise, de nombreux secteurs clés obtiennent des résultats mesurables dans des cas d'utilisation innovants :

Fabrication

L'iPad permet aux employés de production d'accéder aux données de la chaîne d'approvisionnement en temps réel et de bénéficier des avantages de workflows numériques. Selon une enquête IDC, 85 % des entreprises qui ont **investi dans les technologies de transformation numérique (DX)** ont observé une corrélation intéressante : « l'amélioration de l'expérience et de l'engagement des employés se traduit par une meilleure expérience client, un plus haut niveau de satisfaction et des revenus plus élevés pour l'organisation. »

Santé

Les iPads et les iPhones décuplent les moyens des soignants en leur donnant un accès instantané et sécurisé aux données personnelles de santé (PHI) électroniques et aux outils de télémedecine. Selon le National Institute of Health (NIH), sur les dix études examinées pour l'article intitulé **Smartphone and Mobile App Use Among Physicians in Clinical Practice** (« Utilisation des smartphones et des applications mobiles par les médecins dans la pratique clinique »), « 70 % *disaient utiliser des applications mobiles* » pour améliorer les résultats des patients et simplifier la prestation des soins en se basant sur des données probantes pour éclairer la prise de décision clinique.

Administration

L'iPhone offre partout un accès sécurisé aux ressources de l'administration tout en facilitant la collecte de données sur le terrain. Lorsqu'on sait que plus de 90 % des appareils mobiles déclarés perdus ou volés sont à l'origine d'une « divulgation de données confirmée » selon le **Rapport 2024 sur les enquêtes sur les violations de données de Verizon**, il faut une sécurité complète et évolutive, capable de s'adapter à la croissance des parcs et à l'évolution des règles tout en assurant une protection cohérente et holistique.

Optimiser la prise en charge du parc d'appareils mobiles

Les équipes informatiques ont besoin de stratégies de mobilité modernes pour étendre la prise en charge des appareils, assurer la conformité du parc et protéger la vie privée des utilisateurs, qu'il s'agisse d'appareils personnels ou institutionnels. La sécurité multiplateforme garantit l'homogénéité de la protection et de la conformité, tandis que la reconfiguration simplifiée des appareils sécurisés réduit les risques, maximise leur disponibilité et optimise la productivité des employés sans bureau. En améliorant l'efficacité opérationnelle et en garantissant une protection cohérente, cette approche permet aux responsables informatiques de faire évoluer la gestion du parc mobile avec les besoins de l'entreprise et des équipes.

Prise en charge évolutive des modèles de propriété

Lorsque leur parc combine appareils personnels et institutionnels, les entreprises modernes sont confrontées à d'importants défis d'évolutivité. Les équipes informatiques ont besoin de solutions dédiées **prenant différents modèles d'inscription** pour :

- alléger la complexité
- appliquer les mesures de sécurité de façon globale
- segmenter les données professionnelles et personnelles
- garantir la mise en conformité
- protéger la vie privée des utilisateurs de façon équilibrée

Une fonction clé permet de maintenir la sécurité tout en préservant la vie privée sur les appareils personnels : elle consiste à **protéger les données de l'entreprise en chiffrant les connexions réseau** vers et depuis les ressources professionnelles, tout en acheminant le trafic personnel directement vers Internet. On obtient ainsi une posture de sécurité homogène pour tous les appareils, et les règles sont appliquées à grande échelle, quel que soit le modèle de propriété.

Sécurité des points de terminaison homogène sur toutes les plateformes

Outre le défi posé par la diversité des modèles de propriété, les entreprises modernes opèrent fréquemment dans des environnements mixtes où figure une multiplicité de systèmes d'exploitation : iOS/iPadOS, Windows et Android sont tous représentés. Cette complexité introduit de nombreuses variables qui, multipliées par le nombre d'appareils, augmentent considérablement la difficulté des efforts d'atténuation des risques.

Il faut donc associer des stratégies de défense en profondeur et des contrôles adaptés :

- télémétrie avancée
- détection comportementale des menaces
- règles d'accès unifiées

et assurer une prise en charge multiplateforme pour sécuriser l'ensemble des points de terminaison mobiles de manière cohérente, à la fois sur l'appareil et sur le réseau, **quelle que soit la plateforme**. Cette approche globale réduit la fragmentation tout en **maintenant des normes de sécurité strictes dans l'ensemble du parc mobile**.

Appareils partagés et employés sans bureau

Dans les secteurs qui s'appuient beaucoup sur des appareils partagés et des environnements multi-utilisateurs, la réduction des temps d'arrêt aux changements de sessions est un enjeu majeur. Qu'il s'agisse de :

- configurer rapidement un iPhone pour conseiller des clients lors d'une période de forte affluence,
- fournir des iPhone au personnel navigant pour simplifier la vente de nourriture et de boissons à bord des avions,
- ou reconfigurer un iPad en mode kiosk à la volée pour faciliter des soins infirmiers,

Lorsque chaque seconde compte, simplifier la reconfiguration des appareils devient crucial : c'est ce qui **permet aux utilisateurs de changer rapidement de rôle** ou **d'effacer et superviser des appareils sans intervention du service informatique**. Des solutions dédiées assurent la sécurité des appareils partagés et les préparent pour l'utilisateur suivant, tout en limitant les recours à l'assistance et en améliorant l'efficacité opérationnelle globale.

De nouveaux workflows pour stimuler la productivité

La simplification de la gestion des appareils mobiles est un catalyseur pour l'efficacité du service informatique et la productivité des utilisateurs. Intégrée aux outils d'identité et de sécurité, elle accélère l'approvisionnement et simplifie les rapports de conformité et le contrôle d'accès. L'automatisation du déploiement réduit le temps de configuration et les erreurs manuelles, tandis que les fonctions de libre-service offrent aux utilisateurs un accès sur demande aux applications et aux ressources essentielles. Ces workflows novateurs capitalisent sur l'efficacité pour minimiser les temps d'arrêt et libérer les équipes informatiques, qui peuvent ainsi se consacrer au développement de processus utiles aux objectifs de l'entreprise.

Intégration transparente avec les outils existants

Il n'existe pas de « solution miracle ».

Pour cette raison, **l'intégration est un aspect clé du succès de l'approche de gestion et de sécurité des appareils mobiles**, car c'est elle qui :

- étend et généralise les services
- ajoute des couches de sécurité complètes
- permet aux entreprises d'enrichir les outils existants
- personnalise les workflows pour répondre aux besoins de conformité

Pour prendre un exemple, l'**intégration avec des fournisseurs d'identité** tels que Microsoft Entra ID et Okta centralise le contrôle d'accès, applique les règles d'accès conditionnel et ajoute la MFA anti-phishing aux workflows d'authentification. L'atténuation du risque d'accès non autorisé aux ressources protégées n'est qu'un exemple parmi d'autres de la puissance de l'intégration des plateformes de sécurité, qui offre de nombreux avantages au service informatique :

- simplification du déploiement des appareils
- provisionnement plus rapide
- simplification des rapports de conformité
- réduction des frictions dans l'ensemble de la pile technologique
- alignement sur les workflows des entreprises

Automatiser le déploiement et le provisionnement des appareils

Selon les besoins de l'organisation, l'intégration manuelle d'un appareil mobile peut prendre jusqu'à 30 minutes – un frein à la productivité et une charge inutile pour le service informatique.

Mais **l'automatisation du déploiement des appareils mobiles sans intervention** avec Apple Business Manager (ABM) réduit considérablement les délais de provisionnement. En plus de **doper l'efficacité du service informatique**, cette approche apporte de nombreux avantages aux organisations :

- elle élimine la configuration manuelle et réduit le risque d'erreur humaine
- elle accélère le déploiement, notamment l'installation et la configuration des applications
- elle garantit que chaque appareil répond aux normes de sécurité et de conformité dès le premier jour
- elle fournit aux utilisateurs toutes les ressources dont ils ont besoin pour travailler dès l'activation de l'appareil

Donner aux utilisateurs l'accès aux ressources indispensables à tout moment

On considère généralement qu'un délai de 24 heures ou d'un jour ouvrable est une **bonne performance** pour la prise en charge d'une demande d'assistante informatique. Mais quand un employé demande une application ou une configuration indispensable pour terminer une tâche, chaque minute de retard est une perte de productivité, avec des conséquences sur les opérations de l'organisation et ses revenus.

Le **Self Service autonomise les équipes** en leur donnant accès à :

- un catalogue sélectionné d'applications approuvées
- des ressources et des services professionnels
- des configurations et des réglages sécurisés

– tout cela sans soumettre de tickets d'assistance !

Les utilisateurs accèdent en toute sécurité aux ressources indispensables à leur travail, mais le service informatique garde le contrôle sur ce qui est mis à leur disposition. Le résultat : moins de travail pour l'assistance, et des équipes capables d'agir en autonomie et en confiance.

Mettez en œuvre une stratégie de sécurité globale

Pour répondre efficacement aux menaces modernes dans des environnements mobiles diversifiés, les entreprises n'ont pas d'autre choix que de faire évoluer leurs pratiques de sécurité. L'automatisation de la gestion des correctifs minimise les vulnérabilités : elle garantit en effet que les appareils et les applications restent à jour tout en allégeant la charge du service informatique. La détection avancée des menaces exige des analyses en temps réel et une intégration approfondie. Elle doit en outre être associée à des défenses multicouches pour identifier et atténuer les risques.

Basée sur la santé des appareils et l'identité des utilisateurs, une stratégie « zero trust » sécurise l'accès aux ressources, quels que soient la localisation, la plateforme ou le modèle de propriété de l'appareil.

Automatisez la gestion des correctifs

L'erreur humaine est la menace la plus évitable dans le plan de cybersécurité d'une entreprise. Les logiciels obsolètes entrent dans cette catégorie ; ils rendent les appareils mobiles vulnérables et compromettent les objectifs de conformité de l'organisation. Mais il y a une bonne nouvelle : en **automatisant la gestion des correctifs pour les systèmes d'exploitation et les applications**, cette menace peut être atténuée de plusieurs manières :

- Suivi et alertes en temps réel
- Examen proactif des journaux unifiés
- Utilisation des **Groupe**s intelligents
- Application de règles dynamiques
- Workflows des **programmes d'installation des apps**
- Épinglage d'une version minimale de l'application

En misant sur l'automatisation, le service informatique allège ses tâches manuelles tout en veillant à ce que les appareils restent constamment à jour et conformes aux exigences internes et réglementaires. Autre avantage, il minimise les interruptions et les temps d'arrêt pour les utilisateurs.

Détection et prévention des menaces

Les cyberattaques ont atteint un pic en 2020, puis ont décliné, jusqu'à ce que **les menaces mobiles fassent un bond de 147 %** entre le 1er au le 4e trimestre 2023, selon Kaspersky. Les menaces mobiles sont devenues plus sophistiquées, et elles contournent souvent les capacités des logiciels antivirus traditionnels. Pour être efficace, une solution de sécurité mobile doit arrêter les menaces connues et exploiter l'analyse comportementale sur l'appareil et sur le réseau pour détecter les risques avancés en temps réel. Une intégration poussée entre gestion, identité et sécurité offre à ce titre de puissants avantages aux équipes informatiques :

- Visibilité accrue sur l'activité des appareils mobiles
- Évaluation des postures à risque en temps réel
- Réduction des temps de réponse aux incidents sur une pluralité de plateformes,

de types de propriété et d'environnements de travail

- Intégration parfaite avec les SIEM tiers
- Contrôles complets et multicouches sans sacrifice des performances de l'appareil

Accès réseau « zero trust » (ZTNA)

Face à l'évolution des environnements de travail et des usages des appareils mobiles, les entreprises peuvent-elles continuer à s'en remettre à des outils conçus d'un autre temps pour gérer et sécuriser leur parc ?

Pour le dire simplement : non.

Avec l'adoption du cloud computing, des environnements de travail hybrides et des appareils mobiles, le contrôle d'accès basé sur l'identité de l'utilisateur et l'intégrité de l'appareil devient un impératif pour la conformité. Aujourd'hui, les entreprises sans périmètre y parviennent en combinant plusieurs techniques :

- Elles remplacent les VPN traditionnels par des microtunnels chiffrés pour isoler le trafic du réseau
- Elles appliquent des règles d'accès conditionnel qui n'accordent l'accès qu'aux utilisateurs approuvés munis d'appareils vérifiés.
- Elles intègrent étroitement l'identité à leur pile de gestion et de sécurité
- Elles adoptent une **stratégie « zero trust »** qui sécurise les ressources de l'entreprise de manière globale, quels que soient le lieu de travail des employés, l'appareil utilisé et son propriétaire.

Standardiser et généraliser la conformité

Une conformité efficace commence par la mise en œuvre de références de sécurité fondées sur les normes du secteur, l'objectif étant de garantir que tous les appareils mobiles respectent les règles en vigueur dès le premier jour. La surveillance active de l'intégrité des terminaux apporte une visibilité en temps réel et l'IA facilite la détection des risques pour aider le service informatique à maintenir la conformité et à réagir rapidement aux menaces. Enfin, les contrôles basés sur les critères du CIS permettent aux organisations de réaliser des audits, de corriger les défauts et de produire des rapports de conformité.

Renforcez les postures de sécurité en appliquant des profils de référence

Les contrôles techniques et les règles sont des piliers de la conformité. Mais comment mettre en place une stratégie et respecter les exigences d'un secteur spécifique ? Basés sur des normes et des cadres reconnus par un secteur, les profils de référence offrent un excellent point de départ.

Ces configurations fondamentales garantissent que chaque point de terminaison, qu'il appartienne à l'entreprise ou à un employé, respecte les **exigences de sécurité dès son inscription dans la solution MDM**. C'est une étape essentielle au développement et à la mise en œuvre d'une stratégie de défense en profondeur. Elle aide en effet le service informatique à :

- **établir la conformité par le déploiement de profils de configuration structurés** auprès de Groupes intelligents ciblés
- automatiser un provisionnement cohérent et réduire les dérives de configuration à grande échelle
- aligner les processus relatifs aux appareils mobiles sur la sécurité des données pour soutenir les efforts de continuité des activités
- **adapter les stratégies de sécurité aux besoins de l'organisation et aux réglementations du secteur.**

Surveillance active de la santé des points de terminaison

L'étape suivante, après la mise en place de profils de référence, consiste à surveiller activement le parc d'appareils mobiles. En effet, une conformité durable exige une visibilité continue sur l'état de santé, qui garantit également une réponse rapide en cas de défaut de conformité. L'intégration étroite entre gestion, identité et sécurité décroïsonne les équipes informatiques, **qui peuvent alors s'appuyer sur l'IA pour renforcer la posture de sécurité de l'organisation**, mais aussi :

- utiliser la **télémétrie et des informations en temps réel sur le comportement des points de terminaison**
- détecter les risques à l'aide du machine learning (ML) pour des corrections plus rapides encore
- rechercher proactivement les menaces sophistiquées sur les terminaux mobiles, les analyser et les neutraliser

vérifier la conformité aux critères de référence et les faire respecter

La troisième étape conclut le cycle de vie de la conformité des appareils mobiles : c'est elle qui fait le lien entre application des règles, vérification et amélioration en fournissant aux organisations un moyen d'auditer la conformité en continu. Elle facilite également la **production des preuves de conformité exigées dans les secteurs réglementés**.

Les solutions de gestion modernes autonomisent les organisations à double titre : elles systématisent et surveillent la conformité, et elles fournissent nativement les outils qui vérifient la conformité aux niveaux 1 et 2 des critères du CIS. Toujours pour soutenir les efforts de gouvernance interne et de préparation réglementaires :

- Elles offrent au service informatique la possibilité de personnaliser les **critères** selon les besoins particuliers de l'entreprise
- Elles mesurent automatiquement les valeurs de référence pour **corriger automatiquement les écarts par rapport aux critères**
- Elles permettent de créer des directives en un clic aux formats PDF, HTML et Adoc pour faciliter les audits

Pratique ou sécurisé : les chiffres

En donnant la priorité aux aspects pratiques ou économiques, on sacrifie souvent la sécurité, ouvrant la porte à risques opérationnels importants à long terme. Les incohérences dans la protection des différents types d'appareil affaiblissent la posture de sécurité globale et exposent des failles aux pirates. L'impact des cyber-incidents ne se limite pas à la sécurité ; ils dégradent également les performances des appareils, la productivité des utilisateurs et la continuité des activités. Pour éviter ces écueils, les leaders informatiques doivent privilégier les solutions qui sécurisent tous les points de terminaison, indépendamment du modèle de propriété ou du système d'exploitation. Seules, ces solutions garantissent l'efficacité, la résilience, la performance et la santé de l'organisation à long terme.

Pourquoi les économies réalisées pour des questions de « simplicité » finissent-elles par coûter plus cher aux entreprises que la « sécurité » ?

Le coût est un facteur déterminant pour les organisations lorsqu'elles choisissent des solutions pour gérer et sécuriser leur parc d'appareils mobiles. Certes, conserver les solutions existantes ou opter pour une solution généraliste peut réduire les délais d'installation et les investissements de départ. Il faut toutefois garder en tête que ce compromis se fait souvent aux dépens d'une sécurité mobile complète.

Et ces lacunes dans la couverture peuvent conduire à des failles coûteuses. Selon le rapport d'IBM sur le coût d'une violation de données en 2025, **le coût moyen mondial d'une violation de données s'élève à 4,44 millions de dollars** – et même à 10,22 millions de dollars aux États-Unis.

À l'inverse, une analyse des coûts réalisée à partir du rapport d'IBM a mis en évidence que « les équipes de sécurité utilisant l'IA et l'automatisation » réalisaient en moyenne une économie de 1,9 million de dollars par rapport à celles dont les solutions n'offrent qu'une prise en charge de base de la gestion, des identités et de la sécurité. Comment ? En réduisant les délais de détection des failles de 80 jours et en diminuant le coût moyen des violations.

En bref, les investissements dans la cybersécurité sont étroitement liés aux opérations, à la réputation et à la conformité réglementaire, trois facteurs clés qui impactent les résultats de l'organisation.

L'absence d'homogénéité affaiblit la posture de sécurité de l'organisation.

Lorsque la sécurité des appareils mobiles change en fonction de la plateforme, les organisations se retrouvent aux prises avec une couverture lacunaire.

En clair, certains appareils mobiles ne bénéficient pas des mêmes protections que d'autres.

Dans un article récent d'[Infosecurity Magazine](#), on apprenait que 41 % des personnes interrogées avaient cité le vol d'appareils contenant des données sensibles comme la principale cause de perte de données, devant le vol ou la faiblesse des identifiants (36 %) et les attaques de ransomware (32 %). C'est ce qui se produit lorsque les contrôles varient d'une plateforme prise en charge à l'autre ; ce scénario donne un faux sentiment de protection face à des failles exploitables qui dégradent la résilience globale.

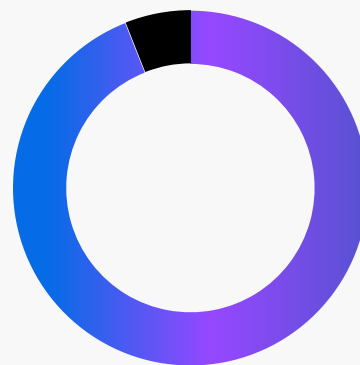
Pour résumer, les mesures de sécurité de l'entreprise doivent s'appliquer à tous les points de terminaison qui accèdent à son infrastructure, car chaque appareil représente un risque pour l'entreprise, quels que soient son type, son OS et son propriétaire. Le risque est une réalité.

Impact sur les performances des appareils et la productivité des employés

Comme nous l'avons vu plus haut, les cyber-incidents n'ont pas uniquement des conséquences financières. Certes, ils dégradent la posture de sécurité des appareils et de l'organisation, mais ils impactent aussi les performances et la productivité des utilisateurs, et cela se répercute sur les opérations de l'entreprise.

Dans son rapport couvrant les violations de plusieurs types d'environnements (clouds publics, cloud privés et sur site), IBM a constaté que le délai moyen d'identification d'une violation de données était de 207 jours. À cela s'ajoute 70 jours supplémentaires de délai moyen de confinement (MTTC), ce qui porte à 276 jours le temps nécessaire pour identifier et contenir une violation de données dans divers environnements. Pendant tout ce temps, l'impact sur les performances des appareils et des systèmes d'entreprise concernés se traduit par des coûts financiers et des pertes d'opportunités.

Pensez également que les retombées de certaines attaques peuvent avoir des conséquences directes sur la productivité des utilisateurs. Prenons l'exemple d'une attaque de ransomware. Dans un article consacré aux conséquences d'un arrêt prolongé du réseau et de l'activité, [Help Net Security](#) souligne que



« 94 % des personnes ayant subi une attaque de ransomware ont connu une longue période d'interruption et des retards de productivité. Parmi elles, 40 % témoignent d'une période d'arrêt total de travail et une perte complète de productivité. »

Autrement dit, les effets des cyberattaques vont bien au-delà des coûts immédiats : perte d'opportunités commerciales, baisse de productivité, érosion de la confiance du public et diminution de la valeur marchande sont autant de conséquences sensibles souvent bien après qu'une faille a été contenue.

Principaux points à retenir :

1.

La mobilité a une importance stratégique :

Parce qu'ils permettent de communiquer en temps réel, de mettre en place des workflows flexibles et d'assurer la continuité des activités dans les environnements distants, hybrides et locaux, les appareils mobiles sont des outils essentiels dans tous les secteurs.

2.

L'impasse des outils traditionnels :

Les solutions de gestion traditionnelles et génériques ne peuvent pas garantir un niveau de sécurité homogène dans les parcs mobiles modernes : la diversité des modèles de propriété et des OS les rend particulièrement complexes.

3.

La sécurité doit être holistique :

Les entreprises modernes ont besoin de stratégies de sécurité multiplateforme et intégrées aux systèmes d'identité, qui combinent la détection des menaces en temps réel, des politiques d'accès conditionnel et la gestion automatisée des correctifs.

4.

La conformité n'est pas négociable :

Une gestion mobile efficace est un atout pour la conformité aux audits : elle déploie des profils de référence sécurisés, surveille la santé des points de terminaison et vérifie le respect des normes du secteur.

5.

La clé : évolutivité et automatisation :

Les solutions dédiées uniformisent le déploiement, simplifient l'approvisionnement et réduisent les tâches manuelles. Le service informatique peut ainsi apporter un soutien complet et homogène aux équipes distribuées.

6.

L'importance de l'expérience utilisateur :

Les outils en libre-service et un accès cohérent aux ressources professionnelles autonomisent les employés et améliorent la productivité. Ils réduisent la charge de travail des équipes informatiques, sans compromettre la protection de la vie privée ni la sécurité.

7.

L'alignement métier, créateur de valeur :

L'alignement de la gestion des appareils mobiles sur les objectifs stratégiques est un puissant catalyseur d'efficacité opérationnelle. Il fait du service informatique un moteur d'innovation et de croissance dans l'entreprise.

Conclusion

La généralisation des appareils mobiles permet d'être productif partout, au bureau comme en dehors. Les objectifs commerciaux ne sont pas seulement des indicateurs en vogue, ils définissent l'entreprise moderne.

Face à la diversité croissante des types d'appareils, des modèles de propriété et des systèmes d'exploitation, les outils de gestion traditionnels ne sont plus en mesure de répondre à certaines exigences fondamentales des entreprises modernes en matière de sécurité, de conformité et d'expérience utilisateur.

La mission du service informatique ne se limite plus à la gestion des appareils.

On lui demande d'aligner la technologie et les processus de gestion sur la stratégie et les objectifs de l'entreprise. Il doit désormais protéger les actifs critiques tout en accompagnant des utilisateurs qui attendent un accès transparent partout, sur l'appareil de leur choix et avec leur système d'exploitation de prédilection.

1.

Les enjeux sont plus vastes.

2.

Les risques sont plus importants.

3.

Et la marge d'erreur se réduit.





Les solutions modernes de gestion des points de terminaison sont conçues pour répondre à ces nouvelles exigences. Du déploiement sans intervention à la détection des menaces avancées, en passant par la prise en charge multiplateforme et la sécurité « zero trust », des outils dédiés permettent aux équipes informatiques d'adapter, de sécuriser et d'optimiser les tâches exécutées sur mobile. Et cela, sans compromettre la sécurité, l'efficacité, ni la productivité de l'entreprise.

Une question reste en suspens :

*Votre solution de gestion actuelle répond-elle toujours aux besoins de votre entreprise, de votre service informatique et de vos employés ?
Si vous avez le moindre doute, il est temps de réévaluer votre approche ; la réussite de votre entreprise en dépend.*

Essayez Jamf