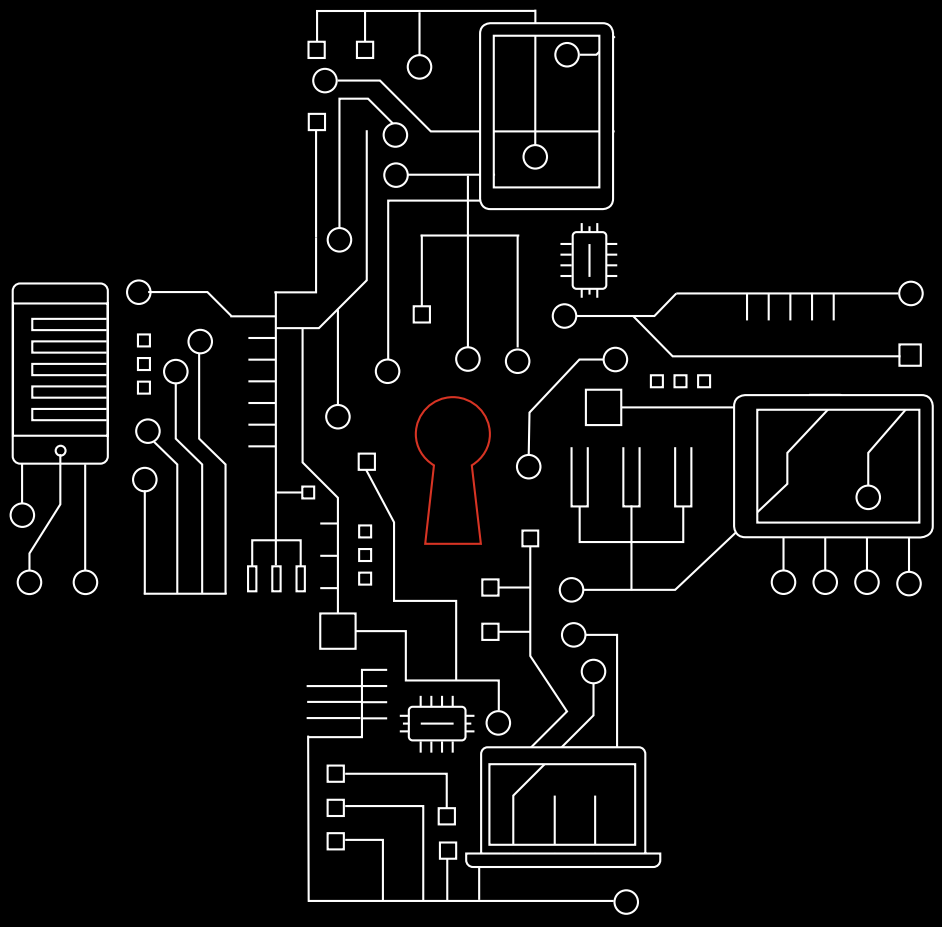
# Mobile Security Index 2020

## Gros plan sur le secteur de la santé

Une plongée au cœur de la sécurité mobile dans les centres de santé, hôpitaux, services d'ambulances, cliniques et établissements de soins.



verizon

# Prenez-vous soin de vos appareils mobiles ?

## Si les technologies mobiles représentent un vivier d'opportunités pour les organismes de santé, elles brassent également une grande quantité de données confidentielles – une manne attractive pour les cybercriminels. Pour protéger leurs informations et systèmes critiques, les prestataires de santé vont donc devoir renforcer leur sécurité mobile.

**88 %**

**Pourcentage d'acteurs de la santé disant dépendre de plus en plus de données stockées dans le cloud**

La mobilité est un enjeu littéralement vital pour les acteurs de la santé. Elle permet aux équipes soignantes de transmettre et consulter des données cliniques en temps réel. Elle améliore le monitoring à distance pour un suivi plus efficace des patients et une réduction du taux de réadmission. Enfin, elle fournit des analyses pointues servant à améliorer la précision des diagnostics et des traitements. Quant aux services cloud, ils n'ont fait que renforcer l'impact des technologies mobiles. Ainsi, 88 % des établissements de santé disent dépendre de plus en plus de données stockées dans le cloud

**Nous avons demandé à un cabinet d'étude indépendant de mener une enquête auprès de responsables chargés de l'achat, de la gestion et de la sécurité des appareils mobiles. Au total, 876 personnes y ont participé, parmi lesquelles 9 % travaillent pour des organismes de santé, dont des hôpitaux, des centres médicaux, des services d'ambulances et d'autres établissements de soins. Sauf indication contraire, toutes les données fournies dans ce rapport proviennent de cette étude.**

verizon

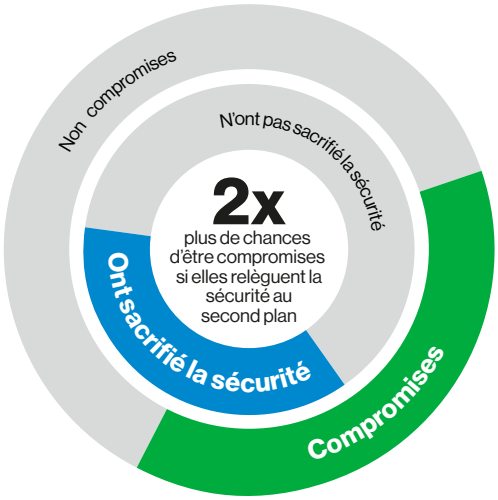
## Près de 2 organismes sur 5 touchés.

Près de deux cinquièmes (38 %) des prestataires de santé interrogés admettent avoir subi une compromission impliquant un objet connecté au cours des 12 derniers mois. Une hausse significative par rapport aux 25 % de l'année précédente.

L'enjeu est de taille. Les organismes de santé traitent des données ultrasensibles de leurs patients comme de leurs salariés. Pour les hackers, ces informations constituent une manne lucrative pour la revente sur le marché noir ou la conduite d'actes d'extorsion et de chantage.

En 2017, le système de santé britannique (NHS) a ainsi été victime d'une attaque par ransomware qui a engendré de sérieuses perturbations dans le réseau hospitalier de tous le pays. Des milliers de consultations et d'opérations ont dû être annulées ou transférées vers d'autres établissements.[1] Comme on le constate, l'onde de choc d'une compromission peut avoir des répercussions profondes. Autre exemple, en 2019, une compagnie américaine de recouvrement de frais hospitaliers a été victime d'une faille de sécurité impactant plus de 20 prestataires de santé, dont des cliniques et des laboratoires de diagnostic. Au total, pas moins de 25 millions de personnes ont été touchées.[2]

Malgré le risque potentiel pour les patients et les effectifs, 37 % des établissements reconnaissent avoir relégué la sécurité mobile au second plan pour pouvoir parvenir à leurs objectifs métiers. Comme dans d'autres secteurs, cette décision n'a pas été sans conséquences. Ainsi, les structures adeptes de l'IoT faisant l'impasse sur la sécurité ont 1,9 fois plus de risques de subir une compromission liée à ces équipements.




**Proportion d'organismes victimes d'une compromission mobile qualifiant l'impact de « majeur ».**




**37 %**

**Pourcentage des établissements de santé ayant relégué la sécurité au second plan.**

**38 %**

**Pourcentage de prestataires de santé reconnaissant avoir subi une compromission de sécurité.**

Figure 1. Votre structure a-t-elle été victime d'une compromission impliquant des appareils mobiles/IoT (Internet des objets) au cours de l'année écoulée ? Votre structure 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 ?

**71 %**

**Part des établissements ayant réévalué les risques associés aux appareils mobiles suite à l'introduction de nouvelles réglementations.**

**1 300**

**Selon une étude Netskope, les entreprises utilisent en moyenne près de 1 300 applications et services cloud, parmi lesquels 95 % échappent à tout contrôle de la DSI.[3]**

## Principales préoccupations de sécurité mobile des établissements de santé

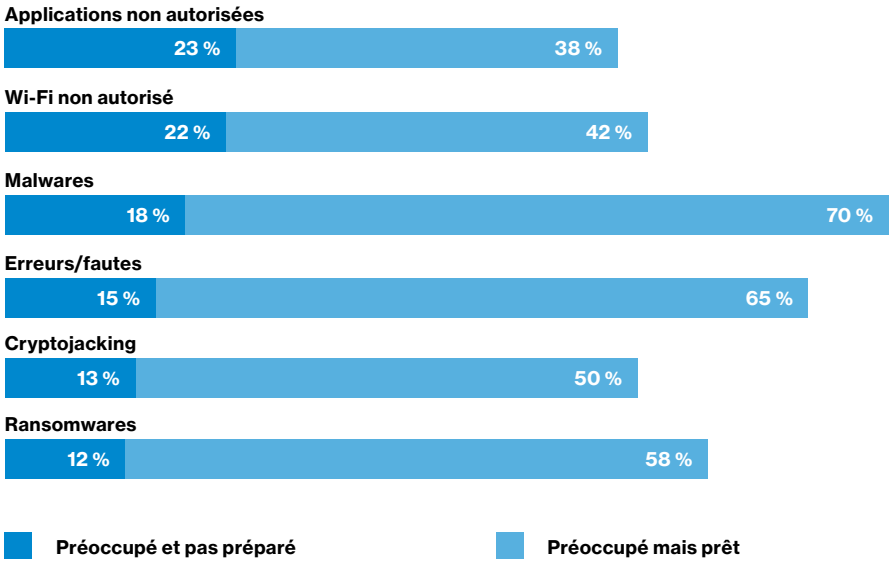



Figure 2. Comment vous sentez-vous face aux menaces/vulnérabilités suivantes ?

### Les risques du cloud

Cloud et technologies mobiles deviennent de plus en plus indissociables. Concrètement, 85 % des prestataires de soins affirment que d'ici cinq ans, les terminaux mobiles seront le principal mode d'accès aux services cloud. Pour une majorité, le cloud est devenu la plateforme *de facto* pour le développement et l'exécution d'applications. De même, 44 % des établissements interrogés stockent dans le cloud plus de la moitié des données nouvellement créées.

**Dans leur majorité, les acteurs de la santé sous-estiment grandement le nombre d'applications utilisées au sein de leurs établissements. Pour 65 % des sondés, leur total est inférieur à 100, tandis que seulement 4 % pensent qu'il est supérieur à 1 000. Or, dans la réalité, ce chiffre est bien plus élevé.**

### La peur du connu

Les acteurs de la santé se disent préoccupés par les menaces liées aux appareils mobiles. Pour 73 % d'entre eux, ce risque va de modéré à élevé. Leurs craintes concernent différents types de menaces, notamment des risques émergents comme le cryptojacking. Mais c'est surtout face à des dangers bien connus que la plupart des établissements se sentent mal préparés : applications non approuvées (23 %), bornes Wi-Fi non autorisées ou non sécurisées (22 %) et malwares (18 %).

En cas de compromission, les prestataires de santé craignent diverses répercussions, notamment l'atteinte à leur image de marque (50 %) et les amendes en cas d'infraction (32 %). Mais ce qui semble les préoccuper le plus, c'est bel et bien la perte de données (62 %), notamment le vol ou la divulgation de dossiers médicaux. Et les informations des patients ne sont pas les seules exposées : 51 % des sondés s'inquiètent d'une fuite de données de leurs salariés, notamment dans le cadre d'attaques de phishing ultra ciblées visant à des malversations fiscales.

## Un accident est si vite arrivé

Les dossiers médicaux représenteront toujours des cibles lucratives pour les cybermalfaiteurs. Pour autant, ce sont les menaces internes qui suscitent le plus d'inquiétude dans le secteur. Pour 75 % des organismes de santé, les salariés seraient même le maillon faible de la sécurité mobile. Et pourtant, seules 52 % de ces organisations ont mis en place des actions de pédagogie visant à sensibiliser leurs équipes aux questions de sécurité.

Même à leur insu, les salariés peuvent compromettre la sécurité de leur employeur. Installation d'applications non autorisées, connexion à des hotspots Wi-Fi non sécurisés… ces comportements augmentent considérablement la surface d'attaque. Mais comment un établissement de santé qui, en toute conscience, fait preuve de laxisme en matière de sécurité mobile – au point de ne pas respecter les règles qu'elle s'est elle-même fixée – peut-elle jeter la pierre à ses salariés ?

## Peut mieux faire

Malgré tous les risques encourus, nombreuses sont les structures à ne pas prendre les précautions élémentaires. Moins de la moitié d'entre elles (43 %) prennent la peine de modifier les mots de passe d'usine et par défaut ou de chiffrer les données sensibles avant de les envoyer sur un réseau public. Pourtant, il s'agit là du b.a.-ba des mesures de sécurité, au même titre que la mise en place de tests de sécurité réguliers ou l'application du principe des « accès limités et sélectifs ». Au final, seuls 12 % des sondés prennent ces quatre mesures d'hygiène numérique de base.

De même, malgré l'utilisation croissante du cloud, seules 35 % des structures limitent l'usage des applications cloud non éprouvées du point de vue de la sécurité. Et seuls 49 % bloquent certaines fonctionnalités des applications cloud lorsque l'accès se fait depuis des réseaux ou des endroits inconnus. Sans ces mesures de vigilance, c'est l'ensemble des données qui sont menacées, tant celles des patients que des salariés.

## Pourquoi tant de compromis sur la sécurité ?

Les principales raisons avancées par les personnes interrogées : gain de temps (64 %) et commodité (46 %). Autrement dit, ce qui préoccupe les décideurs, c'est l'impact potentiel des mesures de sécurité sur la productivité et l'efficacité. Une telle préoccupation paraît justifiée dans un contexte où l'accès rapide aux données peut sauver des vies.

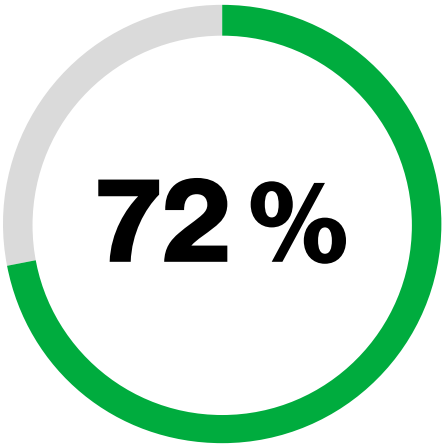
Si elles sont mal définies ou mal appliquées, des politiques de sécurité peuvent nuire aussi bien aux salariés qu'aux patients. De simples règles de mots de passe peuvent ainsi freiner la productivité des personnels, augmenter les coûts de support (du fait d'une multiplication des réinitialisations), voire augmenter les risques (en incitant les salariés à prendre des raccourcis, surtout en situation d'urgence médicale).

## Jouer la carte de la fluidité

À l'inverse, des solutions de sécurité implémentées dans les règles de l'art peuvent réduire radicalement les risques sans impacter l'expérience utilisateur. L'implémentation de passerelles de sécurité mobile, d'une authentification adaptative et de services Zero Trust peut même diminuer le nombre de fois où les utilisateurs doivent s'identifier, sans risque accru pour les systèmes et les données.

# 65 %

**Pourcentage de prestataires déclarant utiliser des Wi-Fi publics à des fins professionnelles. Pour 23 % d'entre eux, cette pratique est pourtant formellement interdite par leur entreprise.**




**Pourcentage de structures de soins estimant que la nécessité d'accéder rapidement aux données complique la mise en place d'une sécurité efficace.**

# 20 %

**Une étude NetMotion révèle que les restrictions informatiques de leur entreprise représente la première source de frustration de 20 % des travailleurs mobiles – la lourdeur de la procédure d'authentification arrivant en cinquième position.[4]**

# L'IoT pour les métiers de la santé : une menace en hausse ?

Les objets connectés ont connu une croissance fulgurante en termes de volume et de diversité, au point de révolutionner les services médicaux. Pour la grande majorité (94 %) des professionnels de santé, ces appareils intelligents jouent un rôle crucial dans la transformation digitale.

L'innovation s'invite ainsi dans de nombreux domaines : emballages intelligents de comprimés améliorant l'observance thérapeutique des patients, ambulances équipées de capteurs embarqués transmettant les diagnostics avant l'arrivée aux urgences, etc.
Plus particulièrement, les objets connectés servent à surveiller les équipements et l'efficacité (77 %), la sécurité physique des bâtiments (71 %), et l'état de santé ou le bien-être des patients (59 %).

Pour mieux cerner les risques spécifiques à l'IoT, nous avons interrogé un sous-groupe de professionnels de santé en charge des achats, de la gestion et de la sécurisation de ces terminaux. Selon 75 % d'entre eux, les menaces ciblant leur parc IoT vont de modérées à élevées. Et 35 % rapportent avoir déjà été victimes d'une compromission impliquant au moins un appareil IoT.

Malgré leurs craintes, 35 % relèguent la sécurité IoT au second plan afin de « remplir leurs objectifs ». Pourquoi ? Pour gagner du temps : tous les sondés considèrent les contraintes de temps comme l'une des raisons sous-jacentes à cette décision. Dans la course à l'innovation, la sécurité devient souvent le cadet des soucis. Pour 27 % des participants, la sécurité des appareils IoT n'est pas une priorité lors de la phase initiale de développement.
Elles estiment qu'elles peuvent renvoyer cette question à plus tard.

## Sécurité des objets IoT

Heureusement, il existe divers axes de renforcement de la sécurité de l'IoT. Parallèlement à nos recommandations pour la sécurité mobile, la mise en place de ces quatre bonnes pratiques IoT vous permettra de protéger efficacement votre organisation :

**1. Faites un bilan de sécurité avant d'effectuer le moindre achat.**
Que vous achetiez des solutions clé-en-main ou des composants pour créer vos propres appareils IoT, interrogez les fournisseurs sur les mesures de sécurité qu'ils prennent, et évaluez-en la fiabilité. Soyez tout particulièrement attentifs à leurs politiques d'authentification, de chiffrement et de correctifs. Parmi les entreprises interrogées, 77 % ont déployé des appareils IoT sur des sites éloignés ou difficiles d'accès. Les mises à jour OTA (Over-The-Air) aident à maintenir la sécurité de ces appareils.

**2. Renforcez la sécurité de tous les appareils avant de les raccorder au réseau.**
Vérifiez avant tout que l'appareil soit lui-même inviolable et équipé d'un système de scellée signalant toute atteinte à son intégrité physique. Ensuite, veillez à modifier tous les mots de passe d'usine ou par défaut. Enfin, réduisez votre exposition aux menaces en désactivant tout ce dont vous n'avez pas besoin. Par exemple, bloquez tous les ports ou protocoles non utilisés.

**3. Chiffrez les données en transit et au repos.**
Parmi les 83 % de sondés déclarant collecter des données personnelles, 25 % ne les chiffrent pas. Pourtant, en chiffrant vos données, vous les rendez inutilisables par les hackers et réduisez les risques d'exposition nuisibles à votre réputation.

**4. Utilisez une plateforme IoT.**
Misez sur une plateforme qui vous permet de surveiller et gérer tous vos appareils, en toute simplicité. Ce type de plateforme aide à réduire les failles grâce au déploiement de certificats numériques et d'autres fonctions de sécurité. De même, il vous sera plus facile de neutraliser les attaques résultant d'un vol de carte SIM en associant chaque carte à un appareil.

**44 %**

**Lorsqu'elles incorporent l'IoT à leurs produits, 44 % des entreprises utilisent des certificats numériques dans une optique de sécurité.**

**71 %**

**Pourcentage d'établissements de santé estimant que le risque associé à l'IoT a augmenté au cours de l'année écoulée.**

**93 %**

**Part des organismes de santé pensant que la sécurité des appareils IoT doit être prise plus au sérieux.**

## Mieux vaut prévenir que guérir.

Pour 93 % des acteurs de la santé, la sécurité des appareils mobiles doit être prise plus au sérieux. En outre, 77 % pensent que les menaces mobiles augmentent à un rythme plus soutenu que dans d'autres domaines.

Les établissements victimes d'une compromission ont été 30 % à augmenter fortement leurs dépenses de sécurité mobile au cours des 12 derniers mois. Ce chiffre chute à 16 % chez les participants n'ayant pas subi de compromission.

S'il est rassurant de constater que les prestataires de santé ont pris conscience du problème, on peut néanmoins s'inquiéter du manque de mesures concrètes.

Nul besoin de rappeler que les conséquences d'un incident de sécurité mobile peuvent être désastreuses. Parmi les participants victimes d'une compromission, près de la moitié (48 %) ont subi une interruption de service, tandis que 39 % ont vu certaines de leurs données perdues ou exposées. Dans ces situations, le retour à la normale peut être long, complexe et coûteux.

En clair, n'attendez pas d'essuyer une attaque pour repenser votre sécurité mobile. C'est maintenant qu'il faut agir.

# Prochaines étapes

### MSI 2020 : rapport principal

Ce gros plan est un extrait du rapport Mobile Security Index (MSI) 2020. La version intégrale du rapport contient toute une mine de statistiques et d'analyses des menaces visant les appareils 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.

### MSI 2020 : outil d'évaluation de la sécurité

Cet outil d'évaluation en ligne se fonde sur les statistiques du rapport MSI pour déterminer le niveau de maturité de votre entreprise dans quatre domaines clés de la sécurité mobile : compréhension, perception du risque, exposition et préparation. Un outil essentiel pour identifier les axes d'amélioration de votre sécurité.


### MSI 2020 : guide des politiques d'utilisation acceptable

Ce guide détaille les 10 étapes de l'élaboration d'une politique d'utilisation acceptable (PUA) complète visant à sensibiliser les collaborateurs sur les comportements à adopter, et à éviter, lorsqu'ils utilisent des appareils mobiles. L'adoption d'une telle politique contribue à réduire le risque de menaces, notamment les malwares et le phishing.

# Recommandations

## 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 limités et sélectifs.
- 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 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 en savoir plus, rendez-vous sur enterprise.verizon.com/msi**

# À propos du Verizon Mobile Security Index

Le MSI est l'une des principales sources d'informations sur la sécurité mobile. Pour cette troisième édition, nous avons demandé à un cabinet indépendant d'interroger 876 responsables des achats, de la gestion et de la sécurité des appareils mobiles et IoT. Pour étoffer notre enquête, nous avons par ailleurs collaboré avec Asavie, IBM, Lookout, MobileIron, NetMotion, Netskope, Symantec, VMware et Wandera. Ces leaders de la sécurité des appareils mobiles nous ont fourni des informations complémentaires, notamment en termes de données sur les usages et les incidents. Enfin, nous avons reçu la contribution du FBI et des services secrets américains. Nous tenons à remercier l'ensemble de ces acteurs, dont la précieuse collaboration nous a permis de dresser un tableau plus complet des menaces qui planent sur les appareils mobiles, ainsi que des mesures engagées pour les neutraliser.

verizon

1 « NHS 'could have prevented' WannaCry ransomware attack, » BBC, 27 octobre 2017.
2 « AMCA Data Breach Total Nears 25M as Wisconsin Diagnostic Laboratories Confirms 115K Record Breach, » HIPAA Journal, 28 août 2019.
3 Netskope Cloud Report, Netskope, août 2019, https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019
4 Employee Frustration Index, enquête réalisée en Amérique du Nord auprès de 285 utilisateurs de différents types d'appareils et provenant de différentes tranches d'âge, NetMotion, septembre 2019, https://www.netmotionsoftware.com/blog/connectivity/mobile-frustration-index

© 2020 Verizon. RPT5140220-FR