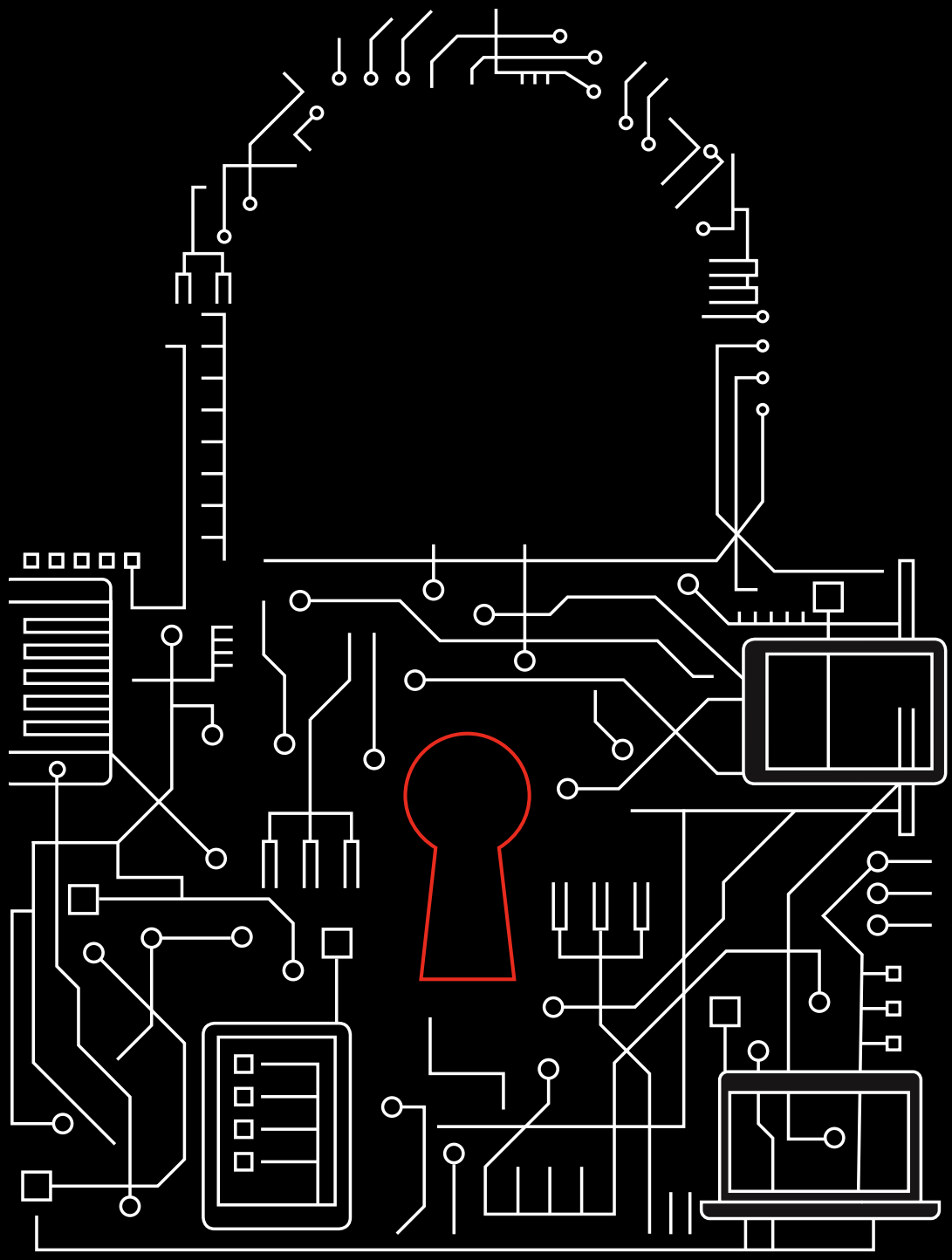
Mobile Security Index

Synthèse 2020



verizon

Sécurité mobile, clé de l'innovation.

Pour survivre dans le contexte économique actuel, les entreprises doivent sans cesse innover. Et aujourd'hui, qui dit innovation dit technologies mobiles.

Dans le cadre de notre édition 2020 du Mobile Security Index, nous avons demandé aux participants de quantifier l'importance des technologies mobiles pour leur entreprise sur une échelle de 1 à 10. Résultat : 83 % ont répondu 8 ou plus. La sécurité mobile n'est donc plus un choix, mais bel et bien un impératif absolu de leur transformation et de leurs futures innovations. Ceci se vérifie d'autant plus que l'étau règlementaire se resserre et que les consommateurs et clients professionnels se montrent davantage sensibles aux questions de protection de leurs données, tout en restant intraitables sur la qualité de l'expérience globale attendue.

Seulement voilà, beaucoup d'organisations peinent à garder un coup d'avance sur des menaces de plus en plus avancées et des attaquants de plus en plus habiles. Pour y parvenir, vous avez besoin non seulement des bons outils, mais aussi d'une stratégie IT centrée sur la sécurité mobile.

C'est pourquoi ce document dresse un état des lieux de cette facette essentielle de la sécurité et des menaces qui planent aujourd'hui sur les entreprises.

54 %

Pourcentage d'entreprises moins confiantes dans la sécurité de leurs terminaux mobiles que dans celle de leurs autres systèmes

verizon

Un bilan qui s'alourdit

Le chiffre le plus perturbant du Mobile Security Index 2020 n'a malheureusement rien de surprenant : la courbe des entreprises victimes d'une compromission ne cesse de grimper. Concrètement, ce taux a augmenté de 41 % depuis notre premier rapport en 2018. Il faut dire que les cyberattaquants n'ont pas traîné. Au vu de l'importance grandissante des technologies mobiles pour les entreprises à travers le monde, ils ont vite flairé la valeur des informations auxquelles ces appareils ont accès.

Pour mettre la main sur vos données, les hackers utilisent les vieilles recettes qui marchent, comme le phishing et les malwares, mais aussi de nouveaux stratagèmes. Utilisateurs, applications, appareils, réseaux… tout l'écosystème mobile est pris pour cible.

Entreprises compromises

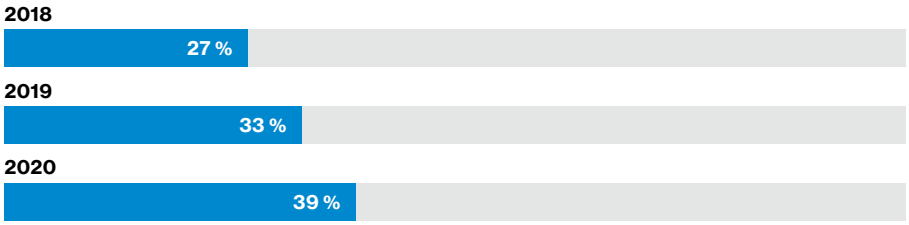


Figure 1 : Votre entreprise a-t-elle été victime d'une compromission liée à des appareils mobiles/IoT (Internet des objets) au cours de l'année passée ?

Utilisateurs

Qu'ils enfreignent volontairement les règles, ouvrent inconsciemment des brèches ou nuisent délibérément à l'entreprise, les utilisateurs peuvent poser un véritable problème de sécurité. Et ce alors même que les attaquants redoublent d'inventivité pour tromper et piéger vos salariés. À cet égard, l'ingénierie sociale compte parmi les outils les plus efficaces dans leur arsenal.

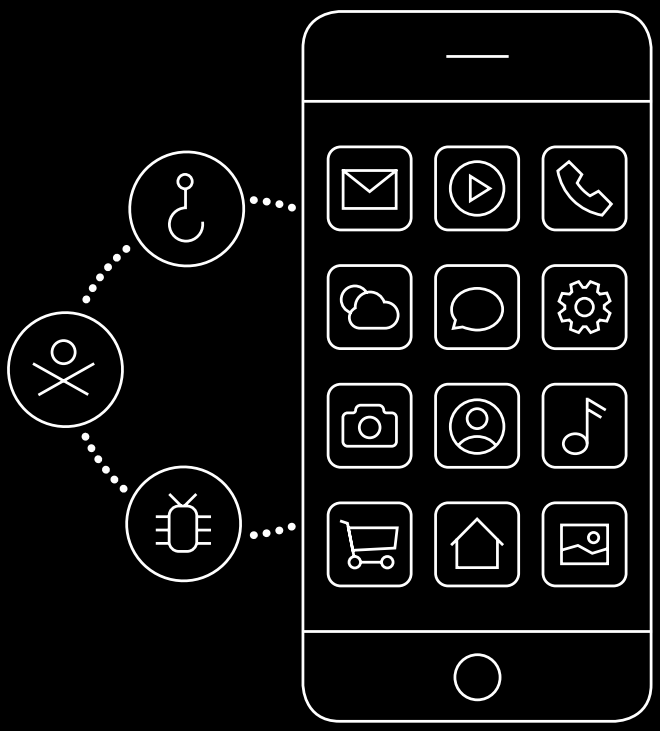
Le phishing et les compromissions de comptes de messagerie d'entreprise constituent deux exemples emblématiques des méthodes d'ingénierie sociale. D'après les services de renseignement américains, qui ont contribué au rapport de cette année, les pertes consécutives à un braquage de banque avoisinent les 3 000 dollars en moyenne. Une goutte d'eau par rapport aux 130 000 dollars que coûte une compromission de compte de messagerie.[1]

Il n'existe pas de remède miracle contre les menaces mobiles. Toutefois, pour fixer des règles claires et sensibiliser vos collaborateurs aux risques encourus, une politique d'utilisation acceptable (PUA) constitue un bon point de départ. Une PUA forte définira des volumes de données acceptables et des critères de distinction entre sites légitimes et sites proscrits. Elle conseillera également vos salariés sur les questions de conformité, le tout dans un souci permanent de protection de vos données. Le problème, c'est que 44 % des entreprises sondées n'ont aucune PUA en place.

15 %

Pourcentage d'utilisateurs mobiles professionnels confrontés à des liens de phishing au troisième trimestre 2019 (18 % aux États-Unis)

Besoin d'aide pour peaufiner votre PUA ? Lisez notre guide sur le sujet. ›



Quand la palme de l'innovation revient aux attaquants

Cette année, notre étude a révélé que des hackers introduisaient des applications malveillantes sur les app stores officiels et utilisaient des techniques de contournement comme les polices de caractères personnalisées et les déclenchements de code malveillant à retardement pour prendre à défaut les logiciels d'analyse de messages électroniques.

21 %

Pourcentage d'entreprises compromises affirmant qu'une application non autorisée ou non validée était à l'origine de l'incident

Applications

Si les malwares et les ransomwares font encore trop souvent des ravages, des techniques comme le cryptojacking deviennent elles aussi de plus en plus répandues. Le cryptojacking consiste à exploiter un équipement compromis pour miner des cryptomonnaies comme le Bitcoin. En plus de vider la batterie de l'appareil, cette technique peut entraîner des interruptions de service et autres perturbations.

Dans l'édition de cette année, 86 % des entreprises expriment des craintes vis-à-vis des malwares. Pourtant, elles sont une grande majorité à laisser carte blanche à leurs salariés quant aux applications utilisées. En effet, seules 43 % affirment qu'elles restreignent leurs collaborateurs à l'utilisation d'un app store officiel ou contrôlé par l'entreprise.

Appareils

Cette année, notre étude s'est penchée sur des entreprises aux parcs mobiles très variés : certaines avaient moins de 100 appareils, tandis que d'autres en géraient plus de 10 000. Des pertes de terminaux aux failles des systèmes d'exploitation, toutes expriment les mêmes types de craintes. Concrètement, 83 % des sondés s'inquiètent des éventuels vols ou pertes de terminaux. Parmi eux, 20 % qualifient leur protection d'inadaptée. Les entreprises peuvent recourir à des fonctionnalités de sécurité standards comme le chiffrement et l'effacement à distance pour limiter les risques.

Autre source d'inquiétude, les systèmes d'exploitation des appareils mobiles sont rarement à jour. Pour preuve, presque la moitié des entreprises interrogées (49 %) n'ont mis en place aucune politique de gestion des mises à jour de ces terminaux.

31 %

Pourcentage de terminaux infectés par des menaces connues d'après les données de MobileIron[2]

Réseaux

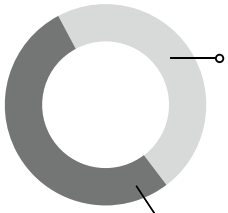
En se laissant tenter par le Wi-Fi public, vos utilisateurs accroissent les risques pour votre entreprise. En effet, 20 % des entreprises victimes d'une compromission d'appareil mobile déclarent qu'une borne Wi-Fi non autorisée ou non sécurisée était en cause.

D'après Wandera, les salariés se connectent à 24 bornes Wi-Fi par semaine en moyenne.[3] Et selon Netmotion, la plupart des terminaux se connectent à deux, voire trois bornes Wi-Fi non sécurisées par jour.[4]

2 ou 3

Nombre de bornes Wi-Fi non sécurisées auxquelles la plupart des terminaux mobiles se connectent chaque jour

Politique d'utilisation du Wi-Fi public



48 %
des entreprises interdisent son utilisation

52 %
des entreprises autorisent son utilisation ou n'ont aucune politique en place.

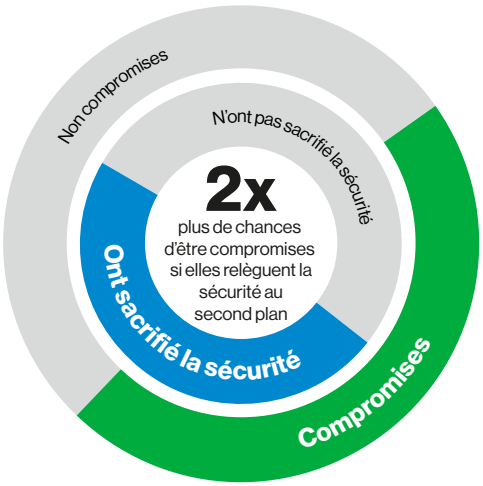
Utilisation du Wi-Fi public par les salariés

Figure 2 : Autorisez-vous vos salariés à utiliser le Wi-Fi public (par ex., dans un café ou à l'hôtel) à des fins professionnelles ? Utilisez-vous vous-même le Wi-Fi public dans votre vie professionnelle ?

Des choix lourds de conséquences

De nos jours, on pourrait penser que les entreprises ont parfaitement conscience du rôle central des technologies mobiles dans leur architecture globale de sécurité. Pourtant, rien n'est moins clair. Dans 43 % des entreprises interrogées, la sécurité mobile est régulièrement sacrifiée sur l'autel des deadlines et autres objectifs de productivité, doublant du même coup le risque d'une compromission.

Alors pourquoi prendre autant de risques ? Pour justifier cette décision, les sondés invoquent des questions de rapidité (62 %), puis de praticité (52 %) et de rentabilité (46 %). Certes, il s'agit là d'impératifs métiers incontournables. Mais lorsqu'ils finissent par doubler les risques de compromission d'une entreprise, un tel choix devient difficile à défendre.



Sacrifice et compromission

43 %

Pourcentage d'entreprises ayant sacrifié leur sécurité

39 %

Pourcentage d'entreprises victimes d'un incident de sécurité

Figure 3 : Votre entreprise a-t-elle été victime d'une compromission liée à des appareils mobiles ou IoT au cours de l'année passée ? Votre entreprise a-t-elle déjà fait volontairement l'impasse sur la sécurité de ses terminaux mobiles (y compris les appareils IoT) pour parvenir à ses objectifs métiers ?

Des victimes touchées de plein fouet

Parmi les entreprises victimes d'une compromission, 66 % qualifient l'impact de « majeur ». Le retour à la normale n'est pas non plus une mince affaire. Dans ce domaine, 37 % des sondés font état d'une remédiation difficile et coûteuse.

Les conséquences de ces compromissions vont également bien au-delà des terminaux mobiles. Parmi les impacts immédiats :

- Interruption de service (59 %)
- Perte de données (56 %)
- Sanctions règlementaires (29 %)

Si vous pensez que la taille et le secteur d'activité de votre entreprise vous dispensent des questions de sécurité mobile, détrompez-vous. Nous n'avons pas trouvé une seule industrie immunisée contre les compromissions. Qu'une entreprise ait moins de 50 salariés ou plus de 10 000 collaborateurs, les attaquants logent tout le monde à la même enseigne.

Impact des compromissions

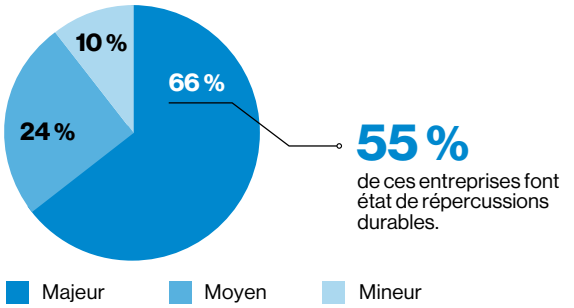


Figure 4 : Si votre entreprise a subi une compromission, quelle a été la gravité de l'impact ? En cas de compromission majeure, le préjudice s'est-il fait sentir sur la durée ?

Cloud, IoT et 5G : le point sur les technologies d'avenir

L'adoption progressive du cloud, les systèmes IoT (Internet des objets) et les réseaux 5G réinventent les expériences des clients et des salariés, sur fond de transformation de tous les secteurs d'activité. C'est pourquoi cette édition Mobile Security Index s'est penchée sur chacune de ces technologies et leur impact sur la sécurité mobile.

Cloud

On ne saurait surestimer la part croissante du cloud dans les infrastructures d'entreprise. Ainsi, 57 % des entreprises interrogées disent stocker plus de la moitié des nouvelles informations créées ou collectées dans le cloud. En outre, 84 % déclarent qu'elles dépendent de plus en plus de ces données. Malgré cela, seulement la moitié des sondés (52 %) bloque l'accès aux applications cloud depuis des réseaux inconnus.

IoT

Pour les besoins de notre étude sur l'Internet des objets, nous avons identifié un sous-groupe de participants en charge des achats, de la gestion et de la sécurisation des équipements IoT, puis leur avons posé une série de questions sur le sujet. Conclusion : les environnements IoT sont confrontés aux mêmes problèmes que les technologies mobiles. En effet, près du tiers de ce sous-groupe (31 %) admet avoir subi une compromission impliquant un objet connecté. En cause, les mêmes raccourcis que pour les technologies mobiles. Les deux cinquièmes des sondés (41 %) reconnaissaient effectivement avoir relégué la sécurité de l'IoT au second plan pour pouvoir remplir leurs objectifs, avec les répercussions que l'on connaît. Les entreprises adeptes de l'IoT faisant l'impasse sur la sécurité ont 1,7 fois plus de risques de subir une compromission liée à ces équipements.

5G

Grâce à la 5G, les entreprises vont pouvoir offrir et consommer de nouveaux services qui dépassent notre imagination, à l'image de la réalité virtuelle ou augmentée. Voitures connectées, espaces et bâtiments intelligents… la technologie devrait également accélérer le développement d'applications IoT. La sécurisation de ces services et applications constitue un volet essentiel de l'architecture sous-jacente de la 5G.

Parmi ces nouvelles fonctionnalités de sécurité :

- Protection renforcée contre le traçage non autorisé et le vol d'identifiants grâce aux identifiants SUCI (Subscription Concealed Identifiers) et 5G-GUTI (Globally Unique Temporary Identifiers)
- Meilleure résilience face aux attaques grâce aux réseaux SDN (Software-Defined Network) et à la virtualisation des fonctions réseau (NFV)
- Sécurité personnalisable pour une prise en charge des nouveaux équipements et cas d'usage
- Vérification et clés implicites sur les réseaux hors 3GPP comme le Wi-Fi pour une protection renforcée contre les bornes non autorisées

Des entreprises poussées à agir

Dans le monde entier, les pouvoirs publics continuent de placer des garde-fous et de renforcer les règlementations régissant la sécurité mobile. Ce resserrement du cadre règlementaire a déjà incité 67 % des entreprises interrogées à investir davantage dans leur sécurité en général.

Toutefois, il est regrettable que de nombreuses entreprises attendent qu'un incident survienne pour se pencher sérieusement sur leur sécurité mobile. En effet, 43 % des entreprises victimes d'une compromission prévoyaient une augmentation importante de leur budget de sécurité mobile au cours des 12 prochains mois, contre seulement 17 % des entreprises non victimes.

84 %

Pourcentage d'entreprises disant dépendre de plus en plus de données stockées dans le cloud

31 %

Pourcentage de sondés du sous-groupe IoT ayant subi une compromission liée à un objet connecté

Une compromission engendre souvent une forte augmentation des dépenses en sécurité

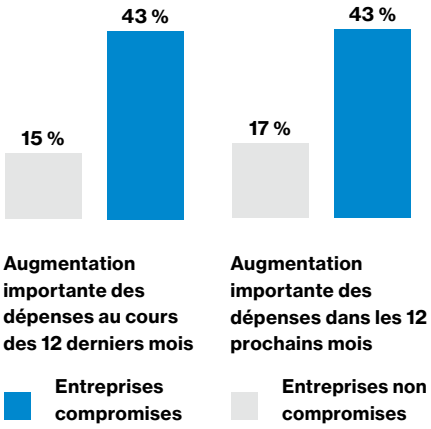
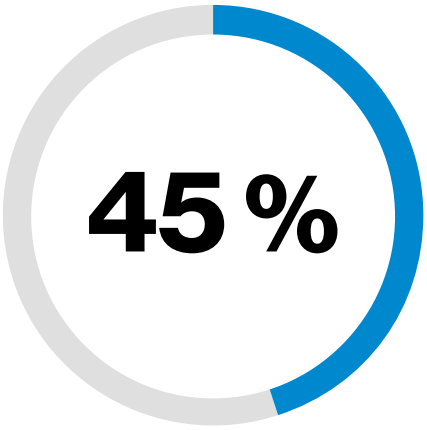


Figure 5 : Évolution des budgets de sécurité mobile des entreprises compromises et non compromises

Améliorer la sécurité mobile

Parmi les entreprises interrogées, 45 % déclarent perdre du terrain face aux capacités des attaquants. C'est là que notre rapport Mobile Security Index 2020 entre en jeu. Dans l'édition de cette année, des experts vous livrent des recommandations détaillées sur les mesures à prendre pour optimiser votre stratégie de sécurité.

Voici en substance leurs principaux conseils :



Pourcentage d'entreprises admettant accuser un certain retard face aux capacités des attaquants

Utilisateurs :

- Instaurez une PUA formelle stipulant les règles et responsabilités liées au BYOD, ainsi que les applications et les réseaux autorisés.
- Faites de la sécurité une priorité, formez régulièrement tous vos salariés à ces questions et informez-les sur la démarche à suivre pour signaler des événements suspects.
- Définissez et diffusez une politique de mots de passe forts traitant des questions de réutilisation et d'authentification à deux facteurs.

Applications :

- Octroyez des accès sur le principe des accès sélectifs et limités, selon les informations nécessaires à chacun.
- Contraignez vos salariés à n'installer que des applications de sources validées et bloquez celles téléchargées sur Internet.
- Veillez à installer rapidement tous les correctifs.

Appareils :

- Modifiez tous les mots de passe d'usine et par défaut, et évitez de réutiliser les mêmes mots de passe.
- Implémentez des politiques pour verrouiller et isoler les appareils vulnérables, infectés, perdus ou volés.
- Utilisez une solution de gestion des terminaux mobiles (Mobile Device Management - MDM) pour simplifier la gestion des correctifs et faire respecter votre PUA, y compris vos politiques d'authentification.
- Déployez un logiciel de détection des vulnérabilités sur vos terminaux.

Réseaux :

- Chiffrez toutes vos données transmises via des réseaux non sécurisés.
- Sensibilisez vos utilisateurs aux dangers du Wi-Fi public et bloquez les réseaux Wi-Fi inconnus et non sécurisés.
- Envisagez l'adoption d'une approche Zero Trust.

Services cloud :

- Limitez l'utilisation d'applications cloud non validées, notamment les plateformes de stockage en ligne.
- Autorisez l'accès aux services cloud aux seuls terminaux utilisant des VPN ou des réseaux de confiance.

Pour renforcer votre sécurité, lisez notre rapport.

Vous avez déjà fait un premier pas vers l'amélioration de votre sécurité mobile. Pourquoi vous arrêter en si bon chemin ? Téléchargez l'intégralité de notre rapport Mobile Security Index (MSI) 2020. Vous aurez alors toutes les cartes en main pour implémenter une sécurité multi-niveau efficace sur tout votre environnement mobile.

Rapport complet MSI 2020

La version intégrale du rapport Mobile Security Index 2020 contient encore toute une mine de statistiques et d'analyses des menaces qui planent sur vos terminaux mobiles. Également au sommaire : des entretiens avec des experts en sécurité, notamment un chef d'unité du FBI et le responsable de la sécurité des systèmes d'information (RSSI) de Verizon.

Outil d'évaluation de la sécurité MSI 2020

Notre outil d'évaluation vous permet de comparer votre sécurité mobile à celles des entreprises de notre enquête MSI 2020. Vous recevrez un rapport personnalisé définissant les différents axes d'amélioration de votre sécurité.

Guide MSI 2020 sur les politiques d'utilisation acceptable

Ce guide interactif vous présente les caractéristiques d'une bonne PUA et vous conseille sur la création ou l'amélioration de votre propre politique.

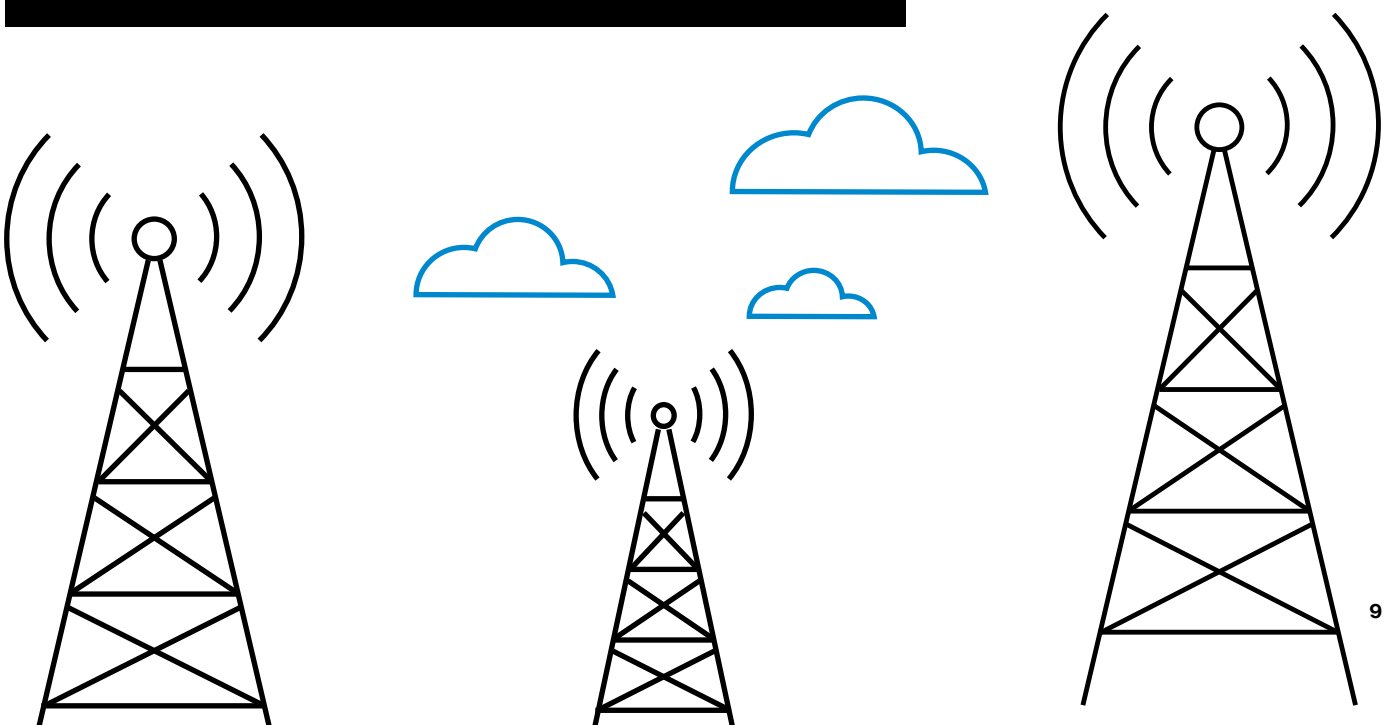
Rapports sectoriels MSI 2020

Bénéficiez d'un état des lieux approfondi de votre secteur en matière de sécurité mobile. Au choix : services financiers, santé, retail, industrie, secteur public, ainsi qu'un gros plan sur les petites et moyennes entreprises.

Entretien vidéo sur la sécurité mobile

Envie de découvrir comment Verizon sécurise son environnement mobile ? Cette vidéo vous montre comment l'approche multi-niveau s'est érigée en bonne pratique de sécurité.

Pour en savoir plus, rendez-vous sur enterprise.verizon.com/msi



verizon

[1] Christopher McMahon, services de renseignement des États-Unis
[2] Données d'utilisation agrégées de 2019 fournies par MobileIron
[3] Données couvrant la période allant de novembre 2018 à octobre 2019, Wandera Threat Research
[4] Globalement, la plupart des terminaux mobiles se connectent à deux voire trois bornes Wi-Fi non sécurisées par jour. D'après NetMotion, ces connexions surviennent surtout dans des commerces, des hôtels et des lieux de transit comme les aéroports.